UNIVERZITA KARLOVA

Právnická fakulta

JUDr. Miroslav Uřičař

Zásahy do práva na ochranu soukromí ze strany orgánů veřejné moci

Disertační práce

Školitel: prof. JUDr. Aleš Gerloch, CSc.

Studijní program: Teoretické právní vědy – Ústavní právo a státověda

Datum vypracování práce: 29. června 2024

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

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 789.732 znaků včetně mezer.

Disertant

V Praze, dne

Poděkování

Děkuji panu prof. JUDr. Aleši Gerlochovi, CSc. za podnětné komentáře, odborné náměty a připomínky, které mně v průběhu zpracování disertační práce poskytl.

Obsah

Použité zkratky

BIS – Bezpečností informační služba

ČNB – Česká národní banka

ČTÚ – Český telekomunikační úřad

Data Retention Směrnice – Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES.

Směrnice o soukromí a elektronických komunikacích – Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích), ve znění pozdějších předpisů.

EDPB – Evropský sbor pro ochranu osobních údajů (zkratka z anglického European Data Protection Board), zřízený čl. 68 Obecného nařízení o ochraně osobních údajů GDPR jako subjekt Evropské unie se samostatnou právní osobností.

ESLP – Evropský soud pro lidská práva

Evropská úmluva – Úmluva o ochraně lidských práv a základních svobod, společně s Dodatkovým protokolem a Protokoly č. 2, 4, 6 a 7.

GDPR – Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Listina – Listina základních práv a svobod, ve znění pozdějších předpisů

Listina EU – Listina základních práv Evropské unie (2016/C 202/02; Úř. věst. C 202, 7.6.2016, s. 389–405)

Nařízení eCall – Nařízení Evropského parlamentu a Rady (EU) 2015/758 ze dne 29. dubna 2015 o požadavcích na schválení typu pro zavedení palubního systému eCall využívajícího linku tísňového volání 112 a o změně směrnice 2007/46/ES.

Rozsudek Digital Rights – Rozsudek Soudního dvora EU (velkého senátu) z 8. dubna 2014. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další. Žádosti o rozhodnutí o předběžné otázce podané High Court (Irsko) a Verfassungsgerichtshof (Rakousko). Spojené věci C-293/12 a C-594/12.

Rozsudek Tele2 Sverige AB – Rozsudek Soudního dvora EU (velkého senátu) ze 21. prosince 2016. Tele2 Sverige AB v. Post – och telestyrelsen (C-203/15) a Secretary of State for the

Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis, za přítomnosti Open Rights Group, Privacy International, The Law Society of England and Wales (C-698/15). Žádosti o rozhodnutí o předběžné otázce podané rozhodnutím Kammarrätten i Stockholm (správní odvolací soud ve Stockholmu, Švédsko) a rozhodnutím Court of Appeal (England & Wales) (Civil Division) [odvolací soud pro Anglii a Wales, občanskoprávní oddělení, Spojené království]. Spojené věci C-203/15 a C-698/15.

Směrnice 95/46/ES – Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. L 281, 23.11.1995, s. 31).

Směrnice PNR – Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti.

SDEU – Soudní dvůr Evropské unie

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

Trestní řád – zákon č. 141/1961 Sb. o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

ÚOHS – Úřad pro ochranu hospodářské soutěže

ÚOOÚ – Úřad pro ochranu osobních údajů

Ústava ČR – zákon č. 1/1993 Sb. Ústava České republiky, ve znění pozdějších změn.

VZ – Vojenské zpravodajství

WP 29 – Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováváním osobních údajů zřízená na základě článku 29 směrnice 95/46/ES.

ZoEK – zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

ZoZOÚ – zákon č. 110/2019 Sb. o zpracování osobních údajů.

Úvod

Technický rozvoj a zejména narůstající digitalizace nejen jednotlivých odvětví ekonomiky, ale i běžných aktivit a situací v lidském životě se v posledních letech projevuje mimo jiné i v nárůstu rozsahu a intenzity zásahů do soukromí osob, včetně toho, že přibývají nové formy takovýchto zásahů. Technickým rozvojem v této oblasti míní autor jednak stále větší rozšíření moderních technologií a digitalizace i do oblastí, ve kterých donedávna převládaly méně sofistikované, avšak z hlediska možného zneužití bezpečnější, metody zpracování údajů či v nich k automatizovanému zpracování nedocházelo vůbec, ale také výrazně narůstající kapacitní a rychlostní možnosti při zpracování značných objemů dat, při jejich procházení, vyhodnocování, vyhledávání v nich a další práci s nimi. Tento rozvoj pochopitelně nelze zastavit ani zpomalit, nelze ani mnohá automatizovaná zpracování nahradit manuálními. Dle hodnocení autora je však potřebné být si vědom také konkrétních negativních aspektů a rizik, která s sebou vývoj přináší pro základní práva a svobody, zde v prvé řadě pro právo na ochranu soukromí.

Zpracování údajů, která představují potenciální zásahy do soukromí, resp. která takovéto zásahy umožňují či usnadňují, existuje celá řada. Dle hodnocení autora je jejich základním společným rysem to, že se nevyhnutelně musí jednat o zpracování osobních údajů, ve smyslu vymezení obsažených v Obecném nařízení o ochraně osobních údajů – GDPR[1], a to v případě obou pojmů – „osobní údaj“ i „zpracování“.

Osobními údaji se dle tohoto vymezení rozumějí *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“*[2]. Pro účely této práce považuje autor za klíčové dva aspekty takto vymezeného pojmu. Musí se jednat o informace týkající se fyzické osoby (v opačném případě nelze hovořit o osobních údajích) a informace se musejí vztahovat k identifikované či identifikovatelné fyzické osobě. Při splnění

[1] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), známé i v odborném prostředí pod zkratkou GDPR.
[2] Viz čl. 4 bod 1 GDPR.

těchto dvou kritérií jsou osobním údajem jakékoli informace, jak vyplývá z výše citované definice.

Zpracováním se rozumí *„jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení“*[3]. Zpracování tedy v případě osobních údajů dle této definice zahrnuje prakticky jakékoli operace s takovýmito údaji, bez ohledu na použité postupy, jak dokládá rovněž příkladmý výčet použitý ve vymezení evropským zákonodárcem, bez ohledu na druh nebo kategorie takovýchto údajů i bez ohledu na celkové množství údajů či další faktory. Jedná se tedy o vymezení velmi široké, dopadající na prakticky jakékoli aktivity, při nichž dochází k nakládání s osobními údaji, a to např. i včetně výmazu či zničení těchto údajů. Zcela totožné vymezení pojmů „osobní údaj“ a „zpracování“ obsahuje též Trestněprávní směrnice, která je pro problematiku posuzovanou v této práci taktéž velmi relevantní, společně s její transpozicí do právního řádu ČR, jak podrobně rozvedeno dále.

Mnohá zpracování osobních údajů mohou subjekty údajů vnímat jako potenciální zásah do soukromí fyzických osob. Obecně však platí, že zpracování, která probíhají v souladu s požadavky platné právní úpravy a bez bezpečnostních incidentů, ve většině případů za zásah do soukromí bez dalšího považovat nelze, k zásahu do soukromí u nich dojde zpravidla pouze v případech, kdy nastane porušení zabezpečení zpracovávaných osobních údajů. Autor v této práci pro další analýzu vybral pouze taková zpracování, u kterých lze dopad do soukromí dotčených osob předpokládat již při samotném zpracování. Tak je tomu dle autorova hodnocení v případech zpracování, k němuž dochází bez souhlasu subjektů údajů, mnohdy dokonce bez možnosti subjektů údajů tato zpracování a jejich rozsah ovlivnit (např. odvoláním souhlasu, vznesením námitek proti zpracování, požadavkem na výmaz osobních údajů apod.). Jak výstižně konstatoval Ústavní soud ČR v souvislosti s rozhodováním o povinném uchovávání provozních a lokalizačních údajů elektronických komunikací, ve *„virtuálním prostoru informačních technologií a elektronické komunikace“* dochází v současnosti k zaznamenávání, shromažďování či zpřístupňováním značného množství údajů a tato

[3] Viz čl. 4 bod 2 GDPR.

zpracování *„zasahují i do soukromé sféry každého jednotlivce, ačkoliv on sám do ní vědomě nikoho vpustit nechtěl“*[4].

Mezi základní kritéria, podle kterých lze takováto zpracování osobních údajů identifikovat, tak dle hodnocení autora patří v prvé řadě právní základ zpracování a účel zpracování. Právní základy jsou stanoveny platnou právní úpravou, jak autor ukáže dále. Sledovaný účel zkoumaných zpracování údajů bývá často vymezen jako boj proti trestné činnosti či boj proti terorismu – zvláště u shromažďování údajů s potenciálně závažnou mírou dopadu do soukromí, výjimkou však nejsou ani další účely, mezi něž patří kontrola výběru daní či jiných dávek a jiné.

Pro situace, na které dopadá GDPR, vymezuje právní základy zpracování taxativně přímo toto nařízení[5] tak, že jimi mohou být pouze: 1. souhlas udělený ke konkrétnímu zpracování subjektem údajů, 2. nezbytnost zpracování pro splnění smlouvy, nebo pro provedení opatření před uzavřením smlouvy na žádost subjektu údajů (za předpokladu, že subjekt údajů je smluvní stranou), 3. nezbytnost zpracování pro splnění právní povinnosti správce, 4. nezbytnost zpracování pro ochranu životně důležitých zájmů, a to buď subjektu údajů nebo jiné fyzické osoby, 5. nezbytnost zpracování pro splnění úkolu správce prováděného ve veřejném zájmu nebo při výkonu veřejné moci a 6. nezbytnost zpracování pro účely oprávněných zájmů správce či třetí strany, přičemž v tomto případě je nezbytné, aby tyto oprávněné zájmy převážily nad zájmy nebo základními právy a svobodami subjektu údajů. Účelem je využití zpracovávaných údajů ze strany orgánů veřejné moci, konkrétní účely využití by měly být vždy jednoznačně vymezeny relevantní právní úpravou.

Trestněprávní směrnice, která se dle autorova předpokladu použije na některá takováto zpracování rozebíraná v této práci, stanoví s ohledem na své zaměření právní základ zpracování odlišně, opět však nikoli volně k uvážení osobě, která zpracování provádí, nýbrž kogentním určením. Zákonnost zpracování činí tato směrnice závislým na stanovení této zákonnosti členskými státy, současně směrnice stanoví tři podmínky, které musejí být kumulativně naplněny. Musí se jednat o zpracování nezbytná ke splnění úkolů příslušných orgánů pro účely stanovené směrnicí, rozsah zpracování musí být též nezbytný pro dané účely a zpracování musí mít základ v právu EU nebo členského státu; Trestněprávní směrnice

[4] Ústavní soud ČR tuto tezi konstatoval nejprve v nálezu sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011 a posléze ji, s odkazem na tento předchozí nález, považoval za vhodné použít opět v nálezu sp. zn. Pl. ÚS 24/11 ze dne 20. prosince 2011.

[5] Viz článek 6 GDPR, upravující v rámci vymezení zákonnosti zpracování v odst. 1 taxativním výčtem jednotlivé právní základy, tedy podmínky, za nichž je zpracování zákonné.

stanoví taxativní výčet účelů, kterými jsou *„prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení“*.

Dalším rysem společným pro zpracování osobních údajů, která autor v této práci zamýšlí zkoumat, je skutečnost, že zpracování provádějí buď přímo orgány veřejné moci, případně je sice provádějí jiné osoby, jimž však byla povinnost zpracování takových údajů uložena obecně závazným právním předpisem – v takových případech povinné osoby (např. poskytovatelé služeb elektronických komunikací) zpracovávají údaje ke splnění povinnosti nikoli pro své vlastní účely (jako je tomu např. u povinného uchovávání účetních dokladů a dalších účetních záznamů účetní jednotkou dle zákona o účetnictví[6]), nýbrž pro jejich možné vyžádání a využití orgány veřejné moci. V případě osobních údajů uchovávaných povinně plošným a nerozlišujícím způsobem tak zásah představuje nejen využití údajů, k němuž navíc dochází zpravidla pouze u zlomku všech uchovávaných údajů, nýbrž již samotné jejich povinné zpracování, byť zpravidla pouze ve formě shromáždění údajů a jejich uchovávání.

Charakteristickým znakem takovýchto zpracování je zpravidla také jejich plošný charakter, jedná se tedy o nerozlišující zpracování údajů všech osob patřících do určité skupiny, bez ohledu na jakýkoli relevantní vztah těchto osob k vymezenému účelu daného zpracování. Zásah do soukromé sféry fyzických osob v podobě shromažďování a zpracování osobních údajů těchto osob by obecně měl být alespoň do určité míry předvídatelný. Legitimním očekáváním fyzických osob totiž je možnost předem se seznámit s okolnostmi, při jejichž splnění může dojít k zásahu do jejich soukromé sféry, a případně v reakci na to přizpůsobit své jednání a zásah minimalizovat či se mu zcela vyhnout. V případech plošných a nerozlišujících zpracování však charakter těchto zpracování takovou možnost do značné míry omezuje či mnohdy přímo vylučuje, když v důsledku plošného charakteru zpracování mnohdy zásah do práva na ochranu soukromí těchto osob není předem předvídatelný.

Předmětem této práce autor učinil pouze případy, v nichž jsou zpracovávané osobní údaje určeny k využití orgánů veřejné moci, když takováto zpracování se dle hodnocení autora vyznačují společnými rysy, které je od ostatních odlišují. Tato zpracování jsou též zpravidla dlouhodobé a systematické povahy a jsou způsobilá zásadních dopadů do soukromí dotčených osob, která v některých případech mohou v daných osobách vyvolat dojem sledování jejich aktivit. I při omezení na takováto zpracování by bylo možno zkoumat zásahy do soukromí ze

[6] Povinnost uložená účetním jednotkám v § 31 a násl. zákona č. 563/1991 Sb. o účetnictví, ve znění pozdějších předpisů, vč. doby uchování stanovené v § 31 odst. 2 tohoto zákona.

strany veřejné moci bez ohledu na právní základ zpracování, tedy např. i v případě zpracování osobních údajů dobrovolně zveřejněných či předaných ke zpracování konkrétními fyzickými osobami. Pro účely dalšího zkoumání však autor předmět této práce dále omezil na zpracování osobních údajů uložená či předpokládaná právními předpisy.

Právním základem diskutovaných zpracování jsou v některých případech předpisy obsažené v právním řádu ČR, četné jsou však též případy založené právem EU, s následným provedením do národního právního řádu (jak autor podrobně rozvádí dále, u jednotlivých zkoumaných případů). Tato zpracování zpravidla spočívají ve shromažďování a dalším zpracování řady kategorií osobních údajů, navíc se zpravidla týkají velkého množství osob a také celkové množství zpracovávaných údajů je zpravidla značné. Dopad takovýchto zpracování do práva na ochranu soukromí proto může být velmi významný.

Pro vymezení zásahů rozebíraných v této práci je relevantním hledisko intenzity zásahu. Vedle množství zpracovávaných kategorií osobních údajů je významným aspektem pro posouzení intenzity zásahu jeho celkový rozsah, autor proto považoval za nutné zabývat se kritérii pro vymezení rozsahu zpracování. Za relevantní autor v tomto směru považoval kritéria používaná v GDPR, evropský zákonodárce zde kritérium rozsáhlosti zpracování uplatnil především ve vztahu k povinnosti správce údajů provést posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů[7] a u povinnosti správce či zpracovatele jmenovat pověřence pro ochranu osobních údajů[89].

Samotný pojem „rozsáhlého“ zpracování GDPR nevymezuje, k postupu jeho určení v praxi se vyjadřuje Pracovní skupina WP 29[10], přičemž v Pokynech týkajících se pověřenců pro ochranu osobních údajů[11] *„doporučuje, aby byly při určování toho, zda je zpracování prováděno ve velkém rozsahu, vzaty v úvahu především“* čtyři faktory, které výslovně uvádí;

---

[7] Čl. 35 odst. 1 GDPR aplikuje kritérium rozsahu společně s povahou, kontextem a účelem zpracování: *„Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.“*; v témže ustanovení je pak kritérium rozsáhlosti použito též v odst. 3 písm. a), b) i c).

[8] V čl. 37 odst. 1 GDPR se kritérium rozsahu, resp. rozsáhlého zpracování vztáhne ke zvláštním kategoriím osobních údajů: *„c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů uvedených v článku 9 a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10.“*

[9] K tomuto viz také EHMANN, Eugen, SELMAYR, Martin. *Datenschutz-Grundverordnung: DS-GVO. 3. Auflage*. München: C.H.BECK Verlag, 2024.

[10] Podrobně k tomuto viz UŘIČAŘ, Miroslav, RÁMIŠ, Vladan a kol. *Obecné nařízení o ochraně osobních údajů. Komentář. 1. vydání.* Praha: C. H. Beck, 2021. s. 803 a násl.

[11] Pracovní skupina WP 29. *Pokyny týkající se pověřenců pro ochranu osobních údajů WP 243 rev.01*. Přijaté dne 13. prosince 2016 a naposledy revidované a přijaté dne 5. dubna 2017. EDPB na svém prvním plenárním zasedání tyto pokyny WP 29 schválil. [online] [cit. 24.2.2024]. Dostupné z www.uoou.gov.cz.

na prvním místě je mezi nimi *„počet dotčených subjektů údajů – buď jako konkrétní číslo, nebo jako podíl příslušné skupiny obyvatelstva“*. Obdobně WP 29 kritérium rozsáhlosti vymezuje též v Pokynech pro posouzení vlivu na ochranu údajů a stanovení, zda „*je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“* pro účely nařízení 2016/679[12]. WP 29 v těchto pokynech uvádí, že ani „*obecné nařízení o ochraně osobních údajů přesně nevymezuje, co znamená rozsáhlé, i když 91. bod odůvodnění určité vodítko poskytuje*“. Právě z kritérií obsažených v bodě 91 odůvodnění (recitálu) GDPR lze dle hodnocení autora do jisté míry vyjít i v tomto případě. Tento bod zmiňuje „*…rozsáhlé operace zpracování, jež mají sloužit ke zpracování značného množství osobních údajů na regionální, celostátní nebo nadnárodní úrovni, jež by mohly mít dopad na velký počet subjektů údajů*“.

Konkrétně se k posouzení rozsahu zpracování při použití kritéria počtu dotčených subjektů údajů vyjádřil také ÚOOÚ v návrhu dokumentu K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA)[13], kde jako „velký rozsah zpracování osobních údajů“ vymezil taková zpracování, která se týkají *„od 10001 subjektů údajů a/nebo nad 20 přistupujících osob“*. Autor při výběru případů posuzovaných v této práci vycházel z takto vymezených kritérií rozsahu zpracování. S případy zpracování zkoumaných v této práci jsou spojeny dopady do soukromí konkrétních skupin osob, tyto skupiny jsou zpravidla velmi početné, v některých případech se může jednat prakticky o celou populaci ČR.

U shromažďování a dalších zpracování údajů upravených v obecně závazných právních předpisech jsou zpravidla již v rámci legislativního procesu zkoumány mimo jiné i možné dopady do soukromí. Návrhy předpisů však v průběhu schvalování často doznají změn, včetně uložení dodatečných, v původní verzi nepředpokládaných, povinností, zmírnění původně navržených kontrolních mechanismů majících zamezit zneužití či úpravy takových mechanismů s následkem jejich omezené funkčnosti a efektivity v praxi a další. Dopady do soukromí se navíc často v průběhu času, v důsledku aplikace v praxi, vyvíjejí. Jako příklad může sloužit povinnost k uchovávání provozních a lokalizačních údajů (tzv. povinnost Data Retention). Ta v současnosti nabyla míry, která patrně v okamžiku schvalování příslušného právního předpisu nebyla předvídána – jak vyplývá z informací zveřejněných Českým

[12] Pracovní skupina WP 29. *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679 WP 248 rev.01*. Přijaté dne 4. dubna 2017 a naposledy revidované a přijaté dne 4. října 2017 v aktualizovaném znění. EDPB na svém prvním plenárním zasedání tyto pokyny WP 29 schválil. [online] [cit. 24.2.2024]. Dostupné z www.uoou.gov.cz.

[13] Úřad pro ochranu osobních údajů. *K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA)*. Nedatováno, zveřejněno 7. února 2018. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.

telekomunikačním úřadem („ČTÚ“)[14], oprávněné orgány si v ČR v roce 2018 vyžádaly údaje o účastnících či uživatelích mobilních sítí elektronických komunikací celkem ve 339.151 případech, což je dle tiskové zprávy ČTÚ „*o čtvrtinu více než v roce 2017, kdy operátoři tyto údaje předali celkem ve 253 380 případech*“, vyžádány byly v 259.202 případech[15].

U některých zásahů byly v rámci legislativního procesu stanoveny kontrolní mechanismy, s cílem omezit dopady do soukromí, zabránit zneužívání jednotlivých institutů či poskytnout dotčeným osobám možnost získat následnou informaci o zásahu a na jejím základě případně také iniciovat následný přezkum oprávněnosti takovéhoto zásahu v konkrétním případě, jakož i některé další. Tyto kontrolní mechanismy však nejsou nastaveny jednotně, v praxi jsou u jednotlivých zpracování údajů a s nimi spojených zásahů do soukromí velmi různorodé; v některých případech lze pozorovat odlišnosti i v rámci jednoho druhu zpracování, resp. zásahu, např. v závislosti na oprávněných orgánech a vymezení jejich oprávnění v konkrétních právních předpisech, jako je tomu např. u již zmiňovaného uchovávání provozních a lokalizačních údajů. Také tímto aspektem se autor v této práci u jednotlivých zkoumaných případů bude podrobně zabývat, včetně snahy o návrh obecných kontrolních mechanismů a záruk de lege ferenda.

Některá z předmětných zpracování údajů a též odpovídající oprávnění orgánů veřejné moci k jejich získávání a využití byla v minulosti předmětem přezkumu Soudního dvora EU. Další případy posuzovaly také národní soudy členských států EU, s ohledem na dopad těchto zpracování do základních lidských práv šlo zpravidla o ústavní soudy posuzující ústavnost napadených právních úprav, včetně Ústavního soudu ČR. V konkrétních případech se též dopady do soukromé sféry jednotlivců zabýval Evropský soud pro lidská práva. Relevantní judikatura uvedených soudů bude v rámci tohoto projektu použita jako podklad pro posouzení jednotlivých případů právních úprav zakládajících předmětná zpracování osobních údajů a pro vyvození závěrů a doporučení.

U každého z takovýchto zpracování považuje autor za nezbytné důsledně porovnat sledovaný účel s mírou narušení základních práv a svobod, především práva na ochranu soukromí, jakožto jednoho ze základních lidských práv, a práv souvisejících. Mnohé z metod a prostředků boje proti trestné činnosti či specificky boje proti terorismu, vyvolávají z

[14] Podrobně viz www.ctu.gov.cz, ČTÚ takto v minulosti zveřejňoval přehledy vyžádaných provozních a lokalizačních údajů za každý kalendářní rok zpětně, dle hlášení poskytovatelů služeb elektronických komunikací a provozovatelů sítí elektronických komunikací.

[15] Podrobně viz Český telekomunikační úřad. *Tisková zpráva. Operátoři v roce 2018 na žádost oprávněných orgánů předali 332 tisíc provozních a lokalizačních údajů.* Dostupné z www.ctu.gov.cz. [cit. 8.2.2024].

právního hlediska řadu otázek. Se zřetelem na ochranu soukromí zde lze v prvé řadě uvažovat o proporcionalitě zásahu do soukromí ve vztahu ke sledovanému cíli. Pro vyhodnocení tohoto aspektu je nepochybně významná v prvé řadě míra a závažnost, s jakou je do soukromí zasahováno, tedy zcela jistě i rozsah okruhu osob, jejichž soukromí je takto přímo dotčeno jakožto vedlejší efekt použitých prostředků, aniž by tyto osoby byly zamýšlenou cílovou skupinou ve vztahu k danému účelu (např. v boji proti trestné činnosti) i celkový počet těchto osob. Z hlediska závažnosti zásahu do soukromí pak je zásadní otázka, zda se jedná o pouhé monitorování údajů ze soukromí osob či zda jsou monitorované údaje ukládány pro potřeby možného dalšího použití a zejména, zda jsou ukládány do databází umožňujících jejich propojení s jinými údaji a informacemi. Ve druhém případě je pochopitelně míra zásahu do soukromí mnohem vyšší, vyšší je i riziko možného zneužití takovýchto údajů, a to úměrně délce jejich doby uchování, okruhu osob oprávněných k jejich využití a především rozsahu uchovávaných údajů u každého jednotlivce. K tomu se přidává další aspekt – otázka, zda jde o uchovávání údajů cílená pouze na konkrétní osoby, u nichž existuje specifická potřeba takovéhoto zpracování či jistá, předem definovaná míra rizika, či zda jde naopak o plošné a preventivní uchovávání údajů veškerých osob patřících do určité skupiny, v krajním případě – který však není výjimkou, nýbrž mnohdy spíše pravidlem – pak takovouto skupinou jsou prakticky veškeré osoby vyskytující se na území státu, který dané prostředky aplikuje. Jak již autor uvedl, případy zkoumané v této práci mají zpravidla charakter plošného zpracování.

Příkladem v tomto směru může být např. zpracování osobních údajů v rámci tzv. povinnosti Data Retention, u něhož dochází k uchovávání provozních a lokalizačních údajů veškerých účastníků služeb elektronických komunikací; na základě zákonem uložené povinnosti jej provádějí poskytovatelé služeb elektronických komunikací a provozovatelé sítí elektronických komunikací, pro účely jejich možného následného vyžádání oprávněnými orgány. Přestože v tomto případě je plošný charakter zásahu možno považovat za zřejmý, v jiných v této práci rozebíraných případech tomu tak být nemusí, navíc autor považuje pro účely této práce za potřebné používat objektivní metody a kritérium míry zásahu tak vymezit exaktním způsobem. Označení shromažďování a dalšího zpracování osobních údajů termínem „plošné a nerozlišující“ použil např. SDEU v rozsudku ve spojených věcech C-203/15 a C-698/15 (Tele2 Sverige AB), v rozsudku ve věci C 623/17[16] a obdobně též v dalších

[16] Rozsudek Soudního dvora EU (velkého senátu) ze 6. října 2020. Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service. Žádost o rozhodnutí o předběžné otázce podaná

rozhodnutích týkajících se povinného uchovávání provozních a lokalizačních údajů[17], a to ve slovním spojení „plošné a nerozlišující zpracování“[18]. V dřívějším rozsudku ve spojených věcech C-293/12 a C-594/12, označovaném v praxi jako Rozsudek Digital Rights Ireland a považovaném za základní rozhodnutí v oblasti uchovávání provozních a lokalizačních údajů, SDEU a obdobně ani generální advokát ve svém stanovisku v této věci tento termín ještě nepoužili. Přesto v tomto rozhodnutí dle hodnocení autora vymezili význam plošného zpracování, když při posuzování platnosti Data Retention Směrnice dospěl k závěru, že „*Směrnice 2006/24 se totiž týká globálně všech osob, které využívají služeb elektronických komunikací, aniž se však osoby, jejichž údaje jsou uchovávány, nachází byť nepřímo v situaci, která může vést k trestnímu stíhání. Vztahuje se tedy i na osoby, v jejichž případě neexistuje žádný důvod se domnívat, že by jejich chování mohlo byť nepřímo nebo vzdáleně souviset se závažnou trestnou činností.*“ a doplnil, že posuzovaná směrnice „*dále nevyžaduje žádnou souvislost mezi údaji, jejichž uchovávání je stanoveno, a ohrožením veřejné bezpečnosti a zejména se neomezuje na uchovávání údajů vztahujících se buď k určitému časovému období či určité zeměpisné oblasti či okruhu určitých osob, které mohou být jakýmkoli způsobem zapojeny do závažné trestné činnosti, anebo k osobám, které by prostřednictvím uchovávání jejich údajů mohly z jiných důvodů přispívat k předcházení, odhalování nebo stíhání závažných trestných činů*“. Následné konstatování Soudního dvora EU v témže rozsudku, dle kterého „*Uvedená směrnice se mimoto podle svého článku 3 vztahuje na všechny účastníky a registrované uživatele. Představuje tedy zásah do základních práv téměř celé evropské populace.*“, autor považuje spíše za vymezení rozsahu zpracování, přestože i v tomto závěru lze spatřovat prvky plošného zpracování. V této souvislosti autor vychází z textu rozsudku Soudního dvora, když lze souhlasit s hodnocením Michala Bobka, dle kterého *„Rozhodnutí Soudního dvora tvoří nedílný celek“*, což Bobek vztahuje zejména k rozhodnutím o předběžných otázkách, u nichž nelze text rozhodnutí členit na výrokovou část a odůvodnění, jak je tomu v rozhodnutích obecných soudů v ČR; dle Bobka je nutno si uvědomit, že rozhodování o předběžných otázkách není rozhodováním sporu, nýbrž poskytnutím odpovědi

rozhodnutím Investigatory Powers Tribunal (tribunál pro kontrolu vyšetřovacích pravomocí, Spojené království). Věc C-623/17.

[17] Viz např. Rozsudek Soudního dvora EU (velkého senátu) ze 20. září 2022. Bundesrepublik Deutschland, zastoupená Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen v. SpaceNet AG a Telekom Deutschland GmbH. Žádosti o rozhodnutí o předběžné otázce podané rozhodnutími Bundesverwaltungsgericht (Spolkový správní soud, Německo). Spojené věci C 793/19 a C 794/19.

[18] V anglické jazykové verzi tohoto rozsudku je použit termín „*general and indiscriminate*“, v německé jazykové verzi pak termín „*allgemein und unterschiedslos*“, které autor hodnotí v daném kontextu jako významově téměř totožné.

na právní otázky[19]. Obecně navíc dle hodnocení autora platí, že plošné (resp. plošné a nerozlišující) zpracování osobních údajů je zpravidla současně též rozsáhlým zpracováním z hlediska množství dotčených osob; ne každé rozsáhlé zpracování je však možno označit za plošné zpracování.

Význam, který termínu „plošné zpracování" přikládá SDEU ve výše zmiňovaných dalších rozhodnutích, je dle autora shodný s vymezením obsaženým v rozsudku ve spojených věcech C-293/12 a C-594/12, byť zde bez explicitního použití tohoto termínu. Ostatně také, v těchto následujících rozhodnutích, např. právě v rozsudku C-623/17, SDEU odkazuje mj. právě na toto předchozí rozhodnutí ve spojených věcech C 293/12 a C 594/12, když uvádí, že „*Předávání provozních a lokalizačních údajů se vzhledem k tomu, že k němu dochází plošně a nerozlišujícím způsobem, týká globálně všech osob, které využívají služeb elektronických komunikací. Vztahuje se tedy i na osoby, v jejichž případě neexistuje důvod se domnívat, že by jejich chování mohlo, byť nepřímo nebo vzdáleně, souviset s cílem zajistit národní bezpečnost, a především bez nutnosti prokázat souvislost mezi údaji, k jejichž předání má dojít, a hrozbou pro národní bezpečnost (v tomto smyslu viz rozsudky ze dne 8. dubna 2014, Digital Rights Ireland a další, C-293/12 a C-594/12, EU:C:2014:238, body 57 a 58, jakož i ze dne 21. prosince 2016, Tele2, C-203/15 a C-698/15, EU:C:2016:970, bod 105)*"[20].

Obdobně se k aspektu plošného charakteru zásahu do základního práva na soukromí vyjadřuje též Ústavní soud ČR, opět v případě povinného uchovávání provozních a lokalizačních údajů. Tak v nálezu Pl. ÚS 24/10[21] Ústavní soud ČR v poznámce učiněné obiter dictum obecně hodnotil Data Retention Směrnici a s odkazem na kritická hodnocení řady členských států, Evropského inspektora ochrany údajů, Pracovní skupiny WP 29 a dalších uvedl, že „*Všichni výše uvedení se domáhali buď úplného zrušení předmětné Směrnice o data retention a nahrazení nástroje plošného a preventivního uchovávání provozních a lokalizačních údajů jinými, více přiměřenými nástroji (např. tzv. data freezing, jež za splnění stanovených podmínek umožňuje sledování a uchovávání potřebných a vybraných údajů pouze u konkrétního, předem určeného účastníka komunikace)*". Je tedy zřejmé, že Ústavní soud ČR

[19] BOBEK, Michal, KOMÁREK, Jan, PASSER, Jan M., GILLIS, Mark. *Předběžná otázka v komunitárním právu.* Praha: Linde Praha, a.s., 2005. s. 390.
[20] Rozsudek Soudního dvora EU (velkého senátu) ze 6. října 2020. Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service. Žádost o rozhodnutí o předběžné otázce podaná rozhodnutím Investigatory Powers Tribunal (tribunál pro kontrolu vyšetřovacích pravomocí, Spojené království). Věc C-623/17.
[21] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011.

zde staví plošné zpracování osobních údajů do protikladu ke zpracování údajů pouze vybraných osob, v tomto případě vybraných jako konkrétní fyzické osoby. Ústavní soud ČR v tomto případě rozhodoval k návrhu skupiny 51 poslanců Parlamentu ČR na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích[22], přisvědčil přitom návrhu i v hodnocení povinného uchování provozních a lokalizačních údajů jako plošného zpracování osobních údajů. Navrhovatelé ve svém návrhu upozorňovali mj. též na to, že požadavek na předvídatelnost a dostupnost zákonného podkladu státních zásahů do soukromého života přitom dle navrhovatelů vyplývá z judikatury ESLP formulující jej jakožto jeden ze základních požadavků zákonného podkladu státních zásahů do soukromého života[23].

Případy plošného zpracování, uchovávání a potenciálního využívání údajů zakotvené v obecně závazných právních předpisech v současnosti zahrnují velmi širokou škálu údajů, počínaje např. provozními a lokalizačními údaji způsobilými monitorovat prakticky veškeré činnosti a každodenní zvyklosti účastníků a uživatelů sítí elektronických komunikací, včetně četnosti jejich cestování, nakupování, trávení volného času a dalších aktivit, přes údaje zaznamenávané v systémech v automobilech, zejména v systému eCall monitorujícím pohyb automobilu, až například po zpracování údajů cestujících v letecké dopravě, především údajů záznamy jmenné evidence cestujících, zaznamenávající kromě samotných údajů o letech i řadu dalších, se samotným letem do značné míry nesouvisejících údajů. Autor se těmito případy zabývá podrobně dále. Současně také platí, že údaje zaznamenávané v rámci jednotlivých institutů se v některých případech dotýkají prakticky celé populace a celkové množství shromažďovaných a uchovávaných údajů dosahuje značných objemů.

S ohledem na tyto skutečnosti autor považuje za potřebné pokusit se návrhy kontrolních mechanismů a záruk v závěru této práce zaměřit nikoli pouze k jednotlivým zkoumaným institutům odděleně, nýbrž šířeji na úrovni obecně aplikovatelné pro typově podobná plošná zpracování osobních údajů. Za zásadní skutečnost autor považuje také zrychlující se nárůst případů plošného shromažďování a uchovávání údajů založených na povinnostech uložených právní úpravou. Jak autor podrobně rozebere dále, jen od roku 2018, tedy v průběhu uplynulých několika málo let, přibyly tři případy velmi rozsáhlého shromažďování osobních údajů, které autor v této práci zamýšlí zkoumat podrobně. Konkrétně

[22] Návrh skupiny 51 poslanců Parlamentu ČR na zrušení § 97 odst. 3 a 4 zákona č. 127/2005 Sb., o elektronických komunikacích podaný k Ústavnímu soudu ČR dne 26. března 2010; Ústavní soud ČR o návrhu rozhodl v nálezu sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011.
[23] Navrhovatelé konkrétně odkazují např. na rozsudky ESLP ve věci Kruslin v. Francie, Huvig v. Francie ze dne 24. 4. 1990 či Zakharov proti Rusku ze dne 4. 12. 2015.

má autor na mysli povinnost výrobců osobních a lehkých nákladních vozidel vybavit od 31. března 2018 všechny nové typy těchto vozidel palubním systémem eCall, vč. vestavěné SIM karty, určeným pro automatická tísňová volání eCall[24], povinnost leteckých dopravců shromažďovat s účinností od 24. dubna 2019 údaje obsažené v tzv. jmenné evidenci cestujících (Passenger Name Records - PNR)[25] či zpracování údajů v rámci „Evidence vozidel v systému časového zpoplatnění“, označovaných běžně jako elektronické dálniční známky dle novely zákona o pozemních komunikacích[26], která tuto evidenci zavedla, spolu se systémem monitorování jejich úhrady, byla přijata v roce 2019, jí vložená ustanovení v zákoně o pozemních komunikacích nabyla účinnosti od 1. ledna 2021.

[24] Nařízení Evropského parlamentu a Rady (EU) 2015/758 ze dne 29. dubna 2015 o požadavcích na schválení typu pro zavedení palubního systému eCall využívajícího linku tísňového volání 112 a o změně směrnice 2007/46/ES.
[25] Povinnost je v právním řádu ČR obsažena v zákoně č. 49/1997 Sb., o civilním letectví, ve znění pozdějších předpisů.
[26] Zákon č. 227/2019 Sb. kterým se mění zákon č. 13/1997 Sb., o pozemních komunikacích, ve znění pozdějších předpisů, a další související zákony.

1 Struktura a cíle práce

V této práci se autor nejprve v úvodní kapitole stručně zaměří na vymezení zkoumané problematiky, tedy na identifikaci v této práci zkoumaných případů shromažďování a dalšího zpracování osobních údajů založených právními předpisy se zásadním dopadem do soukromí osob a následně se bude věnovat ochraně soukromí v relevantní právní úpravě a v rozhodovací a výkladové praxi.

Poté se autor v dalších kapitolách bude podrobně zabývat jednotlivými zkoumanými případy zpracování osobních údajů. V rámci toho autor v prvé řadě identifikuje právní základ každého ze zkoumaných zpracování, tedy příslušný právní předpis, o který se opírají, a relevantní právní předpisy navazující, posoudí účel zpracování definovaný příslušným právním předpisem a aktuální faktický dopad do soukromí, v relevantních případech autor též shrne dosavadní vývoj jednotlivých právních institutů, které představují zásahy do soukromí. Současně má autor v úmyslu vymezit právem chráněné zájmy, do nichž konkrétní zpracování zasahuje, tedy zejména právo na respektování soukromí, resp. právo na informační sebeurčení a případně související práva a právem chráněné zájmy. Vedle toho považuje autor za potřebné identifikovat též konkrétní veřejný zájem, jak je vymezen relevantní právní úpravou v každém ze zkoumaných případů zpracování údajů, případně též včetně vývoje, pokud k němu u veřejného zájmu sledovaného v konkrétním případě došlo, a vyhodnotit intenzitu takového veřejného zájmu. Podle mínění autora je současně relevantní analyzovat také klíčové právní problémy, které právní úprava některých zkoumaných zpracování zahrnuje, a provést rozbor možných řešení těchto problémů. Autor má v úmyslu zahrnout do tohoto zkoumání i porovnání s relevantními zahraničními právními úpravami vymezujícími obdobná zpracování v jiných členských státech EU v případech, kdy lze takové porovnání učinit a využít je pro rozbor zkoumaných právních institutů.

Rozbor jednotlivých případů zpracování musí dle hodnocení autora zahrnovat též identifikaci kategorií osobních údajů, které jsou zpracovávány, vymezení orgánů oprávněných k využití údajů, včetně právního základu vymezení oprávněných orgánů v podobě odkazu na konkrétní právní předpis. Autor se dále též pokusí z dostupných informačních zdrojů zjistit informace o rozsahu okruhu subjektů údajů daným zpracováním aktuálně dotčených, dobu uchování zpracovávaných údajů, pokud je v konkrétním právního předpise stanovena, jakož i další relevantní okolnosti, dle jednotlivých případů zkoumaných zpracování.

Významná jsou dle hodnocení autora také existující omezení a kontrolní mechanismy obsažené v právní úpravě zakládající každé ze zkoumaných zpracování.

Příkladem může být omezení situací, v nichž může některý z oprávněných orgánů uchovávané údaje využít, existence povinnosti informovat dotčenou osobu o proběhnuvším zpracování, byť i formou následné informace. V rámci kontrolních mechanismů autor za potenciálně významný prvek považuje také veřejnou dostupnost statistických údajů o počtech využitých údajů či o jiných kvantifikovatelných měřítcích míry zásahu do soukromí dotčených osob, když takové informace mohou být významné jak při časovém porovnání vývoje aplikace konkrétního institutu v praxi, tak při porovnání s mírou a četností využití údajů mezi jednotlivými oprávněnými orgány či při porovnání s obdobnými instituty existujícími v zahraničí. Autor se jimi proto bude zabývat v rámci zkoumání vymezených zpracování. U existujících omezení a kontrolních mechanismů považuje autor za potřebné zjistit také informace o jejich vývoji, když v některých případech takováto omezení a kontrolní mechanismy stanovil již od počátku existence daného zpracování (daného právního institutu) právní předpis konkrétní zpracování vymezující, v jiných případech vznikly tyto prvky až následně, v průběhu aplikační praxe, nejčastěji vlivem požadavků judikatury.

Identifikace relevantních rozhodnutí soudů, stanovisek orgánů dohledu nad ochranou osobních údajů či dalších orgánů a jejich analýza proto budou dílčím předmětem autorovy práce u každého z vymezených zpracování. Pro tento účel autor považuje s ohledem na zpracovávané téma za relevantní zejména rozhodnutí Soudního dvora EU, Evropského soudu pro lidská práva, Ústavního soudu ČR, jakož i relevantní stanoviska orgánů příslušných k ochraně osobních údajů. V přiměřené míře autor zohlední též další dostupnou judikaturu soudů vybraných členských států EU, zejména Spolkového ústavního soudu Německa a v některých případech též Ústavního soudu SR. Autor zde bude usilovat nikoli o pouhý encyklopedický výčet rozhodnutí relevantních ke každému ze zkoumaných zpracování, cílem autora bude na základě těchto rozhodnutí a stanovisek identifikovat klíčové právní otázky a problémy, s ohledem na zaměření práce zejména v rovině ústavněprávní, které konkrétní povinná zpracování ve své aktuální podobě vyvolávají. Právní problémy, které v těchto zpracováních spatřovaly soudy, když se jejich posouzením ve své rozhodovací praxi zabývaly, včetně problémů nalezených soudy v jednotlivých národních právních úpravách obdobných právních institutů a také v unijní úpravě, považuje autor za velmi relevantní pro posouzení míry, v níž relevantní právní úprava v jednotlivých případech vyhovuje požadavkům vymezeným v těchto soudních rozhodnutích.

Významnou součástí analýzy každého z identifikovaných případů zpracování bude posouzení splnění ústavněprávních požadavků u relevantních právních předpisů zakládajících

zásahy do soukromí, především prostřednictvím provedení testu proporcionality. Pokud bude z dostupných informací zřejmé, že takový test byl v případě konkrétního právního předpisu proveden, zpravidla ze strany Ústavního soudu ČR posuzujícího danou úpravu v konkrétním řízení, autor posoudí, zda předpoklady, na kterých byl test proporcionality založen, v současné době stále odpovídají skutečnosti, tedy aktuálnímu faktickému stavu aplikace daného právního předpisu a dále též, zda provedený test proporcionality dle hodnocení autora objektivně zohlednil všechny relevantní okolnosti daného zpracování, u nichž jsou v současnosti dostupné informace. Autor se zaměří na to, zda případně v mezidobí nedošlo po stránce faktické či právní v posuzovaném zpracování k zásadním změnám (typicky zejména ke změnám v rozsahu zpracovávaných kategorií údajů, k novelizacím rozšiřujícím orgány oprávněné ke zpracování konkrétních uchovávaných údajů, k rozšíření situací, v nichž je zpracování možné apod.).

Dle výsledku testu proporcionality provedeného v předchozím bodě se autor následně pokusí navrhnout případné úpravy a doplnění vhodných omezení a kontrolních mechanismů a záruk s cílem eliminovat dopady do soukromé sféry. Autor se zde bude také věnovat odpovědím na otázky nastolené v předchozích kapitolách a návrhům možných řešení identifikovaných právních problémů, a to zejména s přihlédnutím k dostupné judikatuře, v níž soudy v některých případech nastínily v úvahu přicházející, ústavně konformní řešení. Zvláštní důraz bude autor klást na posouzení vhodnosti a přiměřenosti stávající právní úpravy jednotlivých zpracování s ohledem na cíle sledované každým z právních předpisů dané zpracování zakládající, na vymezení oprávněných orgánů, rozsah a dobu uchovávání údajů a nastavení kontrolních mechanismů, jako výsledek provedeného testu proporcionality. Autorovým cílem přitom bude formulovat závěry, které z předchozích bodů této práce vyplývají a které by měly platit de lege ferenda pro jednotlivá zkoumaná zpracování, tak aby vyhovovala závěrům provedeného testu proporcionality, opřeného o shora zmiňované požadavky judikatury, včetně požadavků obsažených v základních ústavních dokumentech právního řádu ČR, resp. na úrovni práva EU zejména Listiny základních práv Evropské unie a Evropské úmluvy.

Cílem tohoto projektu bude v závěrečné kapitole provedení syntézy závěrů předchozích bodů. Autor se při formulaci opatření de lege ferenda bude snažit tyto závěry zobecnit tak, aby byly použitelnými nejen na zkoumaná zpracování, nýbrž obdobně též na ostatní zpracování, která autor pro tuto práci neučinil předmětem zkoumání a která ovšem jinak vykazují některé rysy obdobné zpracováním zde posuzovaným. Závěry obsažené v této

závěrečné kapitole by však také měly být obecně platné i pro další možná zpracování založená právními předpisy přijatými v budoucnu. Autor totiž považuje za vysoce pravděpodobné, že množina v současnosti existujících plošných zpracování osobních údajů pro účely jejich využití orgány veřejné moci, kterážto zpracování představují zásah do soukromí fyzických osob, není ani zdaleka konečná a v budoucnu lze očekávat snahy o další, s vysokou pravděpodobností ještě sofistikovanější případy zpracování založených novými právními úpravami. Jelikož autor očekává, že cíle a oblasti veřejného zájmu deklarované při těchto budoucích návrzích zpracování osobních údajů budou obdobné těm obsaženým v aktuálních relevantních právních úpravách, bude se snažit v této práci s ohledem na tuto skutečnost formulovat i své závěry v míře přiměřeně obecné, přitom však dostatečně určité pro jejich možnou aplikaci na tyto budoucí případy.

2 Vymezení zkoumané problematiky

2.1 Zkoumané případy shromažďování a zpracování osobních údajů

Existuje řada případů shromažďování osobních údajů a jejich využívání veřejnou mocí, které jsou uloženy zvláštními právními předpisy či jsou těmito předpisy v konkrétních případech s dostatečnou jednoznačností a určitostí předpokládány. Cílem této práce je zkoumat zpracování osobních údajů se zásadním dopadem do soukromí osob, výsledkem práce tedy dle autora nemá být taxativní výčet všech případů zpracování či využívání osobních údajů ze strany veřejné moci a jejich detailní popis, nýbrž zaměření se na klíčové aspekty vybraných případů a zobecnění závěrů. Autor proto vymezil několik případů takovýchto zpracování, která z hlediska jejich rozšíření, uchovávaných kategorií osobních údajů a celkového množství zpracovávaných údajů vyhodnotil jako zpracování s potenciálem závažného dopadu do soukromí podstatného množství osob.

Mezi zpracování údajů předpokládaná či uložená obecně závaznými právními předpisy, která mají dle názoru autora nejzávažnější dopad do sféry soukromí jedince, a to z hlediska zpracovávaných kategorií údajů, rozsahu zpracování, celkové míry zásahu do soukromé sféry jedince či dalších faktorů, patří dle hodnocení autora zejména následující případy:

A) Povinnost uchovávání provozních a lokalizačních údajů elektronických komunikací uložená provozovatelům sítí elektronických komunikací a poskytovatelům služeb elektronických komunikací (tzv. povinnost Data Retention) a jí odpovídající oprávnění některých orgánů k vyžádání těchto údajů.

Povinnost je obsažena v zákoně o elektronických komunikacích[27], který v tomto směru provádí tzv. Data Retention směrnici[28]; směrnici samotnou v mezidobí SDEU prohlásil za neplatnou[29].

Tento případ autor bude zkoumat jako první, s ohledem na jeho závažnost a celkový rozsah zpracování a z toho vyplývající četnou judikaturu soudů, vč. Ústavního soudu ČR a Soudního dvora EU, která měla celkově zásadní význam pro širší oblast zásahů do soukromí.

[27] Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů.
[28] Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES.
[29] Rozsudek Soudního dvora EU (velkého senátu) z 8. dubna 2014. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další. Žádosti o rozhodnutí o předběžné otázce podané High Court (Irsko) a Verfassungsgerichtshof. Spojené věci C-293/12 a C-594/12.

Soudní rozhodnutí výrazně ovlivnila též postupný vývoj právní úpravy povinnosti Data Retention v elektronických komunikacích. Z těchto důvodů se autor tomuto právnímu institutu bude v této práci věnovat podrobně a v rámci rozboru následujících případů v některých aspektech odkáže na povinné uchovávání provozních a lokalizačních údajů elektronických komunikací.

B) Zpracování osobních údajů systémy v osobních automobilech zahrnuje především systém automatického tísňového volání eCall. Výrobcům všech nových typů osobních a lehkých nákladních vozidel je od 31. března 2018 uložena povinnost vybavit tato vozidla palubním systémem využívajícím linku tísňového volání 112, vč. vestavěné SIM karty. Palubní systém průběžně zaznamenává a aktualizuje mimo jiné informace o vozidle, o počtu zapnutých bezpečnostních pásů a také údaje o přesné poloze vozidla a směru jízdy.

Právním základem systému eCall je tzv. Nařízení eCall[30].

Vedle eCall existuje samostatné palubní zařízení pro sledování spotřeby paliva a/nebo energie (OBFCM – On-board Fuel and/or Energy Consumption Monitoring Device) od roku 2021 zaznamenává údaje o počtu najetých kilometrů a spotřebě každého individuálního automobilu, tyto údaje jsou předmětem hlášení Evropské agentuře pro životní prostředí.

Právním základem systému OBFCM je Prováděcí nařízení Komise (EU) 2021/392 o sledování a hlášení údajů týkajících se emisí CO2 z osobních automobilů a lehkých užitkových vozidel[31], to bylo přijato Evropskou komisí na základě Nařízení Evropského parlamentu a Rady (EU) 2019/631, kterým se stanoví výkonnostní normy pro emise CO2 pro nové osobní automobily a pro nová lehká užitková vozidla[32].

C) Zpracování osobních údajů cestujících v letecké dopravě zahrnuje tzv. předběžné údaje o cestujících (Advance Passanger Information – API) určené ke zdokonalení hraničních kontrol a boje proti nedovolenému přistěhovalectví a údaje jmenné evidence cestujících (Passenger Name Records – PNR) shromažďované povinně leteckými dopravci pro možné

[30] Nařízení Evropského parlamentu a Rady (EU) 2015/758 ze dne 29. dubna 2015 o požadavcích na schválení typu pro zavedení palubního systému eCall využívajícího linku tísňového volání 112 a o změně směrnice 2007/46/ES.
[31] Prováděcí nařízení Komise (EU) 2021/392 ze dne 4. března 2021 o sledování a hlášení údajů týkajících se emisí CO2 z osobních automobilů a lehkých užitkových vozidel podle nařízení Evropského parlamentu a Rady (EU) 2019/631 a o zrušení prováděcích nařízení Komise (EU) č. 1014/2010, (EU) č. 293/2012, (EU) 2017/1152 a (EU) 2017/1153.
[32] Nařízení Evropského parlamentu a Rady (EU) 2019/631 ze dne 17. dubna 2019, kterým se stanoví výkonnostní normy pro emise CO2 pro nové osobní automobily a pro nová lehká užitková vozidla a kterým se zrušují nařízení (ES) č. 443/2009 a (EU) č. 510/2011.

využití pro účely prevence, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti.

Právním základem předběžných údajů o cestujících je Směrnice o povinnosti dopravců předávat údaje o cestujících[33], provedená v právním řádu ČR zákonem o civilním letectví[34]. Jmennou evidenci cestujících zavedla tzv. PNR směrnice[35], kterou do právního řádu ČR transponovala novela zákona o civilním letectví provedená s účinností od 24. dubna 2019 tzv. změnovým zákonem[36] přijatým v souvislosti s GDPR.

D) Zpracování osobních údajů systémy dopravních kamer autor v této práci vymezuje jako zpracování prováděná kamerovými systémy umístěnými na pozemních komunikacích a zaměřenými na projíždějící vozidla a na jejich identifikaci dle registrační značky. Systémy dopravních kamer, zpravidla se záznamem, představují specifický druh kamerových systémů monitorujících veřejná prostranství řady obcí i pozemních komunikací. obcí i pozemních komunikací v ČR. Tyto systémy zahrnují systémy využívané Policií ČR a obecní policií, včetně systémů měření rychlosti vozidel zahrnujících též kamerové systémy úsekového měření, a dále též zařízení pro kontrolu úhrady časového poplatku za užití komunikace, tzv. elektronické dálniční známky. Systémy úsekového měření rychlosti automobilů, na rozdíl od jiných způsobů měření rychlosti, automaticky na začátku i na konci měřeného úseku zaznamenají všechna projíždějící vozidla, včetně těch, která povolenou rychlost nepřekračují, a teprve následně se vyhodnotí porušení pravidel silničního provozu.

Dle zákona o Policii ČR[37] je Policie ČR oprávněna pořizovat *„zvukové, obrazové nebo jiné záznamy osob a věcí nacházejících se na místech veřejně přístupných“*, pokud je to nezbytné pro plnění jejích úkolů. Obdobné oprávnění obecní policie vymezuje zákon o obecní policii[38], podmínkou je, že je taková činnosti potřebná pro plnění úkolů obecní policie podle zákona o obecní policii nebo podle jiného zákona. Zákon o silničním provozu[39] stanoví obecně oprávnění Policie ČR a obecní policie k měření rychlosti vozidel, bez podrobnější specifikace; systémy úsekových měření rychlosti vozidel nejsou založeny na konkrétní právní úpravě.

[33] Směrnice Rady 2004/82/ES ze dne 29. dubna 2004 o povinnosti dopravců předávat údaje o cestujících.
[34] Zákon č. 49/1997 Sb., o civilním letectví, ve znění pozdějších předpisů.
[35] Směrnice Evropského Parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti.
[36] Zákon č. 111/2019, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.
[37] Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.
[38] Zákon č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů.
[39] Viz § 79a zákona č. 361/2000 Sb. o provozu na pozemních komunikacích a o změnách některých zákonů, ve znění pozdějších předpisů (zákon o silničním provozu).

Elektronické dálniční známky (časový poplatek za užití komunikace) a související zařízení pro kontrolu jejich úhrady zavedla s účinností od 1. ledna 2021 novela zákona o pozemních komunikacích, provedená zákonem č. 227/2019 Sb.[40]

E) Zpracování údajů o zdravotním stavu zahrnuje řadu situací, autor jako zpracování s dopadem na nejširší okruh dotčených osob a přitom zahrnující typové aspekty zpracování zkoumaných v této práci zvolil povinná zpracování údajů v Národních zdravotních registrech. Tyto registry byly zavedeny s cílem sledovat vývoj, příčiny a důsledky onemocnění, včetně důsledků ekonomických; aktuálně zahrnují Národní onkologický registr, Národní registr hospitalizovaných, Národní registr reprodukčního zdraví, Národní registr kardiovaskulárních operací a intervencí, Národní registr kloubních náhrad, Národní registr nemocí z povolání, Národní registr léčby uživatelů drog, Národní registr úrazů, Národní registr osob trvale vyloučených z dárcovství krve, Národní registr pitev a toxikologických vyšetření prováděných na oddělení soudního lékařství, Národní diabetologický registr, Národní registr intenzivní péče, Národní registr osob nesouhlasících s posmrtným odběrem tkání a orgánů, Národní registr dárců orgánů, Národní registr osob čekajících na transplantaci orgánů a Národní registr provedených transplantací orgánů.

Národní zdravotní registry zřídilo Ministerstvo zdravotnictví v roce 2002 na základě zmocnění v zákoně o péči o zdraví lidu[41], v současné době jsou vymezeny v zákoně o zdravotních službách[42] a v transplantačním zákoně[43], jako součást Národního zdravotnického informačního systému.

2.2 Ochrana soukromí v platné právní úpravě a v rozhodovací a výkladové praxi

Ještě před vlastním zkoumáním jednotlivých případů zásahů do soukromí považuje autor za potřebné v prvé řadě vymezit práva, která mohou být v případě těchto zásahů dotčena.

2.2.1 Základy práva na ochranu soukromí

Právo na ochranu soukromí, resp. právo na respektování soukromého života je, jakožto jedno ze základních lidských práv, v právním řádu ČR zaručeno v prvé řadě Listinou základních práv a svobod. Dle Ústavního soudu ČR je toto právo v Listině „*rozloženo do více*

[40] Zákon č. 227/2019 Sb., kterým se mění zákon č. 13/1997 Sb., o pozemních komunikacích, ve znění pozdějších předpisů, a další související zákony.
[41] Zákon č. 20/1966 Sb. o péči o zdraví lidu, ve znění pozdějších předpisů.
[42] Zákon č. 372/2011 Sb. o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů.
[43] Zákon č. 285/2002 Sb. o darování, odběrech a transplantacích tkání a orgánů a o změně některých zákonů (transplantační zákon), ve znění pozdějších předpisů.

ustanovení a doplněno dalšími v ní deklarovanými aspekty práva na soukromí“[44]. Dílčí atributy tohoto práva dle Ústavního soudu ČR tvoří právo na informační sebeurčení; ústavní základ práva na informační sebeurčení dovozuje Ústavní soud ČR v prvé řadě z čl. 10 odst. 3 Listiny, ve spojení s čl. 7 odst. 1 a čl. 13 Listiny.

První zmiňovaný článek 10 Listiny ve svém odstavci 3 zakotvuje v právním řádu ČR právo každého na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě, tedy právo na ochranu osobních údajů, a to vedle článku 10 odst. 2 poskytujícího každému právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života. Tato práva bývají v praxi vykládána šířeji, jak autor rozebírá dále v této práci. Článek 7 odst. 1 Listiny zaručuje nedotknutelnost osoby a jejího soukromí a stanoví, že tato může být omezena jen v případech stanovených zákonem. K článku 7 Listiny v souvislosti s ochranou soukromí rozebíranou v této práci považuje autor za potřebné uvést též, že někteří odborníci zastávají odlišný názor na výklad tohoto článku, dle jejich hodnocení se vztahuje primárně na nedotknutelnost osoby ve významu garance *„práva na zachování tělesné a duševní integrity, tj. vyjádření zásadní nepřípustnosti jakýchkoli nedobrovolných zásahů do tělesné schránky člověka a jeho vědomí“* přestože článek 7 výslovně zmiňuje též nedotknutelnost soukromí[45]. Článek 13 Listiny pak chrání listovní tajemství, tajemství dalších písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných komunikačními prostředky a telekomunikační tajemství v podobě tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením. Čl. 13 Listiny zaručuje jejich ochranu tím, že zakazuje všem tato tajemství porušit, předvídá však možnou výjimku z tohoto zákazu, když výslovně stanoví, že tento zákaz platí „*s výjimkou případů a způsobem, které stanoví zákon*“; v praxi mezi takové výjimky patří typicky např. odposlech telekomunikačního provozu upravený v trestním řádu[46].

Jednotlivé články Listiny, resp. práva jimi zaručená, však nelze interpretovat izolovaně, jak opakovaně zdůraznil i Ústavní soud ČR. Samotné právo na ochranu osobních údajů zaručené Listinou v čl. 10 odst. 3 je nutno vykládat ve spojitosti s dalšími relevantními články Listiny, které „*svou povahou i významem dotvářejí privátní sféru jednotlivce a jeho individuální integritu jako zcela nezbytnou podmínku důstojné existence člověka a občana a rozvoje lidského života vůbec*“, jak zdůrazňuje Ústavní soud ČR v nálezu Pl. ÚS 3/14,

[44] Viz nález Ústavního soudu ČR Pl. ÚS 10/17 ze 3. listopadu 2020.
[45] Viz WAGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch, LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer, 2012, str. 278-279.
[46] Viz § 88 zákona č. 141/1961 Sb. o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

konkrétně ve spojitosti s čl. 7 (nedotknutelnost osoby a jejího soukromí), čl. 8 (osobní svoboda), čl. 12 (nedotknutelnost obydlí) a čl. 10 odst. 1 (zachování lidské důstojnosti, osobní cti, dobré pověsti a jména) a odst. 2 (ochrana před neoprávněným zasahováním do soukromého a rodinného života). Dle Ústavního soudu je ochrana soukromé sféry jednotlivce v Listině „*rozložena a doplňována dalšími aspekty práva na soukromí, deklarovanými na různých místech Listiny (např. čl. 7 odst. 1, čl. 10, 12 a 13 Listiny)*“[47].

Vedle toho však navíc dle Ústavního soudu ČR *„interpretace práva na ochranu osobních údajů, je-li vystavena požadavku vyvažování konkurujících zájmů, je ovlivňována aktuálním sociálním a politickým kontextem“*[48]. Ani hranice mezi soukromou a veřejnou sférou přitom v této souvislosti nelze považovat za zcela trvalé a jednoznačné, jak vyzdvihl Ústavní soud ČR v nálezu Pl. ÚS 3/14, v němž v tomto směru odkázal na obdobný závěr, ke kterému dospěli autoři komentáře k Listině: *„[P]ředstavy o tom, co náleží do sféry soukromé a co do sféry veřejné, se rovněž velmi dynamicky mění … hranice mezi privátním a veřejným … se plynule posouvá, a to ve prospěch rozšiřování veřejné sféry … každý jednotlivec je chápán jako osoba se sociálními vazbami existujícími uvnitř občanského společenství a jako osoba uvědomující si odpovědnost vůči celku … každý musí akceptovat pro všechny osoby platné a obecně spravedlivě vyžadované (zákonné) podmínky a omezení své svobody realizované v rámci soukromí, avšak vždy za předpokladu, že zůstane, obecně řečeno, zachován prostor pro svébytnou existenci individua“*[49]. Za zásadní autor považuje, že přestože autoři komentáře zde konstatovali postupný posun a rozšiřování veřejné sféry na úkor sféry soukromé, zdůraznili současně nezbytnost zachování prostoru *„pro svébytnou existenci individua“*. Ústavní soud ČR v nálezu Pl. ÚS 3/14 citoval shora uvedenou pasáž komentáře k Listině a omezil se přitom pouze na výše uvedenou část textu. Autor však, mj. i s ohledem na zaměření této práce, považuje za velmi významný a relevantní také celkový kontext citované pasáže a její závěry, k nimž autoři komentáře v této souvislosti dospívají. Eliška Wagnerová zde v komentáři k čl. 10 Listiny, tedy k právu na soukromí v širším smyslu, dodává závěr, který jednoznačně zdůrazňuje ohrožení soukromí v důsledku aktuálního technického a ekonomického vývoje, kteréžto ohrožení v minulosti neexistovalo a nebylo v tomto rozsahu a v této podobě ani představitelné, a to včetně zařízení využívaných veřejnou mocí k pátrání a sledování, která mají oporu v legislativě, odůvodňované často pouze

[47] Nález Ústavního soudu ČR Pl. ÚS 24/10 ze dne 22. března 2011.
[48] Viz Nález Ústavního soudu ČR Pl. ÚS 3/14 ze 20. prosince 2016.
[49] WAGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch, LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer, 2012, str. 278-279.

„nekonkrétním poukazem na zájem na ochraně bezpečnosti osob i státu“. Wagnerová takovou legislativu výslovně hodnotí jako *„k ochraně soukromí značně nevyváženou“* a v této souvislosti zvláště upozorňuje na skutečnost, že bezpečnostní rizika obecně rostou, je však nutno si uvědomit, že nárůst bezpečnostních rizik umožňuje prezentovat zásahy do soukromí způsobem, z něhož nejsou nové hrozby pro soukromí *„vždy a na první pohled zcela zřetelné“*[50]. Lorenzo Zucca v úvodu publikace k ústavním dilematům soukromí označil jako dobrý příklad toho, *„jak malou hodnotu má vlastní svoboda v porovnání s veřejným zájmem“*, jako jeho příklad uvádí bezpečnost[51].

Autor tedy považuje za jednoznačné a současně za velmi významné, že Eliška Wagnerová ve zmiňovaném komentáři k Listině nepovažuje onen zmiňovaný plynulý posun hranice mezi privátním a veřejným ve prospěch rozšiřování veřejné sféry za prostou skutečnost, kterou nezbývá než vzít na vědomí a proti níž nelze ničeho namítat, jelikož k ní dochází důsledkem přirozeného vývoje, jak by mohla naznačovat výše uvedená pasáž citovaná Ústavním soudem ČR, izolovaně vnímaná, bez celkového kontextu (srov. v citované pasáži obsažené formulace, dle kterých „*každý musí akceptovat …podmínky a omezení své svobody*“, v návaznosti na zmínku o „*velmi dynamicky se měnící hranici mezi privátním a veřejným … ve prospěch rozšiřování veřejné sféry*“ následovanou jedinou podmínkou – nutností zachovat „*prostor pro svébytnou existenci individua*“, co do rozsahu neupřesněný). V kontextu výše citovaného komentáře však autor závěry uváděné výše vykládá v tom smyslu, že autoři komentáře k Listině naopak považují takovýto posun ve prospěch sféry veřejné za sice

---

[50] Viz pokračování Ústavním soudem ČR citované pasáže komentáře: *„Např. dnes bez dalšího neplatí, že lze vyvodit souhlas se vzdáním se práva na soukromí toliko z faktu, že se soukromé jednání uskutečňuje ve veřejném prostoru. Mj. i proto, že především technický a ekonomický vývoj přináší velký, dříve nemyslitelný a ohrožující potenciál, a to nejen pro soukromí realizované právě a jenom v tradičně chápané prostorové dimenzi. Jen namátkou lze uvést problematiku zpracovávání dat [pořízených např. z Rasterfahndung - tj. síťového (plošného) sledování, shromažďování dat z elektronické komunikace, vytvářené a ukládané databáze DNA a další], nových forem komunikace (internet a různé sociální sítě), změny v mediálním prostředí (masivní nástup bezohledné bulvarizace) a různá bezpečnostní (pátrací a sledovací) zařízení, využívaná veřejnou mocí, jakož i soukromými aktéry mnohdy s oporou v nedostatečné - ve smyslu k ochraně soukromí značně nevyvážené - legislativě. Její existence bývá odůvodňována jen nekonkrétním poukazem na zájem na ochraně bezpečnosti osob i státu.*

Nelze také (nečinně - tj. včetně a především jde o legislativní nečinnost) přehlížet využívání naznačených technik a technologií ze strany soukromých osob. Ty mnohdy reálně disponují mnohem většími, a proto pro soukromí nebezpečnějšími možnostmi. To vše a další nové fenomény vytvářejí jakousi šedou zónu mezi tím, co má být soukromé a co veřejné, a tak vznikají nové a nové hrozby pro soukromí, které nejsou vždy a na první pohled zcela zřetelné, zejména jsou-li prezentovány v souvislosti s bezpečnostními riziky, která, hodnoceno obecně, jistě rostou. Velmi záleží na interpretech oněch mnohdy až na hranici snesitelnosti obecných či vágních právních úprav, neboť nalezení zásahu do soukromí ve světle velmi obecné právní úpravy je třeba zkoumat s velmi těsnou návazností na konkrétní skutkový stav. Přesto o míře omezení soukromí ve prospěch jiných soukromých a především veřejných zájmů je a bude vedena neustálá diskuse, v níž základní pozice diskutujícího bude primárně ovlivňována politickou a právní filosofií jím zastávanou a z ní se odvíjejících akcentů.“

[51] ZUCCA, Lorenzo. *Constitutional Dilemmas: Conflicts of Fundamental Legal Rights in Europe and the USA*. Oxford: Oxford University Press, 2008. s. xiii.

nepopiratelnou skutečnost, před jejímiž důsledky však varují a současně považují za nutné, aby na tento posun zákonodárce adekvátně reagoval. Právě toto je hlavním důvodem, pro který autoři onen posun ve svém komentáři uvádějí, a to tím spíše, že jde o posun plynulý, tedy jednak do jisté míry nesnadno postřehnutelný a současně též posun nedokončený, nadále trvající.

Dle Ústavního soudu ČR vedle toho dále také platí, že „*v Listině uvedený výčet toho, co je potřeba zařadit do rámce ochrany soukromí, nelze považovat za taxativní*“[52]. Dle hodnocení autora jsou v této souvislosti relevantní také některá další základní práva a svobody zaručené Listinou, včetně svobody myšlení či svobody projevu, když zákonem předpokládané či uložené zpracování osobních údajů se může v praxi projevit také jako zásah do těchto práv[53]. Ostatně také v Rozsudku Soudního dvora EU ve věci Digital Rigths[54], který autor považuje v rámci tématu této práce – zásahů do soukromí ze strany moci výkonné - za jeden z nejzásadnějších, vyplývá, že Soudní dvůr EU v něm k žádosti irského High Court posuzoval slučitelnost napadené Data Retention Směrnice[55] nejen s právem na respektování soukromého života, stanoveným v článku 7 Listiny EU a s právem na ochranu osobních údajů dle čl. 8 Listiny EU, nýbrž též s právem na svobodu projevu dle čl. 11, s právem na řádnou správu vymezeném v čl. 41 Listiny EU a s právem občanů svobodně se pohybovat a pobývat na území členských států stanoveným v článku 21 Smlouvy o fungování Evropské unie. (S ohledem na význam diskutovaného rozsudku, kterým Soudní dvůr EU vyslovil neplatnost Data Retention Směrnice, se autor tímto rozsudkem a zejména jeho závěry a širšími konsekvencemi, které z nich lze dovozovat, podrobněji zabývá dále v kapitole věnující se povinnému uchovávání provozních a lokalizačních údajů) Rozsudek sice, z povahy věci argumentačně využívá Listinu EU, obdobně je však dle autora jeho závěry možno vztáhnout na srovnatelná práva zaručená v ČR Listinou, jak rozebráno dále.

---

[52] Viz nález Ústavního soudu ČR sp. zn. Pl. ÚS 10/17 ze 3. listopadu 2020.

[53] Obsah samotného pojmu základních lidských práv a svobod není v judikatuře Ústavního soudu ČR rozpracován přímo, Ústavní soud ČR jej vymezuje *„především prostřednictvím principů jejich ochrany při posuzování konkrétních případů“*. Viz HOFMANNOVÁ, Helena. 5. K pojetí lidských práv v judikatuře Ústavního soudu České republiky in GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012 s. 58.

[54] Rozsudek Digital Rights – Rozsudek Soudního dvora EU (velkého senátu) z 8. dubna 2014. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další. Žádosti o rozhodnutí o předběžné otázce podané High Court (Irsko) a Verfassungsgerichtshof (Rakousko). Spojené věci C-293/12 a C-594/12.

[55] Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES.

Jak v oblasti ochrany soukromí, tak rovněž v jiných oblastech, je samozřejmě velmi významné také ustanovení čl. 4 Listiny, a to v popisované souvislosti především čl. 4 odst. 1 a 2 Listiny, dle kterých „*Povinnosti mohou být ukládány toliko na základě zákona a v jeho mezích a jen při zachování základních práv a svobod.*“ a „*Meze základních práv a svobod mohou být za podmínek stanovených Listinou základních práv a svobod upraveny pouze zákonem.*“, a rovněž čl. 4 odst. 4 Listiny, stanovící meze pro omezení základních práv, tak že „*Při používání ustanovení o mezích základních práv a svobod musí být šetřeno jejich podstaty a smyslu. Taková omezení nesmějí být zneužívána k jiným účelům, než pro které byla stanovena.*“. Jak vyplývá z komentáře k čl. 4 odst. 4 Listiny[56], *„Tímto odstavcem je formulována nejzazší (tj. nikoliv vždy uplatnitelná) možná mez pro omezení základních práv tak, že vždy musí být šetřeno jejich podstaty a smyslu s tím, že omezení nesmí být zneužíváno k jiným účelům, než pro které bylo stanoveno.*“, přičemž se však tato mez neuplatňuje „*při omezování základních práv jaksi automaticky, neboť i Ústavní soud (podobně jako jiné evropské ústavní soudy) pravidelně zkoumá při omezování základních práv proporcionalitu omezení základních práv*“. Eliška Wagnerová v Komentáři k tomuto článku Listiny dodává, že „*Jen v případě ekonomických, sociálních a kulturních práv se Ústavní soud, avšak jen občas, vyhýbá uplatnění testu proporcionality a nezkoumá napadený zákon vůbec z hlediska případného omezení základních práv, nýbrž s poukazem na americkou doktrínu rational basis test toliko s ohledem na to, zda přijatá opatření mohou vést k zákonem sledovanému cíli (tj. z pohledu testu proporcionality jde o vhodnost či způsobilost právní úpravy z hlediska možnosti dosáhnout účelu úpravou sledovaného), resp. z hlediska její případné naprosté iracionality, což je metoda značně problematická z mnoha důvodů*“. To však není případ základních práv, která jsou předmětem této práce, tedy především práva na ochranu soukromí a na respekt k soukromému životu v širším smyslu, zahrnující i právo na informační sebeurčení a práva na ochranu osobních údajů, v jejichž případě tak je nutno v případě posuzování kolize s jinými základními práva či kolize s veřejným zájmem uplatnit test proporcionality. Přesto však autor považuje v tomto kontextu za velmi relevantní závěr Jana Kudrny, dle kterého je právě čl. 4 odst. 4 Listiny jejím „pravděpodobně nejvíce porušovaným ustanovením“, přičemž nebezpečí dle jeho hodnocení spočívá v tom, že takto „*k omezování lidských práv často dochází mlčky, bez širší diskuse či veřejné úvahy*“[57]. Diskutované ustanovení Listiny se v souvislosti

[56] WAGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch, LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář.* Praha: Wolters Kluwer (ČR) 2012. 931 s. Dostupné z ASPI.

[57] Pisatel také v textu Pravděpodobně nejvíce porušované ustanovení Listiny (a jedna ze současných hrozeb lidským právům), vedle samotného tohoto označení, hodnotí také z toho vyplývající důsledek jako *„jednu ze*

s tématem této práce uplatní ve vztahu k výkonu veřejné moci, jak autor v dalším textu rozebírá podrobně u jednotlivých v této práci diskutovaných právních institutů. Také Eliška Wagnerová v Komentáři k čl. 4 Listiny stručně shrnuje obsah čl. 4 Listiny tak, že „*Jinými slovy, celé komentované ustanovení stanoví limity výkonu veřejné moci při omezování základních práv.*“ a dodává: „*Adresátem povinností z tohoto ustanovení plynoucích je veškerá veřejná moc*“[58]. Výstižně se k této otázce vyjádřil i Ústavní soud ČR v nálezu Pl. ÚS 41/02: „*K podstatným náležitostem demokratického právního státu náleží minimálně i respekt k základním právům ze strany orgánů veřejné moci při výkonu jejich kompetencí (ze strany orgánů veřejné moci lze v určitých případech vyžadovat i ochranu základních práv), a to ve standardu poskytovaném domácím ústavním pořádkem.*“[59]. Aleš Gerloch k výkladu čl. 4 Listiny dodává, že z jeho dikce plyne, že „*povinnosti mohou být ukládány nejen v prováděcích právních předpisech, ale i v dalších právních předpisech nižší právní síly než zákony, ale též v individuálních právních aktech soudních, správních a dalších orgánů veřejné moci*“ a upozorňuje, že v Listině použitá formulace „*však klade mimořádné nároky na kvalitu soudnictví, neboť jsou to soudy a soudci, vposledku Ústavního soudu, kdo rozhodují o tom, zda byla určitá povinnost uložena „na základě zákona a v jeho mezích“, či nikoliv, ale též, zda bylo šetřeno základních práv a svobod*“[60].

Právo na ochranu soukromí vymezil přiléhavě Ústavní soud ČR ve svém nálezu II. ÚS 517/99, v němž označil právo na ochranu soukromého života za nezadatelné právo fyzické osoby[61], v právní teorii se dle Ústavního soudu ČR lze setkat s přístupem, podle kterého „*Právo na ochranu osobního soukromí je právem fyzické osoby rozhodnout podle vlastního uvážení zda, popř. v jakém rozsahu a jakým způsobem mají být skutečnosti jejího osobního soukromí zpřístupněny jiným subjektům a zároveň se bránit (vzepřít) proti neoprávněným zásahům do této sféry ze strany jiných osob.*“. Ústavní soud ČR však v tomto nálezu upozornil, že „*Přílišná akcentace pozitivní složky práva na ochranu soukromého života vede k*

---

současných hrozeb lidským právům“, když dodává, že „*se navrací čas, kdy jsou lidská práva formálně zakotvena, ale k jejich materiálnímu prosazování již nedochází, anebo ne přinejmenším v předpokládaném rozsahu*“. Viz *Kudrna Jan*. 27. Pravděpodobně nejvíce porušované ustanovení Listiny (a jedna ze současných hrozeb lidským právům) in GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012 s. 275.

[58] WAGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch, LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář.* Praha: Wolters Kluwer (ČR) 2012. 931 s. Dostupné z ASPI.

[59] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 41/02 ze dne 28.1.2004.

[60] GERLOCH, Aleš. Relace práv a povinností v Listině základních práv a svobod in GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012 s. 17.

[61] Nález Ústavního soudu ČR sp. zn. II. ÚS 517/99 ze dne 1. 3. 2000.

neadekvátnímu zúžení ochrany pouze na to, aby skutečnosti soukromého života fyzické osoby nebyly zpřístupňovány veřejnosti bez jejího souhlasu či bez důvodu uznávaného zákonem a tak nebyla narušována integrita vnitřní sféry, která je pro příznivý rozvoj osobnosti nezbytná.". Současně zde Ústavní soud ČR vymezil dvě typické situace porušení práva na ochranu soukromí, a sice, a to především, *„tehdy, jestliže někdo neoprávněně získává vědomosti o skutečnostech soukromého života jiné osoby"* a dále též tehdy, *„jestliže tyto skutečnosti rozšiřuje.*" Ústavní soud ČR však *„nesdílí toto zúžené pojetí*" a v citovaném nálezu poukázal na rozhodnutí Evropské komise a Evropského soudu pro lidská práva, která se týkají interpretace a aplikace čl. 8 odst. 1 Evropské úmluvy a ze kterých „*zdůrazňuje především myšlenku, že respektování soukromého života musí zahrnovat do určité míry právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi*".

Za jedno z klíčových rozhodnutí Ústavního soudu ČR v oblasti zásahů do práva na ochranu soukromí považuje autor nález Pl. ÚS 24/10[62]; autor se mu z tohoto důvodu věnuje podrobně dále, v části týkající se povinného uchovávání a zpracování provozních a lokalizačních údajů elektronických komunikací. V tomto nálezu Ústavní soud ČR upozorňuje na to, že „*Koncept soukromí bývá nejčastěji spojován se západní kulturou a ještě přesněji s anglo-americkou kulturní představou zasazenou do politické filozofie liberalismu. Jde o koncept, který zjevně není obecně zcela sdílený jak v akcentu na význam soukromí, tak v rozsahu toho, co má být soukromím chráněno. V různých kulturách panují různé představy o tom, k jak rozsáhlému soukromí jsou jednotlivé osoby oprávněny a v jakých kontextech*" (pozn. autora: Ústavní soud ČR zde cituje komentář Elišky Wagnerové k čl. 10 Listiny základních práv a svobod, aniž by bylo z textu nálezu zcela zřejmé, že se jedná o citaci[63]). Ústavní soud ČR pak dále též cituje z disentního stanoviska – jak uvádí Ústavní soud ČR, následně hojně citovaného – Louise Dembitz Brandeise, soudce Nejvyššího soudu Spojených států amerických z roku 1928, kteréžto disentní stanovisko (k případu Olmstead v. U. S. 438, 478, 1928) obsahuje hodnocení soukromí, které lze, navzdory již téměř celému století uplynulému od jeho formulace, dle hodnocení autora stále považovat za velmi inspirativní ideové a argumentační východisko. Dle Brandeisova vymezení soukromí "*Tvůrci naší Ústavy na sebe vzali odpovědnost vytvořit příznivé podmínky pro usilování o štěstí (...) Přiznali právo (proti státu) být ponechán "sám sobě" - což je nejkomplexnější či nejobsažnější právo ze všech a*

[62] Nález Ústavního soudu ČR Pl. ÚS 24/10 ze dne 22. března 2011.
[63] WAGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch, LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář.* Praha: Wolters Kluwer (ČR) 2012. 931 s. Dostupné z ASPI.

zároveň i právo, které je nejvzácnější civilizovanému lidstvu." Dle Ústavního soudu ČR se „*z explicitně ústavně nezmíněného práva na soukromí postupem doby stal základní strukturální element U.S. ústavy, který zajišťuje autonomii jednotlivce, byť o jeho uplatnění je stále a opakovaně sváděna uvnitř U.S. Supreme Court bitva*.“

Samotné rozhodnutí Nejvyššího soudu USA, resp. disentní stanovisko soudce Brandeise, lze dle hodnocení autora nadále v mnoha směrech považovat nejen za zdroj inspirace, jedná se navíc rovněž o stanovisko předložené ve věci, v níž Nejvyšší soud USA posuzoval zásah do práva na ochranu soukromí ze strany veřejné moci, konkrétně zásah v podobě odposlechu. V neposlední řadě považuje autor mnohé ze závěrů obsažených ve zmiňovaném disentním stanovisku za stále platné a aplikovatelné a překvapivě aktuální i po téměř 100 letech od své formulace. Autor proto považuje za vhodné a v souvislosti s tématem této práce i za velmi relevantní některé tyto závěry zde stručně zmínit[64]. Soudce Brandeis v prvé řadě zdůraznil, že „*Zlo spojené s narušením soukromí telefonu je mnohem větší než narušení soukromí ve vztahu k poště.*“, což odůvodnil tím, že „*Kdykoli je telefonní linka odposlouchávána, je narušeno soukromí osob na obou koncích linky a mohou být odposlouchávány všechny rozhovory mezi nimi na jakékoli téma, ačkoli jsou řádné, důvěrné a tajné.*“

Tato úvaha soudce Brandeise je dle názoru autora velmi nadčasová, ani v dnešní době neztrácí nic na své aktuálnosti, bylo by možno vztáhnout ji k řadě případů plošných zásahů do soukromí ze strany orgánů veřejné moci. Za zásadní zde autor považuje právě zmínku o možnosti odposlechu všech hovorů, plošně, bez ohledu na téma hovoru, tedy na relevanci tématu ve vztahu k důvodům, pro které byl odposlech zaveden. Tato charakteristika je totiž vlastní všem plošným zásahům, které postihují celou množinu případů, bez ohledu na odůvodnitelnost a relevanci zásahů pouze ve vztahu k velmi malé podmnožině případů. Autor má za to, že v případech rozebíraných v této práci lze tento Brandeisův závěr obdobně vztáhnout např. k plošnému zásahu do práva na ochranu soukromí v podobě shromažďování všech vymezených provozních a lokalizačních údajů veškerých účastníků a uživatelů služeb elektronických komunikací bez rozlišení. Brandeis navíc velmi výstižně vystihl, že „*Odposlech telefonní linky jednoho člověka navíc zahrnuje odposlech telefonu každé další osoby, které může volat nebo která může volat jemu.*“, současně také ve svém zobecnění

[64] Rozhodnutí Nejvyššího soudu Spojených států amerických. Olmstead et al. v. United States. Green et al. v. United States McInnis v. United States sp. zn. 277 U.S. 438 48 S. Ct. 564; 67 L. Ed. 785; 1923 U.S. LEXIS 2588; 24 A.L.R. 1238 ze 20. a 21. února 1928.

vyslovil jednoznačnou predikci dalšího vývoje dle které „*Pokrok vědy poskytující vládě prostředky špionáže se pravděpodobně nezastaví u odposlechů.*“[65] Správnost tohoto odhadu soudce Brandeise potvrzují aktuální případy zásahů do práva na ochranu soukromí, např. dále v této práci rozebírané využití údajů kamerového systému na silnicích v ČR pro účely správce daně při prověřování oprávněnosti nároku na odpočet daně z přidané hodnoty podnikatele, které autor podrobně rozebírá v kapitole věnující se zpracování osobních údajů prostřednictvím dopravních kamerových systémů.

2.2.2 K ochraně soukromí v širším smyslu

V rámci práva na ochranu soukromí Ústavní soud ČR ve své rozhodovací praxi vymezil „podskupinu tzv. osobnostních práv“, mezi něž řadí právo na zachování lidské důstojnosti, osobní cti, dobré pověsti a jména a označuje je za „*„tvrdé jádro“ ochrany soukromí v širším slova smyslu*“ dle čl. 10 odst. 1 Listiny, tato práva jsou dle Ústavního soudu ČR „*přiřazována k nadpozitivním hodnotám jako samotná podstata a nejvyšší účel základních práv*“[66], dle jeho hodnocení se také tato práva do jisté míry vymykají omezujícím zásahům. Úvahu o „nadpozitivních“ hodnotách Ústavní soud ČR zmiňuje již ve svém nálezu II.ÚS 2268/07[67] (výše zmiňovaný nález Pl. ÚS 3/14 na tuto úvahu navazuje a na nález II. ÚS 2268/07 v tomto směru výslovně odkazuje), ve kterém k těmto hodnotám řadí lidskou důstojnost, svobodu a spravedlnost, jakožto hodnoty, které „*představují podstatné náležitosti demokratického právního státu*“. Adjektivem „nadpozitivní“ zde Ústavní soud ČR reflektuje princip nezměnitelnosti podstatných náležitostí demokratického státu obsažený v čl. 9 odst. 2 Ústavy ČR[68], kterýžto princip bývá vykládán jako „*bezprostředně účinný ústavní příkaz závazný pro všechny orgány veřejné moci*“[69].

---

[65] V originálním anglickém znění: *„The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping..“* Pozn.: Přeloženo autorem.

[66] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 3/14 ze 20. prosince 2016.

[67] Nález Ústavního soudu ČR sp. zn. II.ÚS 2268/07 ze dne 29. února 2008.

[68] Dle čl. 9 odst. 2 Ústavy ČR *„Změna podstatných náležitostí demokratického právního státu je nepřípustná“.*

[69] Komentář k čl. 9 Ústavy ČR in RYCHETSKÝ, Pavel, LANGÁŠEK, Tomáš, HERC, Tomáš, MLSNA, Petr a kolektiv. *Ústava České republiky. Zákon o bezpečnosti České republiky. Komentář.* Praha: Wolters Kluwer (ČR) 2015. 1224 s. In: ASPI.

V nálezu Pl. ÚS 3/14[70] Ústavní soud ČR cituje komentář Elišky Wagnerové k Listině základních práv a svobod, v němž autorka uvádí, že „*V českých poměrech jde v případě práva na informační sebeurčení o Pandořinu skříňku.“* Wagnerová toto své hodnocení výslovně vztahuje zejména k databázím obsahujícím *„mnohdy citlivé informace ze soukromého života jednotlivých osob pořízené především státněbezpečnostními orgány v období před listopadem 1989, které stát stále drží“* a které „*mohou vyvolat potřebu řešení“*. Dle jejího závěru však „*lze jen vyslovit údiv, že se takovým individuálním případem Ústavní soud dosud nezabýval*.“[71] Ústavní soud ČR k tomu v předmětném nálezu dodává, že „*rozpoznání takových imperativů v judikatuře Ústavního soudu je dosud stále otevřené*“.

Ústavní soud ČR řadí do rámce ochrany soukromí i právo na čest, v nálezu IV. ÚS 23/05 ve vztahu k soukromé sféře uvádí, že *„Zásadně je však věcí každého, co a v jakém rozsahu z této sféry uvolní jako informaci pro okolní svět. Jinými slovy, v tomto segmentu zpravidla platí naprosté informační sebeurčení“*[72]. Ústavní soud ČR dále též v souvislosti se základními právy obecně zdůrazňuje význam lidské důstojnosti; v nálezu IV. ÚS 412/04[73] vysvětluje, že *„V souladu s poválečnou změnou v chápání lidských práv (jež nalezla vyjádření např. v Chartě OSN či ve Všeobecné deklaraci lidských práv) se stala základní bází, z níž vychází interpretace všech základních práv, lidská důstojnost, která mimo jiné vylučuje, aby s člověkem bylo zacházeno jako s předmětem“*. Také preambule Ústavy ČR výslovně označuje lidskou důstojnost za nedotknutelnou hodnotu, obdobně též Listina v čl. 1 zaručuje rovnost lidí v důstojnosti i v právech, v čl. 10 odst. 1 pak garantuje subjektivní právo každého na zachování lidské důstojnosti, společně s osobní ctí, dobrou pověstí a ochranou jména. Vedle informačního sebeurčení, jakožto ochrany soukromí v užším smyslu, stojí dle Ústavního soudu ČR *„sféra společenských, občanských a profesních vazeb“*, sociální sféra, která *„reflektuje sociální aspekt základních práv, resp. odráží reálný stav, v němž jednotlivec žije ve společenství a vstupuje s ostatními jeho členy do různých forem interakce a komunikace“* a prostřednictvím svého chování, ba dokonce i *„skrze své samotné bytí ovlivňuje ostatní členy společenství“*[74]. Z hlediska možných zásahů do práva na ochranu soukromí je významné, že v této sféře již dle Ústavního soudu ČR naprostá ochrana soukromí neplatí a lze do ní *„za určitých podmínek vstupovat i bez souhlasu subjektu práv, neboť se v ní mohou vyskytovat*

[70] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 3/14 ze 20. prosince 2016.
[71] WAGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch, LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář.* Praha: Wolters Kluwer (ČR) 2012. s. 285.
[72] Nález Ústavního soudu ČR sp. zn. IV. ÚS 23/05 ze dne 17. července 2007.
[73] Viz Nález Ústavního soudu ČR sp. zn. IV. ÚS 412/04 ze dne 7. prosince 2005.
[74] Viz Nález Ústavního soudu ČR Pl. ÚS 3/14 ze 20. prosince 2016.

fakta, která jsou předmětem veřejného zájmu“. Tato sféra *„může být narušena proporcionálními zásahy veřejné moci za účelem ochrany zájmů společenství“*. Tento závěr Ústavního soudu ČR se vztahuje výhradně k výše vymezené sociální sféře, nelze jej tedy zobecňovat, nebylo by ani správné aplikovat jej šířeji, než uvádí Ústavní soud ČR.

2.2.3 K právu na informační sebeurčení

Kromě samotného práva na ochranu soukromí, resp. práva na respektování soukromého života je dle Ústavního soudu ČR v případě zásahů do soukromí na místě uvažovat také o možných zásazích do práva na informační sebeurčení, jakožto specifického práva v širším rámci práva na ochranu soukromí, jak je ostatně zřejmé z některých již výše citovaných pasáží. V nálezu I. ÚS 512/02[75] se Ústavní soud ČR vyslovil k právu na informační sebeurčení, když jej vymezil ve vazbě na čl. 2 Listiny a konstatoval, že „*Ústavní kautele obsažené v čl. 2 odst. 2 Listiny základních práv a svobod odpovídá právo jednotlivce na všeobecnou ochranu svobodné sféry osoby“*, kterou označil za *"sběrnou" či generální klauzuli“*, logicky reagující na *„nemožnost předvídat při formulování základních práv všechny v budoucnu se vyskytující zásahy do svobodného prostoru osoby“*. Do ní Ústavní soud ČR řadí i právo na informační sebeurčení. Na tyto závěry poté Ústavní soud ČR navázal ve svých následných nálezech (viz např. nález IV. ÚS 29/05 ze dne 1. 6. 2005 (N 113/37 SbNU 463)), jako tematicky i argumentačně významný hodnotí autor též nález I. ÚS 705/06[76], ve kterém Ústavní soud ČR zopakoval a dále rozvinul hlavní myšlenku v tomto směru vyslovenou již v nálezu I. ÚS 512/02. Dle nálezu I. ÚS 705/06 právo na informační sebeurčení spadá do oblasti svobodné sféry jednotlivce a spočívá v tom, že „*Jen osoba sama je oprávněna rozhodnout o tom, jaké údaje o sobě poskytne včetně údajů o své pracovní, ekonomické či podnikatelské aktivitě, pokud zákon neukládá v tomto směru osobě povinnost tak, jak to předvídá čl. 4 odst. 1 Listiny“*. Dle Ústavního soudu ČR působí čl. 4 odst. 1 Listiny *„komplementárně ve vztahu k čl. 2 odst. 2 Listiny“* a zpřesňuje jeho dopad na jednotlivce. Také Aleš Gerloch konstatuje, že „*Litera čl. 2 a čl. 4 Listiny musí být tedy vykládána ve vzájemné souvislosti, při použití postupů systematického výkladu*“, když v předchozím textu upozornil na nevhodný a nepřesný výklad, při kterém „*Výše uvedené ustanovení Listiny bylo*

[75] Nález Ústavního soudu ČR sp. zn. I. ÚS 512/02 ze 20. listopadu 2002.
[76] Nález Ústavního soudu ČR sp. zn. I. ÚS 705/06 ze dne 1. prosince 2008.

nezřídka vykládáno jako omezující prováděcí normotvorbu, a to až do absurdních důsledků, totiž že nelze ukládat povinnosti jinak než ve formě zákona“[77].

Další vyjádření k právu na informační sebeurčení, relevantní k tématu této práce, učinil Ústavní soud ČR v nálezu Pl. ÚS 10/17[78]. V této kauze k návrhu Městského soudu v Praze porovnával právo na ochranu soukromého života a na informační sebeurčení na straně jedné a ekonomický zájem podnikatelů na vyhnutí se poskytování zboží a služeb nesolventním spotřebitelům na straně druhé. Ústavní soud ČR, rozhodující v plénu, v tomto nálezu právo na informační sebeurčení označil za součást „*základního práva na ochranu soukromí v širším smyslu, upraveného především v čl. 7 odst. 1 a čl. 10 odst. 2 a 3 Listiny*“. Dle hodnocení pléna Ústavního soudu ČR vysloveného v tomto nálezu je „*požadavek respektu k svébytnému uspořádání života, jehož jednou z hlavních funkcí je i záruka ochrany osobních údajů*“ základním nárokem na autonomii jednotlivce, plynoucím z lidských práv.

Vymezení práva na respektování soukromého života v Listině, jak je v tomto nálezu zhodnotil Ústavní soud, je dle autora velmi výstižné a plně aplikovatelné na případy, které jsou předmětem této práce, tedy na plošné zásahy do soukromí ze strany orgánů veřejné moci založené právním předpisem. Jádrem právní úpravy práva na respektování soukromého života je dle Ústavního soudu „*právo jednotlivce rozhodnout podle vlastního uvážení, zda, popř. v jakém rozsahu, jakým způsobem a za jakých podmínek mají být skutečnosti a informace z jeho soukromí zpřístupněny jiným subjektům*“. Právo na informační sebeurčení pak dle hodnocení Ústavního soudu ČR „*svou povahou i významem … spadá mezi základní lidská práva a svobody, neboť spolu se svobodou osobní, svobodou v prostorové dimenzi (domovní), svobodou komunikační a zajisté i dalšími ústavně garantovanými základními právy dotváří osobnostní sféru jedince, jehož individuální integritu jako zcela nezbytnou podmínku důstojné existence jedince a rozvoje lidského života vůbec je nutno respektovat a důsledně chránit*“[79]. V nálezu Pl. ÚS 1/12[80] označuje Ústavní soud ČR právo na informační sebeurčení za jeden z aspektů práva na respekt k soukromému životu, vedle tradičního vymezení soukromí v jeho prostorové dimenzi a v souvislosti s nerušenou tvorbou sociálních vztahů; toto právo vymezuje jako rozhodování jedince o sobě samém.

---

[77] GERLOCH, Aleš. Relace práv a povinností v Listině základních práv a svobod in GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012 s. 16.
[78] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 10/17 ze 3. listopadu 2020.
[79] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011.
[80] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 1/12 ze dne 27. listopadu 2012.

2.2.4 Mezinárodněprávní zakotvení práva na ochranu soukromí

Na mezinárodněprávní úrovni jsou základní práva související s ochranou soukromí garantována několika dokumenty. V prvé řadě je v tomto směru nutno uvést Všeobecnou deklaraci lidských práv[81]. Tento základní mezinárodní dokument v oblasti lidských práv navazuje na Chartu OSN, která již ve své preambuli vyjádřila víru v základní lidská práva, následně též podporování a posilování „*úcty k lidským právům a základním svobodám pro všechny bez rozdílu rasy, pohlaví, jazyka nebo náboženství*“ zakotvila v čl. 1 do svých cílů a zmiňuje jej ve svém textu i v dalších souvislostech. Dle čl. 12 Všeobecné deklarace lidských práv nesmí být nikdo vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, všeobecná deklarace přiznává každému právo na zákonnou ochranu proti takovým zásahům nebo útokům. Všeobecná deklarace vymezuje také další související práva, vč. práva na svobodu myšlení, svědomí a náboženství či práva na svobodu přesvědčení a projevu. Jak uvádí Pavel Šturma, Všeobecná deklarace „*je prvním mezinárodním instrumentem obecné povahy, který ve stručné podobě vyhlašuje ucelený katalog lidských práv ve prospěch každého (každé lidské bytosti).*“ a dodává, že „*Navzdory své nezávazné podobě (rezoluce Valného shromáždění OSN), považovaná za soft law, stanoví základní katalog lidských práv, který se později rozvinul ve smluvních instrumentech, obecných i specializovaných*“[82].

Na Chartu OSN navazuje a výslovně na ni ve svém textu odkazuje též Mezinárodní pakt o občanských a politických právech, přijatý Organizací spojených národů v roce 1966[83]. Tento dokument v čl. 17 zakazuje mj. svévolné zasahování do soukromého života, do rodiny, domova nebo korespondence a zakotvuje právo na zákonnou ochranu proti takovým zásahům nebo útokům. V dalších článcích pakt zakotvuje též právo na svobodu myšlení, svědomí a náboženství či právo zastávat svůj názor bez překážky a právo na svobodu projevu, zahrnující

[81] Všeobecná deklarace lidských práv vyhlášená Usnesením č. DE 01/48 Valného shromáždění OSN ze dne 10. prosince 1948.
[82] ŠTURMA, Pavel. Všeobecná deklarace lidských práv Kořeny a současné výzvy. In. ŽÁK KRZYŽANKOVÁ, Katarzyna, KÜHN, Zdeněk et al. (eds.) *Právo jako multidimenzionální fenomén. Pocta Aleši Gerlochovi k 65. narozeninám.* Plzeň: Aleš Čeněk, 2020 s. 129.
[83] Mezinárodní pakt o občanských a politických právech byl otevřen k podpisu v New Yorku 19. prosince 1966, společně s Mezinárodním paktem o hospodářských, sociálních a kulturních právech. V právním řádu Československa byl oficiálně vyhlášen Vyhláškou ministra zahraničních věcí č. 120/1976 Sb. o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech. Jménem Československé socialistické republiky byly oba pakty podepsány v New Yorku dne 7. října 1968, Mezinárodní pakt o občanských a politických právech vstoupil v platnost pro Československou socialistickou republiku dnem 23. března 1976.

svobodu vyhledávat, přijímat a rozšiřovat informace a myšlenky všeho druhu, bez ohledu na hranice, ať ústně, písemně nebo tiskem, prostřednictvím umění nebo jakýmikoli jinými prostředky podle vlastní volby.

V rámci ochrany lidských práv v evropském regionu v současné době *„koexistují dva subsystémy této úpravy“*, které *„musí být striktně odlišovány, a to zejména na úrovni Rady Evropy, coby politické organizace (pouze), založené na principech vlády práva a demokracie“* a *„na úrovni Evropských společenství a Evropské unie jako supranacionálních organizací…“*[84]. V unijním právu je právo na ochranu soukromí obsaženo primárně v Listině EU a v dalších dokumentech uvedených dále v této práci, na něž ve svých nálezech často odkazuje taktéž Ústavní soud ČR[85]. V případě Listiny základních práv Evropské unie jde konkrétně zejména o čl. 7 Respektování soukromého a rodinného života a čl. 8 Ochrana osobních údajů, jak již bylo zmíněno výše.

V rámci instrumentů Rady Evropy, jakožto nejstarší evropské politické organizace, založené v roce 1949, je *„smluvní systém ochrany lidských práv založen na dvou pilířích: Evropské úmluvě o ochraně lidských práv a základních svobod (1950) a Evropské sociální chartě (1961)“*[86]. Evropská úmluva o ochraně lidských práv a základních svobod byla sjednána v Římě 4. listopadu 1950. Ve svém článku 8 zaručuje každému právo na respektování soukromého a rodinného života, obydlí a korespondence. ESLP z tohoto článku dovozuje i právo na informační sebeurčení, dle Ústavního soudu ČR ESLP *„opakovaně zdůraznil, že také sběr a uchovávání údajů týkajících se soukromého života jednotlivce spadají pod rozsah tohoto článku, neboť výraz "soukromý život" nesmí být interpretován restriktivně“*, jak konstatuje Ústavní soud ČR v nálezu Pl. ÚS 3/14[87], z konkrétních rozhodnutí ESLP v tomto směru odkazuje zejména na rozsudky ve věci Malone proti UK[88] a Rotaru proti Rumunsku[89]. Právě z rozhodovací praxe ESLP opírající se o čl. 8 Evropské úmluvy vyšel Ústavní soud ČR též v již zmiňovaném nálezu Pl. ÚS 24/10. V něm v návaznosti na tuto rozhodovací praxi vymezil rozsah práva na soukromí ve vztahu k zásahům orgánů veřejné moci a zdůraznil šíři tohoto práva, specificky pak to, že právo na soukromí *„konzumuje i právo na ochranu před*

---

[84] ŠIŠKOVÁ, Naděžda. *Evropská unijní ochrana lidských práv (Charta a další instrumenty ochrany lidských práv v EU).* Praha: Linde Praha a.s, 2001. s. 9.
[85] Jde zejména o Úmluvu o ochraně lidských práv a základních svobod či SFEU. Viz např. nálezy Ústavního soudu ČR sp. zn. Pl. ÚS 24/10, Pl. ÚS 24/11, Pl. ÚS 33/16 a další.
[86] ŠTURMA, Pavel. *Mezinárodní a evropské kontrolní mechanismy v oblasti lidských práv. 3. doplněné vydání.* Praha: C.H.Beck, 2010. s. 31.
[87] Nález Ústavního soudu ČR Pl. ÚS 3/14 ze 20. prosince 2016.
[88] Rozsudek ESLP ve věci Malone v. The United Kingdom č. 8691/79 ze dne 2. srpna 1984.
[89] Rozsudek ESLP ve věci Rotaru proti Rumunsku č. 28341/95 ze dne 4. května 2000.

sledováním, hlídáním a pronásledováním ze strany veřejné moci, a to i ve veřejném prostoru či na veřejně přístupných místech" a dodal, že *„žádný zásadní důvod neumožňuje vyloučit z pojmu soukromého života aktivity profesní, obchodní či sociální"*[90].

Evropská úmluva v čl. 8 odst. 2 výslovně stanoví možná omezení, za kterých mohou státní orgány zasahovat do výkonu tohoto práva; takové zásahy musejí být „*v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných*". Právo na účinné opravné prostředky vyjadřuje Evropská úmluva v čl. 13 pro každého a ve vztahu ke všem právům a svobodám přiznaným úmluvou, které byly porušeny, vč. práv dle čl. 8; dle Evropské úmluvy se musí jednat o opravné prostředky před národním orgánem, text čl. 13 výslovně dodává, že tomu tak musí být, „*i když se porušení dopustily osoby při plnění úředních povinností*". Relevantní je v této souvislosti též čl. 6 Evropské úmluvy vyžadující právo každého na spravedlivý proces[91].

Ústavní soud ČR ve svém nálezu Pl. ÚS 3/14 a obdobně též Pl. ÚS 24/10 rozebírá relevantní judikaturu ESLP k právu na respekt k soukromému životu podle čl. 8 Evropské úmluvy a uvádí, že ESLP takto výslovně „*označil za zásahy do soukromí jednotlivců mimo jiné i zásahy v podobě kontroly dat, obsahu pošty a odposlechu telefonních hovorů [srov. rozhodnutí ve věci Klass a další proti Německu (no. 5029/71) ze dne 6. 9. 1978, rozhodnutí ve věci Leander proti Švédsku (no. 9248/81) ze dne 26. 3. 1987, rozhodnutí ve věci Kruslin proti Francii (no. 11801/85) ze dne 24. 4. 1990 či rozhodnutí ve věci Kopp proti Švýcarsku (no. 23224/94) ze dne 25. 3. 1998], zjišťování telefonních čísel telefonujících osob [srov. rozhodnutí ve věci P. G. a J. H. proti UK (no. 44787/98) ze dne 25. 9. 2001], nebo uchovávání údajů o DNA jednotlivců v databázích obviněných [srov. rozhodnutí ve věci S. a Marper proti UK (no. 30562/04 a 30566/04) ze dne 4. 12. 2008]. V rozhodnutí ve věci Rotaru proti Rumunsku (no. 28341/95) ze dne 4. 5. 2000 ESLP dovodil z práva na soukromý život projevujícího se v podobě práva na informační sebeurčení i pozitivní povinnost státu, zlikvidovat data, která o osobě z její soukromé sféry stát shromáždil a zpracoval.*" Taktéž SDEU ve své rozhodovací praxi týkající se ochrany osobních údajů, resp. zásahů do práva na ochranu osobních údajů výslovně odkazuje na čl. 8 Evropské úmluvy. Z judikatury SDEU

[90] V tomto bodě se Ústavní soud ČR argumentačně opřel o rozhodnutí ESLP ve věci Niemietz proti Německu (no. 13710/88) ze dne 16. 12. 1992.
[91] K tomu podrobně viz KMEC, Jiří, KOSAŘ, David, KRATOCHVÍL, Jan, BOBEK, Michal. *Evropská úmluva o lidských právech. Komentář. 1. vyd.* Praha: C.H. Beck, 2012.

vyplývá, že zpracovávání a uchovávání provozních a lokalizačních údajů účastníků a uživatelů (zde označovány jako „*údaje vytvářené nebo zpracovávané v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí*“) představuje zpracování osobních údajů ve smyslu tohoto článku[92].

2.2.5 ESLP k informovanosti dotčené osoby o zásahu do jejích práv

V rozhodnutí Malone v. UK poukázal ESLP, opět s odkazem na čl. 8 Evropské úmluvy, na významný faktický aspekt, spočívající v tom, že „*pokud stát zavede tajné sledování, jehož existence zůstává kontrolovaným osobám neznámá, v důsledku čehož zůstává toto sledování nenapadnutelné, mohl by být článek 8 do značné míry omezen až k nicotnosti*“. ESLP upozorňuje, že „*V takové situaci je možné, aby se s jednotlivcem zacházelo způsobem, který je v rozporu s článkem 8, nebo aby byl dokonce zbaven práva přiznaného tímto článkem, aniž by o tom věděl, a tudíž aniž by byl schopen dosáhnout nápravy buď na vnitrostátní úrovni, nebo před orgány Úmluvy*“. ESLP se ve svém rozhodnutí v této věci vyjádřil také k aspektu, který je dle hodnocení autora v právu na ochranu soukromí před zásahy zcela zásadní a patří ke klíčovým kontrolním mechanismům, tedy k informovanosti dotčené osoby o proběhnuvším zásahu. ESLP takto zdůraznil, že „*Soud považuje za nepřijatelné, aby zajištění výkonu práva zaručeného Úmluvou mohlo být takto odstraněno pouhým faktem, že dotčená osoba o jeho porušení neví. Právo obrátit se na Komisi pro osoby potenciálně dotčené tajným sledováním je třeba odvodit z článku 25, neboť jinak hrozí, že článek 8 (čl. 8) bude anulován.*“ [93] ESLP v této věci posuzoval i další kontrolní mechanismy, které brání zneužití právního institutu umožňujícího zásahy do soukromí či alespoň riziko takového zneužití snižují, zejména soudní nebo obdobnou kontrolu. Autor však v této souvislosti považuje požadavek na zajištění informovanosti dotčené osoby za velmi významný, proto jej na tomto místě zdůrazňuje,

---

[92] K tomu viz např. Rozsudek Soudního dvora EU (velkého senátu) ze dne 9. listopadu 2010. Volker und Markus Schecke GbR (C-92/09) a Hartumt Eifert (C-93/09) proti Land Hessen. Žádosti o rozhodnutí o předběžné otázce: Verwaltungsgericht Wiesbaden – Německo. Spojené věci C 92/09 a C 93/09. *Soudní dvůr EU* [online]. 2010 [cit. 7.4.2023].

[93] V anglickém znění publikovaném ESLP: *„ The Court points out that where a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 (art. 8) could to a large extent be reduced to a nullity. It is possible in such a situation for an individual to be treated in a manner contrary to Article 8 (art. 8), or even to be deprived of the right granted by that Article (art. 8), without his being aware of it and therefore without being able to obtain a remedy either at the national level or before the Convention institutions.“; „The Court finds it unacceptable that the assurance of the enjoyment of a right guaranteed by the Convention could be thus removed by the simple fact that the person concerned is kept unaware of its violation. A right of recourse to the Commission for persons potentially affected by secret surveillance is to be derived from Article 25 (art. 25), since otherwise Article 8 (art. 8) runs the risk of being nullified.“* Pozn.: Přeloženo autorem.

ostatně také informovanost je nezbytným předpokladem pro uplatnění práv dotčené osoby, zejména možnost iniciovat soudní kontrolu. Obdobně též Ústavní soud ČR v nálezu IV. ÚS 412/04[94] upozornil, že „*izolování subjektivního práva od možnosti toto právo vykonávat je oblíbeným trikem totalitních státu, který používají při schovávání zvůle a bezpráví za formální fasádu práva*“, zdůraznil, že „*v právním státě tyto praktiky tolerovat nelze*“ a uzavřel, že „*v materiálním právním státě nelze připustit, aby práva byla pouze deklarována bez možnosti domoci se jejich účinné ochrany.*“ Nejde přitom pouze o normativní a individuální akty veřejné moci, ale také o aplikační postupy veřejné moci – ani zde nesmějí být porušována základní práva jednotlivců[95].

Přestože se ve shora diskutovaném rozhodnutí Malone v. UK jedná o rozhodnutí, které je již více než 40 let staré, jsou tyto závěry dle hodnocení autora zobecnitelné a využitelné i v dnešní době, kdy v oblasti zásahů do práva na ochranu soukromí došlo pochopitelně k výrazným posunům technického charakteru a v důsledku toho, spolu s dalšími faktory, též ke značnému nárůstu šíře těchto zásahů. Přesto však podstata zásahů, stejně jako dostupné kontrolní mechanismy, které osvědčily svou efektivitu, dle hodnocení autora i nadále neztratily na své relevanci. ESLP takto zdůraznil, že „*Soud se musí ujistit, že bez ohledu na použitý systém sledování existují odpovídající a účinné záruky proti zneužití.*“[96]. Ke konkrétním takovýmto zárukám pak ESLP v rozsudku Klass a další proti Německu[97] zmiňuje závěry Komise G 10[98], dle kterých „*Sledování může být nařízeno pouze na základě písemné žádosti s uvedením důvodů, přičemž takovou žádost může podat pouze vedoucí některých útvarů nebo jeho zástupce; rozhodnutí o ní musí přijmout spolkový ministr, kterého k tomu zmocnil kancléř, případně, pokud je to vhodné, nejvyšší zemský úřad.*“ Německá vláda k tomuto uvedla, že „*čl. 8 odst. 2 nevyžaduje soudní kontrolu tajného sledování a že systém kontroly zavedený podle G 10 účinně chrání práva jednotlivce. Stěžovatelé naproti tomu kvalifikují tento systém jako "formu politické kontroly", která je neadekvátní ve srovnání s principem soudní kontroly, který by měl převládat.*“. ESLP v reakci na to uzavřel, že „*Soud*

[94] Nález Ústavního soudu ČR IV. ÚS sp. zn. 412/04 ze dne 7.12.2005.
[95] Viz Nález Ústavního soudu ČR IV. ÚS sp. zn. 412/04 ze dne 7.12.2005: *„V právním státě (čl. 1 Ústavy České republiky, dále jen "Ústava") platí, že jak akty veřejné moci (normativní i individuální), tak konkrétní aplikační postupy veřejné moci nesmí porušovat základní práva jednotlivců.“*
[96] V anglickém znění publikovaném ESLP: *„The Court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse.“* Pozn.: Přeloženo autorem.
[97] Rozsudek ESLP ve věci Klass a další proti Německu č. 5029/71 ze dne 6. září 1978.
[98] Jako Komise G 10 je v rozsudku označována komise ustavená zákonem o omezení listovního, poštovního a telekomunikačního tajemství ze 13. srpna 1968 (Gesetz zur Beschränkung des Brief-, Post- under Fernmeldegeheimnisses).

má za to, že v oblasti, kde zneužití v jednotlivých případech je potenciálně tak snadné a může mít tak škodlivé důsledky pro demokratickou společnost jako celek, je v zásadě žádoucí svěřit dohled soudci.“ a dodal, že „*Soud dále poznamenává, že jednotlivec, který se domnívá, že je podroben sledování, má možnost podat stížnost ke Komisi G 10 a obrátit se na Ústavní soud (viz bod 23 výše). Jak však vláda připustila, jedná se o opravné prostředky, které mohou přicházet v úvahu pouze za výjimečných okolností.*“ [99] Právě na toto omezení ESLP v rozsudku Klass a další proti Německu upozornil, když uvedl, že rozhodnutí, kterým se nad někým vykonává dohled, je nezpůsobilé soudní kontroly z podnětu dotčené osoby ve smyslu článku 6 Evropské úmluvy po dobu, dokud takové rozhodnutí zůstane dotčené osobě utajeno.

V rozhodnutí ve věci Leander v. Švédsko[100], v kauze týkající se přístupu k osobním údajům, dospěl ESLP ve vztahu ke čl. 8 Evropské úmluvy k závěru, že „*článek 8 za daných okolností nevyžadoval, aby byly panu Leanderovi sděleny informace, které o něm poskytla Národní policejní rada (viz bod 66 výše).*“ Dle hodnocení ESLP totiž platí, že „*Úmluva musí být vykládána jako celek, a proto, jak připomněla Komise[101] ve své zprávě, jakýkoli výklad článku 13 musí být v souladu s logikou Úmluvy. Soud proto v souladu se svým závěrem týkajícím se článku 8 konstatuje, že nesdělení těchto informací samo o sobě a za okolností daného případu neznamená porušení článku 13*“, přičemž ESLP v tomto bodě odkázal mutatis mutandis na výše uvedený rozsudek Klass a další proti Německu[102].

---

[99] V anglickém znění publikovaném ESLP: *„Surveillance may be ordered only on written application giving reasons, and such an application may be made only by the head, or his substitute, of certain services; the decision thereon must be taken by a Federal Minister empowered for the purpose by the Chancellor or, where appropriate, by the supreme Land authority.“. a dále „The Government maintain that Article 8 para. 2 (art. 8-2) does not require judicial control of secret surveillance and that the system of review established under the G 10 does effectively protect the rights of the individual. The applicants, on the other hand, qualify this system as a "form of political control", inadequate in comparison with the principle of judicial control which ought to prevail.“; „The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge.“; „The Court notes in addition that an individual believing himself to be under surveillance has the opportunity of complaining to the G 10 Commission and of having recourse to the Constitutional Court (see paragraph 23 above). However, as the Government conceded, these are remedies which can come into play only in exceptional circumstances.“* Pozn.: Přeloženo autorem.

[100] Rozsudek ESLP ve věci Leander v. Švédsko č. 9248/81 ze dne 26. března 1987.

[101] Pozn. autora: Evropská komise pro lidská práva (European Commission of Human Rights).

[102] V anglickém znění publikovaném ESLP: *„The Court has held that Article 8 (art. 8) did not in the circumstances require the communication to Mr. Leander of the information on him released by the National Police Board (see paragraph 66 above). The Convention is to be read as a whole and therefore, as the Commission recalled in its report, any interpretation of Article 13 (art. 13) must be in harmony with the logic of the Convention. Consequently, the Court, consistently with its conclusion concerning Article 8 (art. 8), holds that the lack of communication of this information does not, of itself and in the circumstances of the case, entail a breach of Article 13 (art. 13) (see, mutatis mutandis, the above-mentioned Klass and Others judgment, Series A no. 28, pp. 30-31, § 68).“* Pozn.: Přeloženo autorem.

K právu na účinné opravné prostředky dle čl. 13 Evropské úmluvy ve vztahu k právu na respektování soukromého a rodinného života zaručenému v čl. 8 se ESLP v tomto rozhodnutí vyjádřil jednoznačně tak, že „*Článek 13 nezaručuje opravný prostředek, který by umožňoval napadnout zákony smluvního státu jako takové u vnitrostátního orgánu z důvodu jejich rozporu s Úmluvou nebo rovnocennými vnitrostátními normami…*“[103]. K pojmu „účinný opravný prostředek“ pak ESLP uvedl, že „*Pro účely tohoto řízení musí "účinný opravný prostředek" podle článku 13 znamenat takový opravný prostředek, který je co nejúčinnější s ohledem na omezený rozsah opravných prostředků, který je vlastní jakémukoli systému tajných prověrek uchazečů o zaměstnání na pozicích důležitých z hlediska národní bezpečnosti. Zbývá tedy přezkoumat různé opravné prostředky, které měl stěžovatel k dispozici podle švédského práva, aby se zjistilo, zda byly "účinné" v tomto omezeném smyslu…*“. Dle hodnocení ESLP se však přitom nemusí nutně jednat o soudní orgán v užším smyslu slova, rozhodující pro posouzení, zda jde o prostředek účinný, jsou dle ESLP pravomoci a procesní záruky, kterými daný orgán disponuje.

S některými ze zásahů do práva na ochranu soukromí souvisí dále též čl. 10 Evropské úmluvy zaručující každému právo na svobodu projevu. Toto právo zahrnuje výslovně též „*svobodu zastávat názory a přijímat a rozšiřovat informace nebo myšlenky bez zasahování státních orgánů a bez ohledu na hranice*“. U některých ze zde dále rozebíraných zásahů do práva na ochranu soukromí, typicky zejména u povinného plošného uchovávání provozních a lokalizačních údajů v rámci povinnosti Data Retention, je relevantní posouzení otázky, zda takové zpracování údajů, přestože nezahrnuje samotný obsah komunikace, avšak řadu dalších údajů s obsahem komunikace úzce souvisejících, může mít negativní vliv na výkon práva na svobodu projevu. Na základě takovýchto úvah se irský High Court v kauze C-293/12[104], rozebírané v této práci dále, ve svých předběžných otázkách adresovaných Soudnímu dvoru EU výslovně dotazoval též na to, zda „*je směrnice 2006/24 slučitelná s právem na svobodu projevu, stanoveným v článku 11 Listiny a v článku 10 EÚLP*“.

---

[103] V anglickém znění publikovaném ESLP: *„Article 13 (art. 13) does not guarantee a remedy allowing a Contracting State's laws as such to be challenged before a national authority on the ground of being contrary to the Convention or equivalent domestic norms…“; „For the purposes of the present proceedings, an "effective remedy" under Article 13 (art. 13) must mean a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret checks on candidates for employment in posts of importance from a national security point of view. It therefore remains to examine the various remedies available to the applicant under Swedish law in order to see whether they were "effective" in this limited sense…“* Pozn.: Přeloženo autorem.

[104] Rozsudek Soudního dvora EU (velkého senátu) z 8. dubna 2014. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další. Žádosti o rozhodnutí o předběžné otázce podané High Court (Irsko) a Verfassungsgerichtshof. Spojené věci C-293/12 a C-594/12.

Dle autora lze z těchto rozsudků ESLP učinit jednoznačný závěr ve vztahu k požadavkům na existenci a zejména na efektivitu kontrolních mechanismů, především pak prostředků umožňujících dotčené osobě iniciovat přezkum zásahů do svého soukromí. Přestože ESLP jak v rozsudku Klass a další proti Německu, tak rovněž v rozsudku Leander v. Švédsko ve výroku těchto rozsudků konstatoval, že v posuzované věci nedošlo k porušení čl. 8 Evropské úmluvy ani jejího čl. 10 zaručujícího svobodu projevu a také čl. 6 a 13, zahrnul do odůvodnění svých rozhodnutí zřejmá upozornění na některé nedostatky existujících kontrolních mechanismů a dostupných nápravných opatření. Dle ESLP jsou jimi jednak nedostatečná oprávnění některých orgánů, které mohou být zapojeny do posuzování zásahů, tedy konkrétně v případě Leander proti Švédsku nedostatek oprávnění takových orgánů, vč. ombudsmana, vydat závazné rozhodnutí, a to navzdory existenci pravomoci zahájit trestní a disciplinární řízení, a především však z povahy věci omezená účinnost jakýchkoli oprávnění, která jsou dostupná dotčené osobě v systému tajných bezpečnostních kontrol[105]. Obdobný závěr o faktické nedostupnosti soudní kontroly po dobu, kdy existence zásahu není dotčené osobě známa, učinil ESLP i v rozsudku Klass a další proti Německu. ESLP naopak jako pozitivní ocenil zvláštní rys švédského systému kontroly v podobě dohledu ze strany parlamentu nad diskutovanými zásahy. V jeho rámci posuzuje každý případ, v němž je požadováno poskytnutí informací, Národní policejní rada, v níž je zastoupeno také 6 osob z řad současných či bývalých poslanců z různých politických stran. Přestože se v tomto případě nejedná o prostředek k nápravě, ESLP tento specifický kontrolní mechanismus označil za významný.

Nelze také opomenout, že ani jeden ze zde diskutovaných rozsudků nebyl přijat zcela bezvýhradně, hlasy všech soudců. V případě rozhodnutí ve věci Klass a další proti Německu připojil soudce Pinheiro Farinha separátní votum, ve kterém uvádí, že se závěry rozsudku souhlasí, avšak na základě odlišných důvodů. Argumentuje přitom pochybnostmi o uplatnění standardních pravidel dělby moci jakožto základního principu demokratické společnosti při rozhodování o použití diskutovaných opatření v konkrétním případě. Dle soudce Farinhy totiž pro použití těchto opatření je nutno posoudit, zda existují věcné náznaky spáchání trestného činu, což ovšem dle jeho hodnocení vyžaduje, aby o opatřeních rozhodoval nezávislý soudce. U rozhodnutí ve věci Leander proti Švédsku pak k rozsudku připojili

[105] V anglickém znění publikovaném ESLP *„lack the power to render a legally binding decision“, „competence to institute criminal and disciplinary proceedings“ a „the necessarily limited effectiveness that can be required of any remedy available to the individual concerned in a system of secret security checks“.*

částečně disentní stanoviska soudce Ryssdal a také soudci Pettiti a Russo, jejich odlišný názor se týkal posouzení možného porušení čl. 13 Evropské úmluvy v daném případě. Soudce Ryssdal zastával názor, že v posuzovaném případě nebyl ve švédském právním řádu dostupný účinný opravný prostředek před vnitrostátním orgánem, jak jej vyžaduje čl. 13, když ani parlamentní ombudsman ani kancléř pro spravedlnost nedisponují zákonným oprávněním vydat právně závazné rozhodnutí; pouhou tradici, v jejímž rámci ve Švédsku názory a stanoviska parlamentního ombudsmana a kancléře pro spravedlnost požívají velkou vážnost, nepovažuje Ryssdal za dostačující k naplnění požadavků diskutovaného čl. 13. Obdobný názor zastávali též soudci Pettiti a Russo, kteří ve svém disentním stanovisku zdůraznili, že dle jejich hodnocení nedostatečně účinné prostředky, které představují pouhá oprávnění ombudsmana a kancléře pro spravedlnost vydávat stanoviska, se ani ve vzájemné kombinaci nemohou rovnat účinnému prostředku vyžadovanému čl. 13 Evropské úmluvy. Stát podle nich nemůže být jediným soudcem ve vlastní věci v citlivé oblasti ochrany lidských práv. Jako příklad účinného prostředku v podobných případech zásahů do soukromí uvádějí systém dozoru ze strany nejvyšších správních soudů existující v Belgii, Francii nebo Itálii.

Z rozhodnutí ESLP ve vztahu k právu na ochranu soukromí dle Evropské úmluvy je dle hodnocení autora relevantní také rozsudek ve věci Kruslin v. Francie[106], v němž se soud zabýval odposlechem telefonních hovorů. Dospěl k závěru, že se v daném případě jednalo o porušení čl. 8 Evropské úmluvy. ESLP v tomto rozsudku posuzoval specificky podmínky, které vyžaduje čl. 8 odst. 2 a které musejí splňovat zásahy státních orgánů do výkonu práva na respektování soukromého a rodinného života. Dle ESLP v prvé řadě „*Výraz "v souladu se zákonem" ve smyslu čl. 8 odst. 2 (čl. 8-2) vyžaduje, aby napadené opatření mělo především určitý základ ve vnitrostátním právu; vztahuje se rovněž na kvalitu dotčeného práva a vyžaduje, aby bylo přístupné dotčené osobě, která navíc musí být schopna předvídat jeho důsledky pro ni, a aby bylo slučitelné s právním státem.*“[107]

Na některé ze závěrů ve věci Kruslin v. Francie navázal ESLP následně v rozhodnutí ve věci Valenzuela Contreras v. Španělsko[108], týkající se odposlechu telefonu a stanovení rozsahu a podmínek výkonu pravomoci při zásahu do práva na ochranu soukromí. Pokud jde

[106] Rozsudek ESLP ve věci Kruslin v. Francie č. 11801/85 ze dne 24. dubna 1990.
[107] V anglickém znění publikovaném ESLP: *„The expression "in accordance with the law", within the meaning of Article 8 § 2 (art. 8-2), requires firstly that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law.“* Pozn.: Přeloženo autorem.
[108] Rozsudek ESLP ve věci Valenzuela Contreras v. Španělsko č. 58/1997/842/1048 ze dne 30. července 1998.

o přípustnost odposlechu telefonické konverzace, jakožto zásahu orgánu veřejné moci do práva na respektování soukromého života a korespondence, ESLP v tomto rozsudku potvrdil, že takovýto zásah bude v rozporu s čl. 8 odst. 2 Evropské úmluvy, ledaže bude „*"v souladu se zákonem", sleduje jeden nebo více legitimních cílů podle odstavce 2 a navíc je "nezbytný v demokratické společnosti" k dosažení těchto cílů*“. Odkázal přitom na rozsudek Kopp v. Švýcarsko[109], který se také týkal zásahu do práva na ochranu soukromí v podobě odposlechu telefonních hovorů. ESLP zde, obdobně jako v rozsudku ve věci Kruslin v. Francie, konstatoval, že „*slova "v souladu se zákonem" vyžadují, aby napadené opatření mělo určitý základ ve vnitrostátním právu“*, přičemž však tento výraz *„neodkazuje pouze zpět na vnitrostátní právo, ale vztahuje se také na kvalitu práva a vyžaduje, aby bylo v souladu s právním státem. Z tohoto výrazu tedy vyplývá, že ve vnitrostátním právu musí existovat určitá míra ochrany proti svévolným zásahům orgánů veřejné moci do práv chráněných odstavcem 1“*, tedy právo na respektování svého soukromého a rodinného života, obydlí a korespondence. Z tohoto požadavku pak dle ESLP, v souladu se závěry rozsudku ve věci Kruslin v. Francie i Kopp v. Švýcarsko, vyplývá potřeba přístupnosti práva dotčené osobě, zahrnující i předvídatelnost důsledků, a to tím spíše, že „*Zejména tam, kde je výkonná moc vykonávána tajně, je riziko svévole zřejmé.“*. ESLP proto v tomto rozsudku vymezil požadavek předvídatelnosti „*v souvislosti s tajnými opatřeními sledování nebo odposlechu ze strany orgánů veřejné moci“* tak, že „*vnitrostátní právo musí být dostatečně jasné, aby občanům dostatečně naznačilo okolnosti a podmínky, za nichž jsou orgány veřejné moci oprávněny přijmout jakákoli taková tajná opatření“*. Velmi relevantní je dle hodnocení autora to, že ESLP zde výslovně upozornil na nezbytnost jasných a podrobných pravidel v této oblasti, *„zejména vzhledem k tomu, že technologie, které jsou k dispozici, se neustále zdokonalují*"[110].

---

[109] Rozsudek ESLP ve věci Kopp v. Švýcarsko č. 23224/94 ze dne 25. března 1998.

[110] V anglickém znění publikovaném ESLP: *„The words “in accordance with the law” require firstly that the impugned measure should have some basis in domestic law. However, that expression does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law. The expression thus implies that there must be a measure of protection in domestic law against arbitrary interference by public authorities with the rights safeguarded by paragraph 1 (see the Malone judgment cited above, p. 32, § 67). From that requirement stems the need for the law to be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him (see the Kruslin judgment cited above p. 20, § 27, and the Kopp judgment cited above, p. 540, § 55).“; „Especially where a power of the executive is exercised in secret the risks of arbitrariness are evident. In the context of secret measures of surveillance or interception by public authorities, the requirement of foreseeability implies that the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to take any such secret measures… It is essential to have clear, detailed rules on the subject, especially as the technology available for use is constantly becoming more sophisticated…“; „The Kruslin and Huvig judgments mention the following minimum safeguards that should be set out in the statute in order to avoid abuses of power: a definition of the categories of people liable to have their telephones tapped by judicial order,*

Především zde však ESLP, konzistentně a s výslovným odkazem na své předchozí rozsudky[111], potvrzuje následující minimální záruky, které „*by měly být stanoveny v zákoně, aby se zabránilo zneužití pravomoci: vymezení kategorií osob, jejichž telefony mohou být na základě soudního příkazu odposlouchávány, povaha trestných činů, které mohou být důvodem k vydání takového příkazu, omezení doby trvání odposlechu telefonu, postup při vypracovávání souhrnných protokolů obsahujících odposlouchávané hovory, opatření, která je třeba přijmout, aby byly nahrávky předány neporušené a v úplnosti k případné kontrole soudci a obhajobě, a okolnosti, za kterých mohou nebo musí být nahrávky vymazány nebo pásky zničeny, zejména pokud byl obviněný vyšetřujícím soudcem propuštěn nebo soudem zproštěn obžaloby*“.

ESLP tyto závěry a požadavky na kvalitativní rysy právní úpravy, která je základem zásahů do soukromí, i požadavky na záruky bránící jejich zneužití vymezil v rozhodnutích týkajících se odposlechů a dalších zásahů do telekomunikačního tajemství, jakož i obecnějšího přístupu k osobním údajům, tedy ve vztahu k zásahům do práva na ochranu soukromí. Autor zastává názor, že tyto závěry lze obdobně vztáhnout i na další případy zásahů do práva na ochranu soukromí popisované v této práci. Z tohoto důvodu autor v dalších kapitolách zabývajících se jednotlivými případy těchto zásahů aplikuje výše uvedené požadavky a podrobí právní úpravy definující každý z takových zásahů analýze se zaměřením na otázku naplnění výše uvedených požadavků vymezených ze strany ESLP. V případech, kdy tyto požadavky dle hodnocení autora naplněny nebudou, prověří autor, zda v konkrétních případech těchto zásahů existuje zvláštní důvod – odlišnost od případů posuzovaných zde ESLP, pro který není nutno trvat na naplnění některého z těchto požadavků ve stejné míře, jako je tomu ve zde rozebíraných případech, a to ať již důvod spočívající v okolnostech faktických či právních. Jedním z významných faktorů je dle autora také posouzení, zda konkrétní, dále popisované případy zásahů do soukromí lze považovat za „tajná opatření“, ve významu, který jim v citovaných rozhodnutích přikládá ESLP, tedy za případy, v nichž je výkonná moc vykonávána tajně, bez vědomí dotčené osoby o probíhajícím zásahu.

---

the nature of the offences which may give rise to such an order, a limit on the duration of telephone tapping, the procedure for drawing up the summary reports containing intercepted conversations, the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge and by the defence and the circumstances in which recordings may or must be erased or the tapes destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court...“ Pozn.: Přeloženo autorem.

[111] ESLP zde uvádí konkrétně rozsudky ve věci Kruslin v. Francie a Huvig v. Francie č. 11105/84 ze dne 24. dubna 1990.

Specificky vymezení práva na ochranu soukromí ve vztahu k organizovanému shromažďování údajů se věnuje rozhodnutí Spolkového ústavního soudu Německa BVerfGE 65, 1 ve věci sčítání lidu, rozhodnutí je známé jako Volkszählungsurteil[112]. Na toto rozhodnutí, které je v oblasti ochrany soukromí a ochrany osobních údajů jedním ze základních, ve své rozhodovací praxi navazují ústavní soudy řady dalších států, Ústavní soud ČR nevyjímaje. Ten se na toto rozhodnutí německého Spolkového ústavního soudu odvolával mj. ve svém, již výše zmiňovaném, nálezu Pl. ÚS 24/10[113], který se významně zabýval plošným sběrem údajů, a to provozních a lokalizačních údajů účastníků a uživatelů elektronických komunikací. Ústavní soud ČR v tomto nálezu v případě práva na informační sebeurčení odkazuje právě na zmiňované rozhodnutí, v němž „*německý Spolkový ústavní soud při posouzení ústavnosti zákonné úpravy procesu sběru a uchovávání dat za účelem sčítání lidu (Volkszählung) mimo jiné konstatoval, že v moderní společnosti, charakterizované i obrovským nárůstem informací a dat, musí být ochrana jednotlivce před neomezeným sběrem, uchováváním, užitím a zveřejňováním dat o její/jeho osobě a soukromí poskytována v rámci obecnějšího, ústavně garantovaného práva jednotlivce na soukromí*“.

Přestože se toto rozhodnutí týká právního a především faktického stavu starého z dnešního pohledu již 40 let, rozhodnutí obsahuje dle hodnocení autora několik závěrů, které lze i s takto značným časovým odstupem označit za velmi relevantní, a to i ve světle aktuálního stavu techniky, který se od toho, který bylo možno byť i jen předvídat v 80. letech 20. století, odlišuje zcela zásadně. Ostatně, z tohoto důvodu Ústavní soud ČR v odůvodnění svého nálezu Pl. ÚS 24/10 odkazoval právě na toto rozhodnutí Spolkového ústavního soudu Německa. Z dnešního pohledu je, vedle konstatování o tom, že „*v podmínkách vševědoucího a všudypřítomného státu a veřejné moci se svoboda projevu, právo na soukromí a právo svobodné volby chování a konání stávají prakticky neexistujícími a iluzorními*“, dle hodnocení autora zásadním především následující varování, v současné době patrně ještě mnohem urgentnější nežli v době svého vyslovení. Spolkový ústavní soud Německa v něm dovodil velmi dalekosáhlé důsledky porušení práva na informační sebeurčení, když uvedl, že „*Pokud jednotlivci nebude garantována možnost hlídat a kontrolovat obsah i rozsah osobních dat a informací jím poskytnutých, jež mají být zveřejněny, uchovány či použity k jiným než původním účelům, nebude-li mít možnost rozpoznat a zhodnotit důvěryhodnost svého potenciálního komunikačního partnera a případně tomu uzpůsobit i své jednání, pak nutně dochází k omezení*

[112] Rozhodnutí Spolkového ústavního soudu Německa ze dne 15. 12. 1983, BVerfGE 65, 1 (Volkszählungsurteil).
[113] Nález Ústavního soudu ČR Pl. ÚS 24/10 ze dne 22. března 2011.

až potlačování jeho práv a svobod, a nelze tak již nadále hovořit o svobodné a demokratické společnosti.“ Na základě toho pak Spolkový ústavní soud Německa formuloval závěr, dle kterého „*Právo na informační sebeurčení (informationelle Selbstbestimmung) je tak nezbytnou podmínkou nejen pro svobodný rozvoj a seberealizaci jednotlivce ve společnosti, nýbrž i pro ustavení svobodného a demokratického komunikačního řádu*“[114].

V souvislosti s vývojem techniky umožňujícím v současnosti zásahy do soukromé sféry zcela nového typu, dosud právní úpravou ani rozhodovací praxí neřešené, autor považuje za relevantní mj. též úvahu Vladimíra Smejkala na téma přípustnosti aktivního zasahování do počítače jiné osoby ze strany Policie ČR, resp. obecněji orgánů činných v trestním řízení, a to případně i na základě souhlasu soudu. Smejkal upozorňuje, že *„zákon zřejmě s takovou možností nepočítal“* a uzavírá, že patrně soudy budou muset zhodnotit *„soulad takto extenzivního výkladu ustanovení § 158d TŘ s Ústavou či Evropskou úmluvou“*[115]. Smejkal však ke svému hodnocení připojuje upozornění na nezbytnou podmínku, pro možný přezkum zásahu soudem, která nemusí být v praxi vždy naplněna, totiž vědomí, byť i následné, dotčené osoby o takovémto zásahu. Ve shodě s tím autor jako jeden z kontrolních mechanismů v závěru práce rozebírá právě povinnou, zákonem uloženou informovanost dotčené osoby o zásahu do jejího soukromí.

Ve vztahu k Evropské úmluvě lze uzavřít, že vedle jejích výše rozebíraných článků s hlavním významem pro oblast ochrany soukromí, tedy čl. 8 zaručujícího právo na respektování soukromého a rodinného života, obydlí a korespondence, čl. 13 obsahujícího právo na účinné opravné prostředky a čl. 6 vymezujícího právo na spravedlivý proces, jsou pro posuzovanou problematiku dle hodnocení autora relevantní též další články této úmluvy, obsahující mj. garance svobody myšlení, svědomí a náboženského vyznání či svobody projevu. Autor přesto čl. 8, s ohledem na jeho význam ve vztahu k případům zkoumaným v této práci považuje pro další rozbor těchto případů za nejzásadnější.

[114] Viz nález Ústavního soudu ČR Pl. ÚS 24/10 ze dne 22. března 2011.
[115] SMEJKAL, Vladimír. *Kybernetická kriminalita. 3. vyd.* Plzeň: Aleš Čeněk, 2022. s. 683. Vladimír Smejkal tuto problematiku v dané publikaci rozebírá v souvislosti s případem modifikace počítačového zařízení, ke které došlo technicky nestandardním způsobem. Odkazuje v této věci mj. na nález Ústavního soudu ČR sp. zn. III.ÚS 3812/12 ze dne 3. října 2013 ke sledování dat uložených v počítačích v rámci institutu sledování osob a věcí pro účely trestního řízení.

2.2.6 Ochrana osobních údajů v relevantní právní úpravě

Zásahy, které autor v této práci zkoumá, spočívají v plošném shromažďování osobních údajů. Autor proto považuje za potřebné zabývat se na tomto místě vymezením ochrany osobních údajů v právní úpravě, specificky ve vztahu ke zkoumané problematice.

Oblast zpracování osobních údajů pokrývá v prvé řadě Úmluva o ochraně osob se zřetelem na automatizované zpracování dat[116], která vymezuje především základní zásady pro ochranu údajů a uplatňuje se na automatizované zpracování osobních údajů ve veřejném i v soukromém sektoru. Úmluva byla přijata v roce 1981 Radou Evropy, jako první právně závazný dokument „*s mezinárodním rozměrem v oblasti ochrany osobních údajů*“[117], v České republice je tato úmluva v platnosti od 1. 11. 2001. Úmluva, označovaná zástupci odborné veřejnosti často též jako Úmluva 108 (Treaty 108), byla kromě členských států Rady Evropy ratifikována také některými dalšími zeměmi, jako např. Argentina, Mexiko, Maroko a další. Význam této úmluvy spočívá mj. v tom, že v ní byla poprvé uznána ochrana osobních údajů jakožto samostatné právo. Jak konstatuje pracovní skupina WP 29 ve Stanovisku 1/2014 k uplatňování pojmů nezbytnosti a proporcionality a ochrany údajů v oblasti vymáhání práva[118], tato úmluva se také posléze stala „*důležitým zdrojem inspirace i pro směrnici 95/46/ES*“.

Směrnice 95/46/ES byla po dlouhou dobu předchůdcem aktuálního Obecného nařízení GDPR, v důsledku toho vycházel z hlavních prvků Úmluvy 108 též zákon č. 101/2000 Sb. o ochraně osobních údajů[119]. Dle WP 29 také právě v důsledku tohoto vývoje se právo na ochranu osobních údajů vyvinulo jakožto samostatné právo v Listině základních práv Evropské unie[120]. Význam Úmluvy 108 dokládá i skutečnost, že taktéž ESLP na ni ve své rozhodovací praxi výslovně odkazuje a vyvozuje z ní požadavky ve vztahu k národním právním řádům[121].

---

[116] Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat, vyhlášena jako Sdělení ministerstva zahraničních věcí č. 115/2001 Sb. m. s., ve znění pozdějších dodatkových protokolů. Anglické znění označení této úmluvy „Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data“ bylo přeloženo do českého jazyka při použití termínu „osobní data“, nikoli „osobní údaje“, aniž by pro to existoval zásadní důvod.

[117] Úřad pro ochranu osobních údajů. Rada Evropy. [online] [cit. 18.3.2024]. Dostupné z www.uoou.gov.cz.

[118] Pracovní skupina WP 29. Stanovisko 1/2014 k uplatňování pojmů nezbytnosti a proporcionality a ochrany údajů v oblasti vymáhání práva, přijato 27. února 2014. [online] [cit. 24.2.2024]. Dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation.

[119] Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, v § 1 odkazuje mimo jiné i na mezinárodní smlouvy, kterými je Česká republika vázána, mezi ně patřila také Úmluva o ochraně osob se zřetelem na automatizované zpracování dat.

[120] Pracovní skupina WP 29. *Stanovisko 1/2014.* [online] [cit. 24.2.2024]. Dostupné z www.uoou.gov.cz.

[121] Viz např. Rozsudek ESLP ve věci Z. proti Finsku, č. 22009/93, rozsudek ze dne 25. února 1997, bod 95, na tento rozsudek i na Úmluvu o ochraně osob se zřetelem na automatizované zpracování dat výslovně odkazuje i Rozsudek ESLP ve věci Peck proti Velké Británii, č. 44647/98, rozsudek ze dne 28. ledna 2003, bod 78.

Smlouva o fungování Evropské unie

Ochrana osobních údajů představuje specifickou oblast nejen v oblasti mezinárodních úmluv, ale i na úrovni EU a právních řádů členských států EU. Právo každého na ochranu osobních údajů, které se jej týkají, je obsaženo v čl. 16 Smlouvy o fungování Evropské unie. Dle odst. 2 tohoto článku mají Evropský parlament a Rada přijmout „*pravidla o ochraně fyzických osob při zpracovávání osobních údajů orgány, institucemi a jinými subjekty Unie a členskými státy, pokud vykonávají činnosti spadající do oblasti působnosti práva Unie, a pravidla o volném pohybu těchto údajů*“, přičemž „*Dodržování těchto pravidel podléhá kontrole nezávislými orgány*“.

Listina základních práv Evropské unie

V rámci evropského práva je základním dokumentem obsahujícím záruky práva na ochranu soukromí Listina základních práv Evropské unie („Listina EU“). Ta obsahuje v čl. 7 právo každého na respektování svého soukromého a rodinného života, obydlí a komunikace. Významná je zejména explicitně zmíněná komunikace podléhající ochraně, jelikož některé ze zásahů do soukromí rozebíraných v této práci se týkají právě komunikace, vč. plošného uchovávání údajů považovaných za součást komunikace, za účelem jejich možného vyžádání a využití oprávněnými orgány.

Čl. 8 Listiny EU se týká specificky pouze ochrany osobních údajů, zaručuje každému právo na ochranu takových osobních údajů, které se ho týkají. Přestože by bylo možno uvažovat o možném dovození ochrany osobních údajů již z ochrany soukromí v širším smyslu dle předchozího čl. 7, osobní údaje podléhají v Listině EU zvláštní ochraně specifikované v samostatném ustanovení čl. 8. Jak upozorňuje stanovisko WP 29 1/2014 zmiňované výše, je zařazení samostatného ustanovení k ochraně osobních údajů důsledkem vlivu Úmluvy 108. Ustanovení čl. 8 je komplexnější, kromě samotné ochrany osobních údajů dle odst. 1 stanoví v odst. 2 též některé ze základních zásad ochrany osobních údajů, konkrétně povinnost zpracovávat tyto údaje „*korektně, k přesně stanoveným účelům“,* zakotvuje též povinnost založit zpracování na *„souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem*“. Vymezuje dále též výslovně dvě základní práva subjektů údajů – právo každého na přístup „*k údajům, které o něm byly shromážděny*“ a na jejich opravu. V odst. 3 pak čl. 8 požaduje dohled nezávislého orgánu nad dodržováním těchto pravidel.

Obdobně jako v případě čl. 10 Evropské úmluvy zaručujícího právo na svobodu projevu, který autor zmiňuje v této práci výše, je ve vztahu k rozebíraným případům zásahů do práva na ochranu soukromí relevantní taktéž čl. 11 Listiny EU – Svoboda projevu a informací. Toto ustanovení zaručuje každému právo na svobodu projevu, které ve znění čl. 11 výslovně zahrnuje též „*svobodu zastávat názory a přijímat a rozšiřovat informace nebo myšlenky bez zasahování veřejné moci a bez ohledu na hranice*“. Taktéž již výše, v souvislosti s čl. 10 Evropské úmluvy, zmiňovaná žádost irského High Court v kauze C-293/12, se v případě práva na svobodu projevu opírala jak o čl. 10 Evropské úmluvy, tak rovněž o čl. 11 Listiny EU. Jedna z předběžných otázek, které formuloval Irský High Court ve své žádosti předložené SDEU, se týkala také čl. 41 Listiny EU, konkrétně toho, zda „*je směrnice 2006/24 slučitelná s právem na řádnou správu, stanoveným v článku 41 Listiny*“. SDEU se touto otázkou v daném případě nezabýval, to ovšem ryze z procesních důvodů, s ohledem na to, že ve svém rozsudku konstatoval neplatnost posuzované směrnice již z důvodů obsažených v posouzení předchozích předběžných otázek.

Aplikace ustanovení Listiny EU je však do jisté míry omezena samotným jejím textem, když její čl. 51 upravující oblast použití výslovně stanoví v odst. 1, že ustanovení Listiny EU „*jsou při dodržení zásady subsidiarity určena orgánům, institucím a jiným subjektům Unie, a dále členským státům, výhradně pokud uplatňují právo Unie*“. Toto ustanovení doplňuje odstavec 2, dle kterého Listina EU „*nerozšiřuje oblast působnosti práva Unie nad rámec pravomocí Unie, ani nevytváří žádnou novou pravomoc či úkol pro Unii, ani nemění pravomoc a úkoly stanovené ve Smlouvách*“. Autoři komentáře k Listině EU dodávají, že *„LZPEU je pro členské státy závazná pouze v případech „uplatňování“ unijního práva“*, k němuž *„dochází tehdy, když daná vnitrostátní právní úprava či právní situace „spadá do působnosti unijního práva“, resp. řídí se unijním právem“*, tento závěr dokládají řadou rozsudků Soudního dvora EU[122]. Jak upozorňuje Ústavní soud ČR v nálezu Pl. ÚS 3/14 v souvislosti s právní úpravou zákona o archivnictví[123], která byla v daném případě předmětem jeho posuzování, „*Základní právo na ochranu osobních údajů podle čl. 8 Listiny EU, které je zároveň zaručeno v čl. 16 Smlouvy o fungování Evropské unie (dále jen „SFEU“) a je podle předpisů unijního práva přijatých k provedení této Smlouvy vykonáváno za podmínek a v mezích v ní stanovených (čl. 52 odst. 2 Listiny EU), je zdrojem kritérií pro*

[122] TOMÁŠEK, Michal, ŠMEJKAL, Václav a kol. *Smlouva o fungování EU. Smlouva o EU. Listina základních práv EU. Komentář.* Praha: C.H.Beck, 2022. s. 1637.
[123] Zde zákon č. 499/2004 Sb., o archivnictví a spisové službě, ve znění účinném do dne 30. 6. 2009.

(eurokonformní) výklad právních předpisů členských států v oblasti ochrany osobních údajů, jež zásadním způsobem dopadají na aplikaci vnitrostátních norem, ležících mimo přímý dosah unijního práva, jako je tomu právě v případě napadeného ustanovení zákona o archivnictví." Za takováto kritéria Ústavní soud ČR v citovaném nálezu označuje „*pravidla, vydaná na základě zmocnění čl. 16 SFEU*", tedy v současné době pravidla ochrany osobních údajů obsažená v GDPR[124].

Dalšími v souvislosti s diskutovaným tématem relevantními ustanoveními Listiny EU jsou čl. 52 upravující rozsah a výklad práv a zásad a čl. 53 Úroveň ochrany. Tato ustanovení jsou, obdobně jako v případě čl. 51, obecnější, na rozdíl od čl. 7 a 8 se nevztahují specificky k právu na ochranu soukromí, resp. na ochranu osobních údajů. Např. rakouský Verfassungsgerichtshof se v několika svých předběžných otázkách k SDEU v kauze projednávané jako C-594/12[125] výslovně opírá právě o čl. 52 a 53 Listiny EU. Dotazuje se takto zejména na aplikaci ustanovení čl. 52 odst. 3 (dle kterého platí, že „*Toto ustanovení nebrání tomu, aby právo Unie poskytovalo širší ochranu.*"), konkrétně ve vztahu ke směrnicím upravujícím ochranu osobních údajů („*V jakém vztahu se nachází ‚právo Unie' uvedené v čl. 52 odst. 3 poslední větě Listiny ke směrnicím v oblasti ochrany údajů?*") a dále též na výklad základních práv vyplývajících z ústavních tradic společných členským státům dle ustanovení čl. 52 odst. 4 a jejich vztah k úrovni ochrany dle čl. 53 („*„Má s ohledem na čl. 52 odst. 4 Listiny zásada dodržování vyšší úrovně ochrany uvedená v článku 53 Listiny za důsledek, že relevantní rozsah omezení přípustných podle Listiny musí být zúžen sekundárním právem?"*). SDEU se bohužel k těmto, jinak velmi relevantním, otázkám nevyjádřil, když dospěl k závěru, že není namístě na ně odpovídat, s ohledem na to, že již v reakci na předchozí předběžné otázky položené týmž soudem vyslovil neplatnost posuzované směrnice.

Obecné nařízení o ochraně osobních údajů – GDPR, Zákon o zpracování osobních údajů

Zajištění ochrany osobních údajů v právních řádech členských států EU je cílem právní úpravy Obecného nařízení o ochraně osobních údajů známého i v odborné literatuře

[124] Pozn. autora: Ústavní soud ČR v nálezu Pl. ÚS 3/14 v této souvislosti neuvádí primárně GDPR, nýbrž předchozí právní úpravu Směrnice 95/46/ES, dle hodnocení autora však také zde platí, že tento závěr lze obdobně vztáhnout též na GDPR. Citovaný nález Ústavního soudu ČR navíc v této souvislosti výslovně zmiňuje GDPR jako právní úpravu, která do budoucna „*spolutvoří – jako součást právního řádu České republiky – výkladový rámec pro úpravu ochrany osobních údajů*".

[125] Viz Rozsudek Soudního dvora EU (velkého senátu) z 8. dubna 2014. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další. Žádosti o rozhodnutí o předběžné otázce podané High Court (Irsko) a Verfassungsgerichtshof. Spojené věci C-293/12 a C-594/12.

pod zkratkou GDPR. V některých specifických otázkách GDPR do určité míry na národní úrovni, v právním řádu ČR, doplnil ZoZOÚ[126]. GDPR má totiž formu nařízení, v některých případech nicméně umožňuje upravit určité záležitosti na úrovni právních řádů členských států odchylně, někdy ve stanovených mezích, jindy bez striktního vymezení limitů, které musí národní právní úprava respektovat. GDPR přímo a výslovně odkazuje na čl. 8 Listiny EU, když v bodě 1 recitálu stanoví, že „*Ochrana fyzických osob v souvislosti se zpracováním osobních údajů je základním právem. Ustanovení čl. 8 odst. 1 Listiny základních práv Evropské unie (dále jen „Listina“) a čl. 16 odst. 1 Smlouvy o fungování Evropské unie (dále jen „Smlouva o fungování EU“) přiznávají každému právo na ochranu osobních údajů, které se jej týkají.*“.

V souladu s hodnocením formulovaným Ústavním soudem ČR v nálezu Pl. ÚS 3/14[127] lze říci, že Obecné nařízení GDPR konkretizuje a rozšiřuje „*zásady práva na soukromí, jež vyplývají pro členské státy*“ z Úmluvy 108. Ústavní soud ČR v tomto nálezu dokonce v případě Směrnice 95/46/ES a jejího vztahu k Listině EU dovozuje, že „*Tato Směrnice má postavení prováděcího předpisu k čl. 8 Listiny EU, ve skutečnosti ale byla jedním z jeho normativních zdrojů a lze jí proto přiznat v rámci unijního práva „ústavní“ význam, a stala se i předlohou pro přijetí zákona č. 101/2000 Sb.*[128]“. V současnosti, kdy již Směrnice 95/46/ES byla nahrazena GDPR, je dle autorova hodnocení relevantní zabývat se posouzením, zda obdobný závěr lze dovodit i ve vztahu ke GDPR. Jak totiž autor uvádí výše, GDPR Směrnici 95/46/ES zrušilo a nahradilo, je tedy otázkou, zda lze obdobný „ústavní význam“ v rámci unijního práva přiznat v kontextu uvedeném v nálezu Pl. ÚS 3/14 nejen Směrnici 95/46/ES, nýbrž v současnosti také GDPR. Jelikož argumenty, na jejichž základě Ústavní soud ČR ve výše citovaném nálezu dospěl k závěru o „ústavním“ významu Směrnice 95/46/ES, jsou platné i ve vztahu ke GDPR, lze tento závěr dle autora vztáhnout i na něj. Ostatně Ústavní soud v témže nálezu GDPR výslovně zmiňuje a konstatuje, že GDPR nahradí Směrnici 95/46/ES a *„spolutvoří – jako součást právního řádu České republiky – výkladový rámec pro úpravu ochrany osobních údajů“*. Dle autorova hodnocení je takovýto závěr plně akceptovatelný – přestože je zřejmé, že u GDPR neplatí (výhradně z důvodů časových), že by

[126] Zákon č. 110/2019 Sb. o zpracování osobních údajů.
[127] Pozn. autora: Ústavní soud ČR toto hodnocení vztáhl nikoli k GDPR, nýbrž k předchozí právní úpravě Směrnice 95/46/ES, když GDPR tuto směrnici zrušilo až s účinností od 25. 5. 2018, zmiňovaný nález Ústavního soudu ČR je přitom datován už 20. prosince 2016. Dle hodnocení autora však závěry formulované Ústavním soudem ČR platí obdobně i ve vztahu k GDPR.
[128] Pozn. autora: Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů byl s účinností od 24. dubna 2019 zrušen ZoZOÚ.

toto nařízení bylo jedním z normativních zdrojů čl. 8 Listiny EU, je však nutno vzít v úvahu, že GDPR obsahově plně navazuje na Směrnici 95/46/ES a tuto směrnici v mnoha směrech rozvíjí[129][130], v návaznosti na faktický, zejména technologický vývoj. Z těchto důvodů je dle autora nutno přiznat GDPR v rámci unijního práva obdobné postavení, jaké měla dle závěrů Ústavního soudu ČR tato směrnice. Na tomto autorově závěru nemění nic ani odlišnosti mezi oběma předpisy, kterých si autor je vědom. Nejzásadnější odlišností je, že v případě GDPR neplatí navazující závěr Ústavního soudu ČR obsažený v rozebíraném nálezu, tedy závěr, dle kterého podle Směrnice 95/46/ES „*mají členské státy značnou diskreci při stanovení podmínek, za kterých je zpracování osobních údajů zákonné*“. GDPR, které má právní formu nařízení, takovýto prostor pro diskreci členských států v dané oblasti ve srovnatelném rozsahu neposkytuje, byť v některých oblastech, v GDPR výslovně uvedených, umožňuje i GDPR národnímu zákonodárci určitou diskreci[131]. Tento rys obecně nebývá pro formu nařízení zcela typický, proto se někdy v souvislosti s GDPR hovoří o smíšené formě na pomezí nařízení a směrnice či o nařízení, které však „*neobsahuje skutečně jednotnou právní úpravu v EU*“ a *„není plně aplikovatelné bez dalšího, ale vyžaduje vnitrostátní konkretizaci či adaptaci vnitrostátních právních předpisů“*, jak dovozuje Magdaléna Svobodová[132].

GDPR, jakožto nařízení, je v souladu s článkem 288 Smlouvy o fungování Evropské unie přímo použitelné, s ohledem na výše uvedené důvody však bylo nutno implementovat GDPR do právního řádu ČR a zajistit adaptaci na toto nařízení a také soulad vnitrostátní právní úpravy ČR s tímto předpisem. Vedle toho též z Trestněprávní směrnice vyplývala nutnost přijetí právního předpisu, který v právním řádu ČR zajistí soulad s touto směrnicí. Z těchto důvodů byl přijat ZoZOÚ. Z hlediska tématu této práce autor nepovažuje za nutné věnovat se

---

[129] K tomuto viz např. ÚOOÚ v textu Desatero omylů, v němž zpracoval dle hodnocení ÚOOÚ přehled nejčastějších omylů či zavádějících tvrzení o Obecném nařízení GDPR: *„…jedním ze základních znaků ochrany osobních údajů podle obecného nařízení je kontinuita - nařízení navazuje ve sledovaných cílech a obsahových zásadách zpracování a ochrany osobních údajů na směrnici 95/46/ES“*, *„Z jednoduchého porovnání obsahu obecného nařízení a směrnice 95/46/ES je zřejmé, že jsou používány stejné definice klíčových pojmů (osobní údaj, subjekt údajů, zpracování - čl. 2 směrnice 95/46/ES a čl. 4 obecného nařízení) a obdobně formulované, obsahově velmi blízké, zásady zpracování“*. Úřad pro ochranu osobních údajů. *Desatero omylů. N*edatováno. [online] [cit. 18.3.2024]. Dostupné z www.uoou.gov.cz.

[130] K tomuto srov. také EHMANN, Eugen, SELMAYR, Martin. *Datenschutz-Grundverordnung: DS-GVO. 3. Auflage*. München: C.H.BECK Verlag, 2024.

[131] Jak rovněž zhodnotil ÚOOÚ ve stanoviscích poskytnutých v rozebírané věci Ústavnímu soudu ČR, tato hodnocení ve vztahu ke GDPR Ústavní soud ČR v odůvodnění nálezu též zmiňuje.

[132] Magdaléna Svobodová označuje GDPR za příklad „kulhajícího nařízení“, z německého „hinkende Verordnung“, kterýžto pojem použil L.-J. Constantinesco v publikaci CONSTANTINESCO, L.-J. *Das Recht der Europäischen Gemeinschaften*. Baden-Baden: Nomos, 1977. Viz SVOBODOVÁ, Magdaléna. *Nahrazování směrnic nařízeními v právu Evropské unie. Habilitační přednáška.* Právník 5/2022. s. 469 a násl.

na tomto místě v obecné rovině více ZoZOÚ. Tento předpis má význam především pro některé další rozbory obsažené v této práci, jak rozvedeno dále.

Trestněprávní směrnice

Ochrana osobních údajů vymezená v GDPR, spolu se ZoZOÚ, je úpravou obecnou, vztahující se jak na zpracování osobních údajů v soukromoprávních, tak rovněž ve veřejnoprávních vztazích. Tato úprava se ovšem uplatní pouze na některá zpracování prováděná orgány veřejné moci rozebíraná v této práci. Ve vymezení věcné působnosti GDPR jsou vyloučena mimo jiné zpracování osobních údajů prováděná členskými státy při výkonu činností spadajících do oblasti společné zahraniční a bezpečnostní politiky a zejména zpracování prováděná v souvislosti s prevencí, vyšetřováním, odhalováním či stíháním trestných činů, ale také v souvislosti s ochranou před hrozbami pro veřejnou bezpečnost a jejich předcházení – tyto oblasti upravuje zvláštní právní předpis, kterým je Trestněprávní směrnice. Tato směrnice se dle vymezení obsaženého v jejím čl. 1 zaměřuje na zpracování prováděná „*příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení",* jejím předmětem je přitom jak dle celého, nezkráceného názvu směrnice, tak rovněž dle předmětu a cíle vymezeného v jejím čl. 1, stanovení pravidel ochrany fyzických osob v souvislosti se zpracováním osobních údajů pro shora vymezené účely. Trestněprávní směrnice, obdobně jako GDPR, vymezuje základní zásady zpracování osobních údajů a obsahuje i další obdobné instituty, včetně úpravy práv subjektů údajů, informací poskytovaných subjektům údajů, povinností při zabezpečení zpracovávaných údajů apod., to vše samozřejmě v podobě odpovídající zpracováním, která jsou předmětem směrnice.

Základní odlišnost Trestněprávní směrnice od GDPR spočívá ve vymezení působnosti obou předpisů. Zatímco GDPR se vztahuje obecně na zpracování osobních údajů s několika výjimkami, mezi které patří zpracování *„příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení"* [133], Trestněprávní směrnice se vztahuje právě na zpracování osobních údajů příslušnými orgány pro účely dle uvedené výjimky. Aby se na zpracování osobních údajů aplikovala výjimka formulovaná

[133] Výjimky z věcné působnosti GDPR stanoví čl. 2 odst. 2 GDPR, dle dalších výjimek se toto nařízení nevztahuje také na zpracování osobních údajů prováděné při výkonu činností nespadajících do oblasti působnosti práva Unie, zpracování prováděné členskými státy při výkonu činností v rámci společné zahraniční a bezpečnostní politice a zpracování fyzickou osobou v průběhu výlučně osobních či domácích činností.

v GDPR, musejí být kumulativně naplněny obě podmínky – zpracování musí být prováděno pro vymezené účely a rovněž příslušnými orgány. V praxi bývá v některých případech rozhraničení obtížné, příkladem může být zpracování údajů jmenné evidence cestujících (PNR), kdy zpracování těchto údajů prováděné útvarem pro informace o cestujících spadá do působnosti Trestněprávní směrnice, zatímco zpracování údajů PNR prováděné leteckými dopravci, včetně jejich shromažďování a předávání útvaru pro informace o cestujících spadá do působnosti GDPR. Jak odůvodnil SDEU[134], letečtí dopravci, *„i když mají zákonnou povinnost předávat údaje PNR“*, nejsou pověřeni *„výkonem veřejné moci ani jim nejsou svěřeny výsady veřejné moci“* a nelze je tak považovat za „příslušné orgány“[135].

Trestněprávní směrnice byla do právního řádu ČR zapracována ZoZOÚ, zmiňovaným již výše v souvislosti s úpravou některých specifických otázek doplňujících úpravu GDPR. V této souvislosti je nutno zmínit také tzv. „změnový zákon“[136], který byl přijat společně se ZoZOÚ a který v této souvislosti novelizoval řadu existujících právních předpisů. Kromě změn provedených v těchto předpisech v souvislosti s požadavky GDPR a Trestněprávní směrnice tento zákon taktéž do právního řádu ČR provedl již výše zmiňovanou PNR směrnici[137] a vložil povinnosti z ní vyplývající do zákona o civilním letectví[138].

GDPR i Trestněprávní směrnice a obdobně též výše uvedený ZoZOÚ vymezují jako základní předmět právní úpravy, tedy i jako základní předmět ochrany, obecně osobní údaje[139]. Tyto právní předpisy rozlišují v rámci osobních údajů pouze obecné osobní údaje, tzv. zvláštní kategorie osobních údajů a též osobní údaje týkající se rozsudků v trestních věcech a trestných činů či souvisejících bezpečnostních opatření. Pro tyto dvě kategorie osobních údajů stanoví jak GDPR, tak Trestněprávní směrnice specifická, přísnější kritéria ochrany a tedy striktní podmínky jejich zpracování. GDPR definuje zvláštní kategorie osobních údajů jejich taxativním výčtem, současně, jako výraz jejich přísnější ochrany, zakazuje zpracování těchto kategorií osobních údajů, s výjimkami výslovně uvedenými. Taktéž Trestněprávní směrnice vymezuje zvláštní kategorie osobních údajů a pro jejich zpracování stanoví přísnější podmínky v porovnání s ostatními osobními údaji. Předchozí právní úprava Směrnice 95/46/ES

[134] Viz Rozsudek Soudního dvora (velkého senátu) ze 21. června 2022 ve věci C-817/19.
[135] Příslušné orgány vymezuje Trestněprávní směrnice v čl. 3 bodě 7.
[136] Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.
[137] Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti.
[138] Zákon č. 49/1997 Sb. o civilním letectví, ve znění pozdějších předpisů.
[139] Vymezení osobních údajů viz čl. 4 bod 1 GDPR, resp. čl. 3 bod 1 Trestněprávní směrnice.

obdobným způsobem až na výjimky zakazovala zpracování zvláštních kategorií osobních údajů; v právním řádu ČR, v zákoně č. 101/2000 Sb. o ochraně osobních údajů, použil zákonodárce pro tyto údaje termín „citlivé údaje“, jejich vymezení bylo obdobné[140].

Je zřejmé, že český i evropský zákonodárce byli vedeni snahou poskytnout některým kategoriím osobních údajů zvýšenou úroveň ochrany a umožnit jejich zpracování pouze za přísnějších podmínek. Vymezení kategorií osobních údajů podléhajících takovéto zvýšené úrovni ochrany je v právních předpisech ochrany osobních údajů poměrně konstantní, nedochází tedy ke změnám či nahrazování kategorií osobních údajů zahrnutých do takto zvýšené úrovně ochrany, pouze v důsledku technologického vývoje je jejich rozsah postupně rozšiřován o nově doplňované kategorie osobních údajů, u kterých předchozí právní úprava zvýšenou ochranu výslovně nestanovila. K doplnění dochází zpravidla z důvodu narůstajícího zpracování určitých kategorií údajů, u kterých z tohoto důvodu zákonodárce dospěje k potřebě zvýšené úrovně ochrany. Tak tomu bylo i v případě doplnění údajů genetických a údajů biometrických, s dodatkem jedinečné identifikace fyzické osoby.

Z hlediska zaměření této práce považuje autor za zásadní skutečnost, že zvýšená úroveň ochrany je u těchto kategorií osobních údajů spojena se zvýšenou mírou zásahu do práva na ochranu soukromí v případě zpracování takto vymezených údajů, přinejmenším dle hodnocení evropského zákonodárce. Bod 51 recitálu ke GDPR tak uvádí výslovně ve vztahu ke zvláštním kategoriím osobních údajů, že *„Osobní údaje, které jsou svou povahou obzvláště citlivé z hlediska základních práv a svobod, zasluhují zvláštní ochranu, jelikož by při jejich zpracování mohla vzniknout závažná rizika pro základní práv a svobody“*. Obdobně též bod 53 recitálu hovoří o zvláštních kategoriích osobních údajů jako o takových, které *„zasluhují*

[140] Dle čl. 9 GDPR jsou zvláštními kategoriemi osobních údajů osobní údaje, *„které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech“, a dále genetické údaje, biometrické údaje zpracovávané „za účelem jedinečné identifikace fyzické osoby“ a údaje o zdravotním stavu či o „sexuálním životě nebo sexuální orientaci fyzické osoby“*; podmínky zpracování *„osobních údajů týkajících se rozsudků v trestních věcech a trestných činů či souvisejících bezpečnostních opatření“* upravuje čl. 10 GDPR. Trestněprávní směrnice v čl. 10 definuje zvláštní kategorie osobních údajů jako osobní údaje, *„které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filosofickém přesvědčení nebo členství v odborech“*, a genetické údaje, biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu nebo údaje o sexuálním životě či sexuální orientaci fyzické osoby. Čl. 8 odst. 1 Směrnice 95/46/ES zvláštní kategorie údajů vymezoval jako takové údaje, *„které odhalují rasový či etnický původ, politické názory, náboženské nebo filozofické přesvědčení, odborovou příslušnost“* a údaje týkající se zdraví a sexuálního života. V zákoně č. 101/2000 Sb. o ochraně osobních údajů, v § 4 písm. b) byl „citlivý údaj“ (ve znění po úpravách provedených dalšími předpisy) vymezen jako osobní údaj *„vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů“* a doplnil, že *„citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů“*.

vyšší stupeň ochrany“ a specificky ve vztahu k některým ze zvláštních kategorií údajů, zde ke genetickým a biometrickým údajům a údajům o zdravotním stavu, pak zdůrazňuje potřebu zvláště chránit základní práva subjektů údajů[141][142].

2.2.7 Ochrana provozních a lokalizačních údajů v právní úpravě a rozhodovací praxi

Vedle obecné právní úpravy ochrany osobních údajů obsažené primárně v GDPR se některé z případů plošného shromažďování a dalšího zpracování osobních údajů rozebíraných v této práci týkají též údajů podléhajících navíc zvláštním právním institutům, jakými jsou telekomunikační tajemství, resp. důvěrnost komunikace či ochrana specifikovaná v jednotlivých zvláštních právních předpisech, jako např. lékařské tajemství upravené v zákoně o zdravotních službách[143]. Autor se na tomto místě zaměří specificky na provozní a lokalizační údaje, jelikož tyto kategorie údajů považuje z hlediska možného zásahu do práva na ochranu soukromí při zpracování těchto údajů za zvláště významné, jak rozebráno dále.

Důvodem tohoto zvláštního významu je především zvýšená míra zásahu do soukromí, která je spojena s jejich zpracováním, a to již ve stadiu shromažďování těchto údajů, jakož i s možností následného využití takto shromážděných údajů. Tato zvýšená míra zásahu se dle hodnocení autora vztahuje k oběma kategoriím údajů – k údajům provozním i k údajům lokalizačním, v případech, kdy jde o údaje týkající se konkrétních fyzických osob, tedy o osobní údaje. Lokalizační údaje, jak jsou upraveny platnou právní úpravou, ve většině případů tuto podmínku budou splňovat, neplatí to však zcela bezvýhradně. V případě plošného shromažďování provozních a lokalizačních údajů značného množství fyzických osob, jako je tomu u dále rozebrané povinnosti Data Retention, která se týká podstatné části obyvatel ČR, resp. podstatné části obyvatel členských států EU, pak narůstá nejen intenzita zásahu takového plošného zpracování. Současně též v rámci využití těchto údajů přichází reálně do úvahy možnost vzájemného spojování a kombinování provozních a lokalizačních údajů jednotlivých fyzických osob.

---

[141] Viz bod 53 recitálu ke GDPR: *„Právo Unie nebo členského státu by mělo stanovit zvláštní a vhodná opatření s cílem chránit základní práva a osobní údaje fyzických osob“*.

[142] K ochraně biometrických údajů a k omezením v této souvislosti viz též KRAUSOVÁ, Alžběta. *Zásada autonomie vůle v ochraně soukromí: Možnosti a limity v rozhodování o vlastních biometrických údajích.* Právní rozhledy. Roč. 26, č. 6 (2018), s. 191-197.

[143] Povinnost mlčenlivosti v souvislosti se zdravotními službami upravuje zákon č. 372/2011 Sb. o zdravotních službách, ve znění pozdějších předpisů v § 51.

Jak uvedl generální advokát SDEU, Pedro Cruz Villalón ve stanovisku k věci C-293-12[144], *„shromažďování a především uchovávání – v enormních databázích – mnoha údajů vytvářených či zpracovávaných v rámci velké části běžné elektronické komunikace občanů Unie představuje závažný zásah do jejich soukromého života, i když jen vytvářejí podmínky pro možnost zpětně kontrolovat jejich osobní i profesní aktivity"*; generální advokát Villalón v této souvislosti dokonce hovoří o *„dojmu jakéhosi sledování"*. Dle Villalóna platí, že *„Shromažďování těchto údajů vytváří podmínky pro sledování, které i přesto, že k němu dochází jen zpětně při jejich využívání, představuje pro právo občanů Unie na utajení jejich soukromého života permanentní hrozbu trvající po celou dobu uchovávání oněch údajů"*. Z tohoto důvodu je dle jeho hodnocení v této souvislosti zásadní otázka doby uchovávání těchto údajů. Generální advokát Villalón ve svém stanovisku velmi přesně popsal též efekt, který lze dle hodnocení autora do jisté míry vztáhnout obecně i na další případy plošného shromažďování osobních údajů, nejen na povinné uchovávání provozních a lokalizačních údajů elektronických komunikací. Dle Villalóna totiž *„účinky tohoto zásahu jsou znásobeny významem, který v moderních společnostech nabyly prostředky elektronické komunikace, ať už jde o mobilní telefonní sítě nebo o internet, a masivním a intenzivním využitím těchto prostředků vysokým podílem občanů Unie ve všech oblastech jejich soukromého i profesního života"*.

Při využití provozních a lokalizačních údajů elektronických komunikací lze fakticky sledovat konkrétní osobu, případně monitorovat její pohyb v minulosti, a to včetně vazeb konkrétní osoby na další osoby, jejichž výskyt na stejném místě ve stejném časovém úseku může vypovídat o setkání těchto osob. Na základě provozních a lokalizačních údajů elektronických komunikací lze také vytvářet vzorce chování konkrétní osoby a predikovat tak její chování do budoucna, jak upozornil mj. Ústavní soud ČR v nálezu Pl. ÚS 24/10[145]. Z těchto údajů lze v poměrně podrobné míře usuzovat též na řadu dalších charakteristik konkrétních osob. Takto lze např. z lokalizačních údajů elektronických komunikací získat informace o cestování konkrétní osoby, včetně četnosti a vzdálenosti uskutečněných cest, z rychlosti přesunů a z tras je také mnohdy zřejmý použitý dopravní prostředek, přičemž ze

[144] Jak již autor uvedl výše, Soudní dvůr EU ve věci C-293-12 posuzoval platnost Data Retention Směrnice, ve svém následném rozsudku v této věci se Soudní dvůr přiklonil ke stanovisku generálního advokáta a z důvodů uvedených v tomto stanovisku směrnici prohlásil za nepl,atnou.

[145] Dle Ústavního soudu ČR lze *„na základě uchovávaných údajů … sestavit komunikační a pohybový profil jednotlivce, z kterého lze získat nejen údaje o jeho minulých aktivitách, ale s vysokou mírou pravděpodobnosti i správně předvídat jeho aktivity v budoucnosti, což rovněž představuje významný zásah do práva na ochranu soukromí a korespondence jednotlivců"*.

všech těchto údajů lze učinit závěr např. o finanční situaci dané osoby, o jejím pracovním zařazení a další. Tím se provozní a zejména lokalizační údaje elektronických komunikací odlišují od řady dalších kategorií osobních údajů, které taktéž poskytují určité informace o soukromí konkrétní fyzické osoby – subjektu údajů.

Obecně platí, že každý osobní údaj je nositelem určité informace o identifikované či identifikovatelné fyzické osobě, jak ostatně vyplývá rovněž z definice pojmu osobní údaj[146]. Intenzita zásahu do soukromí je však v případě zpracování většiny „běžných kategorií" osobních údajů zpravidla nižší v porovnání s provozními a zejména lokalizačními údaji elektronických komunikací. Taktéž generální advokát Soudního dvora EU Villalón na základě výše uvedených argumentů dospěl ve svém stanovisku ve vztahu k provozním a lokalizačním údajům u služeb a sítí elektronických komunikací k závěru o odlišném charakteru těchto údajů v porovnání s osobními údaji obecně. Dle jeho hodnocení *„Dotčenými údaji – což je na tomto místě znovu třeba zdůraznit – nejsou osobní údaje v tradičním slova smyslu, tedy údaje vztahující se ke konkrétním informacím o totožnosti osob, nýbrž osobní údaje – dalo by se říci – kvalifikované, jejichž využívání může vést k přesnému a úplnému zmapování velké části chování určité osoby, jež spadá do jejího soukromého života, či dokonce k sestavení úplného a věrného obrazu její soukromé identity."*

Provozní a lokalizační údaje elektronických komunikací jsou upraveny v ZoEK, resp. ve Směrnici o soukromí a elektronických komunikacích. V případě provozních a lokalizačních údajů se vztah mezi GDPR na straně jedné a Směrnicí o soukromí a elektronických komunikacích, resp. ZoEK na straně druhé jeví být vztahem mezi obecnou právní úpravou ochrany osobních údajů a zvláštní právní úpravou lokalizačních údajů v oblasti elektronických komunikací, jak je vymezena v ZoEK. Čl. 95 GDPR výslovně zmiňuje Směrnici o soukromí a elektronických komunikacích a konstatuje v této souvislosti, že GDPR neukládá *„žádné další povinnosti fyzickým nebo právnickým osobám, pokud jde o zpracování ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích v Unii, co se týče záležitostí, u nichž se na ně vztahují konkrétní povinnosti s týmž cílem stanovené ve směrnici 2002/58/ES."* Určité interpretační vodítko ke vztahu těchto předpisů poskytuje též recitál GDPR v bodě 173, dle kterého by se toto

[146] Viz čl. 4 bod 1 GDPR, dle kterého se osobními údaji rozumí *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů"); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby"*.

nařízení *„mělo použít na všechny záležitosti týkající se ochrany základních práv a svobod při zpracování osobních údajů, na které se nevztahují specifické povinnosti stanovené ve směrnici Evropského parlamentu a Rady 2002/58/ES (2) a sledující stejný cíl, včetně povinností správce a práv fyzických osob.“* GDPR současně v témže bodě recitálu výslovně zmiňuje též nejasnosti ve vztahu obou zmiňovaných právních předpisů, když dodává, že „*Za účelem vyjasnění vztahu mezi tímto nařízením a směrnicí 2002/58/ES by měla být uvedená směrnice odpovídajícím způsobem změněna. Jakmile bude toto nařízení přijato, směrnice 2002/58/ES by měla být podrobena přezkumu, zejména s cílem zajistit soudržnost s tímto nařízením.“*

„Přezkumem“ zde patrně evropský zákonodárce mínil zamýšlené nařízení ePrivacy[147], které v době vzniku GDPR bylo připravováno, s původním záměrem nabytí účinnosti obou předpisů ve stejnou dobu. Nařízení ePrivacy bylo zamýšleno jako náhrada Směrnice o soukromí a elektronických komunikacích. Ani několik let po přijetí GDPR až do data přípravy této práce však k finalizaci textu nařízení ePrivacy nedošlo, přestože bylo v mezidobí postupně připraveno několik verzí návrhu tohoto předpisu. Žádná nich však nebyla přijata a v blízké budoucnosti nelze přijetí tohoto nařízení očekávat; s ohledem na mnohaleté zpoždění je otázkou, zda bude vůbec kdy přijato. Jedním z deklarovaných cílů nařízení ePrivacy bylo zajištění vyšší ochrany nejen obsahu komunikace, ale též souvisejících údajů, v návrzích označovaných jako metadata, mezi ně patří i lokalizační údaje[148]. Taktéž důvodová zpráva k návrhu nařízení ePrivacy konstatuje, že obdobně jako obsah elektronických komunikací, *„i metadata odvozená z elektronických komunikací mohou odhalit velmi citlivé a osobní informace“*.

Důvodová zpráva uvádí příklady metadat, jako jsou „volaná čísla, navštívené internetové stránky, zeměpisná poloha, čas a datum, kdy daná osoba uskutečnila volání, a jeho doba trvání“, dle důvodové zprávy tyto údaje *„mohou odhalit velmi citlivé a osobní informace“*, jelikož *„umožňují vyvozovat přesné závěry týkající se osobního života osob účastnících se elektronické komunikace, například jejich sociální vztahy, zvyky a každodenní činnosti, zájmy, vkus atd.“*. Dle bodu 17 recitálu návrhu nařízení ePrivacy by za metadata

[147] Jako ePrivacy je označováno Nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích), ve stadiu návrhu.

[148] Dle čl. 4 odst. 3 písm. c) návrhu nařízení ePrivacy z 10. ledna 2017 se „metadaty elektronických komunikací“ rozumí *„údaje zpracovávané v síti elektronických komunikací pro účely přenášení, šíření nebo výměny obsahu elektronických komunikací, a to včetně údajů sloužících k vysledování a identifikaci zdroje a cíle komunikace, údajů o poloze zařízení generovaných v kontextu poskytování služeb elektronických komunikací a data, času, době trvání a typu komunikace“*.

„neměly být považovány lokalizační údaje, které jsou generovány v jiném kontextu, než je poskytování služeb elektronických komunikací.“ Je tedy zřejmé, že zamýšlená ochrana provozních a lokalizačních údajů obsažená v návrhu nařízení ePrivacy se má v případě lokalizačních údajů omezit výhradně na ty, které vznikají při poskytování služeb elektronických komunikací, přestože lokalizační údaje vznikají i v jiných souvislostech, jak ostatně i jednoznačně připouští textace návrhu nařízení ePrivacy při formulaci tohoto omezení. Toto omezení zamýšlené právní úpravy nařízení ePrivacy dle hodnocení autora vyplývá ze skutečnosti, že nařízení ePrivacy, obdobně jako Směrnice o soukromí a elektronických komunikacích, je sektorově specifickým předpisem oblasti elektronických komunikací, nikoli obecným předpisem ochrany osobních údajů.

Aktuálně platná obecná právní úprava ochrany osobních údajů, jak ji autor vymezil výše, nedefinuje a ani nepoužívá pojmy „provozní údaje“ ani „lokalizační údaje“. Provozní údaje dle definice obsažené v ZoEK se omezují výhradně na údaje vznikající v souvislosti s poskytováním služeb v sítích elektronických komunikací[149]. Kromě toho, údaje obdobné provozním údajům elektronických komunikací, avšak generované v jiných souvislostech nevykazují dle hodnocení autora obdobné rysy s provozními údaji. Autor se proto v dalším výkladu soustředí primárně na údaje lokalizační.

V GDPR, v Trestněprávní směrnici ani v ZoZOÚ lokalizační údaje nejsou vymezeny jako samostatná kategorie údajů, nejsou v těchto předpisech ani výslovně zmíněny, ostatně lokalizační údaje obdobně nebyly uvedeny ani v předchozí směrnici 95/46/ES. Lokalizační údaje tak v případě, kdy se týkají fyzických osob, nejsou zahrnuty mezi zvláštní kategorie osobních údajů. Lokalizační údaje pro oblast elektronických komunikací vymezuje zvláštní právní předpis, Směrnice o soukromí a elektronických komunikacích[150] a v právním řádu ČR ZoEK. Ve Směrnici o soukromí a elektronických komunikacích a obdobně též v ZoEK jsou lokalizační údaje vymezeny jako údaje určující zeměpisnou polohu, jde přitom

[149] ZoEK vymezuje provozní údaje v § 90 odst, 1 tak, že se jimi rozumí *„jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování“*; toto vymezení lze považovat za konstantní, též předchozí právní úprava zákona č. 151/2000 Sb. o telekomunikacích a o změně dalších zákonů vymezovala jako součást telekomunikačního tajemství v § 84 odst. 3, vedle obsahu přepravovaných zpráv a provozních dokladů, z jejichž obsahu je zjevný obsah přepravovaných zpráv, též pojmově odlišně označená, avšak obsahově obdobná „osobní a zprostředkovací data“ vymezená jako *„data související s poskytováním telekomunikační služby, zejména údaje o účastnících telekomunikačního spojení“*.

[150] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

nikoli přímo o zeměpisnou polohu samotné fyzické osoby, nýbrž koncového zařízení[151], to však ve vazbě na konkrétní fyzickou osobu – uživatele služby elektronických komunikací, jak vyplývá z definice v obou těchto předpisech, které uživatele ve spojení s koncovým zařízením výslovně uvádějí[152]. Sítě elektronických komunikací zahrnují pevné i mobilní komunikační sítě, výše uvedené vymezení lokalizačních údajů v ZoEK mezi oběma případy nerozlišuje. Z hlediska zaměření této práce, tedy zásahů do soukromí, je však zásadní rozdíl mezi „zeměpisnou polohou koncového zařízení uživatele služby elektronických komunikací" v síti pevné a v síti mobilní. V pevné síti je takovouto zeměpisnou polohou z povahy věci adresa, na které se koncové zařízení nachází v zásadě trvale, a míra zásahu do soukromí v případě zpracování tohoto lokalizačního údaje je tak plně srovnatelná se situací při zpracování jakýchkoli jiných osobních údajů, takovéto lokalizační údaje lze označit jako „statické", v čase neměnné. Na rozdíl od toho v mobilních komunikačních sítích takováto zeměpisná poloha koncového zařízení je v čase proměnlivá a je zpravidla totožná s aktuální zeměpisnou polohou účastníka či uživatele. Autor má za to, že je z tohoto důvodu především důležité odlišovat ve smyslu výše uvedeného vymezení osobní údaje v podobě lokalizačních údajů statických, v čase neměnných, mezi které patří typicky např. adresa koncového zařízení pevné sítě, zpravidla totožná s adresou pobytu fyzické osoby (trvalého či přechodného), od osobních údajů v podobě lokalizačních údajů „dynamických", které v čase podléhají změnám, a to změnám četným a na sebe navazujícím, v závislosti na pohybu fyzické osoby – účastníka či uživatele. V případě lokalizačních údajů, které u konkrétní osoby dokumentují změnu zeměpisné polohy této osoby, a jde tedy o dynamické, v čase se měnící lokalizační údaje, platí plně závěry uvedené výše, zatímco v případě statických lokalizačních údajů tyto závěry platí pouze v míře omezené. S ohledem na aktuální rozšíření mobilních komunikačních služeb v

[151] ZoEK vymezuje koncové zařízení v § 73 odst. 4, a to jako „telekomunikační koncové zařízení", kterým se rozumí *„zařízení přímo nebo nepřímo připojené k rozhraní veřejné komunikační sítě, které může vysílat, zpracovávat nebo přijímat informace bez ohledu na použitou technologii"*, a to včetně družicové pozemské stanice. Pro účely vymezení pojmu „lokalizační údaje" půjde tedy o telefonní přístroj či obdobné komunikační zařízení, včetně zařízení pro využívání datových služeb.

[152] Lokalizační údaje jsou ve Směrnici o soukromí a elektronických komunikacích vymezeny v čl. 2 písm. c) jako *„jakékoli údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací"*, ZoEK obsahuje jejich obdobnou definici v § 91 odst. 1, v rámci ochrany osobních, provozních a lokalizačních údajů a důvěrnost komunikací. Lokalizačními údaji jsou dle ZoEK *„jakékoli údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací"*. V případě koncových zařízení používá termín „telekomunikační", tedy pojem náležející předchozí právní úpravě. Jde o výjimku (vedle tohoto případu tak činí pouze u Českého telekomunikačního úřadu a u Telekomunikačního věstníku), která nemá zásadní dopad na význam pojmu lokalizačních údajů.

ČR[153] lze uzavřít, že „dynamické lokalizační údaje“ elektronických komunikací, jak je autor vymezil výše, se týkají podstatné části obyvatel ČR. V případě plošného zpracování těchto lokalizačních údajů jde tak o zásah do práva na ochranu soukromí, který lze hodnotit jako velmi rozsáhlý, umožňující sledování konkrétních osob.

Dle hodnocení autora lze konstatovat, že v souladu se Směrnicí o soukromí a elektronických komunikacích je předpokladem zvýšené ochrany lokalizačních údajů, oproti ostatním kategoriím údajů, vazba koncového zařízení, tedy i lokalizačních údajů, na konkrétní fyzickou osobu. Tato vazba vyplývá z čl. 9 odst. 1 této směrnice, který zpracování lokalizačních údajů vztahujících se k uživatelům nebo účastníkům povoluje pouze za splnění některé z taxativně stanovených podmínek. Směrnice o soukromí a elektronických komunikacích zvýšenou ochranu poskytuje jen pro údaje vztahující se k uživatelům nebo účastníkům komunikačních sítí nebo služeb, a to navíc pouze veřejných komunikačních sítí nebo veřejně dostupných služeb elektronických komunikací[154]. Obdobně též ZoEK ukládá povinnosti k ochraně důvěrnosti komunikací, včetně lokalizačních údajů jako součást důvěrnosti komunikací, pouze podnikatelům zajišťujícím veřejné komunikační sítě nebo poskytujícím veřejně dostupné služby elektronických komunikací. Důvod nesouvisí s předmětem ochrany, je jím pouze skutečnost, že regulace v oblasti elektronických komunikacích a odpovídající ukládání povinností podnikatelům jsou v ZoEK omezeny pouze na zajišťování veřejných komunikačních sítí a poskytování veřejně dostupných služeb[155].

Jak již uvedeno, ZoEK upravuje ochranu lokalizačních údajů v rámci institutu důvěrnosti komunikací[156], samotný pojem „důvěrnost komunikací“ přitom nedefinuje. Obsah tohoto pojmu je však v ZoEK vymezen[157] v rámci povinností ukládaných podnikatelům

---

[153] Dle Výroční zprávy Českého telekomunikačního úřadu za rok 2022 *„Ze souhrnných ukazatelů o mobilním trhu v ČR mj. vyplývá, že celkový počet aktivních SIM karet dle odhadu Úřadu na konci roku 2022 přesáhl 15,2 mil“*. ČTÚ. *Výroční zpráva Českého telekomunikačního úřadu za rok 2022.* s. 17. Dostupné z www.ctu.gov.cz. [cit. 8.2.2024].

[154] Dle čl. 9 odst. 1 Směrnice o soukromí a elektronických komunikacích *„Mohou-li být zpracovávány lokalizační údaje odlišné od provozních údajů, které se vztahují k uživatelům nebo účastníkům veřejných komunikačních sítí nebo veřejně dostupných služeb elektronických komunikací, je možné tyto údaje zpracovávat pouze poté, co byly anonymizovány údaje, anebo se souhlasem uživatelů nebo účastníků v nezbytném rozsahu a po nezbytnou dobu pro poskytování služeb s přidanou hodnotou.“*

[155] Výjimky jsou dle ZoEK omezeny pouze na případy, které je nezbytné regulovat i v případě neveřejných sítí, jde o oprávnění k využívání čísel a připojování neveřejných komunikačních sítí k sítím veřejným.

[156] Důvěrnost komunikací viz § 88 a násl. ZoEK. K tomuto tématu viz též UŘIČAŘ, Miroslav. Telekomunikační tajemství. In: SCHELLE, Karel, TAUCHEN, Jaromír (eds). *Encyklopedie českých právních dějin. XVIII. svazek Ta-Ty*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2019 v koedici s Ostrava: KEY Publishing s.r.o. 2019.

[157] Viz § 89 odst. 1 ZoEK: *„Podnikatelé zajišťující veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací jsou povinni zajistit technicky a organizačně důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů, které se přenášejí prostřednictvím jejich veřejné komunikační sítě*

zajišťujícím veřejné komunikační sítě či poskytujícím veřejně dostupné služby elektronických komunikací, a to tak, že zahrnuje jak důvěrnost zpráv ve vztahu k obsahu těchto zpráv, tak i důvěrnost provozních a lokalizačních údajů. Povinnost zajistit důvěrnost komunikací spočívá v povinnosti ochrany zpráv před neoprávněným přístupem, v ZoEK vymezeným jako odposlech, ukládání nebo jiné druhy zachycení nebo sledování zpráv a s nimi spojených údajů, tedy údajů provozních, jinými osobami nežli uživateli, bez jejich souhlasu; výjimku představují případy stanovené zákonem. Pojem „zpráva" je v tomto ustanovení definován[158] jako jakákoli informace spojená s určitým počtem účastníků nebo uživatelů služby elektronických komunikací, a to opět pouze služby veřejně dostupné, ze stejných důvodů jako bylo rozebráno výše.

Ve vztahu k ochraně dotčených fyzických osob – účastníků a uživatelů – neexistuje dle hodnocení autora pro zde rozebírané omezení pouze na veřejné sítě a veřejně dostupné služby, místo obecné aplikace ochrany důvěrnosti komunikací na sítě a služby elektronických komunikací, racionální důvod, když účastníci a uživatelé neveřejných sítí a služeb elektronických komunikací, resp. důvěrnost komunikace těchto osob, by měly požívat obdobné ochrany. Ostatně, jak Listina, tak rovněž trestní zákoník[159] zaručují ochranu telekomunikačního tajemství obecně, bez takto či obdobně formulovaného omezení. Současně však toto omezení z jazykového výkladu Směrnice o soukromí a elektronických komunikacích i ze ZoEK vyplývá jednoznačně a překlenout jej a dovodit z textu těchto předpisů ochranu obecnější, bez omezení na veřejné komunikační sítě či veřejné služby, nelze, mj. i s ohledem na důvody uvedené výše, spočívající v obecném zaměření regulace podnikání v elektronických komunikacích.

Je tedy zřejmé, že ochrana poskytovaná v platné právní úpravě elektronických komunikací lokalizačním údajům v závislosti na tom, zda jsou či nejsou generovány ve veřejných komunikačních sítích či při poskytování veřejných komunikačních služeb[160], je

---

a veřejně dostupných služeb elektronických komunikací. Zejména nepřipustí odposlech, ukládání zpráv nebo jiné druhy zachycení nebo sledování zpráv a s nimi spojených údajů osobami jinými, než jsou uživatelé, bez souhlasu dotčených uživatelů, pokud zákon nestanoví jinak."

[158] ZoEK vymezuje pro tento účel „zprávu" v § 89 odst. 1 tak, že se jí rozumí *„jakákoli informace, která se vyměňuje nebo přenáší mezi konečným počtem účastníků nebo uživatelů prostřednictvím veřejně dostupné služby elektronických komunikací, s výjimkou informace přenášené jako součást veřejného rozhlasového nebo televizního vysílání sítí elektronických komunikací, nelze-li ji přiřadit k určitelnému účastníkovi nebo uživateli, který tuto informaci přijímá"*.

[159] V zákoně č. 40/2009 Sb. trestní zákoník, ve znění pozdějších předpisů, se jedná o ochranu porušení tajemství dopravovaných zpráv obsaženou v § 182 odst. 2.

[160] Veřejnou komunikační síť vymezuje ZoEK v § 2 odst. 2. písm. d) odkazem na charakter služeb, k jejichž poskytování komunikační síť slouží, jako *„síť elektronických komunikací, která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací a která podporuje přenos informací mezi*

nerovnoměrná. Také tato skutečnost dle hodnocení autora svědčí o tom, že řešení ochrany pro lokalizační údaje obsažené pouze ve zvláštní právní úpravě elektronických komunikací, jejímž primárním cílem je regulace podnikání v odvětví elektronických komunikací, není v současnosti ve vztahu k právu na ochranu soukromí ideálně nastaveno.

Reálný dopad tohoto nedostatku právní úpravy je sice nižší v důsledku menšího množství dotčených osob – účastníků a uživatelů „neveřejných komunikačních sítí" a „neveřejných služeb" elektronických komunikací, v porovnání s účastníky a uživateli veřejných komunikačních sítí a veřejně dostupných služeb elektronických komunikací, po stránce právní tím však neztrácí na relevanci. V praxi nejsou navíc neveřejné komunikační sítě nikterak výjimečným jevem a celkové množství jejich účastníků není dle informací autora zanedbatelné[161]. „Neveřejné komunikační sítě" (jiné nežli veřejné komunikační sítě) nejsou v platné právní úpravě jako pojem přímo definovány, význam tohoto pojmu je však na základě ostatních definic obsažených v ZoEK jednoznačně dovoditelný[162]; také sám ZoEK pojem „neveřejné komunikační sítě" používá[163]. Taktéž vyhláška č. 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů výslovně s existencí neveřejných komunikačních sítí počítá, když mezi provozní údaje povinně uchovávané a následně

koncovými body sítě, nebo síť elektronických komunikací, jejímž prostřednictvím je poskytovaná služba šíření rozhlasového a televizního vysílání", veřejně dostupnou službou elektronických komunikací se pak dle § 2 odst. 3 písm. e) rozumí *„služba elektronických komunikací, z jejíhož využívání není nikdo předem vyloučen"*.

[161] Např. Vysokorychlostní datová síť Moravskoslezského kraje, etapa I. Datové propojení v Bruntále byla v rámci Jednacího řízení bez uveřejnění s jediným účastníkem v rámci projektu „Postupné budování vysokorychlostní datové sítě Moravskoslezského kraje", kde vymezeným účelem sítě je *„zajištění síťového prostředí pro vzájemnou komunikaci zřizovatele – Krajského úřadu Moravskoslezského kraje a jím zřízenými příspěvkovými a obchodními organizacemi"* označena jako neveřejná komunikační síť. [online] [cit. 15.1.2024]. Dostupné z Portálu pro vhodné uveřejnění https://www.vhodne-uverejneni.cz/.

[162] Jak uvádí např. Ministerstvo průmyslu a obchodu v materiálu Metodická pracovní pomůcka. Vztah mezi zákonem č. 127/2005 Sb. o elektronických komunikacích, zákonem č. 194/2017 Sb. o opatřeních ke snížení nákladů na zavádění vysokorychlostních sítí elektronických komunikací, zákonem č. 183/2006 Sb. stavební zákon a zákonem č. 416/2009 Sb. o urychlení výstavby dopravní, vodní a energetické infrastruktury a infrastruktury elektronických komunikací, *„věcnou náplň tohoto pojmu lze dovodit a contrario z definice veřejné komunikační sítě. Za neveřejnou komunikační síť tak lze považovat všechny sítě elektronických komunikací, které nejsou veřejnou komunikační sítí, tedy neslouží k poskytování veřejně dostupných služeb elektronických komunikací. Typicky se jedná o sítě využívané jedním subjektem ryze pro jeho potřeby. Není vyloučeno, aby neveřejná komunikační síť byla postavena ve veřejném zájmu."* Ministerstvo průmyslu a obchodu. *Metodická pracovní pomůcka. Metodické doporučení Ministerstva pro místní rozvoj a Ministerstva průmyslu a obchodu.* 5. června 2019. [online] [cit. 15.1.2024]. Dostupné z www.mpo.gov.cz.

[163] Dle § 30 ZoEK ČTÚ rozhoduje o udělení oprávnění k využívání čísel pro všechny veřejné i neveřejné komunikační sítě a veřejně dostupné služby elektronických komunikací; dle § 98 ZoEK pak ČTÚ při vydávání síťových plánů vymezí mj. rozhraní pro připojování neveřejných komunikačních sítí a zajištění bezpečnosti a kontinuity dodávek služeb.

předávané oprávněným orgánům zahrnuje mj. i údaje o identifikaci osoby zajišťující neveřejnou komunikační síť[164], tedy provozovatele takové sítě.

V případě neveřejných komunikačních sítí nejsou jejich provozovatelům povinnosti k zachování důvěrnosti komunikací uloženy zákonem, když § 88 ZoEK ukládající povinnosti k zabezpečení ochrany osobních, provozních a lokalizačních údajů a důvěrnosti komunikací, stejně jako následující ustanovení ZoEK, se aplikují pouze na podnikatele poskytující veřejně dostupnou službu elektronických komunikací, resp. zajišťující veřejnou komunikační síť. Z této skutečnosti ovšem mimo jiné vyplývá, že provozovatelé neveřejných komunikačních sítí či poskytovatelé neveřejných služeb elektronických komunikací jsou – na rozdíl od poskytovatelů veřejně dostupných služeb a provozovatelů veřejných komunikačních sítí - povinni vyhovět i obecným žádostem správních orgánů o poskytnutí informací[165], a to i v případech, kdy požadované informace zahrnují provozní a lokalizační údaje, bez nutnosti respektovat požadavky a omezení stanovená právní úpravou pro vyžádání provozních a lokalizačních údajů. Taktéž orgány oprávněné takové údaje vyžádat se neomezují pouze na orgány výslovně oprávněné k vyžádání provozních a lokalizačních údajů dle ZoEK.

Ochrana provozních ani lokalizačních údajů účastníků a uživatelů neveřejných sítí tak není náležitě zajištěna. Tato skutečnost je dle autora v rozporu s požadavky formulovanými mj. Ústavním soudem ČR v nálezu Pl. ÚS 24/10. Ústavní soud ČR v tomto nálezu jednoznačně konstatoval, že imperativní zákonná úprava umožňující zásah do základního práva jednotlivce na soukromí *„musí především odpovídat nárokům plynoucím z principu právního státu“* a musí také naplňovat *„požadavky vyplývající z testu proporcionality“*. Taková právní úprava musí dle Ústavního soudu ČR *„být přesná a zřetelná ve svých formulacích a dostatečně předvídatelná“* a *„rovněž musí být striktně definovány i pravomoci udělené příslušným orgánům, způsob a pravidla jejich provádění tak, aby jednotlivcům byla poskytnuta ochrana proti svévolnému zasahování.“* Zejména poslední uvedený požadavek zde naplněn není, v případě neveřejných komunikačních sítí a služeb nejsou ani předem vymezeny příslušné orgány ani nejsou definovány jejich pravomoci. Nejinak tomu však je i u obou předchozích podmínek – na splnění požadavků právního státu a proporcionality a na přesnost a předvídatelnost právní úpravy. Jak již konstatováno v této

[164] Viz § 2 odst. 4 písm. c) vyhlášky č. 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.
[165] Např. policista je dle § 18 zákona č. 273/2008 Sb. o Policii České republiky, ve znění pozdějších předpisů, oprávněn vyžadovat pomoc i od právnických a fyzických osob, *„zejména potřebné podklady a informace včetně osobních údajů“*.

práci výše, Ústavní soud ČR v citovaném nálezu upozorňuje, že *„obdobný přístup zastává i ESLP ve své judikatuře“*, ve vztahu k Evropské úmluvě. Ve smyslu čl. 13 Evropské úmluvy musí právní úprava *„rovněž poskytovat přiměřenou ochranu proti svévoli, a v důsledku toho s dostatečnou jasností definovat rozsah a způsob výkonu pravomocí svěřených kompetentním orgánům“*. Jedna z hlavních výtek Ústavního soudu ČR v případě posuzovaném v tomto nálezu směřovala právě k nedostatečnému vymezení oprávněných orgánů v napadeném (a Ústavním soudem ČR tímto nálezem zrušeném) ustanovení § 97 odst. 3 a 4 ZoEK.

Ustálená soudní judikatura dovodila, že provozní a lokalizační údaje elektronických komunikací (včetně takových údajů, jakými jsou telefonní číslo volaného, datum a čas počátku hovoru, délka jeho trvání, označení základnové stanice, která zajišťovala hovor v okamžiku spojení, a označení základové stanice, která hovor zajišťovala v momentu ukončení, datum a čas odeslání textové zprávy SMS, identifikátor mobilního přístroje volajícího a volaného a další) je třeba považovat za nedílnou součást komunikace uskutečněné prostřednictvím telefonu, přičemž jako takové podléhají tyto údaje ochraně dle čl. 13 Listiny. Ústavní soud ČR v nálezu II. ÚS 502/2000 výslovně konstatoval, že „*Soukromí každého člověka je hodno zásadní (ústavní) ochrany nejen ve vztahu k vlastnímu obsahu podávaných zpráv, ale i ve vztahu k výše uvedeným údajům*[166]“, v nálezu IV. ÚS 78/01 Ústavní soud ČR výslovně odkázal právě na čl. 13, když dovodil, že „*Článek 13 Listiny základních práv a svobod nezakládá pouze ochranu tajemství vlastního obsahu telefonických zpráv, ale i dalších údajů evidovaných při registraci telekomunikačního provozu ve vztahu ke konkrétním osobám.*“[167]. Ústavní soud ČR se k této otázce vyjádřil ve svých nálezech opakovaně[168] a tyto závěry tak lze dle autora označit za konstantní rozhodovací praxi, jak ostatně výslovně uvádí Ústavní soud ČR např. také v následném nálezu Pl. ÚS 24/10, v němž na předchozí zde citovaný nález výslovně odkazuje[169]. Ústavní soud ČR se v těchto svých nálezech opírá mimo jiné i o závěry ESLP, když výslovně odkazuje např. na již výše rozebíraný rozsudek ESLP ze dne 2. 8. 1984 ve věci Malone proti Spojenému království[170].

---

[166] Nález Ústavního soudu ČR sp. zn. II. ÚS 502/2000 ze dne 22.1.2001.
[167] Nález Ústavního soudu ČR sp. zn. IV. ÚS 78/01 ze dne 27.8.2001.
[168] Kromě již uvedených nálezů obdobně též např. nálezy Ústavního soudu ČR sp. zn. I. ÚS 191/05 ze dne 18.9.2006 či sp. zn. II. ÚS 789/06 ze dne 27.9.2007.
[169] *„Z ustálené judikatury Ústavního soudu, zejména ve vztahu k problematice odposlechu telefonních hovorů, zřetelně vyplývá, že ochrana práva na respekt k soukromému životu v podobě práva na informační sebeurčení ve smyslu čl. 10 odst. 3 a čl. 13 Listiny se vztahuje nejen k vlastnímu obsahu zpráv podávaných telefonem, ale i k údajům o volaných číslech, datu a čase hovoru, době jeho trvání, v případě mobilní telefonie o základových stanicích zajišťujících hovor [srov. např. nález sp. zn. II. ÚS 502/2000 ze dne 22. 1. 2001 (N 11/21 SbNU 83)“*
[170] Judgment of the European Court of Human Rights, dated 2 August 1984. Case of Malone v. The United Kingdom (Application no. 8691/79).

Správnost zařazení údajů o komunikaci, resp. provozních údajů[171] ve smyslu jejich vymezení v ZoEK, mezi informace chráněné jako součást „*tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením*“ dle čl. 13 Listiny není přijímána zcela jednoznačně bezvýhradně. Pochybnosti ohledně toho, zda takové zařazení zcela odpovídá na straně jedné skutečné podstatě takto chráněných údajů o komunikaci a na straně druhé vymezení obsaženému v čl. 13 Listiny, vyjádřil Jan Kudrna[172], který takovéto zařazení považuje za problematické. Nezpochybňuje ochranu těchto údajů samu o sobě, nýbrž pouze její právní základ a důsledky z toho vyplývající. Argumentuje přitom tím, že „*věcně souvisí ochrana doprovodných údajů o komunikaci spíše s obecnou ochranou soukromí zakotvenou v čl. 10 Listiny*", ačkoli „*není pochyb, že z hlediska praktického je odkaz na čl. 13 Listiny užitečnější*“. Dle jeho názoru je však otázkou, nakolik byl takovýto postup Ústavního soudu ČR v případech řešených v nálezech II. ÚS 502/2000 a IV. ÚS 78/01 nezbytný s ohledem na to, že „*možnost poskytování doprovodných údajů o uskutečněných spojeních právní řád České republiky v roce 2000 neznal*“.

Autor považuje tyto odborné názory za velmi relevantní a hodné stručného rozboru na tomto místě. Uvedené závěry se současně také bezprostředně týkají jednoho z typových případů plošných zásahů do práva na ochranu soukromí, které jsou předmětem této práce, přitom zásahu velmi významného, totiž povinného uchovávání provozních a lokalizačních údajů elektronických komunikací v rámci povinnosti Data Retention. Vedle toho však také nastolené otázky souvisejí i s některými z dalších zásahů v této práci rozebíraných, jejichž předmětem jsou lokalizační údaje bez vazby na elektronické komunikace, tedy údaje o výskytu konkrétní osoby v určitém čase na určitém místě. Jak autor rozvádí dále v této práci, je v této souvislosti namístě uvažovat o správnosti a dostatečnosti stávajícího stavu, kdy lokalizační údaje plošně shromažďované např. v rámci systémů v automobilech či záznamů kamerových systémů na silnicích a dálnicích, vč. kamerových systémů ke kontrole úhrady elektronických dálničních známek a další, tvoří pouze jednu z kategorií osobních údajů. Jako takové též jsou lokalizační údaje v právním řádu pouze předmětem ochrany běžných osobních údajů, jde přitom o údaje umožňující monitorování pohybu konkrétních osob v čase i o sociálních

[171] Zákon o elektronických komunikacích vymezuje provozní údaje v § 90 odst. 1 tak, že *„Provozními údaji se rozumí jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování“*.

[172] Viz *Kudrna Jan*. 27. Pravděpodobně nejvíce porušované ustanovení Listiny (a jedna ze současných hrozeb lidským právům) in GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012 s. 276 a násl.

vazbách s dalšími osobami, vč. vyvozování dalších závěrů ohledně modelů chování dané osoby do budoucna i o jejích jiných osobních aspektech. Je proto relevantní posoudit, zda se nejedná o natolik specifickou kategorii osobních údajů, že je namístě uvažovat o zvláštním režimu jejich ochrany.

Autor se této otázce podrobně věnuje dále, na tomto místě se tak autor zamýšlí primárně nad výše uvedenými námitkami vůči zařazení provozních údajů mezi údaje chráněné dle čl. 13 Listiny, a to jak ve světle vývoje ochrany provozních a lokalizačních údajů v právním řádu ČR, tak rovněž ve světle relevantní rozhodovací praxe Ústavního soudu ČR a též ESLP, v kauzách týkajících se zásahů do práva na ochranu soukromí a do telekomunikačního tajemství. Dle autora není možno opomíjet ani již uvedený odkaz na rozhodovací praxi ESLP. Je zřejmé, že obdobně postupoval i tento soud, a to historicky již v případu Malone proti Spojenému království, kdy se jednalo o rozhodnutí z roku 1984. V té době ještě otázka provozních údajů nebyla nikterak četně řešena, s ohledem na neexistenci technologie mobilních komunikací, jejíž následný nástup výrazně posunul rozsah a tedy i význam provozních a lokalizačních údajů a měl vliv i na další vývoj rozhodovací praxe. U komunikace prostřednictvím pevných linek byl rozsah kategorií zpracovávaných provozních údajů a též dopad do soukromí komunikujících osob z povahy věci nižší nežli u mobilní komunikace, lokalizační údaje se omezovaly pouze na adresu umístění účastnické telefonní stanice. Oproti tomu v současnosti, v případě komunikace prostřednictvím mobilních sítí hrají naopak lokalizační údaje zásadní roli. Mobilní technologie totiž fakticky umožňuje monitorovat polohu osoby účastníka či uživatele, a to i v případech, kdy neuskutečňuje komunikaci. Mobilní telefonní, resp. v současné době spíše komunikační přístroj, je totiž neustále připojen ke konkrétní základnové stanici mobilní sítě elektronických komunikací, která přenáší signál této sítě, kromě toho však mobilní přístroj nepřetržitě cíleně zaznamenává i další dosažitelné základnové stanice, díky tomu je možno s vysokou přesností vypočítat polohu dané osoby[173]. Kromě lokalizačních údajů je dále v současnosti relevantní také druh využité služby, a to

[173] K tomuto podrobněji viz např. Policie ČR. Spuštění lokalizačních SMS na mobilních telefonech: *„Systém, který funguje doposud, předává operátorovi tísňové linky informace o poloze volajícího s odchylkou přibližně 400 m ve městě a teoreticky i několik kilometrů ve volném terénu. Vždy záleží na mnoha okolnostech, mezi ty zásadní patří pokrytí vysílači mobilní sítě. Lokalizační SMS formát Advanced Mobile Location (AML), což je nová funkcionalita jednotného evropského čísla tísňového volání – tísňové linky 112, bude využívána i pro linky 150, 155 a 158 a k jejímu spuštění došlo 11. února 2020 pro zařízení s operačním systémem Android. Pilotní provoz bude probíhat nejdřív na území hl. m. Prahy a postupně se rozšíří do celé České republiky.“* Policie ČR. *Spuštění lokalizačních SMS na mobilních telefonech.* 12. února 2020. [online] [cit. 12.1.2023] Dostupné z www.policie.cz.

zejména, nikoli však pouze v případě mobilních komunikací[174]. Za relevantní autor považuje i skutečnost, že mezi povinně uchovávané a tedy k žádosti oprávněného orgánu předávané údaje patří mj. i neúspěšné pokusy o komunikaci, tedy v případě výpisu mobilní komunikace „*stav komunikace - např. úspěšný/neúspěšný pokus o volání, odmítnutí volání, neúspěšný pokus o zaslání SMS nebo MMS*“[175].

V souvislosti s výše citovanými úvahami o správnosti zařazení ochrany provozních a lokalizačních údajů však autor v prvé řadě považuje za nutné uvést jejich celkový kontext. Jan Kudrna totiž v citovaném textu vyjádřil svou pochybnost ohledně správnosti zařazení ochrany provozních a lokalizačních údajů pod ochranu poskytovanou čl. 13 Listiny pouze jako vedlejší myšlenku, ostatně celá relevantní pasáž k tomuto je vcelku stručná, má povahu pouhé poznámky pod čarou; autor také nenalezl jiný text, v němž by se tento ústavní právník dané problematice věnoval. Hlavním tématem citovaného textu totiž je upozornění na čím dál četnější omezování lidských práv, k nimž dle autora textu dochází „*mlčky, bez širší diskuse či veřejné úvahy*“. Tato úvaha následně dospívá k závěru, který tvoří i název jeho textu, tedy k tomu, že čl. 4 odst. 4 Listiny je *„pravděpodobně nejvíce porušovaným ustanovením Listiny základních práv a svobod“*. Jakkoli se může takto formulovaná myšlenka jevit jako jistá nadsázka, autor s tímto závěrem Jana Kudrny plně souhlasí, ostatně také tato práce dle hodnocení autora do značné míry potvrzuje správnost diskutovaného závěru. Autor se k tomuto obecnému závěru vyjadřuje podrobněji v závěru této práce, v kapitole pojednávající o kontrolních mechanismech de lege ferenda, v rámci zobecnění závěrů vyplývajících ze zkoumání jednotlivých případů zásahů do práva na ochranu soukromí rozebíraných v této práci.

Autor má proto z kontextu citované úvahy za to, že se v případě výše uvedené otázky jednalo pouze o poznámku, jejímž vyslovením Kudrna nezamýšlel vyvolat k tomuto tématu polemiku. Jak však autor uvádí výše, otázka správnosti zařazení ochrany provozních a lokalizačních údajů je velmi relevantní, autor souhlasí s tím, že zařazení ochrany těchto údajů v rámci ochrany dle čl. 13 Listiny nelze automaticky považovat za zcela samozřejmý a

---

[174] K tomu viz Vyhláška č. 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, provádějící příslušné ustanovení ZoEK. Vyhláška v § 2 odst. 1 písm. e) ve spojení s § 1 odst. m) vymezuje údaje uchovávané u veřejných mobilních telefonních sítí, a to mj. vč. *„použité telefonní služby“*, přičemž touto telefonní službou se rozumí „*služba umožňující volání, včetně hlasové služby, hlasové schránky, videohovoru, doplňkových služeb přeložení a přesměrování volání nebo konferenčního volání, a službu zasílání textové zprávy SMS nebo multimediální zprávy MMS*“.

[175] Viz bod 2.3.10 Přílohy k Vyhlášce č. 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, která stanoví formu předávání údajů.

jednoznačný závěr. V uvedené souvislosti považuje autor za zásadní nejprve stručný historický exkurz v rámci právní úpravy telekomunikačního tajemství v právním řádu ČR. Tento právní institut se vyvinul z institutu úzce souvisejícího, z tajemství listovního[176], vlivem vývoje techniky. Již jedna z prvních právních úprav telekomunikačního (resp. v dané době telegrafního) tajemství na území ČR, Telegrafní řád z roku 1905[177], vymezovala obsah povinnosti zachovávat toto tajemství výslovně tak, že zahrnovala též jediné v té době relevantní provozní údaje – identitu komunikujících stran[178]. Obdobně také první československá právní úprava telekomunikací, zákon č. 60/1923 Sb. o telegrafech, „*výslovně vztahovala tajemství telegrafní a telefonní nejen na obsah komunikace, ale také na „jména korespondujících stran" a „čísla rozmlouvajících účastnických stanic"*"[179] Taktéž následující právní úpravy pokračovaly v tato široce vymezeném telekomunikačním tajemství[180].

Autor hodnotí samotnou skutečnost, že historicky bylo telegrafní, telefonní či telekomunikační tajemství v platné právní úpravě (byť nikoli v právním předpise srovnatelném s Listinou[181]) vymezeno a též vykládáno jako zahrnující i provozní údaje, jako významnou, nikoli však postačující pro učinění závěru o správnosti aplikace ochrany „tajemství zpráv podávaných telefonem" dle čl. 13 Listiny na provozní a lokalizační údaje mobilních komunikací, když zde se navíc jedná o ochranu poskytovanou v Listině, nikoli

---

[176] Eliška Wagnerová k tomu v komentáři k LZPS uvádí: *„Patrně poprvé bylo na ústavní úrovni na listovní tajemství pamatováno v belgické ústavě z roku 1831 (čl. 22). Historicky se dimenze práva na soukromí v podobě důvěrnosti komunikace vztahovala na korespondenci a její poštovní přepravu, avšak s rozšiřováním způsobů komunikace se jak pozitivně-právně, tak interpretačně rozšiřuje i oblast, na kterou toto základní právo dopadá."* WAGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch, LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer (ČR) 2012. 931 s. Dostupné z ASPI.

[177] Řád telegrafní, vyhlášen nařízením obchodního ministeria ze dne 18. dubna 1905, na základě Nejvyššího rozhodnutí ze dne 10. dubna 1905 a uvádějíc ve skutek dekret dvorní kanceláře ze dne 25. ledna 1847, č. 2581, sb. z. pol. č. 9.

[178] Viz Telegrafní řád 1905 § 4 O zachování telegrafního tajemství: *„Telegrafní tajemství zachovává se přísně. Původní sepis telegramu nesmí nikomu vydán býti, opis jeho smí býti vydán toliko odesilateli neb adresátovi nebo jeho vykázanému zmocněnci. Zřízencům telegrafním jest přísně zakázáno oznámiti obsah telegramů nebo také jenom jméno korespondentů – odesilatelovo nebo adresátovo – jakož i jinaká data telegramu jiným osobám."*

[179] Viz UŘIČAŘ, Miroslav. Telekomunikační tajemství. In: SCHELLE, Karel, TAUCHEN, Jaromír (eds). *Encyklopedie českých právních dějin. XVIII. svazek Ta-Ty*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2019 v koedici s Ostrava: KEY Publishing s.r.o. 2019.

[180] Zákon č. 72/1950 Sb. o telekomunikacích, ve znění pozdějších předpisů, zákon č. 110/1964 Sb. o telekomunikacích, ve znění pozdějších předpisů, zákon č. 151/2000 Sb. o telekomunikacích a o změně dalších zákonů, ve znění pozdějších předpisů – tento právní předpis taktéž samotný právní institut telekomunikačního tajemství označoval v § 84 jako „Telekomunikační tajemství a ochrana osobních a zprostředkovacích dat", až po do dnešního dne účinný zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).

[181] V době účinnosti Řádu telegrafního i následného zákona č. 60/1923 Sb. o telegrafech upravoval základní práva a svobody nejprve Základní zákon státní č. 142/1867 ř.z. o obecných právech občanů státních v královstvích a zemích v radě říšské zastoupených, který neobsahoval tajemství telekomunikační či srovnatelné, pouze tajemství listovní (tajnost psaní) v čl. 10, posléze Ústavní listina Československé republiky, uvozená zákonem 121/1920 Sb., která taktéž upravovala pouze tajemství listovní v § 116.

v obecné právní úpravě dřívějších telekomunikací či aktuálních elektronických komunikací. Pro jednoznačné vyhodnocení je proto nutno analyzovat také dostupnou rozhodovací praxi, vč. nálezů Ústavního soudu, které ve svém textu zmiňuje i Jan Kudrna, tedy nálezů II. ÚS 502/2000 a IV. ÚS 536/2000[182] a zejména argumentaci, s jejímž použitím Ústavní soud ČR k tomuto závěru dospěl. V nálezu IV. ÚS 536/2000 Ústavní soud ČR vyslovuje svůj jednoznačný názor, dle kterého provozní a lokalizační údaje (které však neoznačuje tímto termínem, jak autor zmiňuje dále) v rozsahu „*mimo jiné číslo volané stanice, datum a čas počátku hovoru, doba jeho trvání, označení základové stanice, která zajišťovala hovor v okamžiku spojení a označení základové stanice, která hovor zajišťovala v momentu ukončení*“ je třeba „*považovat za nedílnou součást komunikace uskutečněné prostřednictvím telefonu*“. Předmětné údaje – v dnešní terminologii vycházející ze ZoEK[183] označované jako provozní a lokalizační údaje – Ústavní soud ČR v tomto nálezu označuje jako „*údaje získané evidováním telekomunikačního provozu*“, když termín „provozní a lokalizační údaje“ právní úprava v době vyhlášení tohoto nálezu ještě nepoužívala. Klíčovým však je, že Ústavní soud ČR nepovažoval tyto údaje pouze za „doprovodné údaje“, jak je mj. ve svém textu označuje i Jan Kudrna, nýbrž přímo za součást telefonické komunikace. Současně konstatuje, že „*Čl. 13 Listiny tedy nezakládá pouze ochranu tajemství vlastního obsahu zpráv, ale i výše uvedených složek*“, a na podporu tohoto svého hodnocení odkazuje na rozsudek ESLP ze dne 2. srpna 1984 ve věci Malone proti Spojenému království a výslovně uvádí, že se s tímto rozsudkem ztotožňuje. Druhý z nálezů Ústavního soudu ČR zmiňovaný ve výše citovaném textu, nález II. ÚS 502/2000, používá ve vztahu k těmto údajům a k jejich podřazení pod ochranu telekomunikačního tajemství dle čl. 13 Listiny totožnou argumentaci. Navíc pak výslovně ochranu dle tohoto článku Listiny vztahuje i na provozní a lokalizační údaje a dodává, že „*Lze tedy konstatovat, že čl. 13 Listiny zakládá i ochranu tajemství volaných čísel a dalších souvisejících údajů, jako je datum a čas hovoru, doba jeho trvání, v případě volání mobilním telefonem i označení základových stanic zajišťujících hovor*“.

Dva výše uvedené nálezy však nejsou jedinými a už vůbec ne ojedinělými rozhodnutími, v nichž se Ústavní soud ČR vyjadřuje k ochraně provozních a lokalizačních údajů v rámci ochrany telekomunikačního tajemství dle čl. 13 Listiny. Kromě nich tak následně činí např. v nálezech sp. zn. IV. ÚS 78/01, sp. zn. I. ÚS 191/05 či sp. zn. II. ÚS

[182] Nález Ústavního soudu ČR sp. zn. II. ÚS 502/2000 ze dne 22. ledna 2001 a nález Ústavního soudu ČR sp. zn. IV. ÚS 536/2000 ze dne 13. února 2001.
[183] Viz § 90 a 91 ZoEK obsahující definici provozních a lokalizačních údajů elektronických komunikací.

789/06[184], v nichž v tomto směru výslovně odkázal na své předchozí nálezy sp. zn. II. ÚS 502/2000 a sp. zn. IV. ÚS 536/2000, kterými je dle vlastního hodnocení v těchto případech vázán, i na již výše uváděný rozsudek ESLP ve věci Malone proti Spojenému království. V Nálezu Pl. ÚS 24/10[185] se Ústavní soud ČR touto otázkou zabýval podrobněji, když předmětem posuzovaným v tomto nálezu byl návrh skupiny poslanců Poslanecké sněmovny Parlamentu ČR na zrušení právní úpravy povinného uchovávání provozních a lokalizačních údajů v § 97 odst. 3 a 4 ZoEK. V odůvodnění tohoto nálezu se navíc Ústavní soud ČR v obecnější rovině vyjádřil k obsahu práva na ochranu soukromí a konstatoval, že „*v Listině uvedený výčet toho, co je třeba podřadit pod „deštník" práva na soukromí, či na soukromý život, nelze považovat za vyčerpávající a konečný. Při výkladu jednotlivých základních práv, která jsou zachycením práva na soukromí v jeho různých dimenzích tak, jak je uvádí Listina, je nezbytné respektovat účel obecně chápaného a dynamicky se vyvíjejícího práva na soukromí jako takového, resp. je třeba uvažovat o právu na soukromý život v jeho dobové celistvosti*".

V tomto nálezu také Ústavní soud ČR podrobněji rozvedl argumentaci vztahující se ke srovnatelnosti zásahu do soukromí v případě zpracování obsahu zpráv se zásahem v podobě získání provozních a lokalizačních údajů. Výslovně zde konstatoval, že „*Ačkoliv se stanovená povinnost uchovávat provozní a lokalizační údaje nevztahuje na obsahy jednotlivých sdělení…, z uvedených údajů o uživatelích, adresátech, přesných časech, datech, místech a formách telekomunikačních spojení, budou-li sledovány po delší časový úsek, lze v jejich kombinaci sestavit detailní informace o společenské nebo politické příslušnosti, jakož i o osobních zálibách, sklonech nebo slabostech jednotlivých osob.*" Na základě tohoto argumentu také výslovně označil názor předkladatele návrhu zákona předestřený ve vyjádření Senátu za „zcela mylný". Konkrétně takto kategoricky hodnotil názor předkladatele, dle kterého „*se "v žádném případě nejedná o něco, co by se dalo přirovnat k odposlechům, už jen proto, že se neuchovávají obsahy jednotlivých telefonátů nebo mailových zpráv*", a vysvětlil, že „*i pouze na jejich základě lze učinit dostatečné obsahové závěry spadající do soukromé (osobnostní) sféry daného jednotlivce*". S odkazem na studii Massachusetts Institute of Technology (MIT), Relationship Inference[186] Ústavní soud ČR upozornil na možnost s velmi vysokou jistotou

[184] Nález Ústavního soudu ČR sp. zn. IV. ÚS 78/01 ze dne 27. srpna 2001, sp. zn. I. ÚS 191/05 ze dne 18. září 2006 a sp. zn. II. ÚS 789/06 ze dne 27. září 2007.
[185] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 24/10[185] ze dne 22. března 2011 (94/2011 Sb.).
[186] Dle odůvodnění citovaného nálezu Ústavního soudu ČR je předmětná studie dostupná z http://reality.media.mit.edu/dyads.php. Na této stránce se však autorovi studii nepodařilo dohledat ani po opakovaných pokusech. Autor však nalezl jiný text relevantní k dané problematice a zveřejněný na webových stránkách MIT, a to text Reality mining: sensing complex social systems autorů Nathan Eagle a Alex (Sandy)

z uchovávaných provozních a lokalizačních údajů dovodit sociální vazby či denní program konkrétní osoby. Na základě těchto argumentů poté Ústavní soud ČR specificky ve vztahu k provozním a lokalizačním údajům formuloval jednoznačný závěr porovnávající význam obsahu komunikace s významem provozních a lokalizačních údajů z hlediska zásahu do práva na ochranu soukromí. Dle tohoto závěru „*Sběr a uchovávání lokalizačních a provozních údajů tak rovněž představuje významný zásah do práva na soukromí, a z toho důvodu je nezbytné pod rozsah ochrany základního práva na respekt k soukromému životu v podobě práva na informační sebeurčení (ve smyslu čl. 10 odst. 3 a čl. 13 Listiny) zahrnout nejen ochranu vlastního obsahu zpráv podávaných prostřednictvím telefonní komunikace či komunikace prostřednictvím tzv. veřejných sítí, ale i provozní a lokalizační údaje o nich*“.

Autor považuje tento závěr nejen za velmi výstižný, nýbrž také za argumentačně podložený a plně se s ním ztotožňuje. Z předestřené argumentace použité v diskutovaném nálezu je totiž zřejmé, že Ústavní soud ČR se zde neomezil pouze na snahu o ryze gramatický výklad čl. 13 Listiny, tedy o pokus zodpovědět otázku, zda ochrana „tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením“ v sobě zahrnuje i něco víc nežli pouhý obsah komunikace. Ústavní soud ČR zde dle autora zkoumal význam této ochrany s přihlédnutím k výše uvedenému závěru vyslovenému v témže nálezu o nutnosti respektovat při výkladu základních práv zakotvujících právo na soukromí účel tohoto práva, je tedy zřejmé, že nejde o pouhou užitečnost zařazení ochrany provozních a lokalizačních údajů pod ochranu telekomunikačního tajemství dle čl. 13 Listiny. Navíc zde Ústavní soud ČR provozní a lokalizační údaje zahrnul nikoli izolovaně do ochrany poskytované buď čl. 10 či čl. 13 Listiny, nýbrž vyvodil ochranu těchto údajů dle obou těchto ustanovení ve vzájemném spojení čl. 10 odst. 3 a čl. 13 Listiny. Ústavní soud ČR se tedy nepokoušel vykládat kterékoli z těchto ustanovení samostatně a volit v případě provozních a lokalizačních údajů mezi ochranou poskytovanou jedním či druhým z nich.

K obdobným závěrům navíc nedospívá pouze Ústavní soud ČR a již uváděný ESLP, nýbrž také např. Spolkový ústavní soud Německa. Na jeho ustálenou rozhodovací praxi Ústavní soud ČR výslovně odkazuje např. právě v nálezu Pl. ÚS 24/10, kde uvádí, že „*obdobný přístup zastává i judikatura zahraničních ústavních soudů*“ a jako konkrétní příklad

---

Pentland publikovaný on-line dne 3. listopadu 2005 nakladatelstvím Springer-Verlag London Limited. Autoři v něm na základě podrobného rozboru dospívají k závěru, dle kterého *„je nevyhnutelné, že mobilní zařízení zítřka budou výkonnější a zároveň zvědavější vůči svému uživateli a jeho kontextu“*. (pozn. přeložil autor). EAGLE, Nathan, PENTLAND, Alex. Reality mining: sensing complex social systems. Massachusetts Institut of Technology. MIT Media Laboratory. Personal and Ubiquitous Computing. Dostupné z https://hd.media.mit.edu/.

uvádí, že „*zmíněný Spolkový ústavní soud SRN prostřednictvím práva na informační sebeurčení garantuje ochranu nejen obsahu předávaných informací, ale chrání i vnější okolnosti, za nichž se uskutečňují - tj. místo, čas, účastníky, druh a způsob komunikace, neboť znalost okolností uskutečněné komunikace může ve spojení s dalšími údaji sama o sobě indikovat samotný obsah komunikace a za pomoci zkoumání těchto údajů a jejich analýzy lze zhotovit individuální profily účastníků dané komunikace [srov. k tomu např. rozhodnutí ze dne 27. 7. 2005, BVerfGE 113, 348 (Vorbeugende Telekommunikationsüberwachung) či ze dne 27. 2. 2008, BVerfGE 120, 274 (Grundrecht auf Computerschutz)]*“[187].

Autorovi jsou známa i další rozhodnutí Spolkového ústavního soudu Německa ve vztahu k provozním a lokalizačním údajům, zejména rozhodnutí ve věcech 1 BvR 256/08, 1 BvR 263/08 a 1 BvR 586/08[188], v němž Spolkový ústavní soud Německa porovnává význam provozních údajů s obsahem komunikace, a to se zcela jednoznačným výsledkem. Údaje o komunikaci jsou dle jeho hodnocení „*z obsahového hlediska nanejvýš přesvědčivé. Přístup k podrobným okolnostem telekomunikace není méně významný nežli přístup k obsahu komunikace. Umožňuje vytvářet komplexní osobnostní a behaviorální profily. Provozní údaje poskytly značné množství informací o sociálních vztazích.*“[189]

Je zřejmé, že když Ústavní soud ČR ve výše citovaném nálezu upozorňoval, že výčet případů, které je nutno podřadit pod právo na soukromí[190], není *„vyčerpávající a konečný“* a konstatoval i nezbytnost vnímat *„dobovou celistvost“* práva na soukromý život, měl tím dle autora na mysli nejen vývoj právní, nýbrž také vývoj faktický, zejména v důsledku vývoje techniky. Technický vývoj je totiž zvláště v oblasti komunikací, zde elektronických komunikací (dříve telekomunikací) faktorem, který značně ovlivňuje právě rozsah provozních a lokalizačních údajů komunikace. Jak však autor ukázal výše, ačkoli v době „telegrafního tajemství“, tedy v době účinnosti zákona o telegrafech[191], nebylo ještě možno hovořit o lokalizačních údajích, přesto již tehdy tento institut v podobě vymezené ve

[187] Rozhodnutí Spolkového ústavního soudu Německa. Bundesverfassungsgericht 1 BvR 668/04. Urteil vom 27. Juli 2005 (Vorbeugende Telekommunikationsüberwachung) a Bundesverfassungsgericht. 1 BvR 370/07, 1 BvR 595/07. Urteil vom 27. Februar 2008 (Grundrecht auf Computerschutz).

[188] Rozhodnutí Spolkového ústavního soudu Německa. Bundesverfassungsgericht 1 BvR 256/08, 1 BvR 263/08 a 1 BvR 586/08. Urteil des Ersten Senats vom 2. März 2010.

[189] V originálním německém znění: „*Die Kommunikationsdaten seien inhaltlich äußerst aussagekräftig. Der Zugriff auf die näheren Umstände der Telekommunikation wiege nicht weniger schwer als der auf den Kommunikationsinhalt. Er ermögliche umfassende Persönlichkeits- und Verhaltensprofile. Verkehrsdaten lieferten eine Vielzahl von Informationen über soziale Beziehungen.“* Pozn. přeloženo autorem.

[190] Viz výše citované odůvodnění nálezu Pl. ÚS 24/10 zmiňující mj. nezbytnost *„respektovat účel obecně chápaného a dynamicky se vyvíjejícího práva na soukromí jako takového, resp. je třeba uvažovat o právu na soukromý život v jeho dobové celistvosti“.*

[191] Zákon č. 60/1923 Sb. o telegrafech, který byl první československou právní úpravou oblasti telekomunikací.

zmiňovaném sektorově specifickém, možno říci technickém, předpise zahrnoval vedle obsahu komunikace i identitu komunikujících stran, dnešní terminologií tedy provozní údaje. Vývoj techniky je zřejmý nejen v rozsahu kategorií provozních a lokalizačních údajů, nýbrž též v otázkách technologie přenosu zpráv, která původně z povahy věci nezahrnovala datový formát ani internetové přenosy. Příkladem budiž ochrana telekomunikačního tajemství obsažená v zákoně o telekomunikacích[192], u níž již v 90. letech 20. století někteří odborníci vyslovili po provedené analýze této úpravy závěr o možné aplikaci této ochrany na prostředí internetu, tehdy nově se rozvíjející[193]. Přestože tyto úvahy nezahrnovaly i rovinu základních práv dle Listiny, autor je přesvědčen, že taktéž ve vztahu k ochraně *„tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením“* dle čl. 13 Listiny by byl i tehdy závěr obdobný.

Právo na informační sebeurčení poprvé formuloval Spolkový ústavní soud Německa v rozhodnutí ve věci sčítání lidu již v roce 1983[194]. Ústavní soud ČR na toto rozhodnutí společně s novějším rozhodnutím Spolkového ústavního soudu Německa ve věci elektronického profilování a vyhledávání (Rasterfahndung) z roku 2006[195], odkazuje v nálezu Pl. ÚS 24/10. Radim Polčák v publikaci Internet a proměny práva připisuje vznik tohoto práva reakci „*na případy, kdy se zásahy do informační diskrece jednotlivce začaly projevovat … jako systémový fenomén se závažnými individuálními i společenskými následky“.* Dle Polčáka bylo postupně *„rozšířeno chápání kategorie soukromí o komplexnější rozměr soukromého života“*[196].

Autor výše zmiňovaná rozhodnutí podrobně analyzoval a ze všech shora uvedených důvodů považuje argumentaci Ústavního soudu ČR i dalších soudů týkající se provozních a lokalizačních údajů jakožto nedílné součásti komunikace a odůvodňující tak jejich ochranu v rámci ochrany telekomunikačního tajemství dle čl. 13 Listiny, spolu s obsahem komunikace, za zcela přiléhavou a plně v tomto směru souhlasí se závěry Ústavního soudu ČR. Autor se v této souvislosti zamýšlel také nad přesnou textací čl. 13 Listiny a nad jejím gramatickým

---

[192] Zákon č. 151/2000 Sb. o telekomunikacích a o změně dalších zákonů, § 84 a násl.
[193] Tento závěr se vztahoval primárně k trestněprávní rovině. Viz SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů.* 1. vydání. Praha : C.H.Beck, 2001, s. 182 - 186, 525 – 526.
[194] Bundesverfassungsgericht – BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83, Rn. 1-215. Spolkový ústavní soud Německa v tomto rozhodnutí právo na informační sebeurčení (das Recht auf "informationelle Selbstbestimmung") vymezil jako *„osobnostní právo na ochranu fyzických osob před neomezeným shromažďováním, uchovávání, používáním a zveřejňováním jejich osobních údajů“*, které v podmínkách moderního zpracování údajů *„zaručuje právo jednotlivce rozhodovat sám o zveřejnění a použití svých osobních údajů“*.
[195] Bundesverfassungsgericht – BVerfG, Urteil des Ersten Senats vom 4. April 2006 - 1 BvR 518/02.
[196] POLČÁK, Radim *Internet a proměny práva*. Praha: Auditorium s.r.o., 2012. s. 324 a násl.

výkladem, když samotný text čl. 13 Listiny nehovoří výslovně o „obsahu“ a ani širší výklad neumožňuje dle hodnocení autora učinit závěr o nutnosti restriktivního výkladu ochrany dle tohoto článku pouze ve vztahu k obsahu komunikace. Text tohoto článku totiž hovoří výslovně o listovním tajemství a *„tajemství jiných písemností a záznamů“*, resp. o „*tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením*“. Závěr, dle kterého by „tajemstvím zpráv“ byl pouze samotný obsah zpráv a nikoli též jejich další aspekty a okolnosti, vč. identity komunikujících stran, nelze dle autora opřít ani o vymezení obsažené ve zvláštním právním předpise, tedy v ZoEK, obdobně tentýž závěr platí též ve vztahu k předchozím právním předpisům upravujícím na území dnešní ČR obdobné právní instituty v elektronických komunikacích, telekomunikacích či dříve telefonii a telegrafii[197].

Autor proto na základě této argumentace nepovažuje podřazení provozních a lokalizačních údajů elektronických komunikací pod ochranu poskytovanou čl. 13 Listiny za nepodložené, zvláště jedná-li se o ochranu odkazovanou na články 10 a 13 Listiny, vykládané ve vzájemné spojitosti. Autor se zcela neztotožňuje ani s hodnocením Jana Kudrny v citovaném textu o pouhé „užitečnosti“ takového zařazení jako o důvodu, pro který Ústavní soud ČR rozhodl (resp. přesněji konstantně rozhoduje) výše uvedeným způsobem. To vše platí dle autora tím spíše, že tento výklad Ústavního soudu ČR se nikterak neodklání od rozhodovací praxe jiných soudů v členských státech EU či též ESLP, naopak, tyto soudy zastávají zcela obdobná stanoviska a Ústavní soud ČR proto ve svých nálezech na jejich závěry výslovně odkazuje. Především však je nutno zdůraznit již výše uvedený závěr Ústavního soudu ČR vykládající ustanovení čl. 10 odst. 3 a čl. 13 Listiny ve vzájemné spojitosti.

Současně však autor považuje za nutné hodnotit myšlenku správnosti či vhodnosti zařazení ochrany provozních a lokalizačních údajů pod ochranu dle čl. 13 Listiny či do režimu obecnější ochrany soukromí obsažené v čl. 10 Listiny též v širším kontextu. V této souvislosti si autor je vědom toho, že otázka správnosti zařazení ochrany provozních a lokalizačních údajů jako součásti tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením, tedy telekomunikačního tajemství[198] dle čl. 13 Listiny či spíše zařazení pod

[197] Viz UŘIČAŘ, Miroslav. Telekomunikační tajemství. In: SCHELLE, Karel, TAUCHEN, Jaromír (eds). *Encyklopedie českých právních dějin. XVIII. svazek Ta-Ty*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2019 v koedici s Ostrava: KEY Publishing s.r.o. 2019.

[198] Autor v této souvislosti považuje za potřebné upozornit na určitý pojmový rozdíl mezi textem Listiny na straně jedné a textem zvláštního právního předpisu – zákona o elektronických komunikacích na straně druhé. Zatímco Listina setrvala v čl. 13 u terminologie omezující se na „*tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením*“, její text tedy v souvislosti s předmětem ochrany výslovně zmiňuje pouze zprávy, nikoli jakékoli další informace, zákon o elektronických komunikacích opustil předchozí termín „telekomunikační tajemství“, používaný v právních předpisech upravujících oblast elektronických komunikací do té doby, včetně

obecnou ochranu soukromí dle čl. 10 Listiny se může jevit jako spíše teoretická. Dle autora však právě v souvislosti s tématem této práce je daná otázka velmi relevantní. Je totiž zřejmé, že ochrana takovýchto informací jako součásti telekomunikačního tajemství, resp. důvěrnosti komunikace, připadá do úvahy (bez ohledu na finální názor o správnosti takového zařazení) pouze v případě, že se informace týkají elektronických komunikací, tedy služeb poskytovaných prostřednictvím sítě elektronických komunikací.

Jak však autor ukazuje dále, vyskytují se obdobné a z hlediska intenzity zásahu do soukromí srovnatelně závažné údaje, zahrnující mj. i lokalizační údaje, nikoli zřídka taktéž mimo oblast elektronických komunikací. Takto je tomu u lokalizačních údajů např. v souvislosti s údaji o transakcích provedených platební kartou či jiným platebním prostředkem, kdy je při fyzickém („off-line“) použití platebního prostředku k transakci zaznamenána, vedle údaje o částce transakce, i přesná lokalita a čas použití platebního prostředku; tyto údaje vypovídají o pravděpodobném osobním výskytu uživatele platebního prostředku v daném místě. Obdobně je nutno zvažovat ochranu lokalizačních údajů v případě informací zaznamenávaných systémy v automobilech, zejména zařízením eCall nebo v případě kamerových systémů dopravních kamer zaznamenávajících konkrétní vozidla a jejich státní poznávací značky ve spojení s přesným časem průjezdu vozidla, v některých případech vč. zaznamenání fotografie osoby řidiče a případně též osoby na místě spolujezdce. O lokalizační údaje vypovídající o konkrétní lokalitě dané osoby jde též v případě údajů jmenné evidence cestujících v letecké dopravě, zde navíc i ve spojení s lokalizačními údaji dalších osob cestujících stejným letem. Dalším příkladem může být u elektronických dálničních známek systém kontroly „úhrady časového poplatku za užití pozemní komunikace“, který rovněž zaznamenává pravděpodobnou lokalitu a čas výskytu konkrétní fyzické osoby.

Dle autora je zřejmé, že, na rozdíl od lokalizačních údajů elektronických komunikací, tyto odlišné lokalizační údaje – pro zjednodušení je autor dále bude označovat jako „netelekomunikační lokalizační údaje“ - dost dobře nelze podřadit pod ochranu poskytovanou čl. 13 Listiny. V těchto případech totiž lokalizační údaje existují samostatně, bez vazby na cokoli, co by bylo možno označit jako „obsah komunikace“. Nejedná se tedy o údaje, u nichž by bylo možno dovodit jakoukoli spojitost s tajemstvím zpráv podávaných

---

předchozího právního předpisu - zákona č. 151/2000 Sb. o telekomunikacích a o změně dalších zákonů, a místo tohoto termínu používá obecnější termín „důvěrnost komunikací“. V § 89 odst. 1 je pak tento termín upřesněn, když zákon zde ukládá podnikatelům povinnost zajistit „*důvěrnost zpráv a s nimi spojených provozních a lokalizačních údajů*“.

telefonem, telegrafem nebo jiným podobným zařízením. Např. posledně zmiňovaná technická zařízení určená ke kontrole „úhrady časového poplatku za užití pozemní komunikace“ a tvořící příslušenství dálnice, silnice a místní komunikace nelze zcela jistě považovat ani za jiná zařízení podobná telefonu či telegrafu ve smyslu čl. 13 Listiny, zejména proto, že taková zařízení neslouží k přenosu zpráv. V tomto, jakož i v dalších případech, se tedy zařazení ochrany zde generovaných lokalizačních údajů týkajících se konkrétní osoby jakožto součásti telekomunikačního tajemství dle čl. 13 Listiny nejeví jako správné a ani možné. Je tak plně namístě uvažovat o podřazení takových lokalizačních údajů pod obecnou ochranu soukromí dle čl. 10 Listiny. V této souvislosti je však relevantní otázka, zda je z hlediska systematiky Listiny a také v zájmu právní jistoty adresátů právní normy – dotčených subjektů údajů i povinných osob – odůvodnitelné, aby údaje udávající zeměpisnou polohu fyzické osoby, tedy osobní údaje ve formě lokalizačních údajů, požívaly ochrany buď dle čl. 13 či dle čl. 10 Listiny v závislosti na tom, zda jde o lokalizační údaje elektronických komunikací či o lokalizační údaje jiných oblastí – údaje netelekomunikační. Rozdíl mezi těmito skupinami údajů nespočívá totiž v jejich podstatě (tou je vždy zeměpisná poloha konkrétní fyzické osoby), nýbrž pouze ve způsobu jejich generování.

Autor očekává, že tato otázka může být do budoucna předmětem dalších diskusí a polemik, zvláště s ohledem na faktický vývoj, v jehož rámci autor předpokládá nárůst významu lokalizačních údajů vznikajících v jiných oblastech nežli v sítích a službách elektronických komunikací. Dle autora nelze vyloučit posun rozhodovací praxe ve prospěch názoru prezentovaného výše Janem Kudrnou. Jako plně odpovídající nejen potřebám praxe, nýbrž rovněž souladné s textem diskutovaných článků Listiny však autor považuje řešení tohoto problému dle pojetí předestřeného výše, v návaznosti na citovaný nález Ústavního soudu ČR. Toto pojetí dle hodnocení autora umožňuje zahrnutí ochrany provozních a lokalizačních údajů, bez ohledu na jejich souvislost se sítěmi a službami elektronických komunikací či s odlišnými oblastmi, pod ochranu dle čl. 10 Listiny, případně – u údajů elektronických komunikací – ve spojení s čl. 13 Listiny. Zatím však tato otázka nebyla v rozhodovací praxi uspokojivě vyřešena.

Za významný faktor autor považuje též odlišnost v délce vývoje samotné existence lokalizační údajů elektronických komunikací a většiny případů lokalizační údajů jiných, „netelekomunikačních“. Zatímco rozhodovací praxe v oblasti provozních a lokalizačních údajů elektronických komunikací se vyvíjela již řadu let (a dále se vyvíjí), rozhodovací praxe soudů a dozorových orgánů ochrany osobních údajů ve vztahu k lokalizačním údajům

netelekomunikačním je stále nová a také její vývoj se nezdá být završen, jak autor rozebírá dále, u jednotlivých v této práci rozebíraných dalších zásahů do soukromí. V této souvislosti lze z relevantních rozhodnutí zmínit zatím pouze rozhodování soudů, včetně Ústavního soudu ČR ve věci využití záznamů dopravních kamerových systémů v případech konkrétní fyzické osoby pro účely řízení vedeného správcem daně[199]. Obě ustanovení – čl. 10 i čl. 13 Listiny jsou v rámci systematiky Listiny zahrnuty do Hlavy druhé, oddílu prvního Základní lidská práva a svobody. Článek 13 připouští výslovně omezení zde upravených práv zákonem (*„s výjimkou případů a způsobem, které stanoví zákon“*), aniž by přitom vymezil další podmínky. Oproti tomu článek 10 takovéto výslovně připuštěné omezení neobsahuje. V tomto směru je však relevantní možnost tzv. imanentních omezení, která plynou přímo z ústavního pořádku.

Nad rámec výše uvedeného autor považuje za nutné stručně se vyjádřit také k již výše zmiňovanému označení provozních a lokalizačních údajů jako „doprovodné údaje", neboť tohoto označení užívá ve svém výše diskutovaném textu mj. též Jan Kudrna. Autor použití tohoto označení v dané souvislosti vnímá jako problematické a zcela se s ním neztotožňuje, byť má z obsahu uvedeného textu za to, že k použití označení „doprovodné údaje“ v něm došlo spíše náhodně a pisatel jeho použitím nesledoval konkrétní cíl. Autorovi je z jeho praxe známo, že tento termín bývá v některých případech používán v odborných právních textech i v současné době, navzdory již zmiňovanému vymezení „provozních údajů“ v ZoEK. Použití termínu „doprovodné údaje“ dle zkušeností autora bývá v praxi mnohdy vedeno záměrem určité bagatelizace významu těchto údajů a tedy i intenzity zásahu do soukromí představovaného jejich zpracováním, v porovnání se samotným obsahem komunikace, a to přestože ustálená rozhodovací praxe, vč. rozhodnutí Ústavního soudu ČR či SDEU, přikládá zpracování provozních údajů jednoznačně zásadní význam z hlediska dopadu do soukromí jednotlivce, plně srovnatelný se zpracováním informací o obsahu komunikace. S ohledem na celkový kontext diskutovaného textu a jeho závěry však dle autorova hodnocení Kudrna naopak ve svém textu zdůrazňuje závažnost zásahu do práva na ochranu soukromí v podobě plošného zpracování provozních a lokalizačních údajů, jeho cílem tak jistě není bagatelizace zpracování takovýchto údajů.

Jak autor ukázal výše, u hodnocení zpracování provozních a lokalizačních údajů jako zásahu do práva na ochranu soukromí se nejedná pouze o izolovaný výklad Ústavního soudu ČR, jde mj. též o konstantní rozhodovací praxi Spolkového ústavního soudu Německa.

[199] Viz nález Ústavního soudu ČR sp. zn. IV.ÚS 2621/22 ze dne 14.2.2023, autor tento případ rozebírá podrobně dále, v kapitole věnující se zpracováním údajů systémy dopravních kamer.

Dle hodnocení autora lze tyto závěry obdobně vztáhnout též na některé další případy shromažďování osobních údajů zahrnujících i lokalizační údaje, byť nikoli vždy nutně ve spojení s obsahem komunikace, nýbrž s možností vyhotovení individuálního profilu jednotlivce. Autor má za to, že takto např. ze shromážděných údajů z dopravních kamerových systémů na silnicích a dálnicích (ať již původně určených k měření rychlosti či ke kontrole úhrady dálničních známek) lze na základě identifikace vozidla dle státní poznávací značky v mnoha případech s relativně vysokou pravděpodobností ztotožnit osobu řidiče (a jak rozebráno dále v této práci, případně též spolujezdce) a na základě porovnání s jednotlivými údaji zachycujícími totéž vozidlo v různých místech či naopak v témže místě v různých časech lze pak vytvořit profil dané osoby, zahrnující její cestovní návyky a další související okolnosti, jako např. pravděpodobný pracovní profil či profil soukromých cest, její spojení s dalšími osobami, a to včetně predikce dalšího pravděpodobného pohybu konkrétní osoby v budoucnu. Autor se tímto zabývá podrobněji dále v kapitole analyzující zpracování údajů systémy dopravních kamer. Závěry, které k problému možného vyhotovení individuálního profilu jednotlivce formuloval Ústavní soud ČR v nálezu Pl. ÚS 24/10, lze dle hodnocení autora do určité míry zobecnit a vztáhnout i na případy „netelekomunikačních" lokalizačních údajů.

2.3 Veřejný zájem sledovaný ve zkoumaných případech, řešení jeho kolize se základními právy a svobodami

Základní práva a svobody nejsou neomezitelná, mohou být omezena pouze zákonem, *„přičemž musí být šetřeno jejich podstaty a smyslu, a to ze dvou důvodů: 1. když je to nezbytné pro výkon jiných práv, 2. z důvodu veřejného zájmu"*, jak uvádí Aleš Gerloch[200]. Ve zkoumaných případech, tedy v případech plošného zpracování osobních údajů značného množství osob, přichází zpravidla do úvahy pouze druhá z možností, tedy omezení základních práv a svobod či zásah do nich z důvodu veřejného zájmu.

Každé zpracování osobních údajů prováděné orgány veřejné moci na základě vymezení obsaženého v jednotlivých právních předpisech zakládajících tato zpracování musí sledovat konkrétní veřejný zájem specifikovaný v těchto právních předpisech. Takový veřejný zájem by měl být účelem daného zpracování. Dle Aleše Gerlocha musí být veřejný zájem „*specifikován a při omezení určitého subjektivního práva musí být dodrženy zákonem stanovené postupy*", platí však také, že důležitou je „*možnost reálné soudní ochrany*"[201].

[200] GERLOCH, Aleš. *Teorie práva, 8. vyd.* Plzeň: Aleš Čeněk, 2021. s. 226.
[201] GERLOCH, Aleš. *Teorie práva, 8. vyd.* Plzeň: Aleš Čeněk, 2021. s. 275.

Právní předpis ukládající povinnost zpracování osobních údajů by také měl vymezit konkrétní cíle, jejichž dosažení zpracování sleduje, a vedle toho též prostředky zpracování. Veřejné zájmy v každém konkrétním případě musejí být natolik závažné, aby odůvodnily zásah do soukromí, ke kterému při zpracování osobních údajů dochází. Tento závěr platí zvláště v případech plošného zpracování osobních údajů značného množství subjektů údajů. Současně musejí být jednotlivá zpracování v těchto předpisech vymezena tak, aby k naplnění stanoveného účelu a dosažení sledovaného veřejného zájmu byly vždy použity prostředky co nejšetrnější k právům a právem chráněným zájmům dotčených osob, včetně vymezených kategorií osobních údajů, které mají být takto zpracovávány. Aleš Gerloch obecně konstatuje, že „*Základní práva a svobody jsou sice nezadatelné, nezcizitelné, nepromlčitelné a nezrušitelné, avšak lze je (až na výjimky) za podmínek stanovených čl. 4 odst. 2-4 omezit*“ a dodává, že Listina vychází z modelu, dle kterého „*východiskem jsou subjektivní práva, nejdůležitější z nich jsou nezadatelná. Protože lidé mají práva, musí jim korespondovat i povinnosti*“[202].

2.3.1 Veřejný zájem odůvodňující omezení základních práv a svobod

Konkrétním veřejným zájmům vymezeným vždy pro konkrétní zkoumané zpracování se autor věnuje dále, v souvislosti s rozborem jednotlivých zpracování. V obecné rovině tyto veřejné zájmy v některých, nejzávažnějších případech odpovídají vymezení obsaženému v čl. 1 odst. 1 Trestněprávní směrnice, jedná se tedy v takových případech nejčastěji o prevenci, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení. Toto však platí pouze pro některé zkoumané případy, když je zřejmé, že ne všechna dále rozebíraná zpracování takovýto účel sledují, ačkoli z hlediska míry zásahu do soukromí jsou srovnatelná s jinými případy zde diskutovaných zpracování a vyznačují se též plošným a nerozlišujícím charakterem. Takto například zpracování založené nařízením eCall sleduje účel vymezený poněkud vágně jako „*další zlepšení bezpečnosti silničního provozu*“[203], účelem uvedeným u zpracování v rámci systému elektronických dálničních známek je kontrola úhrady *„časového poplatku za užití pozemní komunikace“,* resp. *„zvýšení efektivity kontroly úhrady časového*

[202] GERLOCH Aleš. Relace práv a povinností v Listině základních práv a svobod in GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012 s. 17.
[203] Viz bod 4 recitálu Nařízení eCall ve spojení se Sdělením Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů „Systém eCall: čas jej zavést“ ze 21. srpna 2009. CELEX_52009DC0434.

poplatku"[204] apod.*;* podrobnostmi se autor zabývá v tomto textu dále, na tomto místě daná zpracování slouží pouze jako příklad. Vždy by však mělo platit, že závažnost sledovaného účelu je přímo úměrná míře dopadu daného zpracování do soukromí osob, vč. množství osob-subjektů údajů dotčených takovým zpracováním.

Z dostupné relevantní judikatury týkající se vymezení veřejného zájmu sledovaného v případech zásahu do práva na ochranu soukromí lze uvést zejména nález Ústavního soudu ČR sp. zn. II. ÚS 502/2000[205]. V něm se Ústavní soud ČR vyjádřil k možnosti prolomení „práva na ochranu tajemství zpráv podávaných telefonem" v případě využití provozních údajů pro účely vyšetřování trestného činu. Ústavní soud ČR formuloval závěr, dle kterého „*ústavní pořádek České republiky připouští průlom této ochrany, děje se tak pouze a výlučně v zájmu ochrany demokratické společnosti, případně v zájmu ústavně zaručených základních práv a svobod jiných; sem spadá především nezbytnost daná obecným zájmem na ochraně společnosti před trestnými činy a dále tím, aby takové činy byly zjištěny a potrestány*". V témže nálezu Ústavní soud ČR vymezil také ústavněprávní požadavky na takovýto průlom do základního práva nebo svobody, jakým je výše uvedené právo na ochranu tajemství zpráv podávaných telefonem, vč. provozních údajů, jakožto součásti ochrany dle tohoto institutu. Dle Ústavního soudu ČR je v prvé řadě nutno, aby byl splněn požadavek na nezbytnost takového zásahu, který zahrnuje rovněž zákaz překročení mezí nezbytnosti. Tento požadavek však není jediným, dle závěrů formulovaných Ústavním soudem ČR v diskutovaném nálezu musí dále také existovat „*systém adekvátních a dostatečných záruk*". Ten tvoří jednak odpovídající právní předpisy a společně s nimi i účinná kontrola jejich dodržování.

Jako příklad jednoho z nejzávažnějších ústavněprávně chráněných veřejných statků lze uvést nález III. ÚS 256/01[206]. V něm Ústavní soud ČR mezi takové statky zařadil mj i „*úsilí o zajištění vnitřního míru ve společnosti, spočívající v náležitém objasnění trestných činů a spravedlivém potrestání jejich pachatelů v rámci řádného procesu, jež se promítá v rovině ústavní*". Jedná se o ustálený závěr Ústavního soudu ČR, dle kterého podstatou ústavně aprobovatelného veřejného zájmu na stíhání trestných činů a spravedlivém potrestání jejich pachatelů je „*přenesení odpovědnosti za postihování nejzávažnějších porušování základních práv a svobod fyzickými a právnickými osobami na stát*"[207]. Samotná skutečnost, že určitý veřejný zájem je ústavně aprobovatelný, však bez dalšího neznamená, že jakýkoli

[204] Viz § 21c odst. 7 zákona č. 13/1997 Sb. o pozemních komunikacích, ve znění pozdějších předpisů.
[205] Nález Ústavního soudu ČR sp. zn. II. ÚS 502/2000 ze 22. ledna 2001.
[206] Nález Ústavního soudu ČR sp. zn. III ÚS 256/01 ze 21. března 2002.
[207] Viz nález Ústavního soudu sp. zn. ČR Pl. ÚS 24/10 ze dne 22. března 2011.

zásah do základních práv a svobod jednotlivce vedený k naplnění takovéhoto veřejného zájmu je v souladu s ústavními principy. Taktéž při využívání nástrojů umožňujících stíhání trestných činů a potrestání pachatelů je nezbytné respektovat ústavněprávní limity.

2.3.2 Ústavněprávní požadavky na právní úpravu zakládající omezení základních práv a svobod

Jak Ústavní soud ČR opakovaně zdůraznil, podmínkou „*omezení osobní integrity a soukromí osob*“, tedy „*prolomení respektu k nim*“ ze strany veřejné moci je výjimečný charakter takového zásahu, za podmínky, že 1. je to „*v demokratické společnosti nezbytné*“, 2. účelu sledovaného veřejným zájmem nelze dosáhnout jinak a současně 3. je to „*akceptovatelné z pohledu zákonné existence a dodržení účinných a konkrétních záruk proti libovůli*“. Jednotlivec totiž dle závěrů Ústavního soudu ČR obsažených v nálezu Pl. ÚS 24/10 musí být vybaven „*dostatečnými garancemi a zárukami proti možnému zneužití pravomoci ze strany veřejné moci*“, jak to vyžadují „*esenciální předpoklady spravedlivého procesu*“. Mezi takovéto záruky Ústavní soud ČR řadí odpovídající právní úpravu a současně také existenci účinné kontroly jejího dodržování, jde zde především o kontrolu „*těch nejintenzivnějších zásahů do základních práv a svobod jednotlivců nezávislým a nestranným soudem*“.

Předmětná právní úprava pak dle Ústavního soudu ČR musí „*především odpovídat nárokům plynoucím z principu právního státu*“ a také musí splňovat „*požadavky vyplývající z testu proporcionality*“, jak Ústavní soud ČR opakovaně zdůraznil ve svých závěrech formulovaných v nálezech týkajících se přípustnosti zásahu veřejné moci do soukromí[208]. Dále též musí být taková právní úprava dle závěrů Ústavního soudu ČR formulována přesně a zřetelně, současně je také nezbytné, aby byla dostatečně předvídatelná. Požadavek předvídatelnosti je veden nutností poskytnout potenciálně dotčeným jednotlivcům „*dostatečnou informaci o okolnostech a podmínkách, za kterých je veřejná moc oprávněna k zásahu do jejich soukromí, aby případně mohli upravit své chování tak, aby se nedostali do konfliktu s omezující normou*“. Konečně musí takováto právní úprava dle požadavků Ústavního soudu ČR striktně definovat „*pravomoci udělené příslušným orgánům*“, včetně způsobu a pravidel jejich provádění, „*aby jednotlivcům byla poskytnuta ochrana proti svévolnému zasahování*“[209]. V rámci přezkumu ústavnosti Ústavní soud ČR rozpracoval

[208] V nálezu sp. zn. Pl. ÚS 24/10 Ústavní soud ČR odkazuje na své předchozí nálezy týkající se odposlechu telekomunikačního provozu, konkrétně nálezy sp. zn. II. ÚS 502/2000, sp. zn. IV. ÚS 78/01, sp. zn. I. ÚS 191/05 či sp. zn. I. ÚS 3038/07 ze dne 29. 2. 2008.
[209] Viz nález Ústavního soudu ČR sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011.

principy materiálního právního státu, které při takovém přezkumu uplatňuje. Tyto principy zahrnují mimo jiné *„zákaz přepjatého formalismu či princip hodnotově orientovaného výkladu jednoduchého práva“*[210] a další[211].

Výše uvedenou záruku v podobě soudní kontroly označil Ústavní soud ČR v nálezu Pl. ÚS 24/10 za *„nezbytný požadavek soudní ochrany základních práv“*, který se *„v případě užití trestněprávních nástrojů omezujících základní práva a svobody jednotlivce projevuje zejména ve vydání soudního příkazu a v jeho dostatečném odůvodnění“*, jež přitom musí odpovídat *„jak požadavkům zákona, tak především ústavním principům, z nichž zákonné ustanovení vychází, resp. které zpětně limitují jeho interpretaci“*, a to z toho důvodu, že *„aplikace takového ustanovení představuje zvlášť závažný zásah do základních práv a svobod každého jednotlivce“*. Podmínky umožňující zásah do základního práva na soukromí z důvodu ochrany před trestnou činností jsou v nálezech Ústavního soudu ČR vyjádřeny *„zřetelně a ustáleně“*, jak tento soud konstatuje v nálezu I.ÚS 3038/07[212]. V tomto nálezu se Ústavní soud ČR zabýval porušením práv vyplývajících z institutu telekomunikačního tajemství, jako součásti práva na ochranu soukromí vymezeného čl. 13 Listiny. Porušení tajemství zpráv vyhodnotil jako možné *„jen v případech a způsobem stanoveným zákonem“*, pro soudní příkaz k odposlechu a záznamu telekomunikačního provozu platí, že může být vydán *„jen v řádně zahájeném trestním řízení pro zákonem kvalifikovanou trestnou činnost a musí být podložen relevantními indiciemi, z nichž lze dovodit důvodné podezření ze spáchání takového trestného činu“*, příkaz musí také *„být individualizován ve vztahu ke konkrétní osobě, která je uživatelem telefonní stanice“* a musí *„alespoň v minimální míře konkrétně uvést, jaké skutečnosti významné pro trestní řízení mají být takto zjištěny a z čeho je to vyvozováno“*, jak Ústavní soud ČR uvedl již v nálezu II. ÚS 615/06[213]. Na tuto svou judikaturu týkající se především odposlechu telekomunikačního provozu proto Ústavní soud ČR výslovně odkazuje též v nálezu Pl. ÚS 24/10, na závěry této judikatury zde navazuje a dále je rozvíjí ve vztahu k vyžádání provozních a lokalizačních údajů uchovávaných v rámci povinnosti Data Retention, tedy slovy trestního řádu ke *„zjištění údajů o telekomunikačním provozu“*.

---

[210] Viz HOFMANNOVÁ, Helena. 5. K pojetí lidských práv v judikatuře Ústavního soudu České republiky in GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012 s. 57 a násl.

[211] K přezkumu ústavnosti, omezením základních práv a k posuzování proporcionality srov. též BARAK, Aharon. *Proportionality. Constitutional Rights and their Limitations.* Cambridge: Cambridge University Press, 2012.

[212] Nález Ústavního soudu ČR sp. zn. I.ÚS 3038/07 ze dne 29. února 2008.

[213] Nález Ústavního soudu ČR sp. zn. II. ÚS 615/06 ze dne 23. května 2007.

Ústavní soud ČR současně tyto své závěry obsažené v diskutovaném nálezu Pl. ÚS 24/10 opírá o dlouhodobou a ustálenou rozhodovací praxi ESLP[214], částečně již rozebíranou výše. Jde zejména závěry o nutnosti posoudit soulad se zákonem u tvrzeného zásahu do práva na soukromí ze strany veřejné moci, vč. nutnosti posoudit, zda takový zákon byl „*dostupný a dostatečně předvídatelný, tedy vyjádřený s velkou mírou přesnosti*“, zda daný zákon poskytuje „*přiměřenou ochranu proti svévoli*“ a zda dostatečně vymezuje „*rozsah a způsob výkonu pravomocí svěřených kompetentním orgánům*“ a také, zda úkony, kterými je zasahováno do základního práva na soukromý život, nejsou „*mimo jakoukoli bezprostřední (preventivní či následnou) soudní kontrolu*“.

Ústavní soud ČR zde upozorňuje na to, že ESLP ve své judikatuře k zásahům veřejné moci do soukromí *„zdůraznil, že je předně nutné vymezit jasná a detailní pravidla upravující rozsah a použití takových opatření, stanovit minimální požadavky na délku, způsob uložení získaných informací a údajů, jejich použití, přístup třetích osob k nim, a zakotvit procedury vedoucí k ochraně celistvosti a důvěrnosti údajů a rovněž k jejich ničení, a to způsobem, aby jednotlivci disponovali dostatečnými zárukami proti riziku jejich zneužití a svévole“*. V souladu se závěry ESLP i dle hodnocení Ústavního soudu ČR přitom navíc význam těchto záruk narůstá v případech, kdy *„se jedná o ochranu osobních údajů podrobených automatickému zpracování, zejména pokud jsou tyto údaje využívané k policejním cílům a v situaci, kdy se dostupné technologie stávají stále komplikovanějšími“*.

Právě tyto závěry zdůrazňující potřebu zákonných záruk zvláště proti možnému zneužití autor považuje za velmi relevantní především v případech, které jsou předmětem této práce. Jednotlivé autorem popisované situace plošného shromažďování osobních údajů a jejich zpracování buď přímo orgány veřejné moci či sice jinými osobami, avšak pro jejich následné možné vyžádání a využití ze strany orgánů veřejné moci, totiž dle hodnocení autora zpravidla splňují právě kritérium automatického zpracování dle výše citované dikce Ústavního soudu ČR, jakož i kritérium využití komplexních technologií při daných zpracováních – viz např. zpracování provozních a lokalizačních údajů elektronických komunikací, zpracování údajů leteckých cestujících či údajů dopravních kamerových systémů na silnicích a dálnicích, jak je autor podrobně rozebírá dále. Při posuzování zásahu do základního práva na ochranu soukromí je navíc v souladu s hodnocením Ústavního soudu ČR nutno brát v úvahu jako

[214] Konkrétně Ústavní soud ČR odkazuje na rozhodnutí ESLP ve věcech Malone proti UK, Amann proti Švýcarsku či Rotaru proti Rumunsku a také rozhodnutí ESLP ve věci Hassan a Tchaouch proti Bulharsku (no. 30985/96, 39023/97) ze dne 26. 10. 2000 a dále též Kruslin proti Francii či S. a Marper proti UK či též Camenzind proti Švýcarsku (no. 21353/93) ze dne 16. 12. 1997.

významný faktor také intenzitu zásahu. Tu Ústavní soud ČR v případě zákonné povinnosti uchovávat provozní a lokalizační údaje účastníků a uživatelů elektronických komunikací v nálezu Pl. ÚS 24/10 hodnotil jako zdůrazněnou tím, že „*se dotýká obrovského a nepředvídatelného počtu účastníků komunikace, neboť se jedná o plošný a preventivní sběr a uchovávání předmětných údajů*“. Proto zde bylo dle Ústavního soudu ČR nutno uplatňovat co nejpřísnější měřítka na splnění všech požadavků, které autor rozvádí výše.

V posuzovaném případě však Ústavní soud ČR shledal rozpor posuzované zákonné právní úpravy s těmito požadavky v otázce vymezení orgánů oprávněných k vyžádání údajů, v nedostatečném vymezení účelu využití údajů a v neexistenci povinnosti následné informovanosti dotčené osoby. Danou úpravu proto považoval za nedostatečně splňující požadavek předvídatelnosti, jak autor podrobně rozebírá dále, v kapitole věnující se zásahu v podobě povinného uchovávání provozních a lokalizačních údajů. Na tomto místě, v rámci obecného rozboru záruk proti zneužití institutu, který představuje zásah do základního práva, je dle autora zapotřebí dodat, že Ústavní soud ČR hodnotil v daném případě jako nedostatečné též vymezení odpovědnosti a případných sankcí za porušení těch povinností, které právní úprava, jakkoli v nedostatečné míře, obsahuje.

Výše uvedené závěry formulované Ústavním soudem ČR se týkají plošného a preventivního sběru a uchovávání údajů. Dle autora je však možno je zobecnit a obdobné požadavky na zákonné záruky proti možnému zneužití vztáhnout i na jiné případy, nežli představuje pouze povinné zpracování provozních a lokalizačních údajů, které bylo předmětem posuzování v nálezu Pl. ÚS 24/10. Podmínkou je, aby tyto jiné případy splňovaly kritérium srovnatelné intenzity zásahu, ve spojení s výše zmiňovanými kritérii automatického zpracování a využití komplexních technologií při zpracování dotčených osobních údajů. Autor proto považuje za nutné a plně odůvodnitelné vztáhnout obdobné požadavky na záruky bránící možnému zneužití i ve vztahu k některým z dalších případů zásahů do práva na ochranu soukromí, které rozebírá v této práci, byť stále platí, že povinnost Data Retention se z hlediska množství dotčených fyzických osob i množství zpracovávaných údajů a celkové intenzity zásahu bezesporu řadí mezi zásahy do práva na ochranu soukromí na čelné místo.

Ve vztahu k právu na ochranu soukromí je zásadním i to, že ESLP vykládá pojem „soukromý život“ extenzivně, jak na to poukázal Ústavní soud ČR např. v nálezu Pl. ÚS 3/14, s odkazem na rozhodnutí ESLP ve věci Amann proti Švýcarsku[215], přičemž takovýto

[215] Rozsudek ESLP ve věci Amann proti Švýcarsku (no. 27798/95) ze dne 16. 2. 2000.

extenzivní výklad „*je ve shodě s Úmluvou o ochraně osob se zřetelem na automatizované zpracování osobních dat*“. V souvislosti s tím pak ESLP naopak vykládá restriktivně „*výjimky ze zákazu státních zásahů do práva na soukromý život*“, které jsou „*nezbytné v demokratické společnosti a v souladu se zákonem z titulu vypočtených hodnot veřejného zájmu nebo ochrany práv a svobod jiných*“. Ústavní soud ČR navíc v této souvislosti zdůrazňuje význam soudní kontroly v případě zásahu do práva na soukromý život ze strany moci veřejné a v nálezu Pl. ÚS 3/14 dodává, taktéž s odkazem na rozhodovací praxi ESLP (zde konkrétně rozhodnutí ve věci Camenzind proti Švýcarsku[216]), že úkony veřejné moci, které představují takovýto zásah, se „*nesmí ocitnout mimo jakoukoli bezprostřední (preventivní či následnou) soudní kontrolu*“.

V souladu s hodnocením Ústavního soudu ČR spatřuje autor v případě zásahu do práva na ochranu soukromí značný rozdíl mezi preventivní soudní kontrolou zásahu samotného a kontrolou následnou. Liší se zejména vliv a faktický dopad mechanismů soudní kontroly na takovéto zásahy. Soudní kontrola samotného zásahu, tedy kontrola v podobě zapojení soudu ještě před samotným zásahem, zpravidla v podobě soudního povolení zásahu či přímo jeho nařízení, je totiž způsobilá zásah odvrátit a vůbec jej nepřipustit, dospěje-li soud k závěru, že v konkrétním případě nejsou splněny podmínky pro přípustnost zásahu, takovou soudní kontrolu lze označit za preventivní mechanismus. Některé takovéto mechanismy soudní kontroly existují i v platné právní úpravě, jak autor uvádí dále, u rozboru konkrétních případů zásahů do práva na ochranu soukromí[217]. Současně však v této souvislosti nelze opomenout, že takováto soudní kontrola je způsobilá odvrátit pouze následný zásah spočívající ve vyžádání a využití vyžádaných údajů, nikoli zásah v podobě samotného plošného shromažďování osobních údajů pro jejich možné následné využití. Oproti tomu následná soudní kontrola, ke které dochází až poté, co zásah do soukromí nastane, je limitována pouze na případné vyslovení porušení zákona soudem, to však u porušení, ke kterému již došlo[218]. Významným faktorem je dle hodnocení autora také to, že následná soudní kontrola je zpravidla omezena pouze na případy, v nichž dotčená osoba iniciuje zahájení soudní kontroly, ať již ve formě návrhu či podnětu k zahájení soudního řízení. V praxi jde pouze o malé

[216] Rozsudek ESLP ve věci Camenzind proti Švýcarsku (no. 21353/93) ze dne 16. 12. 1997.

[217] Příkladem preventivní soudní kontroly zásahů do soukromí je ingerence soudu u odposlechu a záznamu telekomunikačního provozu v podobě nařízení odposlechu příkazem soudu postupem dle § 88 odst. 2 Trestního řádu či též obdobná ingerence soudu u provozních a lokalizačních údajů elektronických komunikací v podobě nařízení vydání „osobních a zprostředkovacích dat“ příkazem ke zjištění údajů o telekomunikačním provozu vydaným soudem postupem dle § 88a odst. 1 téhož právního předpisu.

[218] Příkladem takovéto následné soudní kontroly je řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu a příkazu k zjištění údajů o telekomunikačním provozu dle § 314l a násl. Trestního řádu.

procento údajů, jak ukazují dostupné statistiky o využití institutu přezkumu příkazu k zjištění údajů o telekomunikačním provozu dle § 314l a násl. Trestního řádu[219]. Na rozdíl od toho soudní kontrola spočívající v povolení či – v závislosti na procesní úpravě – přímo v nařízení zásahu, dopadá z povahy věci na všechny případy zásahů, které na základě zákona takovéto soudní kontrole podléhají. V této souvislosti je ovšem nutno zdůraznit, že zásadním předpokladem pro to, aby dotčená osoba následnou soudní kontrolu mohla iniciovat, je její vědomost o zásahu, byť i vědomost toliko následná. Jak soudní kontrola zásahu, tak rovněž následná soudní kontrola se však pochopitelně týká pouze zásahu do práva na ochranu soukromí spočívajícího ve vyžádání a využití údajů. Jak ovšem autor konstatoval výše v návaznosti na judikaturu Ústavního soudu ČR i SDEU, v případě plošného shromažďování a zpracování osobních údajů značného množství osob spočívá zásah do práva na ochranu soukromí již v samotném povinném plošném shromažďování a zpracování řady kategorií osobních údajů značného množství osob. Autor se relevantními aspekty soudní kontroly (či kontroly jiným nezávislým orgánem) zásahů do soukromí zabývá podrobně dále.

2.3.3 Řešení kolize základních práv s veřejným zájmem

Potřeba řešení kolize mezi více základními právy nebo mezi základními právy na straně jedné a „*ústavně aprobovaným a zákonem jednoznačně definovaným veřejným zájmem*“[220] je dle Ústavního soudu ČR jediným důvodem k, jinak výjimečnému, zásahu veřejné moci do svobodné, autonomní sféry jednotlivce vymezené základními právy a svobodami, jelikož materiální pojetí státnosti charakterizuje respekt veřejné moci k této sféře jednotlivce[221].

K řešení kolize mezi právem na ochranu soukromí a jinými základními právy a svobodami se Ústavní soud ČR ve své rozhodovací praxi vyjadřoval opakovaně. V nálezu Pl. ÚS 3/14[222] Ústavní soud ČR řešil střet práva na informace a jejich šíření s právem na ochranu osobnosti a soukromého života. Konstatoval zde, že jde o střet *„základních práv stojících na stejné úrovni*“ a řešení takového střetu je „*především věcí obecných soudů, které musejí s přihlédnutím k okolnostem každého případu zvážit, zda přijetím zákonného opatření, jež je v*

[219] Viz např. Nejvyšší soud ČR. Tisková zpráva ze dne 28. července 2016. *Reakce Nejvyššího soudu na titulní článek deníku Právo ze dne 28.7.2016* [online] [cit. 27.6.2017].
[220] Viz nález Ústavního soudu ČR sp. zn. Pl. ÚS 24/10 ze 22. března 2011.
[221] Obecně ke konfliktu mezi základními právy, resp, konfliktu základních práv na straně jedné a veřejného zájmu viz také ZUCCA, Lorenzo. *Constitutional Dilemmas: Conflicts of Fundamental Legal Rights in Europe and the USA*. Oxford: Oxford University Press, 2008. s. 52 a násl.
[222] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 3/14 ze 20. prosince 2016.

demokratické společnosti nezbytné pro ochranu práv a svobod druhých popř. pro ochranu ústavním pořádkem aprobovaného veřejného zájmu, nebyla jednomu právu bezdůvodně dána přednost před právem druhým“[223]. Dle Ústavního soudu ČR musí použité omezení „*šetřit podstatu a smysl dotčeného základního práva a nesmí být zneužito k jinému účelu, než pro který bylo stanoveno*“, jak vyplývá z čl. 4 odst. 4 Listiny. Ústavní soud ČR zde výslovně připustil možnost vychýlení ve prospěch jednoho z takto chráněných práv, ovšem pouze za podmínky, že se bude jednat o vychýlení odůvodněné a současně budou existovat dostatečně efektivní a funkční záruky proti zneužití v neprospěch druhého z takto chráněných práv[224].

Jak však autor uvedl výše, v případě zásahů do práva na ochranu soukromí spočívajících v plošném shromažďování osobních údajů připadá do úvahy spíše kolize mezi tímto právem a veřejným zájmem. V souladu s konstantní judikaturou Ústavního soudu ČR je v případě takovéhoto veřejného zájmu nezbytným předpokladem, aby se jednalo o ústavně aprobovaný a zákonem jednoznačně definovaný veřejný zájem, zákonem předvídaný zásah pak musí být „*proporcionální jak s ohledem na cíl, jehož má být tímto zásahem dosaženo, tak s ohledem na míru krácení omezovaného základního práva či svobody*“[225].

K možným omezením práva na ochranu soukromého života se Ústavní soud ČR vyjádřil též v nálezu I. ÚS 321/06[226] zabývajícím se získáváním informací o zdravotním stavu za účelem trestního řízení, a to v rámci posouzení řešení střetu základních práv a svobod na straně jedné a veřejného zájmu (zde konkrétně zájmu na ochraně zdraví a životů) na straně druhé. Ústavní soud ČR v tomto nálezu, v souladu se svou ustálenou rozhodovací praxí, označil právo na ochranu soukromého života za nezadatelné lidské právo, k jehož omezení lze v demokratickém právním státě přikročit, kromě ochrany základních práv jiných osob, také za účelem „*ochrany veřejného zájmu, který je v podobě principu či hodnoty obsažen v ústavním pořádku*“. Pro účely posouzení takovéto kolize Ústavní soud ČR používá hledisko proporcionality, které za „standardní hledisko“ označil i v tomto nálezu a dodal, že je přitom „*třeba dbát, aby bylo dosaženo nejvyšší možné míry souladu mezi nimi, tedy optimálního uplatnění obou chráněných hodnot*“[227]. Na základě posouzení dle kritéria proporcionality pak

---

[223] Ústavní soud ČR zde odkázal na řadu svých předchozích nálezů, např. sp. zn. IV. ÚS 154/97 (N 17/10 SbNU 113).

[224] Dle závěrů Ústavního soudu ČR v citovaném nálezu *„Imperativ hledání spravedlivé rovnováhy tedy nevylučuje odůvodněné vychýlení ve prospěch jednoho z chráněných práv, pokud záruky proti zneužití omezení uvaleného v neprospěch druhého z práv budou fungovat dostatečně efektivně“.*

[225] Nález Ústavního soudu sp. zn. ČR Pl. ÚS 3/14 ze 20. prosince 2016.

[226] Nález Ústavního soudu sp. zn. ČR I. ÚS 321/06 ze dne 18. prosince 2006.

[227] K vymezení a povaze proporcionality, k posuzování proporcionality v konfliktech mezi základními lidskými právy a veřejným zájmem a též k omezením spojeným s posuzováním proporcionality v takových případech viz

Ústavní soud ČR v tomto případě posoudil kolizi mezi právem na ochranu soukromého života a jinými ústavně chráněnými hodnotami – zájmem na objasnění trestných činů a na spravedlivém potrestání jejich pachatelů a také zájmem na ochraně jednotlivce před neodůvodněným stíháním a odsouzením, resp. omezení práva na ochranu soukromí jako omezení, které při uvážení proporcionality obstojí. Uvedené zájmy jsou dle Ústavního soudu ČR „*legitimním a nezbytným cílem demokratické společnosti*“, významné je také, že „*Lze nalézt i racionální spojení mezi tímto cílem a prostředky, kterými ho má být dosaženo, a není zde dána možnost jejich nahrazení alternativními způsoby, které by byly méně zasahující do základních práv garantovaných čl. 10 odst. 2 a 3 Listiny*“.

Omezení práva na soukromí, které se v daném případě projevuje v umožnění nakládat s informacemi o zdravotním stavu osob zraněných při dopravních nehodách, tak Ústavní soud ČR shledal za daných okolností jako přípustné a formuloval v této souvislosti závěr, který autor považuje ve vztahu k tématu této práce za zvláště relevantní, a sice že „*Dosahování účelu trestního řízení je v demokratickém ústavním řádu pravidelně spjato s řadou nezbytných zásahů do osobnostních práv jiných subjektů, než těch, proti nimž se řízení vede.*“ Současně však Ústavní soud ČR v tomto nálezu vyslovil výhradu v otázce zprošťování mlčenlivosti ve vztahu k Ministerstvu zdravotnictví a krajům „*jako orgánům, které by měly mlčenlivosti zprošťovat*“, když v posuzovaném případě bylo posuzováno oprávnění těchto orgánů zprošťovat mlčenlivosti zdravotnické pracovníky. Ústavní soud ČR se místo toho vyslovil ve prospěch zprošťování mlčenlivosti prováděné soudem, když dle jeho hodnocení „*Soud totiž, vzhledem ke svým institucionálním rysům v podobě nestrannosti a nezávislosti, a též ke svému procesnímu postavení v trestním řízení, je bezpochyby lépe předurčen k posouzení důvodnosti návrhu na zbavení mlčenlivosti a s tím spojenému omezení základních práv a svobod.*“ Dle autora lze tedy i z tohoto nálezu jednoznačně dovodit obecný požadavek na to, aby důvodnost omezení základních práv a svobod v konkrétním případě posuzoval soud, eventuálně jiný nezávislý orgán, nikoli však orgán, který nedisponuje zárukami nestrannosti a nezávislosti a není tak v postavení takovéto posouzení možného zásahu do základních práv a svobod korektně provést. Ústavní soud ČR zde také připomněl, že nutnost „*postupovat ústavně konformním způsobem*“ v případech, kdy „*právní předpis umožňuje různou interpretaci norem jednoduchého práva*“, je povinností všech státních orgánů. Je tedy nutno vždy upřednostnit

---

též BARAK, Aharon. *Proportionality. Constitutional Rights and their Limitations.* Cambridge: Cambridge University Press, 2012, zejména s. 131 a násl., s. 163 a násl.

takový výklad, „*který je co nejvíce souladný s ústavním pořádkem*“ ve všech situacích, v nichž „*zákon připouští dvojí výklad*“.

Obecně vymezil Ústavní soud ČR řešení takovýchto kolizí v ústavněprávní rovině mj. v nálezu III. ÚS 256/01[228]. Ke kolizím totiž „*dochází nejen mezi základními právy a svobodami navzájem, nýbrž i mezi základními právy a svobodami a jinými ústavně chráněnými hodnotami*“; tento závěr Ústavní soud ČR dle vlastního hodnocení vyslovil v řadě předchozích rozhodnutí. Dle závěru obsaženého v nálezu Pl. ÚS 15/96[229] může takto k omezení základních práv či svobod dojít i v případě, kdy „*jejich ústavní úprava omezení nepředpokládá*“, a to „*v případě jejich kolize nebo v případě kolize s jinou ústavně chráněnou hodnotou, jež nemá povahu základního práva a svobody (veřejný statek)*“. Také v případě práva na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů dle čl. 10 odst. 3 lze jako o potenciálně možných uvažovat o imanentních omezeních, která plynou přímo z ústavního pořádku, obdobně jako je Ústavní soud ČR dovodil v nálezu I.ÚS 453/03[230] u práva na osobní čest a dobrou pověst garantovaných čl. 10 odst. 1 Listiny, když tato práva dle Ústavního soudu nejsou omezitelná „*obyčejnými zákony, jejichž účel by Listina stanovila v podobě veřejných statků (tak jako např. u svobody projevu)*“

Dle Ústavního soudu ČR *„Ústavní úprava postavení jedince ve společnosti obsahuje ochranu individuálních práv a svobod, jakož i ochranu veřejných statků.“*[231]. Individuální práva a svobody se přitom odlišují od veřejných statků distributivností, když *„Pro veřejné statky je typické, že prospěch z nich je nedělitelný a lidé nemohou být vyloučeni z jeho požívání“*. Jako příklady veřejných statků Ústavní soud ČR v citovaném nálezu uvádí národní bezpečnost, veřejný pořádek, zdravé životní prostředí a na základě toho vymezuje veřejný statek tak, že se jím *„určitý aspekt lidské existence stává za podmínky, kdy není možno jej pojmově, věcně i právně rozložit na části a tyto přiřadit jednotlivcům jako podíly“*. Na rozdíl od veřejných statků je pro základní práva a svobody naopak typická jejich distributivnost, jde totiž o „aspekty lidské existence“, které *„lze pojmově, věcně i právně členit na části a tyto přiřadit jednotlivcům“*. Jako příklady Ústavní soud v témže nálezu uvádí např. *„osobní svobodu, svobodu projevu, účast v politickém dění a s tím spjaté volební právo, právo zastávat veřejné funkce, právo sdružovat se v politických stranách atd.“* V případě jejich kolize je pak nutno *„stanovit podmínky, za splnění kterých má prioritu jedno základní právo či svoboda, a*

[228] Nález Ústavního soudu ČR sp. zn. III ÚS 256/01 ze 21. března 2002.
[229] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 15/96 z 9. října 1996.
[230] Nález Ústavního soudu ČR sp. zn. I.ÚS 453/03 z 11. listopadu 2005.
[231] Nález Ústavního soudu ČR sp. zn. III ÚS 256/01 ze 21. března 2002.

za splnění kterých jiné, resp. určitý veřejný statek"; i zde Ústavní soud zdůrazňuje maximu, dle které *„základní právo či svobodu lze omezit pouze v zájmu jiného základního práva či svobody nebo veřejného statku"*.

Ústavní soud ČR ve svých nálezech[232] opakovaně shrnul kritéria, v nichž dle jeho hodnocení spočívá „*vzájemné zvažování v kolizi stojících základních práv a svobod nebo veřejných statků*":

1. kritérium vhodnosti, tedy *„posuzování toho, zdali institut, omezující určité základní právo, umožňuje dosáhnout sledovaný cíl (ochranu jiného základního práva nebo veřejného statku)"*;
2. kritérium potřebnosti, které spočívá *„v porovnávání legislativního prostředku, omezujícího základní právo, resp. svobodu, s jinými opatřeními, umožňujícími dosáhnout stejného cíle, avšak nedotýkajícími se základních práv a svobod, resp. dotýkajícími se jich v menší intenzitě"* a
3. poslední kritérium, kritérium závažnosti je založeno na *„porovnání závažnosti obou v kolizi stojících základních práv nebo veřejných statků"*.

Ústavní soud ČR poté v citovaném nálezu shrnutí těchto tří kritérií doplňuje vymezením porovnávání závažnosti základních práv, která jsou ve vzájemné kolizi, resp. veřejných statků, jak jsou vymezeny výše (po splnění podmínky vhodnosti a potřebnosti)[233]. Toto porovnávání závažnosti spočívá „*ve zvažování empirických, systémových, kontextových i hodnotových argumentů*". Empirickým argumentem je zde faktická závažnost „*jevu, jenž je spojen s ochranou určitého základního práva*"; systémový argument znamená „*zvažování smyslu a zařazení dotčeného základního práva či svobody v systému základních práv a svobod*"; kontextovým argumentem se rozumí „*další negativní dopady omezení jednoho základního práva v důsledku upřednostnění jiného*"; hodnotový argument „*představuje zvažování pozitiv v kolizi stojících základních práv vzhledem k akceptované hierarchii hodnot*". Jako součást „*porovnávání závažnosti v kolizi stojících základních práv*" Ústavní soud ČR vnímá dále též „*zvažování využití právních institutů, minimalizujících argumenty*

[232] Viz např. nález Ústavního soudu ČR sp. zn. Pl.ÚS 4/94 ze dne 12. října 1994, v němž plénum Ústavního soudu ČR rozhodlo o zrušení některých ustanovení zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

[233] K principu proporcionality a jeho využití při posuzování kolizí mezi základními právy a svobodami na straně jedné a veřejným zájmem na straně druhé viz též ONDŘEJEK, Pavel. *Princip proporcionality a jeho role při interpretaci základních práv a svobod*. Praha: Leges, 2012, zejména s. 58 a násl., 85 a násl, 94 a násl.

podložený zásah do jednoho z nich“. Z článku 4 odst. 4 Listiny[234] pak Ústavní soud ČR dovodil závěr, dle kterého „*základních práv a svobod musí být šetřeno nejenom při používání ustanovení o mezích základních práv a svobod, nýbrž analogicky rovněž v případě jejich omezení v důsledku jejich vzájemné kolize*“. Pro konečné rozhodnutí „*v případě závěru o opodstatněnosti priority jednoho před druhým ze dvou v kolizi stojících základních práv, resp. veřejných statků*“ je v důsledku toho dle Ústavního soudu ČR nutnou podmínkou rovněž „*využití všech možností minimalizace zásahu do jednoho z nich*“[235]. V této souvislosti však autor považuje za vhodné akcentovat též praktickou stránku tohoto problému a připomenout si hodnocení Jana Kudrny vyslovená výše, který právě o čl. 4 odst. 4 Listiny hovoří jako o jejím „pravděpodobně nejvíce porušovaném ustanovení“[236]. Autor se takovému hodnocení věnuje u jednotlivých konkrétních zásahů do práva na ochranu soukromí v další části této práce.

Omezení práv, která Listina garantuje jako základní práva absolutní, je přípustné jen v rámci tzv. imanentní omezení základních práv, tedy omezení za účelem „*ochrany základních práv jiných osob anebo za účelem ochrany veřejného zájmu, který je v podobě principu či hodnoty obsažen v ústavním pořádku*“[237]. U práv na ochranu před neoprávněným zasahováním do soukromého a rodinného života i u práva každého na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě dle čl. 10 odst. 2 a 3 Listiny platí dle hodnocení autora obdobně tentýž závěr, který Ústavní soud konstatoval v nálezu Pl. ÚS 3/14 ve vztahu k právům na zachování lidské důstojnosti,

---

[234] Článek 4 odst. 4 Listiny stanoví, že *„Při používání ustanovení o mezích základních práv a svobod musí být šetřeno jejich podstaty a smyslu. Taková omezení nesmějí být zneužívána k jiným účelům, než pro které byla stanovena.“*.

[235] Ve věci posuzované v tomto nálezu Ústavní soud ČR dospěl k závěru, že zkoumaná právní úprava - ustanovení § 22 odst. 4 zákona č. 72/1994 Sb., kterým se upravují některé spoluvlastnické vztahy k budovám a některé vlastnické vztahy k bytům a nebytovým prostorům a doplňují některé zákony (zákon o vlastnictví bytů), ve znění zákona č. 273/1994 Sb. „*nesplňuje podmínky omezení základního práva, resp. svobody, v důsledku jeho kolize s jiným základním právem, resp. svobodou, nebo veřejným statkem*“, jelikož napadená ustanovení nesplňují „*kritérium potřebnosti, spočívající v porovnávání legislativního prostředku, omezujícího základní právo, resp. svobodu, s jinými opatřeními, umožňujícími dosáhnout stejného cíle, avšak nedotýkajícími se základních práv a svobod, resp. dotýkajícími se jich v menší intenzitě*“. Tento závěr pléna Ústavního soudu ČR však nebyl přijat zcela jednoznačně, když dle jedné ze soudkyň Ústavního soudu ČR „*napadené ustanovení vyhovuje i kritériu potřebnosti v pojetí, jak je definováno v odůvodnění nálezu*“; Dle hodnocení této soudkyně Ústavního soudu ČR „*Veřejný zájem na zabezpečení národní bezpečnosti, obrany země a veřejného pořádku je natolik intenzivní, že musí být zajištěn adekvátními právními prostředky.“,* přičemž podle jejího názoru *„Pod uvedený veřejný zájem nepochybně spadá i zajištění bytových potřeb osob působících v rezortech garantujících obranu státu a ochranu veřejného pořádku.*“

[236] Viz KUDRNA, Jan. 27. Pravděpodobně nejvíce porušované ustanovení Listiny (a jedna ze současných hrozeb lidským právům) in GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012 s. 277 a násl.

[237] Nález Ústavního soudu ČR sp. zn. IV. ÚS 412/04 ze dne 7. prosince 2005.

osobní cti a dobré pověsti zaručenému Listinou v čl. 10 odst. 1, tedy nemožnost omezit tato práva „*podústavními zákony, jejichž účel by Listina stanovila v podobě veřejných statků*“, na rozdíl od některých jiných práv, u nichž Listina takovéto omezení umožňuje, např. omezení dle čl. 17 odst. 4 u „*svobody projevu a práva vyhledávat a šířit informace ve prospěch zákonných opatření nezbytných v demokratické společnosti pro ochranu práv a svobod druhých, bezpečnosti státu, veřejné bezpečnosti, veřejného zdraví a mravnosti*“[238]. V tomto případě je totiž možnost omezení výslovně připuštěna přímo v textu diskutovaného článku 17 odst. 4 Listiny.

Z těchto důvodu vymezil Ústavní soud ČR ve svých nálezech test principu proporcionality a specifikoval jeho jednotlivé kroky[239], jak autor rozebírá dále. Aleš Gerloch ve vztahu k čl. 4 Listiny konstatuje, že „*Právě zde uvedená kritéria testů legality, legitimity a proporcionality jsou další formou implicitního vymezování povinností, které lze z Listiny základních práv a svobod vyvodit.*“[240]. Jak Ústavní soud ČR zdůrazňuje v nálezu IV. ÚS 412/04, tyto kroky „*je třeba vztáhnout jak na zákon, který omezuje tato základní práva, tak na jeho interpretaci a aplikaci nacházející odraz ve vydání individuálního rozhodnutí*“. Dle závěru, který Ústavní soud ČR učinil v nálezu Pl. ÚS 3/14 ve vztahu k uplatnění principu proporcionality, platí, že v situaci, kdy proti sobě stojí „*dva nároky stejné povahy a intenzity, vždy je třeba vážit naléhavost a úroveň konkurujících si hodnot a zájmů s ohledem na konkrétně skutkově utvořený základ tak, aby obě hodnoty byly v co největší míře zachovány*“; pokud tomuto požadavku nelze vyhovět, je nutno „*o to přesvědčivěji zdůvodnit širší zásah do jedné z těchto hodnot při uplatnění principu proporcionality*“. Tyto ústavní zásady se dle Ústavního soudu ČR „*uplatňují při posouzení opatření veřejné moci omezujících základní právo jednotlivce*“, Ústavní soud ČR je obdobně uplatňuje též „*na případy kolize mezi právy soukromých subjektů v rovině horizontální*“[241].

V nálezu Pl. ÚS 3/14 Ústavní soud ČR popsal tři kroky testu proporcionality tak, že v prvním kroku je třeba hodnotit legitimnost sledovaného cíle, tedy to, zda „*je sledován a*

---

[238] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 3/14 ze dne 20. prosince 2016.
[239] K omezením vyplývajícím z aplikace principu proporcionality viz také BARAK, Aharon. *Proportionality. Constitutional Rights and their Limitations.* Cambridge: Cambridge University Press, 2012. s. 481 a násl. či BENDOR, Ariel L., SELA, Tal. *How proportional is proportionality?* International Journal of Constitutional Law, Volume 13, Issue 2, April 2015, s. 530–544.
[240] GERLOCH Aleš. Relace práv a povinností v Listině základních práv a svobod in GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012 s. 17.
[241] K omezením základních práv viz také MADEJ, Martin. *Meze základních práv v České republice.* Praha: Leges, 2018.

prosazován cíl nezbytný ve svobodné demokratické společnosti" a posoudit existenci racionálního spojení „*mezi cílem a prostředky vybranými k jeho prosazení",* ve druhém kroku je nutno zvážit existenci alternativních způsobů *„dosažení cíle, jejichž využití by učinilo zásah do základního práva méně intenzivní, popř. jej zcela vyloučilo*", tedy ověřit, zda „*při používání zákonných omezení základních práv a svobod je šetřeno jejich podstaty a smyslu v souladu s čl. 4 odst. 4 Listiny*" a konečně třetí krok je zaměřen na posouzení proporcionality v užším smyslu [242]. V rámci výše uvedeného přitom ve vztahu ke kritériu vhodnosti platí, že „*Omezující zásah je vhodný, vykazuje-li takovou věcnou souvislost s účelem, že dosažení účelu přinejmenším podporuje*", u posuzování potřebnosti zásahu musí být naplněn předpoklad, že „*k dispozici není žádný jiný, k právům dotčené osoby šetrnější, tj. menší újmu způsobující, a přitom stejně vhodný prostředek*". Konečně pak v případě proporcionality omezení základního práva na ochranu osobních údajů ve vztahu ke sledovanému cíli se toto omezení „*nesmí vymykat z proporcionálního poměru k významu jím sledovaného cíle, musí být v rovnováze s ústavním právem na přístup k informacím, tedy nesmí jít nad rámec toho, co je pro dosažení tohoto cíle nezbytné*", jak konstatoval Ústavní soud ČR v nálezu Pl. ÚS 3/14.

V této souvislosti je vhodné upozornit také na to, že samotný fakt, že byl po formální stránce proveden test proporcionality konkrétního zákonného ustanovení dle výše uvedených kritérií, není sám o sobě zárukou toho, že posuzované zákonné ustanovení skutečně kritéria proporcionality splňuje. Jak dokládá např. již rozebíraný nález Ústavního soudu ČR Pl. ÚS 3/14, je relevantní zabývat se i tím, zda byl test proporcionality proveden řádně – jak konstatuje ve svém separátním votu k tomuto nálezu skupina celkem 7 soudců Ústavního soudu ČR[243]. Tato skupina se připojila k původně samostatnému separátnímu votu Pavla Rychetského, který v něm mj, uvádí, že, „*Při veškerém respektu k odlišnému právnímu názoru většiny pléna musím podotknout, že přijatý nález těmto požadavkům nedostál. Test proporcionality je v něm proveden nedůsledně, což činí celou jeho vlastní právní argumentaci nepřehlednou a jen obtížně uchopitelnou.*" Výhrada nikoli nepodstatné části pléna Ústavního soudu ČR se v tomto případě týkala druhého kroku testu proporcionality, „*posouzení potřebnosti zásahu, tedy zda sledovaného účelu nelze dosáhnout i jiným způsobem, jenž by byl šetrnější k dotčenému základnímu právu*". Skupina soudců Ústavního soudu ČR zde argumentovala zejména nedostatečným srovnáním s obdobnými zahraničními právními

[242] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 3/14 ze dne 20. prosince 2016.
[243] Viz Nález Ústavního soudu ČR Pl. ÚS 3/14 ze 20. prosince 2016. Odlišné stanovisko soudce Pavla Rychetského, k němuž se připojili soudci Ludvík David, Josef Fiala, Jan Filip, Jan Musil, Radovan Suchánek a Milada Tomková.

úpravami, resp. nedostatečným vypořádáním se s výsledky tohoto srovnání v rámci druhého kroku testu proporcionality.

Mají-li zásahy do základních práv obstát v testu proporcionality, musejí být doplněny dostatečnými mechanismy, které účinně brání zneužití zásahů. Jak zdůraznil Ústavní soud ČR v nálezu Pl. ÚS 3/14 ve vztahu k výkonu práva jiných osob vyhledávat informace (v posuzovaném případě konkrétně práva na přístup k archiváliím obsahujícím informace o činnosti bezpečnostních složek bývalého totalitního režimu), „*čím citelnější zásah do osobní integrity dotčeného jednotlivce*“ takovýto výkon práva působí, „*tím účinnějšími zárukami ústavněprávní ochrany proti zneužití získaných informací musí být dotčená osoba vybavena*“. Dle hodnocení autora lze tento závěr o účinných zárukách obdobně vztáhnout též k zásahům do práva na ochranu soukromí v důsledku opatření zamýšlených zákonodárcem k ochraně národní bezpečnosti, veřejného pořádku a dalším, jako je tomu v případech, kterými se autor zabývá v této práci.

V nálezu Pl. ÚS 3/14 se Ústavní soud ČR vyjádřil rovněž k hodnocení přiměřenosti zásahu, a to tak, že je třeba posuzovat ji „*jak intenzitou jeho dopadu do osobní sféry dotčených osob, tak i počtem těchto osob*“, kdy jako příklad Ústavní soud ČR uvádí, s odkazem na nález Pl. ÚS 24/10[244], právě plošnou a preventivní povahu sběru a uchovávání provozních a lokalizačních údajů o elektronické komunikaci, kterážto povaha byla „*hlavním důvodem, proč napadené ustanovení příslušného zákona neobstálo v testu proporcionality*“. Tato kritéria formulovaná Ústavním soudem ČR autor považuje za zvláště relevantní ve vztahu k problematice posuzované v této práci, tedy nejen k otázce uchovávání provozních a lokalizačních údajů elektronických komunikací, ale i k dalším případům zásahů do soukromí, jak je autor vymezil v úvodu této práce, totiž zásahů týkajících se značného počtu dotčených osob a současně vyznačujících se plošným a nerozlišujícím charakterem.

Typickými příklady odpovídajícími tomuto vymezení – kritériím plošnosti zásahu a značného počtu dotčených osob – jsou dle hodnocení autora např. povinný sběr a uchovávání údajů leteckých cestujících či zpracování údajů získávaných kamerovými systémy na silnicích a dálnicích ČR, lze k nim zařadit též povinné vybavení osobních motorových vozidel zařízením eCall zaznamenávajícím mj. i několik aktuálních geografických poloh vozidla a některé další kategorie údajů. V prvních dvou z těchto případů totiž dochází ke shromažďování a zpracování osobních údajů značného počtu osob, které nejsou omezeny pouze na osoby, u

[244] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011.

kterých by existovalo jakékoli konkrétní podezření či i jen spojitost s činností, která by mohla zakládat důvod zpracování. Poslední případ je pak specifický tím, že údaje ze zařízení eCall v osobních automobilech nejsou sice shromažďovány a zpracovávány souhrnně na jednom fyzickém místě – uložišti, avšak z hlediska množství dotčených osob jde o zásah plošný, neboť jím jsou dotčeni všichni uživatelé osobních automobilů, které byly schváleny do výroby po 31. březnu 2018.

Ústavní soud ČR v již rozebíraném nálezu Pl. ÚS 3/14 uvádí, že při posuzování zásahu do základního práva, poté co byl úspěšně proveden test legality zákonného stanovení, v němž je spatřován zásah, „*lze doplnit ještě novější požadavek ESLP, řešený standardně v rámci podmínky proporcionality*“, a to požadavek „*na dostatečnost záruk před svévolnou aplikací omezení základního práva*“. Z rozhodovací praxe ESLP zde Ústavní soud ČR výslovně odkazuje na rozsudek ESLP ve věci Gillan a Quinton proti Spojenému království[245], v němž ESLP dospěl k jednoznačnému závěru, že „*ani pravomoci k vydávání povolení a potvrzení, ani pravomoci k zastavení a prohlídce podle článků 44 a 45 zákona o terorismu nebyly dostatečně vymezeny a nepodléhaly dostatečným právním zárukám proti zneužití. Proto nebyly "v souladu se zákonem".*“

Z výše uvedených rozhodnutí vyplývají ústavněprávní požadavky, které musí být splněny v případě zásahu do základních práv a svobod. Jak konstatoval Ústavní soud ČR v nálezu Pl. ÚS 24/10, při aplikaci nástrojů, jejichž užití má za následek vážné omezení osobní integrity a základních práv a svobod jednotlivce, musí být respektovány ústavněprávní limity. Jde zejména o požadavky na veřejný zájem, na jehož základě jsou omezení či zásahy do základních práv a svobod přípustné, ve zkoumaných případech primárně zásahy do práva na ochranu soukromí, zásadní jsou též požadavky na proporcionalitu zásahu a na kvality, které musí splňovat právní úprava, která takový zásah zakládá, součástí požadavku na proporcionalitu je také nutnost existence mechanismů účinně bránících zneužití zásahů. Autor proto požadavky vymezené v této kapitole následně aplikuje na jednotlivé případy zásahů do základních práv a svobod zkoumané v této práci a vyhodnotí, nakolik jsou v jednotlivých případech naplněny.

[245] Rozsudek ESLP ve věci Gillan a Quinton proti Spojenému království, rozsudek č. 4158/05 ze dne 12. ledna 2010. *„In conclusion, neither the powers of authorisation and confirmation, nor the stop and search powers under sections 44 and 45 of the Terrorism Act, were sufficiently circumscribed or subject to adequate legal safeguards against abuse. Accordingly, they were not "in accordance with the law".“* Pozn.: Přeloženo autorem.

3 Jednotlivé typové případy zásahů do práva na ochranu soukromí

U každého ze zkoumaných případů autor vymezí základy aktuální právní úpravy daného případu, včetně stručného vývoje a důvodů právního zakotvení a v relevantních případech též včetně stručného porovnání se zahraničními právními úpravami. Autor se podrobně zaměří na zpracovávané kategorie osobních údajů a zvláště na orgány oprávněné k vyžádání údajů, jelikož vymezení okruhu oprávněných orgánů patří mezi zásadní aspekty jednotlivých případů plošného shromažďování osobních údajů. Seznam orgánů, které jsou oprávněny k vyžádání údajů, resp. které dle některých interpretací za takové je možno považovat, se navíc u některých případů postupně vyvíjel. Vedle oprávněných orgánů jsou z hlediska intenzity zásahu do práva na ochranu soukromí a též jako prevence nadužití či zneužití shromažďovaných údajů významná též existující omezení, kontrolní mechanismy a další záruky v jednotlivých případech.

V další části autor analyzuje relevantní rozhodnutí a výkladovou praxi. Její rozsah je u některých případů zásahů výrazně četnější nežli v jiných zkoumaných případech, nejbohatší rozhodovací praxe, která se navíc v průběhu času vyvíjela s významným vlivem na existující právní úpravu, se pojí s povinností Data Retention. Následně autor posoudí test proporcionality provedený při přijímání právní úpravy a tento test vyhodnotí z hlediska aktuálně dostupné rozhodovací praxe, zejména Ústavního soudu ČR. Na závěr se autor pokusí na základě předchozích uvedených bodů formulovat doporučení de lege ferenda ve vztahu ke každému ze zkoumaných případů.

Mezi zkoumanými případy zásahů do soukromí má dle hodnocení autora zásadní postavení povinné uchovávání provozních a lokalizačních údajů účastníků a uživatelů elektronických komunikací. Jak autor ukáže dále, tento případ plošného shromažďování osobních údajů je dle hodnocení autora mezi zkoumanými případy nejintenzivnějším zásahem z hlediska rozsahu vyjádřeného absolutním počtem dotčených osob a rovněž z hlediska intenzity zásahu založené na charakteristice shromažďovaných údajů, včetně jejich celkového množství, jak autor rozvede dále. Současně jde u povinného shromažďování provozních a lokalizačních údajů v rámci zkoumaných případů o jeden z nejdéle aplikovaných případů plošného shromažďování údajů. V důsledku těchto faktorů k tomuto zásahu existuje rozsáhlá rozhodovací praxe soudů, jak na národní úrovni, tak i na úrovni EU, k dispozici je i řada stanovisek vydaných k této problematice orgány dozoru nad ochranou osobních údajů.

Nejen rozhodovací praxe, nýbrž též právní úprava a v důsledku řady rozhodnutí i kontrolní mechanismy se v případě povinného plošného shromažďování provozních a

lokalizačních údajů vyvíjely výrazně déle nežli u ostatních zkoumaných zásahů do soukromí. S ohledem na výše uvedené autor rozebere Data Retention jako v pořadí první ze zkoumaných případů, bude se mu též věnovat podrobněji nežli v pořadí dalším zkoumaným případům. U nich pak autor v některých aspektech bude odkazovat na dílčí závěry učiněné ve vztahu k povinnému plošnému uchovávání provozních a lokalizačních údajů. Cílem této práce totiž dle autorova záměru není detailní, encyklopedický popis jednotlivých zkoumaných případů, autor se ve své práci zaměřuje na ústavněprávní rozměr těchto případů, tedy na posouzení vybraných zásahů do základních práv a svobod a zejména vyhodnocení proporcionality těchto zásahů, na základě toho pak na návrh řešení v podobě návrhu úprav relevantní právní úpravy a návrh adekvátních kontrolních mechanismů. Navíc dle hodnocení autora platí, že mnohé kontrolní mechanismy, které se v případě provozních a lokalizačních vyvinuly především v reakci na soudní rozhodnutí, lze aplikovat obdobně i v případech dalších zkoumaných zásahů, jak autor rozvede podrobněji dále. Tato skutečnost je významnou také pro formulaci obecných závěrů a doporučení aplikovatelných potenciálně u více zkoumaných případů.

Taktéž vývoj a stále pokračující snahy o rozšiřování orgánů veřejné moci, které jsou ze zákona oprávněny provozní a lokalizační údaje vyžádat a použít ve své činnosti, svědčí dle názoru autora o mimořádném významu a hodnotě těchto údajů. S rozšiřováním oprávněných orgánů dále narůstá závažnost zásahu. Autor má za to, že obdobný zájem lze očekávat též u osobních údajů plošně shromažďovaných v dalších případech zkoumaných v této práci, ostatně u systémů dopravních kamer se již projevil v praxi, jak autor ukáže dále. Specifickou kategorii osobních údajů tvoří dle názoru autora lokalizační údaje, které jsou v důsledku technického rozvoje plošně zpracovávány nejen v oblasti elektronických komunikací, ale též v jiných zkoumaných případech, jak autor ukáže dále. Autor se tedy v závěrečných doporučeních bude věnovat otázce dostatečnosti ochrany těchto údajů de lege lata.

3.1 Plošné zpracování provozních a lokalizačních údajů elektronických komunikací

Autor se problematikou povinného uchovávání provozních a lokalizačních údajů elektronických komunikací podrobně zabýval ve své rigorózní práci v roce 2017[246]. Mnohé části a závěry této práce považuje autor i nadále za relevantní, v mezidobí však přibyla řada nových aspektů a celkově nastal vývoj též v oblasti rozhodovací praxe i relevantní právní úpravy. Autor v této práci tento vývoj zohlednil a v textu reflektoval, současně je téma této

[246] Miroslav Uřičař. *Data Retention. Povinnost uchovávat provozní a lokalizační údaje.* Právnická fakulta Masarykovy univerzity. Obor právo. Ústav práva a technologií. 2016/2017.

práce výrazně širší nežli předchozí rigorózní práce zaměřená pouze na problematiku provozních a lokalizačních údajů elektronických komunikací. Tato práce se navíc, na rozdíl od autorovy rigorózní práce, zabývá ústavněprávním rozměrem plošných zpracování osobních údajů, včetně, nikoli však toliko, provozních a lokalizačních údajů elektronických komunikací. Z těchto důvodů autor zde, v kapitole týkající se zpracování provozních a lokalizačních údajů, zčásti využije text obsažený v rigorózní práci, tento však podstatně rozvine a doplní aktuální vývoj, závěry a především ústavněprávní hledisko a zasazení do celkového širokého kontextu plošných zpracování osobních údajů.

3.1.1 Vývoj a základní vymezení, relevantní právní úprava

Vývoj povinnosti Data Retention

V odborné literatuře se povinnost k uchovávání vymezených provozních a lokalizačních údajů účastníků a uživatelů uložená poskytovatelům služeb elektronických komunikací a provozovatelům sítí elektronických komunikací[247] označuje jako povinnost Data Retention. Účelem uchovávání údajů je jejich možné vyžádání oprávněnými orgány pro využití k činnostem vymezeným zákonem, primárně pro vyšetřování a stíhání závažné trestné činnosti a další. Doba povinného uchování údajů se v členských státech EU, v nichž je povinnost uložena, pohybuje mezi 6 měsíci a 2 lety. Data Retention povinnost původně vymezovala Data Retention Směrnice a na jejím základě přijaté národní právní úpravy. V současnosti, i po prohlášení této směrnice za neplatnou Soudním dvorem EU[248], povinné uchování provozních a lokalizačních údajů v řadě členských států EU, včetně České republiky, nadále přetrvává, založeno je výhradně národními právními úpravami, když nová směrnice nahrazující Data Retention směrnici ani jiná obdobná úprava pro celou EU přijaty nebyly.

Ještě před samotným právním rozborem povinnosti Data Retention a související problematiky považuje autor za potřebné zabývat se stručně historickým kontextem a souvislostmi, které vedly k legislativnímu zakotvení povinnosti Data Retention a do značné

[247] ZoEK označuje poskytovatele služeb elektronických komunikací zpravidla jako „*podnikatele poskytující veřejně dostupné služby elektronických komunikací*“, provozovatele sítí elektronických komunikací definuje jako „*operátory*“, není to však pravidlem a právní úprava není v užívání těchto pojmů zcela jednotná a systematická. V dalším textu budou pro označení těchto subjektů použity pojmy poskytovatel služeb elektronických komunikací, resp. provozovatel sítě elektronických komunikací, neboť je autor považuje za pojmy zcela jednoznačné a dikci příslušných právních předpisů neodporující.

[248] Rozsudek Soudního dvora EU (velkého senátu) z 8. dubna 2014. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další, Žádosti o rozhodnutí o předběžné otázce podané High Court (Irsko) a Verfassungsgerichtshof ve spojených věcech C-293/12 a C-594/12, kterým se vyslovuje neplatnost Data Retention Směrnice, je podrobně rozebrán dále.

míry podobu tohoto právního institutu determinovaly. Jednalo se o snahu nalézt prostředky využitelné k prevenci terorismu a boje s ním, a to nejprve v rovině politické a posléze legislativní. Tyto souvislosti autor vnímá jako významné pro vymezení a porozumění veřejnému zájmu, který uložení povinnosti Data Retention sleduje, a především pro posouzení a vyhodnocení proporcionality zásahu do základních práv a svobod, který tato povinnost představuje. Ostatně, například také Ústavní soud ČR v nálezu Pl. ÚS 45/17, jakožto zatím posledním z nálezů, v nichž se zabýval napadenou právní úpravou Data Retention v ZoEK a souvisejících právních předpisech, významnou měrou přihlížel k faktické stránce a ke hrozbám teroristických útoků, kterými je existence povinnosti Data Retention v právním řádu ČR odůvodňována.

Vzhledem k narůstající hrozbě teroristických útoků jednaly členské státy EU v posledních letech dvacátého století o možných formách spolupráce v boji proti terorismu, resp. obecně o spolupráci při vyšetřování trestné činnosti. Po útocích v New Yorku z 11. září 2001 jednání nabyla na intenzitě, jak potvrzují například závěry zasedání Rady EU ve složení pro spravedlnost a vnitřní věci ze dne 19. prosince 2002, které zdůrazňují mimořádnou důležitost údajů o použití elektronických komunikací, kteréžto údaje „*představují cenný nástroj pro předcházení, vyšetřování, odhalování a stíhání trestných činů, a zejména organizované trestné činnosti*“, tyto závěry však zůstávaly pouze u zmíněného obecného konstatování. Evropská bezpečnostní strategie[249] přijatá Radou EU dne 12. prosince 2003 sice zmiňuje terorismus společně s šířením zbraní hromadného ničení, regionálními konflikty, selháním státu a organizovanou trestnou činností jako jedny z hlavních hrozeb pro bezpečnost v Evropě, samotná strategie však ještě neobsahovala žádnou výraznější zmínku o potřebě zajistit uchovávání provozních a lokalizačních údajů pro účely takovéhoto boje. Teprve ve Zprávě o provádění Evropské bezpečnostní strategie vyhotovené v prosinci 2008 (tedy již po teroristických útocích v Madridu v roce 2004 a v Londýně v roce 2005) je obecně zmiňována nezbytnost „*účinné a komplexní politiky EU pro sdílení informací, s náležitým zohledněním ochrany osobních údajů*“, samotné provozní a lokalizační údaje v ní však taktéž výslovně označeny nejsou.

[249] Text Evropské bezpečnostní strategie v českém jazyce je dostupný společně se Zprávou o provádění Evropské bezpečnostní strategie z prosince 2008. Potřeby úprav této strategie v průběhu uplynulých let vedly v červnu 2016 k vydání nového dokumentu Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union´s Foreign and Security Policy. Viz European Council. *Evropská bezpečnostní strategie.* [online]. 12. prosince 2003. [cit. 12.1.2023]; European Council. *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union´s Foreign and Security Policy* [online]. 2008. [cit. 12.1.2023].

První větší teroristické útoky na území Evropské unie – útoky v Madridu 11. března 2004 se pak staly bezprostředním impulsem pro přijetí Prohlášení Evropské rady o boji proti terorismu[250], které mimo dalších konkrétních kroků pro efektivní boj proti terorismu zmiňuje také návrh na zavedení pravidel pro uchovávání komunikačních provozních údajů poskytovateli služeb; toto prohlášení uložilo Radě prověřit opatření, která by pro poskytovatele služeb stanovila pravidla uchovávání provozních údajů o komunikaci. V dokumentu z 28. dubna 2004 Francie, Irsko, Švédsko a Velká Británie zdůraznily nutnost celoevropské data retention politiky a předložily Radě EU návrh rámcového rozhodnutí o uchovávání údajů zpracovávaných pro účely poskytování veřejně dostupných služeb elektronických komunikací nebo údajů dostupných ve veřejných komunikačních sítích za účelem prevence, vyšetřování, detekce a stíhání trestných činů, včetně terorismu[251]. Po teroristických útocích v Londýně ze 7. července 2005 Rada v prohlášení ze dne 13. července 2005[252] tyto útoky odsoudila a opětovně potvrdila potřebu co nejrychlejšího přijetí společných opatření o uchovávání telekomunikačních údajů. Jako svou bezprostřední prioritu, vedle několika dalších opatření zaměřených na vyšetřování a boj proti terorismu, deklarovala také nutnost dohodnout se na rámcových rozhodnutích o uchovávání telekomunikační údajů, s termínem říjen 2005.

Faktickým naplněním uvedených jednání a prohlášení pak o několik měsíců později bylo vypracování textu Data Retention Směrnice, s jejímž návrhem přišla Evropská komise 21. září 2005[253]. Navzdory kritickému postoji zejména národních úřadů pro ochranu osobních údajů členských států EU schválila Rada EU text Data Retention Směrnice na svém zasedání 21. února 2006, pouze delegace Slovenska a Irska hlasovaly proti[254]. Následně, dne 15. března 2006 návrh směrnice schválil Evropský parlament. Na jejím základě byly členské státy EU povinny přijmout národní úpravu, dle které budou provozovatelé sítí a poskytovatelé služeb elektronických komunikací povinni uchovávat veškeré provozní a lokalizační údaje o všech svých účastnících po dobu minimálně 6 měsíců, maximálně 2 let. To vše pro případ, že by pro

[250] European Council. *Declaration on Combating Terrorism* [online]. 25 March 2004 [cit. 12.1.2023].
[251] European Council. *Document of the Council 8958/04 of 28 April 2004.* [online]. 2004. [cit. 12.1.2023].
[252] European Council. *Council Declaration on the EU response to the London bombings.* [online]. 13 July 2005. [cit. 12.1.2023].
[253] Návrh Data Retention Směrnice Evropského parlamentu a Rady o uchovávání údajů zpracovávaných v souvislosti s poskytováním veřejných služeb v odvětví elektronických komunikací, kterou se mění směrnice 2002/58/ES ze dne 21. září 2005, COM (2005) 438 final.
[254] European Council. *Press Release, 2709th Council Meeting, Justice and Home Affairs.* [online]. 2006. [cit. 12.1.2023].

účely vyšetřování závažných trestných činů bylo potřebné nejen nařídit odposlech či získat údaje do budoucna, ale také prozkoumat některá data zpětně.

Teprve po přijetí Data Retention Směrnice následovaly ve většině států národní právní úpravy. Existovaly však i výjimky, v několika členských státech EU zákonodárce přijal národní právní úpravu Data Retention již před přijetím zmiňované směrnice. Mezi takovéto země patřila i Česká republika, při zavádění povinnosti Data Retention pak byla ve shora zmiňované lhůtě pouze povinna již existující právní úpravu uvést do souladu s požadavky Data Retention Směrnice. V právním řádu České republiky lze proto o prvopočátcích povinnosti Data Retention hovořit již od doby, kdy nabyl účinnosti zákon č. 151/2000 Sb. o telekomunikacích a o změně dalších zákonů (dále též jen „TelZ"), tedy od 1. července 2000.

V tomto právním předpise byla poprvé v právní úpravě platné na území ČR obsažena, jakožto výjimka z povinnosti zachovávat telekomunikační tajemství[255], povinnost právnických a fyzických osob, které vykonávají telekomunikační činnosti, poskytnout oprávněným orgánům vymezené údaje nikoli pouze v režimu on-line, ale také za určitou dobu zpětně – v tomto případě se jednalo o dobu uplynulých „*nejméně dvou měsíců*". Povinné osoby byly takto povinny[256] „*na vlastní náklady sdělit orgánům oprávněným k tomu zvláštními právními předpisy informace o skutečnostech, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, zejména údaje o veškeré komunikaci, kteréhokoli uživatele v uplynulých nejméně dvou měsících v rozsahu volané a volající číslo, použitá služba, datum, čas, doba trvání komunikace a místo připojení*", což doplňovala povinnost „*U poskytovaných datových celků (databází) jsou tyto osoby povinny provádět jejich aktualizaci podle požadavků orgánů oprávněných k tomu zvláštními právními předpisy nejméně jednou za 6 měsíců.*"

V případě údajů, které byly takto povinné osoby oprávněným orgánům povinny zpětně, za uplynulé dva měsíce, sdělit, se jednalo pouze o takové údaje, které byly tyto povinné osoby oprávněny po danou dobu – nejméně dvou měsíců – zpracovávat i pro pracovní účely

[255] Telekomunikační tajemství vymezovalo v dané době ustanovení § 84 TelZ, a to včetně zákazu uloženého právnickým nebo fyzickým osobám, které vykonávají telekomunikační činnosti, jejich zaměstnancům a jiným osobám, které se podílejí na vykonávání telekomunikačních činností „*získávat pro jiné než pracovní účely, vyplývající z jejich telekomunikační činnosti, informace o skutečnostech, které jsou předmětem telekomunikačního tajemství ve větší míře, než je pro vykonávání telekomunikačních činností nezbytně nutné*", doplněnému povinností uloženou každému, „*kdo se dozví informace o skutečnostech, které jsou předmětem telekomunikačního tajemství*", zachovávat o nich mlčenlivost. Telekomunikačním tajemstvím v právním řádu ČR se autor podrobněji zabývá dále.

[256] Viz ustanovení § 86 odst. 1 TelZ ve znění účinném do 30. dubna 2005, kdy byl TelZ nahrazen novou právní úpravou ZoEK.

vyplývající z jejich telekomunikační činnosti. TelZ přitom obecně stanovil, že „*osobní a zprostředkovací data uživatelů telekomunikačních služeb*“[257], jakož i data, která jsou předmětem telekomunikačního tajemství, „*musí být po uplynutí dvou měsíců od ukončení telekomunikačního spojení vymazána nebo učiněna anonymními*“[258]. Současně však TelZ výslovně počítal s výjimkami, podle kterých tato povinnost „*neplatí pro data, která mají být využita k vyúčtování za telekomunikační služby, k zajištění propojení a přístupu k síti, ke vzájemnému vyúčtování mezi provozovateli veřejných telekomunikačních sítí a poskytovateli veřejných telekomunikačních služeb, pokud slouží k identifikaci zneužívání sítě a služeb sítě a pro data uchovávaná a poskytovaná na základě předchozího vyžádání orgánů oprávněných k tomu zvláštními právními předpisy“*[259].

Vzhledem k výše uvedenému vymezení předmětných údajů se zde dle hodnocení autora ještě nejednalo o pravou povinnost Data Retention, totiž o povinnost uchovávat plošně, pouze pro případná vyžádání oprávněných orgánů, určité kategorie údajů, které by osoba vykonávající telekomunikační činnost pro své účely jinak nebyla oprávněna dále zpracovávat či uchovávat. Poslední citovaná výjimka výslovně zmiňuje existenci orgánů, které byly dle zvláštních právních předpisů oprávněny vyžádat si u provozovatelů telekomunikačních sítí či poskytovatelů telekomunikačních služeb předem uchovávání některých údajů, kteréžto údaje byly předmětem telekomunikačního tajemství, jakož i následné poskytnutí takovýchto údajů oprávněnému orgánu. Takovéto relativně šetrné, jelikož nikoli plošné, prolomení práva na ochranu soukromí je v současné praxi označováno jako „data freeze“, jak podrobněji rozebráno dále.

Autor k tomuto považuje za vhodné doplnit, že se současně jednalo o opatření legislativně poněkud nešťastně formulované, když zmiňované ustanovení § 84 odst. 7 TelZ zahrnovalo u formulace „*sdělit orgánům oprávněným k tomu zvláštními právními předpisy*“ rovněž odkaz na poznámku pod čarou, kterou měly patrně být vymezeny oprávněné orgány. Toto ovšem zákonodárce učinil legislativně ne zcela vhodnou formou, navíc tento odkaz formuloval jako toliko příkladmý výčet („*Například zákon č. 67/1992 Sb., zákon č. 154/1994 Sb., zákon č. 283/1991 Sb., zákon č. 141/1961 Sb. a zákon č. 13/1993 Sb.*“). Především však předpisy, které jsou v tomto výčtu výslovně zmíněny, (jednalo se konkrétně o zákon č.

[257] Tato data byla v ustanovení § 84 odst. 5 TelZ definována jako *„jméno a příjmení, popřípadě obchodní jméno, datum narození, rodné číslo, popřípadě identifikační číslo organizace, akademický titul, adresa, popřípadě sídlo“*.
[258] Viz ustanovení § 84 odst. 7 TelZ.
[259] Viz ustanovení § 84 odst. 7 TelZ.

67/1992 Sb. o Vojenském obranném zpravodajství, zákon č. 154/1994 Sb. o Bezpečnostní informační službě, zákon č. 283/1991 Sb. o Policii České republiky, zákon č. 141/1961 Sb. o trestním řízení soudním (trestní řád) a zákon č. 13/1993 Sb. Celní zákon) a dle analýzy provedené autorem ani žádné jiné, v odkazu pod čarou výslovně neuvedené, právní předpisy takováto oprávnění orgánům, jejichž činnost je danými předpisy upravena, nezakládaly. TelZ však výslovně existenci takovéhoto oprávnění předpokládal, jak dle hodnocení autora vyplývá z výše citované formulace „*na základě předchozího vyžádání orgánů oprávněných k tomu zvláštními právními předpisy*“. Z této formulace je nutno dovodit, že samotný text TelZ touto formulací dané oprávnění pro žádný subjekt nezakládá, a to přesto, že v poznámce pod čarou, ovšem pouze a právě v poznámce pod čarou, nikoli přímo v textu právního předpisu, některé právní předpisy (nikoli však též oprávněné orgány) zmiňuje[260].

Podle autorovi dostupných informací některé z orgánů, jejichž činnost upravovaly předpisy označené v rozebírané poznámce pod čarou, po určitou dobu ustanovení TelZ, případně příslušných právních předpisů ve spojení s rozebíraným ustanovením TelZ, vykládaly tak, že jim zakládají příslušná oprávnění ve vztahu k provozovatelům telekomunikačních sítí, resp. poskytovatelům telekomunikačních služeb a že byly tedy oprávněny vyžadovat údaje, které jsou předmětem telekomunikačního tajemství či osobní a zprostředkovací data uživatelů telekomunikačních služeb. Toto nedorozumění pramenilo zpravidla z mylné interpretace pojmů „zpravodajské prostředky“, resp. „zpravodajská

[260] Dle ustálené rozhodovací praxe soudů ČR nemají poznámky pod čarou normativní charakter, jak vyplývá např. z nálezu Ústavního soudu ČR sp. zn. II.ÚS 485/98 ze dne 30. 11. 1999, v němž se Ústavní soud ČR zabýval povahou poznámek pod čarou v právním předpise a výslovně zde konstatoval „*Ústavní soud se ve své ustálené judikatuře řídí důsledně pravidlem, že to, co je uvedeno v poznámce pod čarou nemá závaznou povahu a není to pravidlem chování subjektů uvedených "nahoře nad čarou" ve vlastním textu právního předpisu.“ a dále doplnil „Poznámky pod čarou či vysvětlivky nejsou normativní, přesněji závaznou součástí pravidla chování (např. nálezy ve Sbírce nálezů a usnesení Ústavního soudu ČR, sv. 1, č. 25, sv. 4, č. 83, sv. 6, č. 105-109). Proto stejně jako jiné části právního předpisu, jejichž posláním je zlepšit přehlednost předpisu a orientaci v právním řádu (nadpis právního předpisu, označení částí, hlav, dílů, oddílů, paragrafů), jsou i poznámky pod čarou pouhou legislativní pomůckou, která nemůže být závazným pravidlem pro výklad právního předpisu a stanovení pravidel chování.*“ Obdobně viz též např. nálezy Ústavního soudu ČR sp. zn. I.ÚS 22/99 ze dne 2. 2. 2000, I. ÚS 653/99 ze dne 29. 8. 2000.

technika“ použitých v některých ze zde diskutovaných předpisů[261] či institutu poskytnutí pomoci policii[262], případně institutu dožádání[263].

Ze znění příslušných předpisů, v nichž jsou tyto pojmy použity, jakož i z jejich gramatického a systematického výkladu, je však zřejmé, že pojmy zpravodajská technika, resp. prostředky se vztahují k aktivnímu použití technických prostředků Bezpečnostní informační službou či Vojenským zpravodajstvím za účelem odposlechu či záznamu telekomunikačního nebo jiného provozu, nikoli k tomu, aby takto byly použity technické prostředky v držení třetích osob – poskytovatelů telekomunikačních služeb nebo provozovatelů telekomunikačních sítí. Taktéž při výkladu zmíněných institutů poskytnutí pomoci Policii ČR či dožádání je nutno dospět k závěru, že s jejich využitím nelze vyžadovat poskytnutí informací, ke kterým se vztahuje zvláštní, zákonem založená povinnost mlčenlivosti a u kterých navíc příslušný právní předpis (zde TelZ) předpokládá existenci zvláštního oprávnění orgánů příslušných k jejich vyžádání, jakožto nezbytnou podmínku. V opačném případě by výkladem a contrario bylo možno dospět k závěru, že povinnost poskytnout vyžádané údaje, včetně takových, které jsou předmětem telekomunikačního tajemství (a obdobně též jiných obdobných, zákonem stanovených institutů), se uplatní vždy, když zákon stanoví obecnou, na všechny právnické i fyzické osoby se vztahující, povinnost poskytnout informace či sdělit vyžádané skutečnosti[264]. Dle závěru autora je zřejmé, že takto široce zákonodárce při formulaci diskutovaného ustanovení TelZ povinnost osob povinných k poskytnutí údajů nezamýšlel. Tento závěr potvrzuje rovněž skutečnost, že řešení ve vztahu k oprávněným orgánům nakonec přinesly novelizace zde rozebíraných právních předpisů. Tyto novelizace výslovně zakotvily oprávnění příslušných orgánů vyžadovat údaje, které jsou

---

[261] Např. ustanovení § 12 písm. b) zákona č. 67/1992 Sb. o Vojenském obranném zpravodajství ve znění účinném k datu nabytí účinnosti TelZ, tedy k 1.7.2000, stanoví, že „*Zpravodajskou technikou se pro účely tohoto zákona rozumějí technické prostředky a zařízení, zejména elektronické, fototechnické, chemické, fyzikálně-chemické, radiotechnické, optické, mechanické, anebo jejich soubory, používané utajovaným způsobem při…odposlouchávání, popřípadě zaznamenávání telekomunikačního, radiokomunikačního a jiného obdobného provozu*“., obdobně též viz ustanovení § 8 zákona č. 154/1994 Sb. o Bezpečnostní informační službě.

[262] Ustanovení § 47 zákona č. 283/1991 Sb. o Policii České republiky ve znění k datu nabytí účinnosti TelZ, tedy k 1.7.2000 zakotvuje oprávnění policejních útvarů požadovat při plnění svých úkolů od státních orgánů, orgánů obcí, právnických a fyzických osob pomoc, „*zejména potřebné podklady a informace*“ a ukládá těmto osobám povinnost „*požadovanou pomoc poskytnout, pokud jim v tom nebrání plnění nebo dodržování povinností podle jiných obecně závazných právních předpisů*“.

[263] Ustanovení § 8 Trestního řádu zakotvuje státním orgánům, právnickým a fyzickým osobám povinnost „*vyhovovat dožádáním orgánů činných v trestním řízení při plnění jejich úkolů*“.

[264] Viz např. v době účinnosti rozebíraného ustanovení TelZ platné a účinné znění § 32 odst. 3 zákona č. 71/1967 Sb. o správním řízení (správní řád), které stanovilo, že „*Na žádost správního orgánu jsou státní orgány a socialistické organizace povinny sdělit skutečnosti, které mají význam pro řízení a rozhodnutí.*“

předmětem telekomunikačního tajemství či osobní a zprostředkovací data uživatelů telekomunikačních služeb[265].

Popisovaný právní problém, resp. kolize interpretací příslušných právních předpisů úzce souvisí s požadavky na potřebu jednoznačného vymezení oprávněných orgánů v právní úpravě Data Retention, včetně jednoznačného založení povinnosti povinných osob prolomit ve vztahu k nim telekomunikační tajemství, resp. ochranu provozních a lokalizačních údajů, jak tuto potřebu ve své rozhodovací praxi postupně vymezily soudy. Tento právní problém zahrnuje rovněž některé implikace ve vztahu k platné právní úpravě, resp. k požadavkům na právní úpravu de lege ferenda, autor se jím tedy podrobněji zabývá dále, v části pojednávající o oprávněných orgánech. Na tomto místě tedy autor shrnuje, že dle jeho názoru oprávnění vyžádat si příslušné údaje dle v té době platné a účinné právní úpravy TelZ, jakož ani ostatních právních předpisů, žádnému orgánu nesvědčila a rozebíraná ustanovení § 84 odst. 7 TelZ ve spojení s § 86 odst. 1 TelZ tak byla v době svého vzniku obsoletní.

Právní úprava obsahující specifickou povinnost provozovatelů sítí elektronických komunikací a poskytovatelů služeb elektronických komunikací plošně uchovávat provozní a lokalizační údaje veškerých účastníků či uživatelů účel jejich možného vyžádání oprávněnými orgány je tak v právním řádu ČR účinná od 1. května 2005, tedy od účinnosti ZoEK, který nahradil předchozí TelZ. Důvodová zpráva k vládnímu návrhu ZoEK popisuje důvody zavedení této povinnosti pouze velmi stručně, zmiňuje zvyšující se rizika vyplývající ze situace v oblasti bezpečnosti a také požadavky některých resortů. Důvodová zpráva v rámci hodnocení dopadů zmiňuje také oblast ochrany soukromí, ovšem místo negativních dopadů naopak tvrdí, že navržená úprava přinese ve vztahu k ochraně soukromí pozitiva v podobě povinností podnikatelů k ochraně soukromí uživatelů a účastníků; povinnost Data Retention, která nepochybně představuje významný zásah do soukromí uživatelů a účastníků, zcela opomíjí.

[265] Takovéto novelizace provedl zákon č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a některé další zákony. Tento zákon vložil nová ustanovení § 8a do zákona č. 154/1994 Sb. o Bezpečnostní informační službě, ustanovení § 9 odst. 5 do zákona č. 289/2005 Sb. o Vojenském zpravodajství (tento zákon s účinností od 1.8.2005 nahradil předchozí, výše rozebíraný zákon č. 67/1992 Sb. o Vojenském obranném zpravodajství) a současně též nové ustanovení § 8 odst. 1 zákona č. 15/1998 Sb. o dohledu v oblasti kapitálového trhu a o změně a doplnění dalších zákonů. Všechna tato nová ustanovení výslovně zakotvila oprávnění diskutovaných orgánů (v případě posledně zmiňovaného zákona České národní banky) požadovat od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací poskytnutí provozních a lokalizačních údajů.

Právní úprava Data Retention v ZoEK byla po dobu počátečních několika měsíců v praxi neaplikovatelná. ZoEK totiž v § 97 odst. 3 odkazoval na prováděcí vyhlášku v některých zcela zásadních otázkách, včetně stanovení rozsahu provozních a lokalizačních údajů a doby jejich uchovávání, pro kterou ZoEK stanovil pouze horní limit 12 měsíců[266], a také včetně formy a způsobu předávání těchto údajů oprávněným orgánům. Vyhláška Ministerstva informatiky č. 485/2005 Sb. o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání však nabyla účinnosti až 15. prosince 2005[267], teprve od této doby tak podle názoru autora lze skutečně hovořit o povinnosti Data Retention v právním řádu ČR. Dobu uchovávání údajů tato vyhláška stanovila obecně v délce 6 měsíců, pro některé údaje u datové komunikace 3 měsíce[268].

Novela ZoEK provedená zákonem č. 247/2008 Sb.[269] do právního řádu ČR transponovala Data Retention Směrnici a právní úpravu povinnosti Data Retention v ZoEK a v prováděcí vyhlášce č. 485/2005 Sb. rozpracovala a zpřesnila některé body[270]. Důvodová zpráva k tomuto vládnímu návrhu zákona konstatovala, že „*Směrnice o data retention je v České republice již transponována výše zmíněnými právními předpisy*“, a to v některých směrech v širší podobě a je tedy nutno implementovat pouze některé její články, např. uchovávání provozních a lokalizačních údajů při neúspěšných pokusech o volání.

Schválením vládního návrhu zákona došlo ke splnění povinnosti transpozice, když žádný z pozměňovacích návrhů podaných v Poslanecké sněmovně Parlamentu ČR k tomuto

---

[266] Návrh zákona o elektronických komunikacích neobsahoval horní hranici délky uchovávání údajů, ta byla do návrhu zákona vložena až pozměňovacím návrhem Hospodářského výboru PSP ČR. Viz Sněmovní tisk Poslanecké sněmovny Parlamentu České republiky č. 768/4 – usnesení Hospodářského výboru ze 37. schůze konané dne 1.prosince 2004 [online]. 2004 [cit. 12.1.2023].

[267] Resp. v části údajů u datové komunikace až 1.12.2006 – viz ustanovení § 5 této vyhlášky.

[268] Viz § 4 Vyhlášky č. 485/2005 Sb. o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání, ve znění pozdějších předpisů.

[269] Zákon č. 247/2008 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

[270] Komentář k zákonu o elektronických komunikacích k této novelizaci uvádí *„Novela zákona č. 247/2008 Sb. pak dokončila implementaci této směrnice. Konkrétně do § 97 odst. 3 byla doplněna povinnost uchovávat také údaje o neúspěšných pokusech o volání (…), dále byla stanovena povinnost poskytnout uchovávané provozní a lokalizační údaje orgánům oprávněným k jejich vyžádání bezodkladně, doba uchovávání dat a povinnost povinných subjektů následně uchovávané údaje zlikvidovat byla v souladu se směrnicí o data retention stanovena na dobu v rozsahu 6 až 12 měsíců, pokud nebyly poskytnuty orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu, a byla zavedena povinnost vedení evidence (viz odst. 10 až 12). Upraveno bylo také zmocňovací ustanovení k vydání vyhlášky Ministerstva“.* Viz CHUDOMELOVÁ, Zuzana, BERAN, Marek, JADRNÝ, Vratislav, NĚMEČKOVÁ, Šárka, NOVÁK, Jaromír. *Zákon o elektronických komunikacích. Komentář.* Praha: Wolters Kluwer ČR, 2016.

sněmovnímu tisku nebyl přijat[271]. Vyhláška č. 485/2005 Sb. zůstala po přijetí uvedené novely nezměněna, ustanovení § 4 odst. 1, dle kterého „*Údaje se uchovávají po dobu 6 měsíců, není-li v odstavci 2 stanoveno jinak.*“, totiž vyhovovalo jak předchozímu zmocňovacímu ustanovení § 97 odst. 3 („*Rozsah provozních a lokalizačních údajů, dobu jejich uchovávání, která nesmí být delší než 12 měsíců, a formu a způsob jejich předávání orgánům oprávněným k jejich využívání, stanoví prováděcí právní předpis.*“), tak rovněž novelizovanému ustanovení § 97 odst. 3 ZoEK, dle kterého „*Doba uchovávání těchto provozních a lokalizačních údajů nesmí být kratší než 6 měsíců a delší než 12 měsíců.*“, v praxi tedy v otázce doby uchovávání údajů v důsledku novely nedošlo k žádné změně, také rozsah uchovávaných údajů zůstal v této vyhlášce širší nežli vyžadovala Data Retention Směrnice.

Ústavní soud ČR nálezem sp. zn. Pl. ÚS 24/10[272] zrušil právní úpravu Data Retention, tedy konkrétně ustanovení § 97 odst. 3 a 4 ZoEK a dále též vyhlášku č. 485/2005 Sb., dnem vyhlášení nálezu ve Sbírce zákonů, tedy ke 12. dubnu 2011 účinnosti, jak rozebráno podrobně dále. Navazujícím nálezem sp. zn. Pl. ÚS 24/11[273] Ústavní soud ČR rozhodl o zrušení ustanovení obsahujícího povinnost Data Retention v Trestním řádu, s účinností od 30. září 2012. Následná novela Trestního řádu provedená zákonem č. 273/2012 Sb.[274] (dále též jen „Novela ZoEK“) s účinností od 1. října 2012 povinnosti dle Data Retention Směrnice do právního řádu ČR, tedy do ZoEK i do Trestního řádu, opět zavedla, a to při respektování většiny výtek Ústavního soudu ČR, tedy v pozměněné podobě. Povinné osoby jsou podle ní povinny uchovávat provozní a lokalizační údaje[275] a na požádání je poskytnout oprávněným

[271] Podané pozměňovací návrhy se týkaly především doby uchovávání údajů – jeden ze zamítnutých poslaneckých pozměňovacích návrhů požadoval v ZoEK výslovně uvést, že doba uchovávání nesmí být delší než 6 měsíců, místo navrhovaného textu, dle kterého nesmí být tato doba kratší než 6 měsíců a delší než 12 měsíců, dále vymezení orgánů oprávněných k vyžádání údajů – pozměňovací návrh Výboru pro bezpečnost navrhoval nahradit formulaci „*orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu*“ výslovným uvedením oprávněných orgánů v ZoEK, a to jen jednoho orgánu, Policie ČR, dále vymezení kategorií uchovávaných údajů, kdy jeden z poslaneckých návrhů předpokládal zařazení seznamu kategorií zpracovávaných údajů přímo do zákona formou přílohy, místo navrhovaného zmocňovacího ustanovení obsaženého v návrhu novely a předpokládajícího vymezení tohoto seznamu v prováděcím právním předpisu. Jak již autor uvádí výše, ani jeden z poslaneckých návrhů nebyl přijat.

[272] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011 vyhlášený ve Sbírce zákonů ČR pod číslem 94/2011 Sb.

[273] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 24/11 ze dne 20. prosince 2011 vyhlášený ve Sbírce zákonů ČR pod číslem 43/2012 Sb.

[274] Zákon č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony.

[275] Kompletní výčet údajů je obsažen v ustanovení § 2 vyhlášky č. 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

orgánům v ZoEK výslovně vyjmenovaným, autor se touto právní úpravou podrobněji zabývá dále.

Relevantní právní úprava

Přestože byla Data Retention Směrnice prohlášena Soudním dvorem EU neplatnou již 8. dubna 2014, a to s okamžitými účinky[276] a v současnosti tedy postrádá právní závaznost, považuje autor za vhodné se na tomto místě Data Retention Směrnici stručně věnovat. Důvodem je skutečnost, že text Data Retention Směrnice dodnes tvoří faktický základ právní úpravy Data Retention v právním řádu ČR, i po modifikacích, ke kterým došlo zejména reakcí zákonodárce na výtky obsažené v dále zmiňovaných nálezech Ústavního soudu ČR).

Data Retention Směnice

Data Retention Směnice byla přijata na základě článku 95 Smlouvy o založení Evropského společenství, tedy jako *„opatření ke sbližování ustanovení právních a správních předpisů členských států, jejichž účelem je vytvoření a fungování vnitřního trhu“*[277], nikoli jako prostředek boje proti terorismu či pro koordinaci postupů pro vyšetřování závažné trestné činnosti. Harmonizaci předpisů členských států Data Retention Směrnice výslovně stanovila jako svůj účel[278].

Data Retention Směrnice stanovila členským státům povinnost přijmout opatření pro zajištění uchovávání provozních a lokalizačních údajů právnických a fyzických osob a souvisejících údajů vytvářených nebo zpracovávaných poskytovateli veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí, a to v kategoriích v této směrnici uvedených. Tuto povinnost měly členské státy nejpozději do 15. září 2007, s možností delší lhůty až do 15. března 2009 pro zavedení opatření pro uchovávání komunikačních údajů týkajících se připojení k internetu, internetové telefonie a internetové elektronické pošty; ČR byla mezi státy, které této delší lhůty využily. Data Retention Směrnice se nevztahovala na obsah elektronické komunikace ani na údaje, které takovýto obsah odhalují, jak její text výslovně stanovil[279].

---

[276] Generální advokát Soudního dvora EU, Pedro Cruz Villalón ve svém Stanovisku pro Soudní dvůr EU, předneseném 12. prosince 2013 navrhoval prohlásit Data Retention Směrnici za neplatnou, ovšem současně navrhoval pozastavit určení neplatnosti do doby, než unijní zákonodárce přijme nezbytná opatření k nápravě, Soudní dvůr se však k tomuto návrhu nepřiklonil. Podrobněji k tomuto viz kapitola 4.2.3. Stanovisko Generálního advokáta Soudního dvora EU, Pedro Cruz Villalóna přednesené 12. prosince 2013 ve věci C-293/12.
[277] Článek 95 odst. 1 (bývalý článek 100a) Smlouvy o založení Evropského společenství.
[278] Viz článek 1 odst. 1 Data Retention Směrnice.
[279] Viz čl. 1 odst. 2 a čl. 5 odst. 2 Data Retention Směrnice.

Řadu základních pojmů Data Retention Směrnice přímo nedefinovala a odkazovala v tomto směru na jiné předpisy, Směrnici 95/46/ES[280], jakožto základní předpis unijního práva v oblasti ochrany osobních údajů a dvě ze směrnic tehdejšího regulačního rámce pro oblast elektronických komunikací – Směrnici o soukromí a elektronických komunikacích a Směrnici 2002/21/ES[281]. Směrnice o soukromí a elektronických komunikacích definovala především provozní údaje jako „*jakékoli údaje zpracovávané pro účely přenosu sdělení sítí elektronických komunikací nebo pro jeho účtování*“ a lokalizační údaje jako „*jakékoli údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací*“[282]. Ve Směrnici 2002/21/ES byly vymezeny základní termíny elektronických komunikací, včetně pojmu účastník, jakožto „*každá fyzická nebo právnická osoba, která uzavřela s poskytovatelem veřejně přístupných služeb elektronických komunikací smlouvu o poskytování takových služeb*“. Data Retention Směrnice vymezovala pojem uživatel, a to jako „*jakákoli právnická nebo fyzická osoba používající veřejně dostupnou službu elektronických komunikací pro soukromé či obchodní účely, přičemž nemusí být nutně účastníkem této služby*“ a z pojmů s relevancí pro tuto práci též pojem neúspěšný pokus o volání: „*komunikace, během které bylo telefonní volání úspěšně spojeno, ale zůstalo bez odezvy nebo došlo k zásahu správce sítě*“ [283].

Směrnice o soukromí a elektronických komunikacích[284]

Zatímco dle Směrnice o soukromí a elektronických komunikacích je v zásadě nutno provozní a lokalizační údaje vytvářené při používání služeb elektronických komunikací, které již nejsou potřebné pro přenos sdělení, vymazat, nebo anonymizovat, Data Retention Směrnice upravovala odchylný postup. Směrnice o soukromí a elektronických komunikacích stanoví výjimku pouze pro údaje potřebné pro účtování nebo stanovení plateb za propojení a na základě souhlasu subjektů údajů též určitých údajů pro marketingové účely a pro poskytování

[280] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Tuto směrnici nahradilo Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů, tzv. GDPR – General Data Protection Regulation).
[281] Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice).
[282] Článek 2 Směrnice o soukromí a elektronických komunikacích.
[283] Článek 2 odst. 2 písm. b) a f) Data Retention Směrnice.
[284] Evropská komise zahájila 12. dubna 2016 proces veřejné konzultace za účelem vyhodnocení a přezkumu Směrnice o soukromí a elektronických komunikacích, následně Evropská komise po několik let opakovaně zveřejňovala návrhy textu nařízení ePrivacy, které by mělo Směrnici o soukromí a elektronických komunikacích nahradit, k datu dokončení této práce však k tomu nedošlo.

služeb s přidanou hodnotou[285]. Současně tato směrnice jako další výjimku z daného pravidla také členským státům EU za určitých okolností umožnuje přijmout opatření, kterými omezí rozsah ochrany poskytovaný provozním, lokalizačním a souvisejícím údajům; každé takové omezení musí být v demokratické společnosti nezbytné, přiměřené a úměrné pro zajištění národní bezpečnosti, obrany, veřejné bezpečnosti nebo pro předcházení, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronických komunikačních systémů[286]. Výklad tohoto článku Směrnice o soukromí a elektronických komunikacích, konkrétně posouzení souladu obecné povinnosti uchovávat provozní a lokalizační údaje obsažené v národních právních řádech s tímto článkem, se následně stal předmětem rozhodování Soudního dvora EU, autor o nich pojednává podrobněji dále.

Dle odůvodnění obsaženého v Data Retention Směrnici několik členských států přijalo takovéto právní předpisy, kterými stanovily poskytovatelům služeb povinnost uchovávat údaje pro potřeby předcházení, vyšetřování, odhalování a stíhání trestných činů. Tyto vnitrostátní předpisy se však vzájemně značně liší, přičemž „*právní a technické odlišnosti mezi těmito vnitrostátními předpisy představují překážku na vnitřním trhu elektronických komunikací, protože poskytovatelé služeb čelí různým požadavkům ohledně druhů provozních a lokalizačních údajů, které se mají uchovávat, a podmínek a lhůt uchovávání*“[287].

Zákon o elektronických komunikacích

V právním řádu ČR nyní definuje povinnost Data Retention ustanovení § 97 odst. 3 ZoEK, které ukládá *„právnické nebo fyzické osobě zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinnost uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytování jejích veřejně dostupných služeb elektronických komunikací“*.

[285] Viz čl. 5, 6 a 9 Směrnice o soukromí a elektronických komunikacích.
[286] Čl. 15 odst. 1 Směrnice o soukromí a elektronických komunikacích: *„Členské státy mohou přijmout legislativní opatření, kterými omezí rozsah práv a povinností uvedených v článku 5, článku 6, čl. 8 odst. 1, 2, 3 a 4 a článku 9 této směrnice, pokud toto omezení představuje v demokratické společnosti nezbytné, přiměřené a úměrné opatření pro zajištění národní bezpečnosti (tj. bezpečnosti státu), obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů nebo neoprávněného použití elektronického komunikačního systému, jak je uvedeno v čl. 13 odst. 1 směrnice 95/64/ES. Členské státy mohou mimo jiné přijmout právní opatření umožňující zadržení údajů na omezenou dobu na základě důvodů uvedených v tomto odstavci. Veškerá opatření uvedená v tomto odstavci musí být v souladu s obecnými zásadami práva Společenství, včetně zásad uvedených v čl. 6 odst. 1 a 2 Smlouvy o založení Evropské unie.“*
[287] Viz body 4, 5 a 6 recitálu Data Retention Směrnice.

V následujících ustanoveních[288] pak ZoEK tuto povinnost dále rozvádí, zejména vymezuje, co se rozumí provozními a lokalizačními údaji pro účely povinnosti Data Retention[289], stanoví poskytovatelům hlasových komunikačních služeb povinnost poskytnout na žádost informace z databáze účastníků (nejčastěji tzv. „ztotožnění" účastníků), v rozsahu stanoveném prováděcím předpisem[290] a také ukládá provozovateli sítě či poskytovateli služeb elektronických komunikací, pokud zavedl „*kódování, kompresi, šifrování nebo jiný způsob přenosu vedoucí k nesrozumitelnosti přenášených zpráv*"[291], povinnost *zajistit, aby „zprávy a s nimi spojené provozní a lokalizační údaje",* byly v koncových bodech *„poskytovány srozumitelným způsobem*"[292]. S ohledem na rozsah povinnosti Data Retention pro povinné osoby – provozovatele sítí a poskytovatele služeb elektronických komunikací jim ZoEK přiznává nárok na úhradu efektivně vynaložených nákladů při plnění této povinnosti[293]. Otázka náhrady nákladů spojených s plněním povinnosti Data Retention není v právních řádech států EU řešena jednotně, také v ZoEK již doznala několika změn.

ZoEK definuje provozní a lokalizační údaje obdobně, jako jsou vymezeny ve výše zmíněné Směrnici o soukromí a elektronických komunikacích [294], tedy jako veškeré údaje vznikající při komunikaci prostřednictvím služeb a sítí elektronických komunikací a v souvislosti s touto komunikací, výjimkou je pouze obsah komunikace[295]. Pokud jsou generovány informace o neúspěšných pokusech o volání, jsou též provozními údaji. Provozní údaje zahrnují tedy údaje veškerých účastníků a uživatelů služeb elektronických komunikací,

---

[288] Ustanovení § 97 odst. 4–9 ZoEK.

[289] Ustanovení § 97 odst. 4 ZoEK – podrobněji rozebráno dále, v souvislosti s vymezením provozních a lokalizačních údajů.

[290] Tímto předpisem je Vyhláška Ministerstva vnitra ČR č. 336/2005 Sb. ze dne 29. srpna 2005 o formě a rozsahu informací poskytovaných z databáze účastníků veřejně dostupné telefonní služby a o technických a provozních podmínkách a bodech pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv.

[291] Ustanovení § 97 odst. 6 ZoEK.

[292] Autor podotýká, že v současnosti je možné a v praxi běžné, že takovéto „znesrozumitelnění" zpráv zajistí sám koncový účastník instalací a využíváním některé z dostupných aplikací, kterou si instaluje do svého koncového zařízení. Podle autorovi dostupných informací u některých z těchto aplikací již oprávněné orgány nalezly cestu k dekódování komunikace, zpravidla ve spolupráci s poskytovatelem aplikace, neplatí to však pro všechny případy. K tomu podrobněji SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 219–223.

[293] Dle ustanovení § 97 odst. 7 ZoEK jejich výši a způsob úhrady stanoví prováděcí právní předpis. Tím je Vyhláška Českého telekomunikačního úřadu č. 462/2013 Sb. ze dne 19. prosince 2013 o stanovení výše a způsobu úhrady efektivně vynaložených nákladů na odposlech a záznam zpráv, na uchovávání a poskytování provozních a lokalizačních údajů a na poskytování informací z databáze účastníků veřejně dostupné telefonní služby, ve znění pozdějších předpisů. Jedná se o náklady provozovatelů sítí a poskytovatelů služeb na pořízení a provozování technického vybavení pro účely plnění povinností a náklady na zajištění činností s plněním povinností spojených.

[294] Ustanovení § 90 odst. 1 a § 91 odst. 1 ZoEK.

[295] Obsah komunikace je předmětem odposlechu provozu v sítích elektronických komunikací, který je právně upraven v ZoEK a v Trestním řádu.

včetně uživatelů předplacených karet, kteří jsou anonymní. Ohledně rozsahu *uchovávaných provozních a lokalizačních údajů, formy a způsobu jejich předávání oprávněným orgánům a některých dalších otázek odkazuje ZoEK na* prováděcí právní předpis. Tím je aktuálně vyhláška č. 357/2012 Sb.[296], která s účinností od 1. listopadu 2012 nahradila předchozí vyhlášku č. 485/2005 Sb. [297], zrušenou před více než rokem Ústavním soudem ČR ke dni 11. dubna 2011[298].

Aktuální vyhláška v ustanovení § 2 stanoví kategorie uchovávaných provozních a lokalizačních údajů zvlášť pro veřejné telefonní sítě s přepojováním okruhů, pro veřejné mobilní telefonní sítě, pro sítě elektronických komunikací s přepojováním paketů. Jedná se prakticky o veškeré údaje, které vůbec v souvislosti s konkrétním spojením (resp. s pokusem o spojení, když mezi údaje povinně uchovávané patří rovněž údaje související s neúspěšným pokusem o spojení) v síti elektronických komunikací mohou vzniknout. Povinně uchovávány jsou takto i takové údaje, u nichž si patrně strany komunikace nejsou vědomy jejich možného zaznamenávání či přenášení v rámci spojení, mnohdy jim ani nejsou známy, např. identifikace koncových zařízení – telefonních přístrojů použitých na obou stranách, prostřednictvím jedinečného čísla IMEI[299], označení základnové stanice veřejné mobilní sítě elektronických komunikací, k níž je každá ze stran v rámci spojení připojena a další. Mezi provozní údaje nepatří obsah komunikace, což je samozřejmé v případě komunikace hlasové, platí to však v plné míře i pro veškeré další formy komunikace, tedy ani v případě SMS zpráv či datové komunikace nejsou poskytovatelé služeb a provozovatelé sítí povinni uchovávat obsah komunikace a nejsou k tomu ani oprávněni. Uchováváním obsahu by se dopustili porušení telekomunikačního tajemství. Výslovný zákaz uchovávat obsah komunikace stanoví navíc též ustanovení § 97 odst. 3 ZoEK, když povinným subjektům ukládá povinnost „*zajistit, aby při plnění povinnosti podle věty první a druhé nebyl uchováván obsah zpráv a takto uchovávaný dále předáván*“.

---

[296] Vyhláška č. 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, ve znění pozdějších předpisů.

[297] Někteří autoři v době účinnosti této vyhlášky uvažovali o tom, že provozní údaje, které lze zajistit dle § 88a Trestního řádu, zahrnují *„zejména pro potřeby vyšetřování počítačové kriminality“* i údaje o provozu *„elektronické pošty (e-mailů)*“. Viz GŘIVNA, Tomáš, POLČÁK, Radim (eds.) *Kyberkriminalita a právo*. Praha: Auditorium s.r.o., 2008. s. 95.

[298] Nálezem Ústavního soudu ČR sp. zn. Pl. ÚS 24/10 se autor zabývá podrobněji v souvislosti se zrušením povinnosti Data Retention v právním řádu ČR.

[299] IMEI – International Mobile Eqipment Identity je unikátní číslo každého mobilního koncového zařízení přidělené výrobcem.

U základnových stanic se povinnost uchovávání vztahuje na označení počáteční a koncové základnové stanice[300] - „*základnová stanice Start*“ a „*základnová stanice Stop*“. Z těchto údajů lze dovodit trasu pohybu koncového zařízení a tedy i pohybu jeho účastníka či uživatele. Aktuální vyhláška vychází při vymezení kategorií uchovávaných údajů z Data Retention Směrnice, liší se však v členění údajů dle technického hlediska, v závislosti na typu sítě elektronických komunikací, na rozdíl od Data Retention Směrnice, která údaje rozdělovala do skupin primárně podle účelu jejich použití[301].

Přes značný rozsah aktuálně uchovávaných kategorií údajů probíhají již delší dobu diskuse o jejich rozšíření, zejména o cílovou IP adresu[302], jakožto doplnění ke zdrojové IP adrese, která již v seznamu uchovávaných údajů je obsažena. Již v říjnu 2015 byla připravena novela této vyhlášky v paragrafovaném znění[303], jejímž cílem bylo u služby přístupu k internetu z pevného či mobilního připojení rozšířit kategorie údajů o adresu IP a číslo portu zařízení, ke kterému bylo přistoupeno. Návrh novely vyhlášky byl následně předložen k připomínkovému řízení, předpokládaný termín její účinnosti byl 1. leden 2016. V rámci připomínkového řízení byl však návrh novely kritizován, ÚOOÚ ve svém stanovisku[304] vytkl chybějící vyhodnocení dopadů navrhovaného řešení do soukromí a do ochrany osobních údajů a požadoval, aby rozšíření kategorií údajů bylo kompenzováno zkrácením doby jejich uchovávání, výslovně se také ohradil proti tvrzení, že s ním bylo navrhované řešení konzultováno. Také poskytovatelé služeb elektronických komunikací vyslovili k návrhu kritické připomínky, včetně vysokých nákladů na implementaci. Novela následně nebyla předložena.

---

[300] Dle Vyhlášky č. 357/2012 Sb. „základnová stanice Start“ a „základnová stanice Stop“.

[301] Viz článek 5 Data Retention Směrnice.

[302] *„IP adresa je série číslic, sloužící k jedinečné identifikaci zařízení připojeného k síti internet. Skládá se ze dvou částí, identifikace sítě, která určuje geografickou lokalizaci sítě, a Host ID přesně určující konkrétní zařízení nebo část sítě. Na základě toho, zda je jedna IP adresa trvale přiřazena konkrétnímu zařízení, nebo zda se IP adresa zařízení mění v průběhu času, rozlišujeme ještě statické a dynamické IP adresy.“* HARAŠTA, J.; MÍŠEK, J. IP adresy v kybernetické bezpečnosti. Revue pro právo a technologie. 2015, roč. 6, č. 12, s. 21.

[303] Návrh novely Vyhlášky Ministerstva průmyslu a obchodu č. 357/2012 Sb. ze dne 17. října 2012 o uchovávání, předávání a likvidaci provozních a lokalizačních údajů. *Hospodářská komora České republiky.* [online]. 2015 [cit. 24.2.2024].

[304] ÚOOÚ. *Uchování údajů – prováděcí vyhláška.* Č.j. UOOU-11928/15-8. 3.listopadu 2015. [online]. [cit. 24.2.2024]. Dostupné z www.uoou.gov.cz.

Trestní řád

Na právní úpravu Data Retention obsaženou v ZoEK navazuje úprava v § 88a Trestního řádu[305], která stanoví podmínky, za nichž lze „*zjistit údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat*“[306]. Ustanovení § 88a v prvé řadě vymezuje trestné činy, pro které je možno vydat příkaz k zjištění údajů o telekomunikačním provozu, dále jsou zde upraveny procedurální aspekty a náležitosti tohoto příkazu. Vymezení trestných činů zde přitom zákonodárce provedl výrazně šířeji v porovnání s trestnými činy, pro které lze nařídit odposlech a záznam telekomunikačního provozu. Příkaz k zjištění údajů o telekomunikačním provozu Trestní řád umožňuje vydat kromě trestných činů výslovně vyjmenovaných v § 88a a pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, také pro jakýkoli trestný čin, za podmínky že jde o úmyslný trestný čin a současně na něj zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky. Pro porovnání, odposlech a záznam telekomunikačního provozu lze nařídit kromě trestných činů výslovně vyjmenovaných v § 88 (již samotný jejich výčet je stručnější) také pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva a dále pro takový zločin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let. Z porovnání je zřejmé, že z hlediska okruhu trestných činů nastavil zákonodárce podmínky nařízení odposlechu a záznamu telekomunikačního provozu výrazně restriktivněji, nežli je tomu u podmínek pro vydání příkazu ke zjištění údajů o telekomunikačním provozu.

Ustanovení § 88 upravující odposlech a záznam telekomunikačního provozu bylo do Trestního řádu vloženo s účinností od 1. července 1990[307], ustanovení § 88a pak bylo doplněno s účinností od 1. ledna 2002[308]. Zatímco § 88 pro nařízení odposlechu[309] stanovil od počátku poměrně striktní podmínky z hlediska vymezení trestných činů, pro které jej bylo možno nařídit, § 88a byl při stanovení podmínek velmi benevolentní, když dle jeho znění

[305] Toto ustanovení společně s § 88 upravujícím podmínky nařízení odposlechu a záznamu telekomunikačního provozu tvoří Oddíl sedmý, nazvaný souhrnně Odposlech a záznam telekomunikačního provozu.
[306] Zákonodárce zde setrval u původního pojmu „*telekomunikace*“, resp. „*telekomunikační provoz*“ a nenahradil jej pojmem „elektronické komunikace“. Praktický dopad ve vztahu k diskutovanému tématu však autor hodnotí jako nevýznamný.
[307] Novela provedená zákonem č. 178/1990, kterým se mění a doplňuje trestní řád.
[308] Novela provedená zákonem č. 265/2001 Sb., kterým se mění zákon č. 141/1961 Sb. o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 140/1961 Sb. trestní zákon, ve znění pozdějších předpisů, a některé další zákony.
[309] Tehdy byl tento institut označen pouze jako odposlech telefonních hovorů, nikoli odposlech a záznam telekomunikačního provozu. Původně upravoval pouze odposlech hlasové telefonie, v současné verzi již odposlech a záznam veškerého telekomunikačního provozu, tedy kromě hlasových služeb též služeb datových.

účinného od 1. ledna 2002 bylo možno příkaz k zjištění údajů o telekomunikačním provozu vydat v jakémkoli trestním řízení, zcela bez omezení trestného činu, pro který bylo vedeno, tedy včetně nejméně závažných trestných činů. Dle hodnocení autora to svědčí o zásadním podcenění významu těchto údajů i významu zásahu do soukromí, který jejich užití představuje, jak ze strany předkladatele vládního návrhu novely, tak rovněž zákonodárce.

Kritéria pro vydání příkazu k zjištění údajů o telekomunikačním provozu byla následně zpřísněna v reakci na nález Ústavního soudu ČR sp. zn. Pl. ÚS 24/11, kterým se uplynutím dne 30. září 2012 ruší § 88a Trestního řádu, právě s ohledem na nedostatečné garance práv uživatelů služeb elektronických komunikací obsažené v tomto ustanovení, v porovnání s garancemi u nařízení odposlechu a záznamu telekomunikačního provozu dle § 88 Trestního řádu. Ke zpřísnění došlo Novelou ZoEK, která s účinností od 1. října 2012 novelizovala Trestní řád. Právní úprava Data Retention, předtím zrušená dvěma nálezy Ústavního soudu ČR[310], byla Novelou ZoEK opět zavedena jak do ZoEK, tak rovněž do Trestního řádu. Nové ustanovení § 88a Trestního řádu již vymezuje trestné činy, pro které je možné vydat příkaz k zjištění údajů o telekomunikačním provozu. Vedle toho Novela ZoEK do Trestního řádu zakotvila rovněž další omezení a záruky, vč. požadavku na uvedení totožnosti uživatele v příkazu k zjištění údajů o telekomunikačním provozu, je-li známa, pokud se žádost vztahuje ke konkrétnímu uživateli.

Zatímco znění § 88a Trestního řádu účinné k datu dokončení této práce hovoří o potřebě „*zjistit údaje o telekomunikačním provozu*“, předchozí znění tohoto ustanovení, posuzované Ústavním soudem ČR v nálezu sp. zn. Pl. ÚS 24/10, obsahovalo formulaci „*zjistit údaje o uskutečněném telekomunikačním provozu*“. Někteří autoři z tohoto rozdílu dovozují, že „*Zjištění údajů o telekomunikačním provozu dle § 88a TŘ je možné realizovat jak do minulosti, tak do budoucnosti.*“ [311] Autor se s tímto výkladem neztotožňuje, v praxi však nezaznamenal problémy z toho vyplývající, rozhodující bude v konkrétních případech textace příkazu k zjištění údajů o telekomunikačním provozu.

Trestní řád nyní též stanoví povinnost informovat o nařízeném zjišťování údajů o telekomunikačním provozu osobu uživatele, pokud je známa, a to po pravomocném skončení věci, s výjimkami v zákoně uvedenými. Tuto informační povinnost Trestní řád ukládá státnímu zástupci nebo policejnímu orgánu, jehož rozhodnutím byla věc pravomocně skončena, resp. v řízení před soudem předsedovi senátu soudu prvního stupně, stanoví též

[310] Nálezy Ústavního soudu ČR sp. zn. Pl. ÚS 24/10 a Pl. ÚS 24/11.
[311] Viz. KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, z.s.p.o., 2016. s. 443.

povinné náležitosti této informace, vč. údaje o období, kterého se příkaz týká. Rozebíraná Novela ZoEK také rozšířila dosavadní procesní úpravu přezkoumání zákonnosti příkazu k odposlechu a záznamu telekomunikačního provozu i o přezkum příkazu k zjištění údajů o telekomunikačním provozu, a to za shodných podmínek[312]. K podání návrhu na přezkum je aktivně legitimován dotčený uživatel, kterému byla určena informace o nařízeném zjišťování údajů o telekomunikačním provozu. Uživatel je oprávněn podat návrh k Nejvyššímu soudu ve lhůtě šesti měsíců ode dne doručení této informace, přičemž již samotná informace musí obsahovat mimo jiné rovněž poučení o právu podat tento návrh. Výsledkem řízení o přezkumu je vydání usnesení, kterým soud vysloví porušení zákona v případě, kdy v rámci přezkumu zjistí, že příkaz byl vydán nebo jeho provedení bylo v rozporu se zákonem, nebo usnesení, kterým soud vysloví, že zákon nebyl porušen.

Souvislost s rozebíranou problematikou má také § 30 odst. 5 Trestního řádu, který vymezuje vyloučení soudce, který se zúčastnil rozhodování v předchozím řízení, z řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu. Takovéto vyloučení se nevztahuje též na řízení o přezkumu příkazu k zjištění údajů o telekomunikačním provozu, což je dle názoru autora patrně vlivem existence ustanovení § 30 odst. 5 Trestního řádu již před zmiňovanou novelou; důvody, proč nebylo též novelizováno, nejsou zřejmé. Autor však dospívá k závěru, že obdobně by mělo platit vyloučení soudce také ve vztahu k řízení o přezkumu zákonnosti příkazu k zjištění údajů o telekomunikačním provozu, když na tuto situaci lze dle hodnocení autora aplikovat obecné ustanovení § 30 odst. 1 Trestního řádu o vyloučení soudce pro pochybnosti o nestrannosti pro poměr k projednávané věci. De lege ferenda by ovšem bylo velmi vhodné toto v Trestním řádu výslovně zakotvit, v zájmu předejití pochybnostem a výkladovým nejasnostem v rozhodovací praxi soudů[313].

Trestní řád konečně také v ustanovení § 8c výslovně stanoví zákaz zveřejnění informací o nařízení či provedení odposlechu a záznamu telekomunikačního provozu nebo informací z něj získaných, stejně jako údajů o telekomunikačním provozu zjištěných na základě příkazu podle § 88a Trestního řádu (a obdobně též informací získaných sledováním osob a věcí podle § 158d odst. 2 a 3 téhož předpisu) bez souhlasu osoby, které se takové informace týkají[314], s výjimkou případů, v nichž by Trestní řád nebo zvláštní právní předpis

[312] § 314l a násl. Trestního řádu.
[313] Viz např. Nález Ústavního soudu ČR sp. zn. Pl. ÚS 13/06 z 8. července 2008, rozsudek Nejvyššího soudu ČR sp. zn. 4 Tdo 1346/2014 ze 29. října 2014, odlišný názor je obsažen v rozsudku Nejvyššího soudu ČR sp. zn. 4 Tdo 630/2005 ze dne 8. června 2005.
[314] Výjimka, která byla v tomto ustanovení v původním znění obsažena a dle které tento zákaz zveřejnění platil jen, pokud Trestní řád nebo zvláštní právní předpis nestanoví jinak, byla vypuštěna zákonem č. 207/2011 Sb.,

stanovil jinak. Tento zákaz se vztahuje nejen na osoby, které jsou osobami oprávněnými údaje o odposlechu a záznamu nebo údaje o telekomunikačním provozu získat, nýbrž na všechny („*nikdo nesmí…zveřejnit…*“) a platí pouze v případě takových informací, které umožňují zjištění totožnosti dotčené osoby a které nebyly použity jako důkaz v řízení před soudem. Zákonem č. 207/2011 Sb.[315] bylo do Trestního řádu doplněno ustanovení § 8d, které umožňuje v určitých situacích zveřejnit informace, na které se vztahuje zde diskutovaný zákaz zveřejnění, např. zveřejnění za účelem pátrání po osobách či velmi vágně vymezené a nikterak konkrétně omezené zveřejnění pro „*dosažení účelu trestního řízení*“, stejně jako obdobně vágně vymezená možnost zveřejnění v situaci, kdy to odůvodňuje „*veřejný zájem, pokud převažuje nad právem na ochranu soukromí dotčené osoby*“. Autor považuje takto vágně a široce vymezené důvody, kdy je zákonem umožněn závažný zásah do soukromí dotčené osoby, jaký představuje dokonce zveřejnění údajů získaných při plnění povinnosti Data Retention, bez vymezení kategorií údajů, které lze zveřejnit a bez konkrétních omezení možnosti zveřejnění, za velmi problematické.

Orgány oprávněné k vyžádání a využití údajů

Z vymezení povinnosti Data Retention obsaženého v úvodu této kapitoly je zřejmé, že osobami povinnými k uchovávání provozních a lokalizačních údajů účastníků a uživatelů elektronických komunikací jsou poskytovatelé služeb a provozovatelé sítí elektronických komunikací. Osoby oprávněné k vyžádání těchto údajů, tedy orgány veřejné moci, si provozní a lokalizační údaje vyžadují u těchto povinných osob. Z ustálené rozhodovací praxe Ústavního soudu ČR vyplývá ve vztahu k orgánům oprávněným k zásahu do základních práv, zde zásahu do soukromí fyzických osob, požadavek na přesně a předvídatelně formulovanou právní úpravu takovýto zásah zakládající, tento požadavek zahrnuje i jednoznačné vymezení orgánů oprávněných k vyžádání údajů a striktní definování jejich pravomocí[316]. Skutečnost, že povinnými osobami v tomto případě nejsou orgány veřejné moci, nýbrž provozovatelé sítí a

---

kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů; tímtéž zákonem bylo do Trestního řádu doplněno ustanovení § 8d, které umožňuje v určitých situacích zveřejnit informace, na které se vztahuje zde diskutovaný zákaz zveřejnění, mezi takovéto situace patří např. zveřejnění za účelem pátrání po osobách či velmi vágně vymezené a nikterak konkrétně neomezené zveřejnění pro „*dosažení účelu trestního řízení*“, stejně jako obdobně vágně vymezená možnost zveřejnění v situaci, kdy to odůvodňuje „*veřejný zájem, pokud převažuje nad právem na ochranu soukromí dotčené osoby*“.

[315] Zákon č. 207/2011 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

[316] Viz nález Ústavního soudu ČR sp. zn. II.ÚS 502/2000 ze dne 22. 1. 2001: *„Tyto právní předpisy musí být přesné ve svých formulacích, aby daly občanům dostatečnou informaci o okolnostech a podmínkách, za kterých jsou státní orgány oprávněny k zásahu do soukromí…“*, obdobně též nálezy sp. zn. Pl. ÚS 24/10 ze dne 22.3.2011 či IV.ÚS 78/01 ze dne 27. 8. 2001.

poskytovatelé služeb elektronických komunikací, tedy právnické osoby soukromého práva, klade navíc dle hodnocení autora na přesné vymezení orgánů oprávněných vyžádat si tyto údaje zvýšené požadavky[317].

V aktuálně platné právní úpravě povinnosti Data Retention jsou orgány oprávněné vyžádat si provozní a lokalizační údaje vymezeny v ZoEK[318], s výhradou dále uvedenou v případě ÚOOÚ. Ne vždy tomu tak ovšem bylo, na počátku povinnosti Data Retention v právním řádu ČR neobsahoval ani ZoEK ani jiný právní předpis jednoznačné vymezení orgánů oprávněných vyžádat si (a tedy využít) provozní a lokalizační údaje. ZoEK v té době počítal s tím, že takovéto orgány existují, jak autor uvádí dále.

Data Retention Směrnice otázku oprávněných orgánů specificky neupravovala, omezila se na požadavek[319], aby členské státy přijaly opatření *„pro zajištění toho, že údaje jsou poskytovány pouze příslušným vnitrostátním orgánům v konkrétních případech a v souladu s vnitrostátními právními předpisy“*, konkrétní vymezení těchto orgánů ponechala právním řádům členských států. Jediným, dosti obecným, omezením byl doplňující požadavek, aby *„jednotlivé členské státy ve svých vnitrostátních právních předpisech“* stanovily *„postupy pro získání přístupu k uchovávaným údajům“*, a to *„v souladu s požadavky nezbytnosti a přiměřenosti“* a dále též *„podmínky, jež mají být za tím účelem splněny“*. Bod 9 recitálu výslovně předpokládal, že mezi oprávněnými orgány budou orgány činné v trestním řízení[320]; bod 17 recitálu zdůrazňoval potřebu plného respektování základních práv dotčených osob při poskytování uchovávaných údajů příslušným vnitrostátním orgánům a současně nezbytnost přijetí právní úpravy členskými státy pro tento účel.

Je otázkou, zda zákonodárce v ČR tyto požadavky Data Retention Směrnice v textu ZoEK naplnil, když ZoEK v podobě účinné v letech 2005–2012, tedy po dlouhou dobu, pouze ukládal provozovatelům veřejné komunikační sítě a poskytovatelům veřejně dostupných služeb elektronických komunikací povinnost *„uchovávat provozní a lokalizační údaje“* a na

---

[317] V uvedeném nálezu sp. zn. Pl. ÚS 24/10 ze dne 22.3.2011 na tuto skutečnost Ústavní soud ČR upozorňuje, když konstatuje, že *„V neposlední řadě považuje Ústavní soud za nutné vyjádřit pochybnosti i nad tím, zda je vůbec žádoucí, aby soukromé osoby (poskytovatelé služeb v oblasti internetu a telefonní a mobilní komunikace, zejm. mobilní operátoři a obchodní společnosti zajišťující připojení k internetu) byly nadány oprávněním uchovávat veškeré údaje o jimi poskytované komunikaci i o zákaznících, jimž jsou jejich služby poskytovány (tzn. údaje jdoucí i nad rozsah údajů, jež jsou dle napadené právní úpravy povinny uchovávat), a volně s nimi za účelem vymáhání pohledávek, rozvoje obchodní činnosti a marketingu disponovaly.“*

[318] Ustanovení § 97 odst. 3 ZoEK.

[319] Viz článek 4 Data Retention Směrnice.

[320] Dle bodu 9 recitálu Data Retention Směrnice: *„se uchovávání údajů osvědčilo jako nezbytný a účinný vyšetřovací nástroj prosazování práva v několika členských státech, a to zejména v závažných případech, jako jsou organizovaná trestná činnost a terorismus“*, z tohoto důvodu bylo nutné *„zajistit zpřístupnění uchovávaných údajů orgánům činným v trestním řízení po určitou dobu a za podmínek stanovených v této směrnici“*.

požádání tyto údaje *„poskytnout orgánům oprávněným k jejich vyžádání podle zvláštního právního předpisu“*. I přes dílčí novelizace ZoEK, které se dotkly i zde rozebíraného ustanovení (formulace byla doplněna tak, že povinností bylo údaje poskytnout „bezodkladně“), nebyl v ZoEK až do účinnosti Novely ZoEK, tedy do 1. října 2012, obsažen výčet oprávněných orgánů. Odkaz na „zvláštní právní předpisy“, které měly zakládat oprávnění konkrétních orgánů, nebyl jednoznačný, tedy ani dostatečný a neodpovídal dle hodnocení autora již v té době dostupným kritériím vymezeným v rozhodovací praxi Ústavního soudu ČR, jak ji autor uvedl výše.

Při úvaze o tom, které zvláštní právní předpisy (a tedy které oprávněné orgány v těchto předpisech upravené) zde konkrétně připadaly v úvahu, lze jako jisté vodítko použít předchozí právní úpravu. Předchozí TelZ, z něhož ZoEK tuto formu vymezení oprávněných orgánů patrně převzal, obsahoval obdobný odkaz na oprávněné orgány vymezené zvláštními právními předpisy[321], doplněný poznámkou pod čarou, která však pochopitelně v souladu s ustálenou judikaturou Ústavního soudu ČR *„nemá závaznou povahu a není pravidlem chování subjektů uvedených "nahoře nad čarou" ve vlastním textu právního předpisu“*[322]. Tato poznámka navíc pouze uváděla několik příkladů v té době platných zvláštních právních předpisů, uvozených slovem „např.“[323], mezi nimi zákony o Vojenském obranném zpravodajství, o Bezpečnostní informační službě, o Policii České republiky a také Trestní řád a Celní zákon. Taktéž v těchto zvláštních právních předpisech připadajících v úvahu ani v předpisech, které je posléze, od účinnosti ZoEK, nahradily, nebyly orgány oprávněné k vyžádání provozních a lokalizačních údajů vymezeny jednoznačně – především v těchto předpisech nebylo obsaženo oprávnění těchto orgánů vyžádat a následně využít ke své činnosti provozní a lokalizační údaje, resp. údaje podléhající zvláštní ochraně, v TelZ upravené jako telekomunikační tajemství a ochrana osobních a zprostředkovacích dat[324].

S přihlédnutím k výše uvedenému považuje autor za vhodné v případě ZoEK analyzovat obdobné právní předpisy platné a účinné v době přijetí ZoEK[325]. V těchto právních předpisech nebylo ve znění účinném v té době u jednotlivých orgánů upraveno oprávnění

---

[321] Viz § 86 odst. 1 TelZ, dle kterého povinné osoby byly povinny *„sdělit orgánům oprávněným k tomu zvláštními právními předpisy“* dále specifikované informace, zahrnující i „osobní a zprostředkovací data“.
[322] Viz Nález Ústavního soudu ČR I. ÚS 22/99 ze dne 2. února 2000.
[323] *„Například zákon č. 67/1992 Sb., zákon č. 154/1994 Sb., zákon č. 283/1991 Sb., zákon č. 141/1961 Sb. a zákon č. 13/1993 Sb.“*
[324] Viz § 84 a násl. TelZ.
[325] Vojenské obranné zpravodajství dle zákona č. 67/1992 Sb. bylo nahrazeno Vojenským zpravodajstvím dle zákona č. 289/2005 Sb., ostatní předpisy nedoznaly ve vztahu ke zkoumaným aspektům výraznějších změn.

vyžadovat a využít provozní a lokalizační údaje elektronických komunikací chráněné v rámci institutu důvěrnosti komunikací v ZoEK. Teprve Novela ZoEK, přijatá v reakci na nálezy Ústavního soudu ČR sp. zn. Pl. ÚS 24/10 a sp. zn. Pl. ÚS 24/11, vedle samotného ZoEK a související úpravy Trestního řádu, novelizovala též zákon o Vojenském zpravodajství a zákon o Bezpečnostní informační službě a v obou těchto předpisech výslovně upravila oprávnění VZ, resp. BIS *„v rozsahu potřebném pro plnění konkrétního úkolu požadovat od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť anebo poskytující veřejně dostupnou službu elektronických komunikací… poskytnutí provozních nebo lokalizačních údajů způsobem, ve formě a v rozsahu stanoveném zvláštním právním předpisem"*[326]. Jak rozebráno dále, obdobné oprávnění Novela ZoEK vložila pro ČNB do zákona o dohledu v oblasti kapitálového trhu[327]; ještě před Novelou ZoEK pak zákonodárce oprávnění vyžádat si provozní a lokalizační údaje upravil pro Policii ČR[328]. Ve vztahu ke zvláštním předpisům platným a účinným v době přijetí ZoEK však lze učinit obdobný závěr o nedostatečném vymezení oprávnění jednotlivých orgánů k vyžádání provozních a lokalizačních údajů v těchto zvláštních právních předpisech.

Právě tuto výtku ve vztahu k napadenému § 97 odst. 3 a 4 ZoEK zdůraznil Ústavní soud ČR v nálezu sp. zn. Pl. ÚS 24/10[329], jak rozvedeno dále. Ústavní soud ČR označil „*uvedený způsob (ne)vymezení spektra oprávněných orgánů veřejné moci, jakož i (ne)vymezení účelu, pro který jsou uchovávané údaje oprávněny požadovat"* za nedostatečný a nepředvídatelný, „*takto vymezená právní úprava umožňující masivní zásah do základních práv nesplňuje požadavky kladené na určitost a jasnost z pohledu právního státu*". V této souvislosti Ústavní soud ČR v citovaném nálezu upozornil na to, že „*k omezení osobní integrity a soukromí osob (tj. k prolomení respektu k nim) tak ze strany veřejné moci může dojít jen zcela výjimečně, je-li to v demokratické společnosti nezbytné, nelze-li účelu sledovaného veřejným zájmem dosáhnout jinak, a je-li to akceptovatelné z pohledu zákonné existence a dodržení účinných a konkrétních záruk proti libovůli*", odkázal přitom na svou judikaturu k odposlechům telekomunikačního provozu, v níž blíže konkretizoval naplnění těchto podmínek při posuzování přípustnosti zásahu veřejné moci do soukromí jednotlivců.

---

[326] Viz ustanovení § 8a zákona č. 154/1994 Sb. o Bezpečnostní informační službě, resp. § 9 odst. 5 zákona č. 289/2005 Sb. o Vojenském zpravodajství.
[327] Zákon č. 15/1998 Sb. o dohledu v oblasti kapitálového trhu a o změně a doplnění dalších zákonů.
[328] Ustanovení § 66 odst. 3, § 68 odst. 2 a § 71 zákona č. 273/2008 Sb. o Policii České republiky.
[329] Nález Ústavního soudu ČR sp.zn. Pl. ÚS 24/10 ze dne 22. března 2011; vyhlášen ve Sbírce zákonů pod číslem 94/2011 Sb.

Jak již uvedeno, vláda ČR reagovala na výtky Ústavního soudu ČR obsažené v nálezech sp. zn. Pl. ÚS 24/10 a sp. zn. Pl. ÚS 24/11 a na zrušení relevantních předpisů těmito nálezy přípravou Novely ZoEK. Ta s účinnosti od 1. října 2012 přímo do ZoEK zapracovala konkrétní oprávněné orgány, kterým jsou provozovatelé sítí a poskytovatelé služeb povinni na jejich požádání „bezodkladně poskytnout" provozní a lokalizační údaje[330], následujícím výčtem:

1. orgány činné v trestním řízení,
2. Policie ČR,
3. Bezpečnostní informační služba,
4. Vojenské zpravodajství,
5. Česká národní banka,

a to pro účely stanovené zvláštním právním předpisem, pouze u Policie ČR Novela ZoEK výslovně uvedla účely. Autor považuje za potřebné na tomto místě jednotlivé oprávněné orgány stručně rozebrat.

Orgány činné v trestním řízení

Orgány činné v trestním řízení vymezuje Trestní řád[331], jsou jimi soud (okresní, příp. obvodní, krajský, příp. Městský soud v Praze, vrchní soud a Nejvyšší soud České republiky), státní zástupce a policejní orgán. Policejní orgány zahrnují řadu orgánů, z nichž některé připadají do úvahy jen ve specifických situacích, včetně Generální inspekce bezpečnostních sborů, pověřených orgánů Vězeňské služby České republiky a dalších[332].

Účel poskytnutí provozních a lokalizačních údajů vymezuje u orgánů činných v trestním řízení Trestní řád v § 88a, při výčtu trestných činů, u kterých lze vyžádat provozní a lokalizační údaje, je-li toho třeba pro účely trestního řízení. Jak již uvedeno výše, široký rozsah těchto trestných činů zvláště vynikne v porovnání s mnohem užším výčtem trestných činů, pro které lze vydat příkaz k odposlechu a záznamu telekomunikačního provozu[333].

S ohledem na kritéria formulovaná Ústavním soudem ČR i SDEU má autor pochybnosti o rozsahu trestných činů odůvodňujících vyžádání provozních a lokalizačních údajů, když tento rozsah se autorovi jeví jako velmi široký, uvedená kritéria ne zcela

[330] V této souvislosti se nabízí porovnání s orgány oprávněnými k odposlechu a záznamu zpráv, které jsou vymezeny v § 97 odst. 1 ZoEK: Policie ČR, BIS a VZ, vždy pro účely stanovené zvláštním právním předpisem.
[331] § 12 Trestního řádu.
[332] Podrobně viz § 12 odst. 2 Trestního řádu.
[333] Viz § 88 Trestního řádu.

respektující. Vzhledem k *„závažnosti zásahu do dotčených základních práv“* právní úpravy Data Retention zdůraznil SDEU v Rozsudku ve spojených věcech C-203/15 a C-698/15, že takové opatření může být *„odůvodněno pouze bojem proti závažné trestné činnosti…*“ Obdobně též Ústavní soud ČR v nálezu sp. zn. Pl. ÚS 24/10 považuje za *„nezbytné, aby … zákonodárce omezil možnost použití uchovávaných údajů jen pro účely trestních řízení vedených pro zvlášť závažné trestné činy“*. Porovnání s vymezením trestných činů, v rámci jejichž trestního řízení může být vydán příkaz k odposlechu a záznamu telekomunikačního provozu, je zcela relevantní. Dle závěrů soudní judikatury představují odposlech a záznam telekomunikačního provozu na straně jedné a zjištění provozních a lokalizačních údajů na straně druhé srovnatelný zásah do práva na ochranu soukromí. Takto se vyjádřil např. Ústavní soud ČR v nálezu sp. zn. Pl. ÚS 24/10[334], s odkazem mj. i na relevantní rozhodnutí ESLP[335].

Vycházeje z těchto závěrů o srovnatelné míře zásahu do práva na ochranu soukromí, autor zkoumal důvody tak rozsáhlých odlišností při vymezení trestných činů, u nichž lze každý z těchto dvou institutů použít. Odůvodnění takovéto potřeby autor nenalezl ani při gramatickém, systematickém či logickém výkladu rozebíraných ustanovení Trestního řádu, včetně důvodové zprávy k novele Trestního řádu provedené zákonem č. 265/2001 Sb., která do Trestního řádu vložila ustanovení § 88a[336] a dostupné judikatury. Dle hodnocení autora by tak bylo plně na místě vymezit trestné činy, u kterých mohou oprávněné orgány pro účely trestního řízení vyžádat provozní a lokalizační údaje, srovnatelně s trestnými činy, v rámci jejichž trestního řízení může být vydán příkaz k odposlechu a záznamu telekomunikačního

---

[334] *„Z ustálené judikatury Ústavního soudu, zejména ve vztahu k problematice odposlechu telefonních hovorů, zřetelně vyplývá, že ochrana práva na respekt k soukromému životu v podobě práva na informační sebeurčení ve smyslu čl. 10 odst. 3 a čl. 13 Listiny se vztahuje nejen k vlastnímu obsahu zpráv podávaných telefonem, ale i k údajům o volaných číslech, datu a čase hovoru, době jeho trvání, v případě mobilní telefonie o základových stanicích zajišťujících hovor…“*

[335] *„ESLP ve své judikatuře k právu na respekt k soukromému životu podle čl. 8 Úmluvy označil za zásahy do soukromí jednotlivců mimo jiné i zásahy v podobě kontroly dat, obsahu pošty a odposlechu telefonních hovorů [srov. rozhodnutí ve věci Klass a další proti Německu (no. 5029/71) ze dne 6. 9. 1978, rozhodnutí ve věci Leander proti Švédsku (no. 9248/81) ze dne 26. 3. 1987, rozhodnutí ve věci Kruslin proti Francii (no.11801/85) ze dne 24. 4. 1990 či rozhodnutí ve věci Kopp proti Švýcarsku (no. 23224/94) ze dne 25. 3. 1998], zjišťování telefonních čísel telefonujících osob [srov. rozhodnutí ve věci P. G. a J. H. proti UK (no. 44787/98) ze dne 25. 9. 2001], zjišťování údajů o telefonním spojení (srov. citované rozhodnutí ve věci Amann proti Švýcarsku) nebo uchovávání údajů o DNA jednotlivců v databázích obviněných [srov. rozhodnutí ve věci S. a Marper proti UK (no. 30562/04 a 30566/04) ze dne 4. 12. 2008].“*

[336] Důvodová zpráva k novele Trestního řádu provedené zákonem č. 265/2001 Sb. ani nemohla obsahovat jakékoli vysvětlení týkající se § 88a Trestního řádu. Toto ustanovení totiž původní vládní návrh zákona neobsahoval, bylo do něj vloženo až při projednávání v Poslanecké sněmovně Parlamentu ČR jako pozměňovací návrh ústavně právního výboru obsažený v usnesení tohoto výboru ze 74. schůze 14. a 15. března 2001 (sněmovní tisk 785/1). Taktéž ústavně právní výbor však tento svůj pozměňovací návrh nijak podrobněji neodůvodnil.
Viz Usnesení Ústavně právního výboru Poslanecké sněmovny Parlamentu ČR ze 74. schůze 14. a 15. března 2001. Pozměňovací návrh k novele Trestního řádu (sněmovní tisk 785/1). [online]. 2001 [cit. 24.2.2024].

provozu. Jak autor uvádí dále, právní úprava de lege ferenda by takového vymezení měla obsahovat.

Policie ČR

V případě Policie ČR existovaly až do účinnosti Novely ZoEK interpretační spory týkající se nejprve § 47 zákona č. 283/1991 Sb. o Policii České republiky, posléze § 18 zákona č. 273/2008 Sb. o Policii České republiky, ve znění pozdějších předpisů (dále též jen „ZoPČR“) upravujícího vyžadování pomoci od osob a orgánů, zahrnující rovněž *„informace včetně osobních údajů“*. Novela ZoEK nezměnila znění ZoPČR, vložila však do ZoEK výslovně povinnost poskytnout provozní a lokalizační údaje Policii ČR, a to pro konkrétně vymezené účely: zahájené pátrání po hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly (§ 68 ZoPČR), předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu (§ 71 ZoPČR) nebo prověřování chráněné osoby (tento účel v ZoPČR upraven není, a to ani v § 49 „*Zajišťování bezpečnosti určených osob*“ ani na jiném místě)[337].

Ustanovení § 66 odst. 3 ZoPČR upravující získávání informací z evidencí výslovně zmiňuje rovněž provozní a lokalizační údaje, dle hodnocení autora však samo o sobě nezakládá zvláštní oprávnění Policie ČR žádat provozní a lokalizační údaje. Jak je zřejmé z uvozující formulace „*v případech stanovených zákonem*“, jedná se patrně pouze o podrobnější vymezení k zákonem vymezeným případům popsaným výše.

Za problematickou autor považuje skutečnost, že u žádného z těchto ustanovení není výslovně stanovena povinnost Policie ČR požádat o vydání příkazu ke zjištění provozních a lokalizačních údajů či jeho povolení soud; ZoPČR ani podpůrně neodkazuje na Trestní řád. Absentuje zde také úprava požadavků na příkaz samotný, obdobná úpravě v § 88a Trestního řádu, dle které „*příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn*“, což je ostatně požadavek, který vyplývá i z výše rozebírané judikatury. Konečně zde také schází úprava povinnosti následné informace dotčené osobě, která by se z výše popisovaných případů týkala v praxi patrně zejména případů boje proti terorismu, u nichž ovšem může existovat potřeba utajení takovéhoto vyžádání údajů, nicméně jde toliko o

[337] K tomu podrobně viz VOBOŘIL, Jan. Využívání provozních a lokalizačních údajů ze strany oprávněných orgánů, zejména Policie ČR. DATA RETENTION RELOADED: ZKUŠENOSTI, PROBLÉMY A APLIKAČNÍ PRAXE. In: *Sborník z workshopu konaného dne 23.4.2013 v Brně*. 1. vyd. Řada teoretická, Ed. S, č. 464. Brno : Masarykova univerzita, Právnická fakulta, 2013, s. 20 a násl.

domněnku autora. Podle autorovi dostupných informací požadavky Policie ČR podle ZoPČR představují v praxi celkově velmi nízké procento celkového počtu žádostí o poskytnutí údajů.

ZoEK u výše uvedeného oprávnění Policie ČR v § 97 odst. 3 obsahuje poznámku pod čarou odkazující na zvláštní právní předpisy, mezi kterými kromě ZoPČR výslovně uvádí též zákon o zvláštní ochraně svědka[338]. Byť poznámka pod čarou, jak autor uvádí výše, nemá normativní význam, autor uváděný předpis prověřil se zřetelem na možné prolomení důvěrnosti komunikací v něm obsažené. Tento právní předpis obsahuje v rámci Oprávnění k prověřování chráněné osoby[339] mj. rovněž oprávnění Policie ČR požadovat provozní a lokalizační údaje, a to pouze s předchozím souhlasem soudu, aniž by však obsahoval další požadavky na žádost o takový souhlas či povinnost dodatečného informování dotčené osoby. Vymezený účel „*je-li dáno podezření, že chráněná osoba nedodržuje povinnosti uvedené v § 6, a nelze-li toto podezření prověřit jiným způsobem*“ se autorovi z hlediska požadavků relevantní judikatury jeví jako dostačující.

Bezpečnostní informační služba

V otázce účelu vyžádání provozních a lokalizačních údajů odkazuje ZoEK na zvláštní právní předpis, kterým je zákon o BIS[340.] V něm však vymezení účelu schází, BIS je oprávněna si údaje vyžádat „*v rozsahu potřebném pro plnění konkrétního úkolu*“. Přestože jde o zpravodajskou službu, jejíž činnosti jsou specifické, s ohledem na shora rozebíranou judikaturu se autorovi toto vymezení jeví jako dosti vágní a nedostatečné. Ze systematického zařazení ustanovení § 8a do oddílu prvního zákona o BIS, vymezujícího zpravodajské prostředky[341] vyplývá, že na vyžádání provozních a lokalizačních údajů dopadá jak v zákoně o BIS obsažený požadavek předchozího písemného povolení soudce, tak rovněž vymezení náležitostí písemné žádosti o poskytnutí těchto údajů a také oprávnění soudce kontrolovat průběh používání zpravodajské techniky a povinnost BIS informovat soudce o ukončení jejího

[338] Zákon č. 137/2001 Sb. o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb. občanský soudní řád, ve znění pozdějších předpisů.
[339] Tento zákon v § 10a používá termín *„údaje o uskutečněném telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství nebo na něž se vztahuje ochrana osobních a zprostředkovacích dat“*.
[340] Zákon č. 154/1994 Sb. o Bezpečnostní informační službě, ve znění pozdějších předpisů. Poznámka pod čarou u ustanovení § 97 odst. 3 ZoEK odkazuje nesprávně na ustanovení § 6 až 8 tohoto zákona, místo správného § 8a, s ohledem na význam poznámky pod čarou autor tuto nepřesnost nepovažuje za relevantní.
[341] Oprávnění BIS požadovat provozní a lokalizační údaje je v tomto právním předpisu upraveno v § 8a, který je zařazen v Oddíle prvním Zpravodajské prostředky, v části Zpravodajská technika. Toto začlenění autor považuje za nevhodné a zavádějící, když získání provozních a lokalizačních údajů od povinného subjektu se neděje za použití zpravodajské techniky.

používání[342]. Podobně jako v ZoPČR, také v zákoně o BIS není upravena povinnost následně informovat dotčené osoby, také zde může být důvodem potřeba utajení takovéhoto vyžádání údajů, zákon však tuto absenci nijak nevysvětluje.

Vojenské zpravodajství

Oprávnění VZ vyžádat si provozní a lokalizační údaje je téměř totožné s výše rozebíranou právní úpravou zákona o BIS, také v zákoně o Vojenském zpravodajství je oprávnění vloženo systematicky ne zcela vhodně[343]. Ve vztahu k tomuto právnímu předpisu tak lze obdobně říci totéž, co autor poznamenává výše k BIS, včetně aplikace kontrolních mechanismů.

K Úřadu pro zahraniční styky a informace

V této souvislosti považuje autor za vhodné zmínit, že zákon o zpravodajských službách ČR[344] mezi zpravodajské služby řadí vedle BIS a VZ též Úřad pro zahraniční styky a informace (dále též jen „ÚZSI“). Jeho činnost není upravena zvláštním předpisem, zákon o zpravodajských službách ČR neupravuje specifické oprávnění ÚZSI k vyžádání provozních a lokalizačních údajů, pouze obecné oprávnění zpravodajských služeb vyžadovat informaci z *„databáze účastníků veřejně dostupné telefonní služby*“[345].

K oprávněním Vojenského zpravodajství v oblasti kybernetické obrany

Ve vztahu k tématu této práce autor považuje za relevantní též činnosti VZ při obraně státu v kybernetickém prostoru. Ty zahrnují i oprávnění přístupu k sítím elektronických komunikací, které v roce 2021, po několikaletých diskusích upravila novela zákona o Vojenském zpravodajství[346]. Ministerstvo obrany je po této novelizaci oprávněno vydat na základě návrhu VZ rozhodnutí, kterým provozovateli sítě uloží povinnost *„zřídit a zabezpečit rozhraní pro připojení nástrojů detekce v určeném bodě veřejné komunikační sítě a povinnost strpět umístění a provozování těchto nástrojů“*, a to na dobu maximálně 12 měsíců, s možností prodloužení. Podle názorů odborníků takovéto rozhraní umožňuje VZ

[342] Viz § 9–12 zákona o BIS. Z textu ustanovení je patrné, že na danou oblast zcela nedopadají, jak vyplývá např. z povinných náležitostí žádosti zahrnujících mj. „*druh zpravodajské techniky, která má být použita*“.
[343] Zákon č. 289/2005 Sb. o Vojenském zpravodajství, ve znění pozdějších předpisů upravuje toto oprávnění v Hlavě první Zpravodajské prostředky.
[344] Zákon č. 153/1994 Sb. o zpravodajských službách České republiky, ve znění pozdějších předpisů.
[345] Viz § 11b Zákona o zpravodajských službách České republiky.
[346] Zákon č. 150/2021 Sb., kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony, novelizoval též ZoEK.

zcela bezprecedentní přístup do sítí elektronických komunikací, včetně faktické možnosti sledování jakékoli komunikace. Dle autora je nutno v této souvislosti upozornit na absenci jakýchkoli kontrolních mechanismů.

Česká národní banka

Jak již zmíněno výše, ČNB je v rámci působnosti k dohledu v oblasti kapitálového trhu oprávněna vyžádat si provozní a lokalizační údaje. Vedle ZoEK je toto její oprávnění zakotveno v zákoně o dohledu v oblasti kapitálového trhu[347], který jako účel stanoví výkon dohledu nad kapitálovým trhem. Tento zákon zakotvuje podmínku v podobě předchozího písemného povolení soudu a také náležitosti žádosti, povinnost následného informování dotčené osoby však nikoli. Jako omezení zákon stanoví, že ČNB tak může učinit *„pokud lze důvodně předpokládat, že poskytnuté údaje mohou přispět k objasnění skutečností důležitých pro odhalení přestupku na úseku podnikání nebo obchodování na kapitálovém trhu … a nelze-li sledovaného účelu dosáhnout jinak, nebo jen s vynaložením neúměrného úsilí“*.

Jelikož oprávnění ČNB k vyžádání provozních a lokalizačních údajů bylo do zákona o dohledu v oblasti kapitálového trhu [348] vloženo novelou[349] s účinností od 1. dubna 2006, autor v prvé řadě analyzoval text důvodové zprávy k této novele. U diskutovaného oprávnění ČNB důvodová zpráva uvádí, že se jedná o „*implementaci Směrnice 2003/6/ES o zneužívání důvěrných informací a manipulace s trhem (zneužívání trhu), která je v dosavadním znění upravena zatím nepřesně*“[350]. Předmětná směrnice byla posléze nahrazena Nařízením Evropského parlamentu a Rady (EU) č. 596/2014, které mezi dohledové a vyšetřovací pravomoci příslušných orgánů zahrnuje i právo požadovat záznamy provozních údajů[351], to však pouze *„pokud to není v rozporu s vnitrostátními právními předpisy“;* nikoli však též lokalizační údaje.

---

[347] Zákon č. 15/1998 Sb. o dohledu v oblasti kapitálového trhu a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, obsahuje toto oprávnění ČNB v § 8 odst. 1 písm. d).

[348] Zákon č. 15/1998 Sb. tehdy nesl název Zákon o Komisi pro cenné papíry.

[349] Novela provedená zákonem č. 57/2006 Sb. o změně zákonů v souvislosti se sjednocením dohledu nad finančním trhem.

[350] Předkladatel v důvodové zprávě dále toto tvrzení rozvádí tak, že Podle čl. 12 odst. 2 písm. d) směrnice *„má mít Komise pravomoc vyžadovat záznamy telefonického a datového provozu“,* navrhovaná úprava umožňuje Komisi „*požadovat od telekomunikačních operátorů tzv. provozní nebo lokalizační údaje, což v případě dozoru nad kapitálovým trhem mohou být např. IP adresa důležitá pro identifikaci šiřitele nepravdivé zprávy při manipulaci trhem nebo identifikace majitele účtu. Všechny tyto pravomoci může Komise využít jen při šetření souvisejícím se zneužitím trhu (tj. manipulace trhem nebo využití insider informace)*“.

[351] Článek 23 odst. 2 písm. h) ve spojení s článkem 3 odst. 1 bod 27 Nařízení Evropského Parlamentu a Rady (EU) č. 596/2014 ze dne 16. dubna 2014 o zneužívání trhu (nařízení o zneužívání trhu) a o zrušení směrnice Evropského parlamentu a Rady 2003/6/ES a směrnic Komise 2003/124/ES, 2003/125/ES a 2004/72/ES.

K oprávnění ÚOOÚ na přístup k provozním a lokalizačním údajům

Kromě výše uvedených orgánů uvedených výslovně v ZoEK se po účinnosti ZoZOÚ vyskytly některé názory, dle kterých tento zákon založil oprávnění ÚOOÚ vyžádat si od provozovatelů sítí a poskytovatelů služeb provozní a lokalizační údaje a tyto údaje využít při své činnosti. Tyto názory se opírají o velmi široce formulované oprávnění obsažené v § 58 ZoZOÚ[352], jehož textace naznačuje možnost prolomení veškerých „povinností mlčenlivosti" obsažených v jiných právních předpisech ve prospěch ÚOOÚ, pouze s omezeními výslovně obsaženými v témže ustanovení ve vztahu k informacím chráněným povinností mlčenlivosti podle zákona o advokacii, resp. povinností mlčenlivosti podle zákona o daňovém poradenství a Komoře daňových poradců České republiky[353]. Výkladu nebývale široce formulovaného oprávnění ÚOOÚ dle těchto názorů nasvědčují též formulace upravující v ZoZOÚ jednak vyloučení informací z nahlížení do spisu, která jako informace, které má ÚOOÚ takto z nahlížení vyloučit, výslovně uvádí *„informace, které jsou obchodním, bankovním nebo jiným obdobným zákonem chráněným tajemstvím"* a některé další, jakož i formulace povinnosti kontrolujícího prokázat oprávnění k přístupu k utajované informaci[354].

Zákonodárce zde tedy vycházel z toho, že termínem „povinnost mlčenlivosti" jsou zde míněny rovněž právní instituty označené v relevantních právních předpisech jako „tajemství" zákonem chráněné, tedy např. výše uvedené bankovní tajemství a že ÚOOÚ je oprávněn k takovýmto informacím přistoupit. Je otázkou, zda bylo cílem zákonodárce takto prolomit též důvěrnost komunikací dle ZoEK (terminologií předchozí právní úpravy TelZ telekomunikační tajemství). Autor má silné pochybnosti o legislativní kvalitě takového řešení, které by paušálně, souhrnně prolamovalo veškeré zákonem stanovené povinnosti k ochraně jakýchkoli informací, aniž by tyto povinnosti konkrétně specifikovalo a především aniž by stanovilo jakékoli další podmínky, v tomto případě paradoxně navíc ve prospěch dozorového orgánu v oblasti ochrany osobních údajů. Přes tyto pochybnosti autor dospěl k závěru, že výkladem lze dovodit oprávnění ÚOOÚ vyžádat si též provozní a lokalizační údaje uchovávané v rámci povinnosti Data Retention[355], čímž se však oprávnění ÚOOÚ k prolomení

[352] Dle § 58 odst. 1 ZoZOÚ *„Úřad je oprávněn seznamovat se se všemi informacemi nezbytnými pro plnění konkrétního úkolu. To platí i pro informace chráněné povinností mlčenlivosti podle jiného právního předpisu, nestanoví-li jiný právní předpis pro přístup Úřadu k takovým údajům jiné podmínky".*
[353] Viz § 58 odst. 2 a 3 ZoZOÚ.
[354] Viz § 58 odst. 4 a 5 ZoZOÚ.
[355] K obdobnému závěru dospěli i autoři Komentáře ke GDPR, s tím, že upozorňují na *„silné pochybnosti o ústavní konformitě § 58 odst. 1 ZZOÚ. Autoři zejména pochybují o tom, zda lze takto vágním způsobem nepřímo novelizovat veškeré právní předpisy, které obsahují konkrétní povinnosti mlčenlivosti či tajemství, a tím prolomit povinnosti mlčenlivosti či zachovávání tajemství v nich uložené. Tyto pochybnosti autoři opírají především o*

důvěrnosti komunikací dle ZoEK stávají výrazně širšími, nežli je tomu u jiných oprávněných orgánů, a to i včetně orgánů činných v trestním řízení, u nichž lze sledovaný účel považovat za významnější.

Autor v praxi zaznamenal též názory, dle kterých oprávnění ÚOOÚ vyžádat si provozní a lokalizační údaje lze opřít o GDPR, konkrétně čl. 58 odst. 1 a), který formuluje velmi obecně vyšetřovací pravomoci dozorových úřadů, vč. pravomoci *„nařídit správci a zpracovateli, případně zástupci správce nebo zpracovatele, aby mu poskytli veškeré informace, které potřebuje k plnění svých úkolů“*. Takovýto výklad však autor považuje za nesprávný, jelikož provozní a lokalizační údaje jsou v ZoEK chráněny v rámci institutu důvěrnosti komunikací a jeho prolomení pouze na základě obecného oprávnění k poskytnutí „veškerých informací“ by bylo nepřípustné.

Legislativní návrhy dalších oprávněných orgánů

Autor zaznamenal a též v současné době zaznamenává snahy o rozšíření orgánů oprávněných k vyžádání provozních a lokalizačních údajů. Návrhy novelizací ZoEK předpokládaly konkrétně rozšíření o Státní hygienickou službu a Úřad pro ochranu hospodářské soutěže. V roce 2020 předložilo Ministerstvo zdravotnictví do legislativního procesu návrh novely zákona o ochraně veřejného zdraví[356]. Dle předkládací zprávy k návrhu zákona bylo jeho cílem *„reagovat na dopady související s šířením onemocnění COVID-19 a přijatá opatření v souvislosti s touto skutečností“* a připravit centralizaci systému hygienické služby, včetně zamýšleného vzniku Státní hygienické služby. Ta, jako ústřední orgán, měla být vybavena některými novými oprávněními, novelou ZoEK by tento orgán byl oprávněn získat lokalizační údaje uživatelů sítí a služeb elektronických komunikací. Návrh novely se setkal s velmi ostrou kritikou, jak pro zamýšlená oprávnění Státní hygienické služby, tak rovněž pro zcela nedostatečné kontrolní prvky a mechanismy[357]. Návrh navíc nespecifikoval

skutečnost, že některé ze zákonem stanovených tajemství či mlčenlivostí mají svou oporu přímo v LPS (listovní tajemství, telekomunikační tajemství), některé jiné pak mají základ v právu EU. Kromě toho zvláštní právní předpisy, které povinnost mlčenlivosti či tajemství obsahují, zpravidla také vymezují podmínky prolomení takové povinnosti, a to velmi striktně.“ Viz UŘIČAŘ, Miroslav, RÁMIŠ, Vladan a kol. *Obecné nařízení o ochraně osobních údajů. Komentář. 1. vydání.* Praha: C. H. Beck, 2021. s. 1071.

[356] Návrh zákona, kterým se mění zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a další související zákony, návrh byl dostupný v elektronické knihovně připravované legislativy eKlep pod č.j. MZDR 53739/2020.

[357] Např. Česká advokátní komora ve svých připomínkách k návrhu uvedla, že *„V některých aspektech dokonce Státní hygienická služba získává nástroje, které jsou typické pro zpravodajské služby, popř. jejichž použití je umožněno orgánům činným v trestním řízení, aniž by tomu odpovídal systém kontroly činnosti této nově zřizované služby.“* Česká advokátní komora. *Připomínky k návrhu zákona, kterým se mění zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a další související*

ani technická a organizační opatření k zabezpečení zpracování lokalizačních údajů, což autor v případě údajů, které mohou být předmětem zneužití, považuje za významný nedostatek. Po vyhodnocení kritických reakcí a komentářů obdržených v rámci připomínkového řízení předkladatel návrh novely nepředložil Parlamentu ČR.

Někteří právní odborníci se však naopak zamýšleli nad možností využít lokalizační údaje uchovávané v rámci povinnosti Data Retention v boji s onemocněním COVID-19 a navrhovali pro tento účel *„explicitně včlenit práva dle čl. 10 LZPS odst. 2 a 3, tj. právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života a právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o osobách, do práv omezitelných dle krizového zákona“* [358]. Autor takovéto účelové přizpůsobování právní úpravy konkrétní situaci nepovažuje za správné a v daném případě dle dostupných informací ani za potřebné, omezení umožněná dle krizového zákona za nouzového stavu nebo za stavu ohrožení státu[359] se zdají být dostatečně rozsáhlá. Návrh však zůstal pouze v rovině teoretických diskusí, autor proto nepovažuje za potřebné si jím na tomto místě podrobněji zabývat.

Úřad pro ochranu hospodářské soutěže („ÚOHS“) v uplynulých letech opakovaně usiloval prostřednictvím novelizace ZoEK získat oprávnění vyžádat si od provozovatelů sítí a poskytovatelů služeb elektronických komunikací povinně uchovávané provozní a lokalizační údaje. Při novelizaci ZoEK v roce 2020 z důvodové zprávy vládního návrhu novely ZoEK vyplynulo, že ÚOHS se primárně jedná o lokalizační údaje účastníků a uživatelů, návrh novelizovaného ustanovení však byl obecný a zahrnoval provozní i lokalizační údaje. Tento zájem ÚOHS odůvodňovala důvodová zpráva jednak tím, že „*klíčové osoby téměř vždy i při osobních schůzkách mají zásadně telekomunikační zařízení (typicky mobilní telefony) při sobě“,* proto *„má pro prokázání jejich obecného kontaktu pro ÚOHS velký význam i zjišťování polohy těchto zařízení v čase“* a dále také potřebou zjišťovat lokalizaci mobilního komunikačního zařízení a tedy i konkrétní osoby v průběhu místního šetření prováděného ÚOHS (*„Právě možnost ověřit, kde se v průběhu inspekce nacházel např. mobilní telefon,*

---

zákony. Č.j.: 07.32-000005/20, nedatováno. [cit. 12.1.2024]. ÚOOÚ ve svých připomínkách uvedl, že *„nepovažuje tento návrh zákona za způsobilý dalšího legislativního procesu a požaduje jeho zásadní dopracování“*. ÚOOÚ. *Připomínky k návrhu zákona, kterým se mění zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a další související zákony.* Nedatováno. Dostupné z www.uoou.gov.cz. [cit. 12.1.2024].

[358] Viz HOLUBÁŘ Adam, MOHELSKÝ Michal, SEBORSKÝ Jaroslav. *Data retention a lokalizační údaje v boji s pandemií onemocnění Covid-19.* Advokátní deník. 26.3.2020.

[359] Viz § 5 zákona č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

umožní ÚOHS prokázat porušení povinnosti spolupracovat a její maření.“)[360]. Novela byla schválena jako zákon č. 374/2021 Sb. bez tohoto oprávnění ÚOHS. V aktuální novele ZoEK, která je v době dokončení této práce v legislativním procesu, ÚOHS o přístup k provozním a lokalizačním údajům opět usiluje[361].

Závěrem k oprávněným orgánům

V této souvislosti je důležité zdůraznit, že se stále jedná o údaje zpracovávané v rámci povinnosti Data Retention, přijaté původně za účelem závažné trestné činnosti, v diskusích předcházejících zavedení této povinnosti byla zmiňována též potřeba boje proti terorismu. Ze skutečnosti, že tyto údaje jsou uchovávány a týkají se značného množství osob, pramení snahy o jejich využití pro další, stále v čase narůstající účely. Současně však je nutno vzít v úvahu vymezení cílů sledovaných v právní úpravě Data Retention při jejím přijetí, tedy boj proti závažné trestné činnosti. Ani zamýšlená Státní hygienická služba ani ÚOHS přitom nejsou orgány oprávněnými k dosahování těchto cílů.

Trend v rozšiřování orgánů oprávněných k vyžádání a využití provozních a lokalizačních údajů svědčí o snaze o podstatné rozšiřování veřejného zájmu, pro jehož naplnění by bylo možno takto zasáhnout do základních práv a svobod, oproti původnímu účelu vyjádřenému v Data Retention Směrnici jako *„vyšetřování, odhalování a stíhání závažných trestných činů“*. Ze souhrnných přehledů zveřejňovaných v minulosti ze strany ČTÚ také vyplývá postupný významný nárůst využívaných provozních a lokalizačních údajů. Zatímco v roce 2013 si oprávněné orgány vyžádaly provozní a lokalizační údaje v případě mobilních sítí (v pevných sítích nelze hovořit o lokalizačních údajích, pouze o údajích provozních) celkem ve 175.524 případech (z toho pouze ve 2.437 případech povinné osoby údaje neposkytly), v roce 2018 to již byl téměř dvojnásobný počet 339.151 případů (neposkytnuto v 6.259 případech)[362]. Přehled za rok 2018 byl posledním, který ČTÚ zveřejnil, v obou případech jde přitom o přehledy založené na totožné metodice a jsou tak plně porovnatelné.

---

[360] Důvodová zpráva k návrhu novely zákona o elektronických komunikacích. Sněmovní tisk 1084. Poslanecká sněmovna, 8. období, 2017–2021.

[361] V tiskové zprávě z 15.1.2024 k tomu ÚOHS uvádí: *„Úřad proto navrhuje, aby byl začleněn mezi subjekty, kterým zákon o elektronických komunikacích umožňuje požádat právnickou nebo fyzickou osobu zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací o provozní a lokalizační údaje telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací.“* ÚOHS. *Úřad předložil řadu legislativních návrhů pro větší efektivitu v oblasti hospodářské soutěže.* [online] [cit. 18.3.2024]. Dostupné z www.uohs.gov.cz.

[362] Viz Český telekomunikační úřad. *Tisková zpráva. Operátoři předali ČTÚ výkaz o poskytnutých provozních a lokalizačních údajích.* 19.3.2014. *Tisková zpráva. Operátoři v roce 2018 na žádost oprávněných orgánů předali 332 tisíc provozních a lokalizačních údajů.* 25.3.2019. Dostupné z www.ctu.gov.cz. [cit. 8.2.2024].

3.1.2 Relevantní rozhodnutí soudů, stanoviska orgánů dohledu nad ochranou osobních údajů

Pro potřeby této práce autor vnímá jako zásadní především stanoviska Pracovní skupiny WP 29. Společně s nahrazením Směrnice 95/46/ES Obecným nařízením GDPR, též WP 29 nahradil – EDPB[363]. Mnohá její stanoviska jsou však nadále velmi relevantní, WP 29 problematiku Data Retention podrobně analyzovala a vyjadřovala se k ní ještě před jejím legislativním zakotvením. K některým dílčím otázkám se vyjadřoval také ÚOOÚ, zpravidla formou komentářů k vybraným soudním rozhodnutím a připomínek k legislativním návrhům.

Klíčovými pro vývoj právní úpravy Data Retention jsou soudní rozhodnutí, a to především nálezy Ústavního soudu ČR a na úrovni EU rozhodnutí SDEU k předběžným otázkám předloženým soudy členských států ve vztahu k národním právním úpravám Data Retention, relevantní jsou též některá rozhodnutí ESLP týkající se zásahů do soukromí, specificky v podobě shromažďování provozních a lokalizačních údajů. K povinnosti Data Retention v právních řádech jednotlivých členských států se vyjadřovala i řada soudů těchto členských států, zpravidla soudů ústavních, s ohledem na to zde autor stručně rozebere pouze vybraná rozhodnutí zahraničních soudů. Německý Spolkový ústavní soud (Bundesverfassungsgericht) dlouhodobě požívá vysokého respektu u ústavních právníků i v jiných státech EU[364], jeho rozhodnutí často cituje i Ústavní soud ČR, a to i v jeho nálezech rozebíraných dále v této práci[365], a to zpravidla jako rozhodnutí jediného zahraničního ústavního soudu. Kromě stručné zmínky několika rozhodnutí z dalších států EU autor považuje za vhodné rozebrat na tomto místě rozhodnutí Ústavního soudu SR ve věci Data Retention[366]. Tento nález byl vydán až poté, co SDEU rozhodl o prohlášení neplatnosti Data Retention Směrnice. Ústavní soud SR v něm tak reflektuje a výslovně zmiňuje závěry

---

[363] Dle čl. 94 odst. 2 GDPR se odkazy na pracovní skupinu pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízenou článkem 29 směrnice 95/46/ES *„považují za odkazy na Evropský sbor pro ochranu osobních údajů zřízený tímto nařízením.“*

[364] Oblast ochrany soukromí má nejen v německé soudní praxi, ale i v oblasti legislativní dlouhodobou tradici. Zákon o ochraně osobních údajů německé spolkové země Hesensko (Hessisches Datenschutzgesetz – HDSG) byl přijat již 7. října 1970 a stal se tak celosvětově prvním právním předpisem v této oblasti. Celoněmecký předpis, zákon na ochranu osobních údajů před zneužitím při jejich zpracování (Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 27. Januar 1977) byl přijat pouze o několik let později, 27. ledna 1977 (aktuální název zní Spolkový zákon o ochraně osobních údajů – Bundesdatenschutzgesetz (BDSG).
Viz. SPOLKOVÁ REPUBLIKA NĚMECKO. Hessisches Datenschutzgesetz vom 7. Oktober 1970 GVBl. I S. 625. [online]. 2005 [cit. 21.4.2017], SPOLKOVÁ REPUBLIKA NĚMECKO. Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Daten bei der Datenverarbeitung vom 27 Januar 1977. [online]. 1977 [cit. 24.2.2024]. V podrobnostech viz též KÜHLING, Jürgen, BUCHNER, Benedikt. *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. Kommentar. 4. Auflage.* München: C.H.BECK Verlag, 2024.

[365] Takto je tomu i ve všech třech nálezech Ústavního soudu ČR k problematice Data Retention, tedy v nálezech sp. zn. Pl. ÚS 24/10, Pl. ÚS 24/11 a Pl. ÚS 45/17.

[366] Nález Ústavného súdu Slovenskej republiky sp.zn. PL. ÚS 10/2014 ze 29. apríla 2015.

rozhodnutí SDEU. Navíc se slovenské rozhodnutí týká sice zahraničního právního předpisu, ten ovšem vykazuje mnohé znaky obdobné právní úpravě aktuálně platné a účinné v ČR. U všech rozhodnutí zahraničních soudů i SDEU se autor specificky zaměří na ty jejich závěry, které považuje za relevantní ve vztahu k aktuální právní úpravě Data Retention platné a účinné v ČR.

Pracovní skupina WP 29

S ohledem na zřízení EDPB až v GDPR[367], tedy v době po zásadních rozhodnutích SDEU k Data Retention Směrnici se k problematice Data Retention EDPB zásadním způsobem nevyjadřoval, relevantní jsou tedy v této oblasti dřívější stanoviska předchozí WP 29. Pracovní skupina WP 29 zamýšlenou právní úpravu Data Retention již před jejím vznikem označila za problematickou z hlediska jejího zásahu do právem chráněných zájmů fyzických osob na ochraně soukromí a také vymezila konkrétní problematická místa. Ve stanovisku[368] z prosince 2001 WP 29 rovněž vyjádřila obavy z narůstající tendence označovat ochranu osobních údajů jako překážku efektivního boje proti terorismu a vyzvala k tomu, aby opatření proti terorismu nesnížila standardy ochrany základních lidských práv.

V průběhu příprav Data Retention Směrnice[369] WP 29 označila návrh Evropské komise za historické rozhodnutí, které zasahuje do nedotknutelného základního práva na důvěrnost komunikace, a vyjádřila pochyby o odůvodněnosti povinného a všeobecného uchovávání údajů, včetně pochybností o tom, zda návrh na takovéto uchovávání je založen na naprosto jasných důkazech. Účel uchovávání údajů by podle WP 29 měl být přímo ve směrnici jasně vymezen jako boj proti terorismu a organizovanému zločinu, nikoli blíže neupřesněná závažná trestná činnost. Upozorňuje také na existenci přístupů mnohem šetrnějších vůči soukromí, jako např. „quick-freeze" procedura[370]. Důkazy pro zavedení takových prostředků, jako je data retention, by také měly být podrobovány pravidelnému vyhodnocování, nejméně

[367] Viz čl. 68 GDPR.
[368] ARTICLE 29 – DATA PROTECTION WORKING PARTY. *Opinion 10/2001 on the need for a balanced approach in the fight against terrorism. WP 53.* Adopted on 14 December 2001. [online]. 2001 [cit. 24.2.2024].
[369] ARTICLE 29 – DATA PROTECTION WORKING PARTY. *Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005)*. *WP 113.* Adopted on 21st October 2005. [online]. 2005 [cit. 24.2.2024].
[370] Výrazem data retention quick freeze, nebo též Data Preservation je v odborné terminologii označována metoda, podle které jsou uchovávány provozní a lokalizační údaje týkající se pouze konkrétní osoby, a to až od okamžiku, kdy vůči této osobě vznikne konkrétní podezření a je tedy vydán příkaz k uchovávání údajů této osoby. Takto je výraz definován v Memu Evropské komise Frequently Asked Qestions: The Data Retention Questions, datovaném 8. dubna 2014. Viz European Commission. *Memo Frequently Asked Qestions: The Data Retention Questions.* [online]. 8 April 2014 [cit. 24.2.2024].

každé 2-3 roky a účinnost legislativy by měla být založena na tzv. „sunset“ konceptu, tedy měla by obsahovat ustanovení, že její účinnost zanikne k určitému konkrétnímu datu (v tomto případě po 3 letech), pokud není výslovným aktem prodloužena. Podle WP 29 není v žádném případě z hlediska existujícího evropského právního rámce akceptovatelné uložit data retention povinnost poskytovatelům komunikačních služeb, aniž by byly předem definovány adekvátní konkrétní záruky k ochraně soukromí. WP 29 připravila seznam 20 konkrétních opatření týkajících se zpracování provozních a lokalizačních údajů, potřeby autorizace, požadavků zabezpečení a logického oddělení dat, potřeby vyloučit obsah komunikace apod.

Krátce po přijetí Data Retention Směrnice[371] WP 29 upozornila, že obavy v předchozím stanovisku vyjádřené si zachovaly svou platnost, a zdůraznila bezprecedentní charakter rozhodnutí zavést data retention povinnost, které naruší každodenní život každého občana a může ohrozit základní hodnoty a svobody všech Evropanů. WP 29 v této souvislosti považuje za zcela zásadní, aby byla Data Retention Směrnice v každém členském státě EU doprovázena opatřeními omezujícími její dopad do soukromí a jelikož text přijaté směrnice dle jejích závěrů ponechává v některých směrech prostor pro odlišné interpretace, navrhuje, aby byla Data Retention Směrnice implementována v celé EU jednotným způsobem. Záruky by dle WP 29 měly zahrnovat především: upřesnění účelu uchovávání a jasná definice pojmu závažný trestný čin, omezení přístupu k údajům pouze na výslovně zákonem oprávněné orgány, u kterých je dána potřeba vyšetřování, odhalování a stíhání trestných činů uvedených ve směrnici, každé použití údajů by mělo být zaznamenáno a záznamy zpřístupněny orgánu dozoru za účelem zajištění efektivního dozoru, omezení kategorií uchovávaných údajů na minimum, jakékoli jejich rozšíření by mělo být předmětem striktního testu potřebnosti, zákaz data mining-u, tedy „vytěžování“ uchovávaných údajů, zejména ve vztahu k cestovním a komunikačním vzorům chování osob, které nejsou podezírány z trestné činnosti a v neposlední řadě též soudní/nezávislá kontrola a autorizace každého případu přístupu k údajům. K jednotné implementaci však nedošlo a také výše uvedené body z velké části nebyly v praxi naplněny.

Soudní dvůr EU

Kromě soudů členských států EU se povinností Data Retention opakovaně zabýval také Soudní dvůr EU. Již krátce po přijetí Data Retention Směrnice, v roce 2006 se Irsko,

[371] ARTICLE 29 – DATA PROTECTION WORKING PARTY. *Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the Retention of data generated or processed in connection with the provision of publicly availabe electronic communications services or of public communications networks and amending Directive 2002/58/EC. WP 119.* Adopted on 25 March 2006. [online]. 2006 [cit. 24.2.2024].

podporované v řízení Slovenskou republikou v žalobě proti Evropskému parlamentu a Radě Evropské unie domáhaly u SDEU zrušení této směrnice. Důvodem žaloby byl právní základ směrnice – opatření k odstranění překážek a narušení na vnitřním trhu EU, ačkoli jejím skutečným účelem bylo harmonizovat uchovávání údajů za účelem usnadnění činnosti členských států v oblasti trestního práva, z tohoto důvodu nemůže být přijata v rámci působnosti Společenství. Slovensko navíc uvádělo i výrazný zásah do soukromí jednotlivců, obtížně odůvodnitelný zájmem na fungování vnitřního trhu. SDEU žalobu zamítl[372], zákonodárce Společenství dle jeho hodnocení nepochybil, jelikož rozdíly mezi vnitrostátními právními úpravami uchovávání údajů o elektronických komunikacích *„mohly mít přímý dopad na fungování vnitřního trhu“*. Právem na respektování a ochranu soukromého života se SDEU prakticky vůbec nezabýval.

V roce 2012 se SDEU opět zabýval Data Retention Směrnicí, k žádostem High Court Irska[373] a rakouského ústavního soudu[374] o rozhodnutí o předběžné otázce ve vztahu k Data Retention Směrnici. SDEU obě řízení spojil a v řízení posuzoval především slučitelnost Data Retention Směrnice s Listinou EU, resp. s Evropskou úmluvou, zejména s právem na respektování soukromého života a právem na ochranu osobních údajů. Měl rozhodnout, zda omezení lidských práv vyplývající z Data Retention Směrnice nejsou nepřiměřená a zda jsou nezbytná k řádnému fungování vnitřního trhu EU, případně k vyšetřování závažných trestných činů.

Generální advokát Pedro Cruz Villalón ve svém stanovisku doporučil SDEU vyslovit neplatnost směrnice, z důvodu její neslučitelnosti s Listinou EU. Provádění Data Retention Směrnice dle jeho závěrů může u občanů EU vyvolat dojem sledování, zvýšenou pozornost proto nevyžaduje až zpracování uchovávaných údajů, nýbrž už jejich samotné shromažďování. Údaje o telekomunikačním provozu se týkají soukromého života a jeho tajemství, včetně intimního života a jsou tak více než osobními údaji. Data Retention Směrnice tak podle generálního advokáta představuje mimořádně závažný zásah do práva na respektování soukromého života, ten je zcela nepřiměřený potřebě zajistit fungování vnitřního trhu, formálně primárního cíle směrnice. U jejího druhotného cíle – stíhání závažné trestné

[372] Soudní dvůr EU v této kauze rozhodl 10.února 2009. Rozsudek Soudního dvora (velkého senátu) C-301/06 Ireland v European Parliament and Council z 10. února 2009.
[373] Digital Rights Ireland Ltd v Minister of Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commisioner of the Garda Síochána, Ireland, The Attorney General, za účasti Irish Human Rights Commision (C-293/12).
[374] Kärtner Landesregierung, Michael Seitlinger, Christof Tschohl u. a. (C-594/12). Rakouský ústavní soud podal žádost z podnětu vlády spolkové země Korutany, k níž se přidalo dalších 11.130 navrhovatelů.

činnosti – pak podle jeho názoru omezení základních práv nejsou doprovázena dostatečnými zárukami. Dle generálního advokáta měl unijní zákonodárce přinejmenším definovat zásady pro uplatňování dostatečných záruk a pro kontrolu jejich dodržování, zejména popis trestných činů odůvodňujících přístup k uchovávaným údajům, soudní kontrolu pro každou žádost o přístup, povinnost orgánů alespoň následně, poté, co pomine nebezpečí narušení vyšetřování, informovat o přístupu k údajům dotčenou osobu a další. Villalón vyslovil výhrady také k době uchovávání údajů. Velký senát SDEU v rozsudku z 8. dubna 2014 Data Retention Směrnici prohlásil za neplatnou, s odůvodněním, že unijní zákonodárce jejím přijetím překročil meze, jež ukládá požadavek na dodržování zásady proporcionality. Směrnici v rozhodnutí vytýká zejména šíři narušení soukromí u celé evropské populace, neomezený přístup národních úřadů k uchovávaným datům a nedostatečné požadavky směrnice na bezpečnost uchovávaných údajů.

Evropská komise v reakci na vyslovení neplatnosti Data Retention Směrnice v prvé řadě vyjádřila názor, že neplatnost směrnice nemá vliv na platnost jednotlivých národních právních úprav v členských státech. Podle autora toto tvrzení sice odpovídá skutečnosti, současně je však pravděpodobné, že důvody, které SDEU v rozsudku o neplatnosti Data Retention uvedl, se mohou vztahovat i na mnohé národní právní úpravy, jak ostatně ukázala následná rozhodnutí SDEU. Evropská komise navíc v reakci na rozsudek SDEU výslovně uvedla[375], že nechystá legislativní návrh, který by zrušenou směrnici nahradil novou právní úpravou, znovu zavádějící povinnost Data Retention, přitom však reagující na obavy a výtky obsažené v rozsudku SDEU. Autor toto vyjádření hodnotí jako velmi překvapivé, zvláště s ohledem na to, že Evropská komise až do vydání Rozsudku Digital Rights důrazně vymáhala transpozici Data Retention Směrnice, a to i žalobami proti Švédsku, Rakousku či Německu[376]. Prohlášením směrnice za neplatnou tak faktický stav zůstal nezměněn a nedostatky právní úpravy Data Retention vytýkané ze strany SDEU zůstaly ve většině členských států součástí právních řádů.

V důsledku toho se SDEU i po prohlášení Data Retention směrnice za neplatnou nadále opakovaně zabýval samotnou povinností Data Retention. Prvním takovým případem byly spojené věci C-203/15 a C-698/15, předmětem rozhodování zde byl především soulad

[375] European Commission. *European Commission statement on national data retention laws*. Brussels, 16 September 2015. [online] [cit. 24.2.2024].
[376] Řízení pro nesplnění povinnosti podle čl. 258 a násl. Smlouvy o fungování Evropské unie. Evropská komise v. Švédské království, věc C-185/09 a C-270/11, Evropská komise v. Rakouská republika, věc C-189/09 a Evropská komise v. Německo, věc C-329/12.

obecné povinnosti uchovávat provozní a lokalizační údaje s ustanovením čl. 15 odst. 1 Směrnice o soukromí a elektronických komunikacích. Toto ustanovení umožnuje členským státům EU při splnění vymezených požadavků přijmout opatření, kterými omezí rozsah ochrany poskytovaný dle této směrnice provozním, lokalizačním a souvisejícím údajům. Kromě toho se v tomto případě SDEU zabýval také otázkou, zda Rozsudek Digital Rights uvádí závazné požadavky unijního práva, které se vztahují na vnitrostátní režim členského státu upravující přístup k údajům uchovávaným podle vnitrostátních právních předpisů a které je nutno dodržet k dosažení souladu s články 7 a 8 Listiny EU.

Základem sporů byla povinnost Data Retention ve švédském právním řádu opírající se o Směrnici o soukromí a elektronických komunikacích a slučitelnost obdobné povinnosti obsažené v právu Velké Británie s články 7 a 8 Listiny EU a článkem 8 Evropské úmluvy. Generální advokát SDEU, Henrik Saugmandsgaard Oe ve svém stanovisku[377] doporučil na předběžné otázky odpovědět tak, že předmětný článek Směrnice o soukromí a elektronických komunikacích a relevantní články Listiny EU musejí být vykládány tak, že členským státům nebrání uložit poskytovatelům služeb elektronických komunikací povinnost Data Retention, za předpokladu splnění několika podmínek. Povinnost Data Retention musí být založena na zákonném nebo regulačním opatření, které je dostatečně předvídatelné a zajišťuje adekvátní ochranu před svévolným zásahem, tato povinnost a záruky s ní spojené musejí respektovat podstatu práv dle čl. 7 a 8 Listiny EU, samotná povinnost také musí být naprosto nezbytná k boji proti závažným trestným činům a současně musejí být naplněny záruky definované v Rozsudku Digital Rights, kromě toho též musí být splněno kritérium přiměřenosti v demokratické společnosti.

SDEU však v Rozsudku Tele2 Sverige AB rozhodl, že článek 15 Směrnice o soukromí a elektronických komunikacích ve spojení s relevantními články Listiny EU musí být vykládán tak, že brání vnitrostátní právní úpravě založené na plošném uchovávání provozních a lokalizačních údajů všech účastníků a uživatelů, a to i v případě národní právní úpravy přijaté za účelem boje proti trestné činnosti. Tento článek Směrnice o soukromí a elektronických komunikacích musí být dle SDEU vykládán dále tak, že brání vnitrostátní právní úpravě, která upravuje ochranu a bezpečnost provozních a lokalizačních údajů, zejména přístup příslušných vnitrostátních orgánů k uchovávaným údajům, přitom však tento přístup neomezuje výlučně pro účely boje proti závažné trestné činnosti, nepodmiňuje jej

[377] Stanovisko Generálního advokáta Soudního dvora EU, Henrika Saugmandsgaard Oe, ze dne 19. července 2016 ve spojených věcech C-203/15 a C-698/15.

předchozím přezkumem ze strany soudu nebo nezávislého správního orgánu a nevyžaduje uchovávání údajů na území EU.

SDEU zde vycházel do značné míry z Rozsudku Digital Rights, jeho závěry však výrazně rozvinul. V prvé řadě posuzoval, do jaké míry (a zda vůbec) se oblast působnosti Směrnice o soukromí a elektronických komunikacích vztahuje na vnitrostátní právní úpravy týkající se uchovávání provozních a lokalizačních údajů a přístupu oprávněných orgánů k nim, když dle Směrnice o soukromí a elektronických komunikacích se oblast její působnosti nevztahuje na činnosti státu ve vymezených oblastech, zejména v oblasti trestního práva a na činnosti týkající se veřejné bezpečnosti, obrany, bezpečnosti státu apod[378]. Dle SDEU je nepochybné, že se legislativní opatření uvedená v článku 15 odst. 1 Směrnice o soukromí a elektronických komunikacích týkají „*činností, jež jsou vlastní státům nebo státním orgánům a nesouvisejí s oblastmi činností jednotlivců*“, nelze však dospět k závěru, že se oblast působnosti směrnice nevztahuje na tato legislativní opatření, v opačném případě by toto ustanovení bylo „*zcela zbaveno užitečného účinku*“.

Při výkladu článku 15 odst. 1 Směrnice o soukromí a elektronických komunikacích SDEU vycházel z toho, že cílem této směrnice je „*ochránit uživatele služeb elektronických komunikací před riziky pro jejich osobní údaje a soukromí*“, směrnice komukoli kromě účastníků zakazuje uchovávat provozní údaje bez souhlasu účastníků[379]. Výjimku představují osoby oprávněné zákonem v souladu s článkem 15 odst. 1 směrnice, v souladu s ustálenou judikaturou musí však být toto ustanovení vykládáno restriktivně[380] a nemůže tedy odůvodnit, aby se výjimka ze zákazu uchovávání údajů stala pravidlem. Z ustálené judikatury SDEU vyplývá rovněž povinnost dodržovat zásadu proporcionality, v posuzovaném případě se tato zásada uplatní tak, že ochrana základního práva na respektování soukromého života vyžaduje, aby výjimky z ochrany osobních údajů a její omezení byly činěny v mezích toho, co je naprosto nezbytné. Na základě těchto východisek SDEU dospěl k závěru, že právní úprava stanovící plošné a nerozlišující uchovávání veškerých provozních a lokalizačních údajů všech účastníků a registrovaných uživatelů, prostřednictvím veškerých prostředků elektronické komunikace a ukládající povinnost ukládat tyto údaje systematicky a průběžně, bez jakékoli

[378] Článek 1 odst. 3 Směrnice o soukromí a elektronických komunikacích.
[379] Článek 5 odst. 1 Směrnice o soukromí a elektronických komunikacích.
[380] K tomu např. Rozsudek Soudního dvora EU (třetího senátu) ze 22. listopadu 2012 Josef Probst v. mr.nexnet GmbH. Žádost o rozhodnutí o předběžné otázce podaná Bundesgerichtshof. Věc C-119/12, bod 23. *Soudní dvůr EU* [online]. 2012 [cit. 24.2.2024] či Rozsudek Soudního dvora EU (třetího senátu) ze 17. února 2011. The Number (UK) Ltd, Conduit Enterprises Ltd proti Office of Communications, British Telecommunications plc. Věc C-16/10, bod 31. *Soudní dvůr EU* [online]. 2011 [cit. 24.2.2024].

výjimky, jako je tomu v případě posuzované právní úpravy, překračuje meze toho, co je naprosto nezbytné a tudíž ji nelze v demokratické společnosti považovat za odůvodněnou. Dle SDEU však současně článek 15 odst. 1 Směrnice o soukromí a elektronických komunikacích nebrání tomu, aby členský stát přijal právní úpravu, která „*preventivně umožňuje cílené uchovávání provozních a lokalizačních údajů za účelem boje proti závažné trestné činnosti za podmínky, že uchovávání je omezeno na to, co je nezbytně nutné*“, pokud jde o: kategorie uchovávaných údajů, komunikační prostředky, na které se uchovávání vztahuje, dotčené osoby a dobu uchovávání. Toto vymezení považuje autor za významné pro definici právní úpravy de lege ferenda.

Dle SDEU lze v zásadě umožnit přístup pouze k údajům osob, u nichž existuje podezření, že připravují, páchají či spáchaly závažný trestný čin, nebo se na takovém trestném činu podílely[381]. V Rozsudku Tele2 Sverige AB však SDEU tyto podmínky rozšířil, dle jeho hodnocení lze v určitých situacích poskytnout přístup také k údajům jiných osob, je však nutné, aby vnitrostátní právní úprava na základě objektivních skutečností vymezila okruh takových osob, jejichž údaje „*mohou vykázat minimálně nepřímou souvislost se závažnou trestnou činností nebo určitým způsobem přispívat k boji proti závažné trestné činnosti, či k předcházení závažného ohrožení veřejné bezpečnosti*“. Konkrétně se může jednat o vymezení na základě zeměpisného kritéria, za podmínky, že příslušné vnitrostátní orgány dospějí k závěru podloženému objektivními skutečnostmi o tom, že v konkrétní územní oblasti existuje zvýšené riziko přípravy či páchání takovéto trestné činnosti.

Dále je dle SDEU nutné, aby, s výjimkou naléhavých případů, byl přístup vnitrostátních orgánů k údajům řádně odůvodněn a podléhal předchozímu přezkumu ze strany nezávislého orgánu a dále aby příslušné orgány o tomto přístupu následně vyrozuměly dotčené osoby v okamžiku, kdy toto vyrozumění nebude moci ohrozit vedené vyšetřování. Dalším nezbytným prvkem vnitrostátní úpravy je zajištění dohledu nezávislého orgánu nad dodržováním úrovně ochrany, kterou unijní právo zaručuje fyzickým osobám v souvislosti se zpracováním osobních údajů – takovýto dohled výslovně vyžaduje článek 8 odst. 1 a 3 Listiny EU.

V dalších letech se SDEU problematikou Data Retention zabýval i nadále, opakovaně, na základě předběžných otázek národních soudů ve vztahu k relevantním

[381] Viz Rozsudek ESLP – Judgment of the European Court of Human Rights, dated 4 December 2015. Case of Roman Zakharov v. Russia (Application no. 47143/06). 260. *European Court of Human Rights* [online]. 2008. [cit. 24.2.2024].

národním úpravám[382]. Tato skutečnost je dle autora přímým důsledkem výše popsané situace, kdy po prohlášení Data Retention Směrnice za neplatnou zůstaly v řadě členských států EU beze změn národní právní úpravy tuto směrnici transponující, lze říci, že jde o faktický rozpor mezi závěry Rozsudku Digital Rights a realitou. S ohledem na obdobné rysy těchto rozsudků a též obdobné závěry SDEU autor nepovažuje za nutné podrobně se zde zabývat každým z nich. Z dalších rozsudků SDEU mají dle hodnocení autora zásadní význam rozsudky ze 6. října 2020 ve věci C-623/17 a ve spojených věcech C-511/18, C-512/18 a C-520/18[383], v nichž SDEU posuzoval belgickou, francouzskou a britskou právní úpravu Data Retention. Obdobně je vyhodnotil ÚOOÚ, který k nim vydal vyjádření[384], v němž upozornil na výroky, kterými *„se obecně zakazují národní legislativní opatření založená ustanovením čl. 15 směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, pokud preventivně ukládají plošné a nerozlišující uchovávání provozních a lokalizačních údajů“*. Jak uvádí ÚOOÚ, takové uchovávání lze dle rozsudku nařídit jen ve specifických případech, v zásadě pouze *„pokud je nutno čelit závažné hrozbě pro národní bezpečnost a jsou splněny další stanovené podmínky“*. Z tohoto důvodu ÚOOÚ *„považuje za primárně nezbytné vyřešit otázku, nakolik může ve světle těchto rozhodnutí obstát stávající pojetí představované především ustanovením § 97 zákona č. 127/2005 Sb., o elektronických komunikacích a souvisejícími předpisy založené na preventivním šestiměsíčním zadržování provozních a lokalizačních údajů“*. ÚOOÚ výslovně zmiňuje, že si v této souvislosti je vědom nálezu Ústavního soudu ČR Pl. ÚS 45/17 a uzavírá, že *„bude proto nutno zvážit, jak naplnit požadavky výslovně uváděné v předmětných rozsudcích Soudního dvora Evropské unie“*. Jako řešení, které by považoval za přiměřené, ÚOOÚ navrhuje *„individuální stanovení lhůt pro uchovávání dat“*, které *„by měly být určeny zvláště pro různé účely (cíle) a s největší pravděpodobností rovněž i pro různé komunikační kanály a též individuálně odůvodněny, tak, aby bylo budoucí vytěžování zadržených údajů pro dotčené subjekty předvídatelné a mohlo obstát.“* ÚOOÚ zvláště upozorňuje na to, že předmětem dalších úvah *„musí být i otázka, do jaké míry k překlenutí nastíněných problémů postačí pouze určitý eurokonformní výklad, či*

[382] Viz Rozsudky SDEU ve věcech C-623/17 (Velká Británie), C-746/18 (Estonsko), C-140/20 (Irsko) či ve spojených věcech C-793/19 a C-794/19 (Německo).
[383] Společně vyhlášené rozsudky Soudního dvora EU (velkého senátu) ze 6. října 2020 ve věci C-623/17 Privacy International a ve spojených věcech C-511/18 La Quadrature du Net a další, C-512/18 French Data Network a další a C-520/18 Ordre des barreaux francophones et germanophone a další.
[384] ÚOOÚ. *Lhůty pro uchovávání dat by se měly pro různé subjekty stanovovat individuálně.* 14.1.2021. [online] [cit. 18.3.2024]. Dostupné z www.uoou.gov.cz.

zda je nutná změna zákona“, čímž patrně naráží na závěry Ústavního soudu ČR v nálezu Pl. ÚS 45/17.

Po analýze uvedených rozsudků SDEU se autor s hodnocením ÚOOÚ plně ztotožňuje, dle hodnocení autora tyto rozsudky konzistentně navazují na předchozí rozhodnutí SDEU ve vztahu k povinnosti Data Retention. V těchto rozsudcích SDEU vymezil situace, ve kterých je dle jeho hodnocení v souladu s unijním právem možno v národních právních řádech uložit povinnost Data Retention v podobě plošného a nerozlišujícího uchovávání provozních a lokalizačních údajů, a současně vymezil podmínky, které při tom musejí být naplněny. SDEU současně potvrdil platnost svých dosavadních závěrů i v posuzovaných případech, Směrnice o soukromí a elektronických komunikacích dle jeho hodnocení brání i takové vnitrostátní úpravě, která umožňuje uložení povinnosti *„plošného a nerozlišujícího předávání provozních a lokalizačních údajů bezpečnostním a zpravodajským službám“*. Jako výjimku z obecné nepřípustnosti plošného uchovávání údajů lze dle SDEU takovouto povinnost legislativním opatřením uložit v situaci závažného ohrožení národní bezpečnosti, které se *„jeví jako skutečné a aktuální nebo předvídatelné“*. Pro účely zajištění národní bezpečnosti, boje proti závažné trestné činnosti a předcházení závažnému ohrožení veřejné bezpečnosti lze také uložit povinnost plošného a nerozlišujícího *„uchovávání IP adres přidělených zdroji připojení“* a *„uchovávání údajů o totožnosti uživatelů prostředků elektronické komunikace“*. Přípustným je dle SDEU též uchovávání provozních a lokalizačních údajů, které je cílené, tedy omezené na určité kategorie osob či omezené zeměpisnými kritérii, vždy však musí být vymezení objektivní a nediskriminační. Ve všech těchto případech lze takto dle SDEU postupovat pouze po časově omezenou dobu, podmínkou jsou též jasná a přesná pravidla a účinné záruky proti riziku zneužití. SDEU v těchto rozsudcích dále vymezil některé další přípustné dílčí případy, zejména shromažďování provozních a lokalizačních údajů v reálném čase apod.

Jelikož SDEU byl v tomto případě omezen položenými předběžnými otázkami, vztahují se diskutované rozsudky pouze na belgickou, francouzskou a britskou úpravu Data Retention. Autor je však toho názoru, že závěry SDEU lze obdobně vztáhnout též na jiné národní právní úpravy členských států EU, které splňují popisovaná kritéria, byť ve vztahu k těmto právním úpravám rozsudky postrádají závazný charakter, s ohledem na absenci předběžné otázky.

Evropský soud pro lidská práva

Vedle rozsudků ESLP zmiňovaných již v předchozím textu autor ve vztahu k problematice Data Retention považuje za významné také dva novější rozsudky ESLP týkající se specificky „hromadného zachycování“ elektronické komunikace a získávání komunikačních údajů od poskytovatelů komunikačních služeb, a to primárně údajů přeshraniční komunikace využívaných zpravodajskými službami.

První z nich, Rozsudek Big Brother Watch a ostatní proti Spojenému království ze 13. září 2018[385], zmiňuje také Ústavní soud ČR v nálezu Pl. ÚS 45/17. ESLP v tomto rozsudku dospěl k závěru, že v posuzovaném případě byl porušen čl. 8 Evropské úmluvy garantující právo na respektování soukromého a rodinného života, a to kvůli chybějícímu dostatečnému nezávislému dohledu nad vyhledávacími procesy, včetně výběru komunikace postoupené analytikům, dále kvůli absentujícím zárukám uplatněným na výběr komunikace a také proto, že právní úprava Velké Británie použitá v posuzované věci nerespektovala požadavek unijního práva na umožnění získávání komunikačních údajů pouze pro potřeby boje se závažnou trestnou činností, když dovolovala získávání údajů za účelem boje s jakoukoliv trestnou činností. Kromě toho také získávání údajů nepodléhalo dle práva Velké Británie *„předběžné kontrole nezávislým orgánem veřejné moci, jak požadovalo unijní právo“*. ESLP z těchto důvodů vyhodnotil posuzovaný zásah jako nikoli v souladu se zákonem ve smyslu článku 8 Úmluvy, který v odst. 2 stanoví výjimku pro obecný zákaz státním orgánům zasahovat do práva na respektování soukromého a rodinného života, obydlí a korespondence. Pro použití této výjimky se však musí jednat o případ v souladu se zákonem a současně nezbytný v demokratické společnosti v zájmu hodnot v tomto ustanovení Evropské úmluvy vymezených. ESLP kromě toho v posuzovaném případě shledal i porušení čl. 10 Evropské úmluvy, zaručujícího každému právo na svobodu projevu. Zákon, který byl v dané věci použit, totiž dle hodnocení ESLP nestanovil dostatečné záruky ochrany novinářských zdrojů.

ESLP také v odůvodnění tohoto rozsudku opět zopakoval šest základních zákonných záruk bránících zneužití moci v oblasti trestního řízení, které již dříve stanovil ve své judikatuře[386]. Jsou jimi: 1. upřesnění povahy trestných činů vedoucích k vydání příkazu tajného odposlechu, 2. vymezení okruhu osob, jejichž komunikace se sleduje, 3. časové omezení trvání sledování, 4. dodržení určitého postupu při nakládání se získanými údaji, 5.

[385] ESLP. Rozsudek ze dne 13. září 2018 ve věcech č. 58170/13, 62322/14 a 24960/15 – Big Brother Watch a ostatní proti Spojenému království.
[386] U šesti zákonných záruk bránících zneužití moci ESLP odkázal konkrétně na svůj předchozí rozsudek Weber a Saravia proti Německu, č. 54934/00, rozhodnutí o nepřijatelnosti ze dne 29. června 2006.

zakotvení záruk pro předávání údajů dalším stranám a 6. vymezení podmínek pro smazání nebo zničení záznamů. Autor považuje takto formulované záruky za významné také ve vztahu k zásahům analyzovaným v této práci a má za to, že zejména zásady č. 1 a 2 lze obecně použít i při analýze právní úpravy Data Retention v právním řádu ČR. Jak uvádí ESLP ve druhém rozsudku (viz dále), první dvě z těchto záruk jsou platné pro cílené sledování, pro hromadné sledování se neuplatní. V podmínkách zde rozebírané plošné povinnosti dle aktuální právní úpravy ZoEK se však dle hodnocení autora tyto dvě záruky uplatní ve vztahu k podmínkám pro vyžádání povinně uchovávaných údajů.

Ve věci založené týmiž stížnostmi následně ESLP rozhodoval 25. května 2021[387], v rozsudku konstatoval, že *„britská právní úprava hromadného sledování elektronické komunikace a souvisejících komunikačních dat zpravodajskými službami stejně jako úprava získávání komunikačních dat od poskytovatelů komunikačních služeb neobsahují dostatečné záruky proti zneužití, a je proto v rozporu s články 8 a 10 Úmluvy“*. Posuzovaná právní úprava totiž dle hodnocení ESLP *„nedosahuje potřebné kvality, aby bylo zajištěno, že zásah do práv způsobený sledováním zůstane v mezích, které jsou v demokratické společnosti nezbytné“*. Autor považuje za důležité, že ESLP, na rozdíl od Ústavního soudu ČR v nálezu Pl. ÚS 45/17, v obou rozebíraných rozsudcích posuzoval záruky výslovně zakotvené v platné právní úpravě, nikoli záruky spočívající v aktuální míře využití údajů v praxi, kterážto míra, z povahy věci, může v čase podléhat změnám i za platnosti téže právní úpravy.

V odůvodnění tohoto rozsudku ESLP hromadné sledování popsal jako proces sestávající ze čtyř na sebe navazujících fází – zachycení a uložení komunikace a s ní souvisejících dat, filtrování těchto dat, analýza vybraných dat a jejich následné uložení, spolu s navazujícím zpracováním a použitím informací z nich získaných, včetně jejích sdílení se třetími osobami. Zásadní je dle autora právě toto rozlišení, přičemž ESLP výslovně konstatoval, že *„i samotné uložení dat, i když je možné je přečíst jen za pomoci zvláštní technologie, představuje zásah do práv chráněných článkem 8 Úmluvy“* a každá z dalších fází *„s sebou nese závažnější zásah do práv, a roste tak i potřeba adekvátních záruk proti zneužití“*. V případě plošného shromažďování a uchovávání údajů autor z hlediska dotčených osob považuje za potřebné rozlišit právě první z vymezených fází od fází následujících, když první fáze se týká nepoměrně rozsáhlejší skupiny osob nežli fáze ostatní, v nichž je zásah závažnější z hlediska své intenzity, týká se však již pouze (na základě určitých kritérií) vybraných osob.

[387] ESLP. Rozsudek ze dne 25. května 2021 ve věcech č. 58170/13, 62322/14 a 24960/15 – Big Brother Watch a ostatní proti Spojenému království.

Soudy jiných členských států EU

Národní právní úpravy Data Retention byly na národní úrovni soudně napadeny v řadě členských států EU, mnohdy ještě před prohlášením Data Retention Směrnice za neplatnou. Jako protiústavní byly takto zrušeny v České republice v důsledku dvou nálezů Ústavního soudu ČR z roku 2011[388], v Německu[389], Rumunsku[390], Bulharsku[391], na Kypru[392], v Polsku[393] nebo Belgii[394] a v některých dalších členských státech[395].

Také po rozhodnutí SDEU o prohlášení Data Retention Směrnice za neplatnou byla v některých členských státech EU iniciována soudní řízení napadající národní právní úpravy Data Retention. Ústavní soud Slovenské republiky již 2 týdny po rozsudku o neplatnosti Data Retention Směrnice pozastavil účinnost národní právní úpravy přijaté na Slovensku k provedení této směrnice[396]. Následně, 29. dubna 2015 Ústavní soud SR finálně rozhodl a příslušná ustanovení slovenských zákonů zrušil[397]. Obdobně rozhodly soudy např. v Rakousku[398], v Bulharsku[399] či v Nizozemí[400]. Slovinský ústavní soud v červenci 2014 zrušil relevantní ustanovení telekomunikačního zákona[401], jedním z důvodů bylo využívání uchovávaných údajů v mnohem širší míře nežli jen pro boj s terorismem či vyšetřování závažné trestné činnosti, např. i pro šetření pracovněprávních sporů nebo pro stíhání řidičů používajících v rozporu s platnou právní úpravou mobilní telefon při řízení motorového vozidla[402].

---

[388] Nálezy Ústavního soudu ČR sp. zn. Pl. ÚS 24/10 a sp. zn. Pl. ÚS 24/11.
[389] Bundesverfassungsgericht. Urteil vom 2. März 2010. 1 BvR 256/08, 1 BvR 263/08 a 1 BvR 586/08. *Bundesverfassungsgericht* [online]. 2010 [cit. 24.2.2024].
[390] Rozhodnutí Ústavního soudu Rumunska č. 1258/2009 ze dne 8. října 2009 v kauze Dragotoniu a Militaru-Pidhorni v. Romania, 2007, publikováno v Monitorul Oficial al Romaniei (v anglickém překladu Official Gazette of Romania) no. 798 ze dne 23, října 2009.
[391] Rozhodnutí bulharského Nevyššího správního soudu ze dne 17. prosince 2008.
[392] Rozhodnutí kyperského Nejvyššího soudu z února 2011.
[393] Rozhodnutí Polského ústavního soudu (Trybunal Konstytucyjny) ze 30. července 2014 sp. zn. K 23/11. Wyrok Trybunalu Konstytucyjnego Sygn. akt K 23/11 z dnia 30 lipca 2014 r.
[394] Rozhodnutí Ústavního soudu Belgie č. 84/2015 z 11. června 2015.
[395] Podrobněji viz KUSCHEWSKY, Monika. *Data Protection & Privacy, Jurisdictional comparisons.* Second Edition 2014. London : Thomson Reuters (Professional) UK Limited.
[396] Uznesenie Ústavného súdu Slovenskej republiky sp.zn. PL. ÚS 10/2014 z 23. apríla 2014.
[397] Nález Ústavného súdu Slovenskej republiky sp.zn. PL. ÚS 10/2014 ze 29. apríla 2015.
[398] Rozhodnutí Ústavního soudu Rakouska ze 27.června 2014 v kauze G-47/2012-49. Verfassungsgerichtshof. Urteil vom 27. Juni 2014. G-47/2012-49.
[399] Rozhodnutí Ústavního soudu Bulharska č. 8/2014 ze 12. března 2015.
[400] Rozhodnutí oblastního soudu v Haagu č.C/09/ 009/KG ZA 14/1575 ze dne 11.března 2015.
[401] Rozhodnutí Ústavního soudu Republiky Slovinsko č. U-I-65/13-19 ze 3.7.2014. Viz Slovenia / Constitutional Court / U-I-65/13-19. 3.7.2014.
[402] Podrobný přehled argumentace obsažené v jednotlivých rozhodnutích zahraničních soudů viz např. BOEHM, Franziska, COLE, Mark D. *Data Retention after the Judgement of the Court of Justice of the European Union.* Münster/Luxembourg, 30 June 2014. [online]. 2014. [cit. 15.1.2024].

Odborná úroveň Spolkového ústavního soudu Německa, jakož i kvalita rozhodnutí[403] rušícího národní právní úpravu Data Retention a jeho odůvodnění vedly k tomu, že toto rozhodnutí (ostatně podobně jako řada dalších rozhodnutí téhož soudu, z nichž některá autor dále v této práci taktéž zmiňuje) se stalo zdrojem názorových inspirací pro soudy jiných členských států EU při rozhodování o problematice Data Retention i obecně o otázkách týkajících se práva na informační sebeurčení. Spolkový ústavní soud zde shledal napadená ustanovení telekomunikačního zákona a trestního řádu tvořící v německém právním řádu úpravu Data Retention v rozporu s článkem 10 odst. 1 ústavy Spolkové republiky Německo, zaručujícím právo na ochranu listovního, poštovního a telekomunikačního tajemství, jako jedno ze základních práv, a jako taková je prohlásil za neplatná.

Rozhodnutí národních soudů se týkají vždy příslušné národní právní úpravy Data Retention, soudy v nich však především posuzovaly, zda tyto úpravy zasahující do práva na ochranu soukromí splňují ústavněprávní požadavky, zejména požadavek na splnění testu proporcionality. Jako nedostatečné soudy často shledaly vymezení účelů, pro něž mohou oprávněné orgány údaje využít a též záruky ochrany práv jednotlivců. Některé státy EU v reakci na soudní rozhodnutí připravily nové právní úpravy Data Retention, v nichž se tyto požadavky snažily zohlednit. Vláda Velké Británie v roce 2014 navrhla novou úpravu Data Retention and Investigatory Powers Act 2014 (dále též jen „DRIPA“), která uchovávání údajů umožnila, velmi výrazně však posílila kontrolní mechanismy a také omezila počet orgánů oprávněných údaje požadovat, samotná právní úprava přitom byla přijata na dobu určitou a výslovně zakotvuje povinnost vlády přehodnotit její potřebu po uplynutí roku 2016. V mezidobí však v rámci jejího soudního přezkumu Court of Appeal (England & Wales) (Civil Division) požádal SDEU o zodpovězení předběžných otázek, výsledkem byl již zmiňovaný rozsudek Tele2 Sverige AB.

Významná je nová právní úprava Data Retention v Německu[404], která zakotvila velmi krátkou dobu uchovávání údajů, rozlišenou navíc podle typu – 10 týdnů pro vymezené kategorie provozních údajů a pouze 4 týdny pro lokalizační údaje, které jsou navíc omezeny výhradně na označení základnových stanic mobilní sítě použitých volající a volanou stranou při začátku spojení (obdobně pro služby přístupu k internetu); na rozdíl od právní úpravy platné a účinné v ČR nejsou uchovávány údaje základnových stanic použitých při ukončení

[403] Bundesverfassungsgericht. Urteil vom 2. März 2010. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.
[404] Spolková republika Německo. Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (VerkDSpG k.a.Abk.) vom 10.Dezember 2015.

spojení. Výslovně jsou stanoveny kategorie údajů, které uchovávány být nesmějí, kromě obsahu komunikace též údaje o navštívených internetových stránkách, o službách elektronické pošty a údaje o telekomunikačních spojeních s osobami, úřady a organizacemi, které působí v sociální nebo církevní oblasti a poskytují poradenství v případech nouze volajícím, kteří zásadně zůstávají anonymními[405]; seznam těchto institucí vede regulační úřad, Bundesnetzagentur. Zakotvena je též řada kontrolních mechanismů, včetně povinnosti vlády vyhodnotit účinek právní úpravy na trestní řízení a na předcházení trestné činnosti, náklady způsobené veřejné správě a německému hospodářství a také dodržování předpisů k ochraně osobních údajů a zprávu předložit německému spolkovému sněmu.

Ústavní soud Slovenské republiky

S ohledem na dlouhý společný právní vývoj obou států vedoucí k obdobným právním a interpretačním tradicím považuje autora za potřebné, věnovat se na tomto místě nálezu Ústavního soudu Slovenské republiky sp. zn. PL.ÚS 10/2014 ze 29. dubna 2015 podrobněji. Soud v nálezu shledal, že napadená ustanovení nejsou v souladu s ústavními předpisy Slovenské republiky a mezinárodních smluv, v důsledku toho tato ustanovení ztratila účinnost dnem vyhlášení nálezu, s tím, že pokud je Národní rada Slovenské republiky ve lhůtě šesti měsíců neuvede do souladu s ústavními předpisy a mezinárodními smlouvami, pak po marném uplynutí této lhůty pozbývají napadená ustanovení taktéž platnost[406].

Napadená právní úprava (jak zákona o elektronických komunikáciách, tak trestného poriadku) vykazovala značnou podobnost s úpravou platnou v ČR, včetně vytýkaných nedostatků, lišila se v délce uchovávání údajů, stanovené ve slovenské úpravě ve dvou variantách: 6 měsíců pro údaje o internetové komunikaci a 12 měsíců pro ostatní provozní a lokalizační údaje. Navrhovatelé argumentovali také tím, že shromažďování provozních a lokalizačních údajů „*nemá žádný pozitivní vliv na odhalování závažných trestných činů v Evropě*“, mj. z důvodu existence méně invazivních, přesto rovnocenně efektivních způsobů boje proti závažné kriminalitě, což odůvodňovali např. výzkumy Institutu Maxe Plancka[407]. Namítali také existenci více způsobů, jak se uchovávání údajů vyhnout (použití sociálních sítí, webů pro sdílení videoobsahu, zpráv typu IM či IRC, P2P komunikace apod.), právní úprava

[405] Viz § 113b odst. 4, 5 a 6 ve spojení s § 99 odst. 2 telekomunikačního zákona ze 22. června 2004 (Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBI. I S.1190)).
[406] Takovéto důsledky předpokládá čl. 125 odst. 3 Ústavy Slovenské republiky.
[407] Max-Planck-Institut für ausländisches und internationales Strafrecht. Kriminologická studie „*Stutzlücken durch Wegfall der Vorratsdatenspeicherung?*“. 2012 [online] [cit. 15.1.2024]. Dostupné z www.grundrechte.ch.

proto není způsobilá dosáhnout sledovaný cíl – boj proti organizovanému zločinu a terorismu. Osoby pohybující se v tomto prostředí znají způsoby, jak se uchovávání údajů efektivně vyhnout, a „*zásah do soukromí se tak paradoxně dotkne více osob, které s trestnou činností nemají nic společného*“. S touto argumentací se Ústavní soud SR neztotožnil, v ostatním jsou právní závěry nálezu dosti podobné předchozím dvěma nálezům Ústavního soudu ČR sp. zn. Pl. ÚS 24/10 a Pl. ÚS 24/11, ostatně Ústavní soud SR právě z těchto nálezů na více místech cituje celé pasáže.

Dle Ústavního soudu SR napadená právní úprava neobstojí ve druhém kroku testu proporcionality, při posouzení kritéria nezbytnosti, resp. potřebnosti právní úpravy a výběru prostředků z hlediska míry jejich šetrnosti k dotčeným základním právům, tedy při posouzení požadavku na použití nejšetrnějších prostředků. Napadená ustanovení totiž *„nevyžadují žádnou souvislost mezi údaji, jejichž uchovávání stanoví, a hrozbou pro veřejnou bezpečnost*“, uchovávání se „*neomezuje ani na údaje z určitého časového období a/nebo z určité zeměpisné oblasti, či na okruh osob, které by jakýmkoli způsobem bylo možno spojovat se závažnými trestnými činy, ani na osoby, jejichž uchovávané údaje by z jiných důvodů mohly přispět k předcházení, odhalování nebo stíhání trestných činů*“. Sledovaného cíle lze dle soudu dosáhnout i jinými prostředky, méně zasahujícími do práva na soukromí, např. tzv. data freezing, zaměřený na údaje jen konkrétních účastníků. Napadená ustanovení by dle Ústavního soudu SR neprošla ani třetím krokem testu proporcionality, posouzením proporcionality v užším smyslu, jelikož nepřikládají žádný význam povaze a závažnosti trestného činu, pro který je vedeno trestní řízení. Soud napadené právní úpravě vytkl též nedostatečné záruky a prostředky ochrany dotčených jednotlivců.

Vláda Slovenské republiky v reakci na nález připravila novelu příslušných právních předpisů[408], která po schválení s účinností od 1. ledna 2016 zcela opustila princip Data Retention, jakožto plošného uchovávání provozních a lokalizačních údajů veškerých účastníků či uživatelů služeb elektronických komunikací a nahradila jej mechanismem Data Freeze. Novela provozovatelům sítí a poskytovatelům služeb uložila jednak povinnost předat oprávněným orgánům k jejich žádosti takové provozní a lokalizační údaje, které mají tyto osoby k dispozici z jiných, zákonem uznaných důvodů (pro účely vyúčtování služeb

[408] Zákon č. 397/2015 Z.z., ktorým sa na účely Trestného zákona ustanovuje zoznam látok s anabolickým alebo iným hormonálnym účinkom a ktorým sa menia a dopĺňajú niektoré zákony, novelizoval v oblasti Data Retention jak příslušná ustanovení zákona č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov, tak rovněž zákona č. 301/2005 Z.z. Trestný poriadok v znení neskorších predpisov, účinný od 1. ledna 2016 a dále též zákony upravující práva a povinnosti oprávněných orgánů.

účastníkovi, vymáhání její úhrady apod.), aniž by tyto údaje uchovávali pouze pro potřeby možného vyžádání oprávněnými orgány a vedle toho také povinnost uchovávat do budoucna po stanovenou dobu údaje pouze u konkrétní, v žádosti oprávněného orgánu označené osoby (data freeze). Novela zavedla i informační povinnost vůči osobě, jejíž údaje jsou takto zjišťovány. V případě lokalizačních údajů (tedy „*údajů potřebných k identifikaci polohy mobilního koncového zařízení*“) se uchovávání týká pouze „*údaje o poloze buňky při započetí komunikace*“.

Ústavní soud ČR – nálezy Pl. ÚS 24/10 a Pl. ÚS 24/11

Jak již uvedeno v předchozím textu, Ústavní soud ČR rozhodoval ve věci právní úpravy Data Retention nejprve v nálezech Pl. ÚS 24/10 a Pl. ÚS 24/11 a posléze v nálezu Pl. ÚS 45/17, první dva nálezy na sebe navazují nejen časově, ale i věcně. Nález Pl. ÚS 24/10 zrušil právní úpravu Data Retention obsaženou v ZoEK, včetně navazující vyhlášky[409]. Dle hodnocení Ústavního soudu ČR tato úprava neodpovídala ústavněprávním požadavkům na právní úpravu umožňující zásah do základních práv jednotlivců na soukromí, soud v nálezu tyto požadavky vymezil. V nálezu Pl. ÚS 24/11[410] Ústavní soud ČR posuzoval povinnost Data Retention obsaženou v Trestním řádu, také zde napadenou právní úpravu zrušil[411].

V nálezu Pl. ÚS 24/10 Ústavní soud ČR nejprve posuzoval, zda Data Retention Směrnice ponechává České republice dostatečný prostor pro její ústavně konformní transpozici do právního řádu; dospěl k závěru, že ano. Dle jeho hodnocení tato směrnice pouze vymezuje povinnost k uchovávání údajů, konkrétní podoba její transpozice je však již projevem vůle českého zákonodárce, který mohl při výběru prostředků variovat, při dodržení účelu směrnice. Ústavní soud ČR proto nevyhověl návrhu předložit SDEU předběžnou otázku ohledně neplatnosti Data Retention Směrnice.

Při posouzení práva na respekt k soukromému životu a práva na informační sebeurčení vycházel Ústavní soud ČR, vedle platného právního řádu ČR, též ze své ustálené judikatury, jakož i z četných rozsudků ESLP[412], v nichž ESLP opakovaně judikoval, že mezi

[409] Ustanovení § 97 odst. 3 a 4 ZoEK, vyhláška č. 485/2005 Sb. o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání.
[410] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 24/11; vyhlášen ve Sbírce zákonů pod číslem 43/2012 Sb.
[411] Ustanovení § 88a Trestního řádu.
[412] Např. Judgment of the European Court of Human Rights, dated 2 August 1984. Case of Malone v. The United Kingdom (Application no. 8691/79), Judgment of the European Court of Human Rights, dated 6 September 1978. Case of Klass and others v. Germany. Application No. 5029/71, Judgment of the European Court of Human Rights, dated 26 March 1987. Case of Leander v. Sweden (Application no. 9248/81) *European Court of Human Rights* [online]. 1987 [cit. 24.2.2024]., Judgment of the European Court of Human Rights, dated 24 April 1990. Case of Kruslin v. France (Application no. 11801/85). *European Court of Human Rights* [online]. 1987 [cit.

zásahy do soukromí jednotlivců patří „*mimo jiné i zásahy v podobě kontroly dat, obsahu pošty a odposlechu telefonních hovorů, zjišťování telefonních čísel telefonujících osob, zjišťování údajů o telefonním spojení…*“. ESLP také z práva na soukromý život v podobě práva na informační sebeurčení dovodil i „*pozitivní povinnost státu zlikvidovat data, která o osobě z její soukromé sféry stát shromáždil a zpracoval*“. Ve vztahu k vymezení aspektu práva na soukromí v podobě práva na informační sebeurčení a v otázce jeho obsahu a šíře Ústavní soud ČR výslovně odkazuje též na několik rozhodnutí Spolkového ústavního soudu Německa[413]. Právo na informační sebeurčení Ústavní soud ČR v tomto nálezu vymezuje jako součást práva na respekt k soukromému životu, „*vedle tradičního vymezení soukromí v jeho prostorové dimenzi (ochrana obydlí v širším slova smyslu) a v souvislosti s autonomní existencí a veřejnou mocí nerušenou tvorbou sociálních vztahů (v manželství, v rodině, ve společnosti)*“.

K omezení osobní integrity a soukromí osob ze strany veřejné moci může dle Ústavního soudu ČR dojít jen zcela výjimečně a za splnění stanovených podmínek, včetně dostatečných garancí a záruk jednotlivce proti možnému zneužití pravomoci ze strany veřejné moci. Takové záruky spočívají dle Ústavního soudu ČR především v odpovídající právní úpravě a v existenci účinné kontroly jejího dodržování, Ústavní soud ČR v tomto směru odkázal na svá rozhodnutí v otázce užití odposlechů telekomunikačního provozu[414]. Samotný zásah do základního práva na soukromí je možný jen právní úpravou, která odpovídá nárokům plynoucím z principů právního státu, zejména je přesná, formulačně zřetelná a dostatečně předvídatelná pro potenciálně dotčené jednotlivce[415] a naplňuje požadavky vyplývající z testu proporcionality. Za účelem ochrany jednotlivců proti svévolným zásahům je též nezbytné, aby právní úprava striktně definovala jak pravomoci udělené příslušným orgánům, tak i způsob a pravidla jejích provádění. Požadavek soudní ochrany základních práv se dle Ústavního soudu ČR v posuzovaném případě projevuje ve vydání soudního příkazu a také v jeho dostatečném odůvodnění, odpovídajícím požadavkům zákona i ústavním principům – musí být vydán

18.4.2017]., Judgment of the European Court of Human Rights, dated 25 September 2001. Case of P.G. and J.H. v. UK (Application no. 44787/98) a další.

[413] Rozhodnutí Spolkového ústavního soudu Německa – Bundesverfassungsgericht 1 BvR 209/83 (Volkszählungsurteil). Urteil vom 15. Dezember 1983. *Bundesverfassungsgericht* [online]. 1983, Bundesverfassungsgericht 1 BvR 518/02 (Rasterfahndungurteil). Urteil vom 4. April 2006. *Bundesverfassungsgericht* [online]. 2006, Bundesverfassungsgericht 1 BvR 668/04. Urteil vom 27. Juli 2005 (Vorbeugende Telekommunikationsüberwachung) a Bundesverfassungsgericht. 1 BvR 370/07, 1 BvR 595/07. Urteil vom 27. Februar 2008 (Grundrecht auf Computerschutz) [cit. 24.2.2024].

[414] Nálezy Ústavního soudu ČR sp. zn. II. ÚS 502/2000, sp. zn. IV. ÚS 78/01, sp. zn. I. ÚS 191/05, sp. zn. II. ÚS 789/06 či sp. zn. I. ÚS 3038/07 (N 46/48 SbNU 549).

[415] V tomto bodě Ústavní soud ČR vychází z judikatury ESLP, který ve výše zmiňovaných kauzách Malone proti UK, Amann proti Švýcarsku nebo Rotaru proti Rumunsku definoval velmi podobné principy pro posuzování ústavněprávních limitů omezení základních práv a svobod jednotlivců garantovaných v čl. 8 Úmluvy.

v řádně zahájeném řízení, pro zákonem kvalifikovanou trestnou činnost, být podložen relevantními indiciemi, individualizován ve vztahu ke konkrétní osobě a musí také uvést konkrétní skutečnosti významné pro trestní řízení, které mají být zjištěny, a z čeho je to vyvozováno[416].

Rozsah uchovávaných údajů v napadené právní úpravě vyhodnotil Ústavní soud ČR jako „*zcela zřetelně…nad rámcem rozsahu předvídaného předmětnou Směrnicí o data retention*“, konkrétně v případě telefonie u údajů o identifikaci předplacené telefonní karty, veřejného telefonního automatu, číslech dobíjecích kuponů a jejich přiřazení k dobíjenému číslu a o vazbách mezi mobilním přístrojem a vloženými SIM kartami a v případě internetového připojení a služeb a e-mailové komunikace u údajů o množství přenesených dat, o použití šifrování, metody a statusu požadavku na službu a její realizace a dále informací o posílání SMS z internetových bran a dalších „zájmových identifikátorů“. Dle Ústavního soudu ČR z uvedených údajů lze při sledování po delší časový úsek *„sestavit detailní informace o společenské nebo politické příslušnosti, jakož i o osobních zálibách, sklonech nebo slabostech jednotlivých osob*“. Názor vyjádřený Senátem ČR, dle kterého se „*v žádném případě nejedná o něco, co by se dalo přirovnat k odposlechům, už jen proto, že se neuchovávají obsahy jednotlivých telefonátů nebo mailových zpráv*“, označil Ústavní soud ČR za „*zcela mylný*“, když i „*pouze na jejich základě lze učinit dostatečné obsahové závěry spadající do soukromé (osobnostní) sféry daného jednotlivce*“, z uchovávaných údajů lze „*až s 90% jistotou dovodit např. s kým, jak často a dokonce v jakých hodinách se daný jednotlivec stýká, kdo jsou jeho nejbližší známí, kamarádi, či kolegové z práce, anebo jaké aktivity a v jakých hodinách provozuje*“. Z těchto důvodů Ústavní soud ČR vyhodnotil, že napadená právní úprava neodpovídá ústavněprávním požadavkům na právní úpravu umožňující zásah do základních práv jednotlivců na soukromí v podobě práva na informační sebeurčení; s ohledem na to, že intenzita zásahu je v posuzovaném případě *„zvýrazněna tím, že se dotýká obrovského a nepředvídatelného počtu účastníků komunikace…, bylo nutné na splnění uvedených požadavků klást co nejpřísnější měřítka“*.

---

[416] Obdobně konkretizoval požadavky na právní úpravu umožňující zásah do práva na soukromý život souhrnně pro zásah veřejné moci v podobě odposlechu telefonních hovorů, tajného dohledu a sběru informací a dat ze soukromé sféry jednotlivce též ESLP, viz Judgment of the European Court of Human Rights, dated 29 June 2006. Case of Gabriele Weber and Cesar Richard Saravia against Germany (Application no. 54934/00). *European Court of Human Rights* [online]. 2006 [cit. 24.2.2024]. či v Judgment of the European Court of Human Rights, dated 1 July 2008. Case of Liberty and others v. The United Kingdom (Application no. 58243/00). *European Court of Human Rights* [online]. 2008 [cit. 24.2.2024] v tomto směru odkázal rovněž na preambuli a čl. 5 Úmluvy o ochraně dat a na zásadu č. 7 Doporučení Výboru ministrů č. R(87)15 ze dne 17.9.1987 týkající se úpravy a využití osobních údajů v policejním sektoru.

Konkrétně Ústavní soud ČR napadené úpravě vytkl zejména vágní a zcela neurčité vymezení orgánů oprávněných údaje požadovat, nevyplývá z ní totiž, o jaké oprávněné orgány se konkrétně jedná. V posuzované právní úpravě také není zcela jasně a přesně vymezen účel, za jakým jsou provozní a lokalizační údaje oprávněným orgánům poskytovány; tento nedostatek pak znemožňuje posouzení úpravy z hlediska její potřebnosti. Na rozdíl od Data Retention Směrnice, která vymezuje jako cíl zajištění údajů pro vyšetřování, odhalování a stíhání závažných trestných činů, napadená právní úprava ani navazující ustanovení Trestního řádu žádné omezení v podobě kritéria závažnosti neobsahuje, přestože srovnatelná úprava podmínek pro nařízení odposlechu a záznamu telekomunikačního provozu v Trestním řádu výslovně tuto podmínku zakotvuje[417]. Dle závěru Ústavního soudu ČR proto posuzovaná úprava nesplňuje nároky vyplývající ze druhého kroku testu proporcionality, tedy potřebnosti výběru prostředků, když v tomto případě zjevně nebyl použit prostředek nejšetrnější k základnímu právu na informační sebeurčení. Ústavní soud ČR v tomto případě své závěry demonstroval konkrétními statistikami dle *„zprávy o bezpečnostní situaci v ČR“* za rok 2008. V ČR bylo v tomto roce zjištěno 343.799 trestných činů, z toho 127.906 jich bylo objasněno, provozní a lokalizační údaje byly ve stejném období vyžádány ve 131 560 žádostech, z čehož Ústavní soud ČR dovodil nadužívání nástroje v podobě vyžádání a použití těchto údajů, v důsledku absence ústavně konformní úpravy.

Další nedostatky posuzované úpravy Ústavní soud ČR shledal v nedostatečných, resp. neexistujících minimálních požadavcích na zabezpečení uchovávaných údajů, v nejednoznačném vymezení doby uchovávání údajů v rozmezí „*ne kratší než 6 měsíců a delší než 12 měsíců*“ a také v neexistenci (byť i následné) informační povinnosti orgánů činných v trestním řízení vůči dotčené osobě a možnosti dotčené osoby domáhat se ochrany proti zneužití. Dozor ÚOOÚ obsažený v ZoEK[418] neovládají sami dotčení jednotlivci, proto Ústavní soud ČR tento nástroj nepovažoval za adekvátní a efektivní prostředek k ochraně jejich základních práv. Zásah do základního práva na soukromí v podobě práva na informační sebeurčení je v tomto případě dle Ústavního soudu ČR mimo jakoukoli kontrolu, zejména soudní.

K samotné podstatě Data Retention, tedy k plošnému uchovávání provozních a lokalizačních údajů, se Ústavní soud ČR v nálezu vyslovil toliko obiter dictum. Vyjádřil

---

[417] V § 88 odst. 1 Trestního řádu je požadavek závažnosti trestného činu obsažen: „*(...) je-li vedeno trestní řízení pro zvlášť závažný trestný čin (...)*“.

[418] Ustanovení § 87 odst. 4 ZoEK ve znění platném a účinném v době diskutovaného rozhodování Ústavního soudu ČR.

pochybnost nad nezbytností a přiměřeností tohoto nástroje, zmínil i možnost jeho nahrazení jinými, více přiměřenými nástroji, jako je data freeze a výslovně vyjádřil též pochyby o efektivitě Data Retention ve vztahu k ochraně před bezpečnostními hrozbami a prevenci zvlášť závažné trestné činnosti[419].

Nálezem sp. zn. Pl. ÚS 24/11 Ústavní soud ČR rozhodl o zrušení ustanovení § 88a Trestního řádu, které navazovalo na úpravu Data Retention v ZoEK a upravovalo podmínky použití uchovávaných údajů pro účely trestního řízení. Obvodní soud pro Prahu 6, který v tomto případě podával návrh k Ústavnímu soudu ČR, konstatoval, že je mu z úřední činnosti známo, že benevolentní procesní postup umožněný napadeným ustanovením „*zapříčiňuje inflaci návrhů na předmětný procesní postup, zejména ze strany Policie České republiky, orgánů celního ředitelství, orgánů Vojenské policie, což znesnadňuje roli soudu jako garanta a ochránce práv osob zaručených ústavním pořádkem v trestním řízení*".

Ústavní soud ČR v tomto případě navázal na závěry předchozího nálezu Pl. ÚS 24/10 a posuzoval, zda napadené ustanovení poskytuje z hlediska základního práva na informační sebeurčení dostatečné garance proti zneužití, především stanovení podmínek přístupu oprávněných orgánů k uchovávaným údajům a existenci účinné kontroly. Ústavní soud ČR přitom shledal, že napadené ustanovení umožňuje orgánům činným v trestním řízení vyžádat a využít uchovávané údaje pouze na základě nějaké souvislosti s probíhajícím trestním řízením, jelikož jediným omezením obsaženým v napadeném ustanovení pro vyžádání údajů je, *že „musí sledovat účel „objasnění skutečností důležitých pro trestní řízení"*. Ústavní soud ČR zdůraznil, že si je vědom povinnosti orgánů veřejné moci aplikovat podústavní právní předpisy v souladu s ústavním pořádkem, jakož i toho, že ochrana základních práv a svobod podléhá v každém jednotlivém případě kontrole ze strany nezávislého a nestranného soudu. Tyto garance sice dle Ústavního soudu ČR „*umožňují poskytnout ochranu před nepřiměřeným zásahem do práva na informační sebeurčení",* ovšem nemohou odstranit nedostatky právní úpravy, která je neurčitá a příliš obecná. Soudy zejména nemohou nahradit *„úvahu zákonodárce o intenzitě určitého veřejného zájmu*", jelikož takovýto postup soudů by neodpovídal čl. 4 odst. 2 Listiny, který umožňuje stanovit meze

[419] Ústavní soud ČR v tomto směru odkázal na analýzu Spolkového úřadu vyšetřování SRN (Bundeskriminalamt) ze dne 26.1.2011, ve které tento úřad na základě porovnání statistických údajů o spáchané závažné trestné činnosti na území SRN za období před a po přijetí právní úpravy Data Retention dospěl k závěru, že „*použití nástroje plošného a preventivního uchovávání provozních a lokalizačních údajů nemělo téměř žádný vliv na snížení počtu spáchaných závažných trestných činů ani na míru jejich objasňování*". Obdobné závěry lze dle Ústavního soudu ČR učinit i „*při zběžném pohledu na statistické přehledy kriminality na území České republiky zveřejňované Policií České republiky*".

základních práv a svobod pouze zákonem; jakožto pro jednotlivce nepředvídatelný by navíc nebyl ani slučitelný s požadavkem právní jistoty. Vyžádání a využití provozních a lokalizačních údajů nemůže být považováno za *„obvyklý nebo rutinní prostředek prevence a odhalování trestné činnosti“,* s ohledem na intenzitu zásahu do základního práva, který tento nástroj představuje. Obvyklost použití tohoto nástroje Ústavní soud ČR i v tomto nálezu dokládá konkrétními statistikami, které dle jeho hodnocení svědčí o využívání, resp. nadužívání údajů i pro vyšetřování běžné, méně závažné trestné činnosti[420].

Také v tomto nálezu Ústavní soud ČR zopakoval své hodnocení srovnatelné míry intenzity zásahu do práva na soukromí u sdělení údajů o uskutečněném telekomunikačním provozu v porovnání s nařízením odposlechu a záznamu telekomunikačního provozu. Ústavní soud ČR taktéž v tomto nálezu zdůraznil potřebu jasných a detailních pravidel zabezpečení uchovávaných údajů a v zájmu účinné ochrany před nezákonným zásahem do základních práv a svobod dotčených osob též požadavek na povinnost dodatečně informovat dotčenou osobu o zásahu a požadavek na navazující právní prostředek k soudnímu přezkumu zásahu. Ústavní soud ČR v tomto nálezu také formuloval potřebu stanovit pravidla pro obsah příkazu ke sdělení údajů, příp. formální náležitostí samotné žádosti orgánů činných v trestním řízení, s cílem zajistit soudci při rozhodování o něm všechny potřebné informace.

Pro absenci požadavku nezbytnosti, jakož i účinných prostředků kontroly napadené ustanovení dle Ústavního soudu ČR neobstojí ve druhém kroku testu proporcionality; neprošlo by ani ve třetím kroku, jelikož ustanovení nepřikládá žádný význam povaze a závažnosti trestného činu, pro které je stíhání vedeno. Ústavní soud uzavírá, že veřejnému zájmu na předcházení a postihování trestných činů nelze v kolizi s právem jednotlivce na informační sebeurčení dát přednost pokaždé, a to ani za splnění podmínky potřebnosti, „*je třeba vždy zvažovat, zda vzhledem k významu objektu určitého trestného činu, jenž měl být spáchán, převáží zájem na jeho stíhání nad právem jednotlivce rozhodovat sám o tom, zda a komu zpřístupní svá osobní data*“.

Ve zjevné snaze předejít negativním konsekvencím, které by v důsledku vydání nálezu mohly následovat v konkrétních případech, Ústavní soud ČR v nálezu upozorňuje, že „*uvedené derogační důvody nelze vykládat tím způsobem, že samotná aplikace napadeného ustanovení měla v případě dotčených uživatelů služeb elektronických komunikací pokaždé za*

[420] Ústavní soud ČR v tomto případě dokládá údaje za rok 2009, podle zprávy vypracované Ministerstvem vnitra ČR *„bylo v tomto roce zjištěno celkem 332 829 trestných činů, přičemž objasněno jich bylo 127 606. Počet žádostí o poskytnutí předmětných údajů však podle…zprávy Evropské komise dosáhl až čísla 280 271, tedy víc než dvojnásobek počtu z předchozího roku.“*

následek porušení jejich základního práva na soukromí“ a nelze tedy „*učinit apriorní závěr, že každým rozhodnutím vydaným na základě § 88a trestního řádu před vyhlášením tohoto nálezu ve Sbírce zákonů došlo k porušení základního práva nebo svobody dotčeného uživatele služeb elektronických komunikací*“. Stejně tak není dle Ústavního soudu ČR dán žádný důvod, který by „*obecně bránil použití doposud získaných údajů o uskutečněném telekomunikačním provozu v rámci dokazování v trestním řízení*“. Ze všech výše uvedených důvodů soud odložil účinnost derogačního výroku na dobu do 30. září 2012[421].

Ústavní soud ČR – nález Pl. ÚS 45/17

Potřetí a zatím naposledy se Ústavní soud ČR povinností Data Retention zabýval v roce 2019, tedy již poté, co SDEU prohlásil Data Retention Směrnici za neplatnou. Skupina 58 poslanců Poslanecké sněmovny Parlamentu ČR podala návrh na zrušení ustanovení, která upravují povinnost Data Retention v ZoEK a v prováděcí vyhlášce k ZoEK, v Trestním řádu a v zákoně o Policii ČR[422]. Ústavní soud ČR tento návrh zamítl[423], když dospěl k závěru, že *„Současná právní úprava data retention je ústavně konformní“*[424]. Ústavní soud ČR svůj závěr v nálezu odůvodnil tak, že napadená právní úprava „*v kontextu dnešního společenského i technologického vývoje*“ naplňuje „*požadavek přiměřenosti zásahu do práva na soukromí ve světle čl. 10 odst. 2 ve spojení s čl. 10 odst. 3 a čl. 13 Listiny a navazující judikatury Ústavního soudu“* a lze ji „*vyložit ústavně konformním způsobem*“. *„Každou žádost a odůvodněnost jejího podání“* je dle jeho hodnocení nutno *„ze strany oprávněného orgánu důkladně zvážit a ze strany soudu pečlivě přezkoumat s ohledem na konkrétní okolnosti posuzovaného případu, a neomezovat se pouze na posouzení splnění formálních náležitostí žádosti“*. Tímto konstatováním obsaženým v části VIII. Nálezu, nadepsané jako Závěr (bod 129.) patrně Ústavní soud ČR zamýšlel zdůraznit možnost ústavně konformního výkladu napadené právní úpravy, dle hodnocení autora se však jedná spíše o jakýsi návod adresovaný oprávněným orgánům a soudům. Jde však přitom jednak o návod velmi obecný a vágní, navíc bez právní závaznosti, především však není zřejmý jeho vztah k posouzení ústavnosti napadené právní úpravy. Autor má za to, že „důkladné zvážení“ či „pečlivé přezkoumání“ by mělo být bez dalšího považováno za standardní postup při aplikaci jakékoli právní úpravy ze strany orgánů

[421] V návaznosti na tuto skutečnost zákonodárce přijal dříve rozebíranou Novelu ZoEK, s účinností od 1. října 2012.
[422] Zákon č. 273/2008 Sb. o Policii ČR, ve znění pozdějších předpisů.
[423] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 45/17 ze 14. května 2019.
[424] Zpráva Ústavního soudu k nálezu Pl. ÚS 45/17. Ústavní soud ČR. TZ 60/2019. 22. května 2019.

veřejné moci, zejména pak právní úpravy zasahující do základních práv a svobod. V případě právní úpravy, která by nesplňovala kritéria proporcionality, však ani zvýšená míra důkladnosti či pečlivosti při jejím používání nezajistí soulad takové právní úpravy s ústavními zákony.

Ústavní soud ČR v odůvodnění tohoto nálezu konstatoval, že *„shromažďování a zadržování provozních a lokalizačních údajů“* v každém případě *„znamená zvlášť závažný zásah do soukromí prakticky všech obyvatel České republiky“* (formulaci „zadržování“ údajů zde Ústavní soud ČR použil ve významu jejich uchovávání). Takto závažné omezení proto dle Ústavního soudu ČR *„jednak musí být prospěšné silnému veřejnému zájmu a zároveň je nutno je v maximální možné míře minimalizovat, aby mezi ním a naplněním sledovaných cílů existovala spravedlivá rovnováha“*. Prostředek k dosažení této rovnováhy a minimalizace zásahu spatřuje Ústavní soud ČR v omezení *„využití dat telekomunikačního provozu jen pro nejnutnější okruhy případů“*, ve stanovení *„přísných podmínek, za kterých jsou data jednak uchovávána, jednak zpřístupňována“* a dále ve vytvoření *„záruk každému jednotlivci, že v případě využití jeho údajů bude mít k dispozici účinné prostředky obrany proti případnému zneužití“*. Dle hodnocení autora je nezbytné, aby tyto požadavky byly naplněny přímo v napadené právní úpravě či v zákonech na tuto úpravu navazujících. Právní úprava ZoEK a související právní úpravy vymezující orgány oprávněné k vyžádání provozních a lokalizačních údajů však tyto požadavky splňují pouze zčásti, jak autor rozebral výše. Poslední požadavek je pak naplněn pouze v případě vyžádání provozních a lokalizačních údajů postupem podle Trestního řádu, nikoli však též v ostatních případech. Ústavní soud ČR také v odůvodnění diskutovaného nálezu neposkytl jasné vodítko, na základě jakých skutečností dospěl k závěru, že posuzované právní úpravy tyto požadavky splňují, když zárukami se nález zabývá pouze ve vztahu k Trestnímu řádu (body 107, 109 a 127) a k zákonu o Policii ČR (body 116 a 128), nikoli však také k ostatním orgánům oprávněným k vyžádání provozních a lokalizačních údajů, přestože výčet těchto orgánů obsahuje právě zde napadené ustanovení § 97 odst. 3 ZoEK.

Ústavní soud ČR dále v odůvodnění diskutovaného nálezu porovnává posuzovanou právní úpravu Data Retention s úpravami v Německu, Slovensku, Rakousku a Polsku, jakožto *„příklady geograficky i historicky nejbližších, tedy sousedních zemí“*. Shledal přitom, že německá úprava aktuálně stanoví dobu uchování pouze 10 týdnů pro provozní údaje a 4 týdny pro údaje lokalizační, navíc jsou vymezeny kategorie údajů, jejichž uchovávání je zakázáno, kromě obsahu komunikace např. údaje o navštívených webových stránkách a službách

elektronické pošty. Vedle toho obsahuje německá úprava též mechanismus „data freeze“, tedy shromažďování pouze údajů konkrétní podezřelé osoby do budoucna. Taktéž na Slovensku je dle zjištění Ústavního soudu ČR platná právní úprava založena na principu data freeze, v Rakousku nová právní úprava nebyla přijata pro nedostatečnou politickou shodu ohledně jejího zaměření. Polsko je jedinou ze sousedních zemí s volnější právní úpravou Data Retention, dle zjištění Ústavního soudu ČR bez zákonem stanoveného časového omezení doby uchovávání údajů a též bez povinného předchozího souhlasu soudu pro vyžádání údajů; tato úprava je v posuzované době na základě návrhu ombudsmana přezkoumávána polským ústavním soudem.

Z analýzy těchto zahraničních právních úprav však Ústavní soud pro své aktuální posouzení nevyvodil žádné relevantní závěry. Ve vztahu k napadené právní úpravě konstatoval, že vývoj *„informačních technologií značně pokročil“* a *„jednotlivci využívají služby elektronických komunikací stále častěji“* a připojil závěr, dle kterého *„údaje o elektronické komunikaci jednotlivce budou v nějaké podobě shromažďovány vždy, i bez právní úpravy data retention“*. Dodal, že provozní i lokalizační údaje *„jsou a budou pro potřeby zajištění realizace těchto služeb, jejich vyúčtování a vyřizování případných reklamací uchovávány i bez zákonné povinnosti (ve více či méně totožném rozsahu, po více či méně totožnou dobu)“,* aniž by toto své tvrzení podložil konkrétními argumenty. Jak autor rozvádí dále, nelze se s tímto hodnocením ztotožnit, zejména ve vztahu k lokalizačním údajům, které jsou pro poskytnutí služby potřebné pouze ve výjimečných případech služeb založených na poloze (tzv. „location-based services“ – LBS), i to pouze po velmi krátkou dobu a platná právní úprava obecně stanoví pro zpracování lokalizačních údajů velmi striktní podmínky. Taktéž ve vztahu k době uchovávání autor považuje závěr Ústavního soudu ČR za mylný a nepodložený, resp. ze samotného závěru uvedeného v odůvodnění nálezu není zřejmé, na čem Ústavní soud svůj závěr založil. Navíc Ústavní soud ČR v této souvislosti dodal, že *„absence legislativně zavedeného principu data retention v konkrétním členském státě neznamená, že by orgány veřejné moci s provozními a lokalizačními údaji nepracovaly, dostávají se k nim pouze jinými cestami – nelze přitom zaručit, že tyto alternativní cesty jsou z hlediska zásahu do práva na soukromí méně invazivní než postup podle právní úpravy využívající princip data retention“,* toto tvrzení o „alternativních cestách“ přitom nijak nekonkretizoval a svůj závěr opřel pouze o blíže nespecifikované výpovědi některých osob vyslechnutých v řízení před Ústavním soudem ČR.

Ze shora uvedených důvodů Ústavní soud ČR v diskutovaném nálezu namísto posouzení napadené právní úpravy – jak v odůvodnění výslovně uvádí – řešil otázku, která z těchto možností představuje „menší zlo“; možnostmi přitom mínil posuzovanou právní úpravu Data Retention a nespecifikované hypotetické „alternativní cesty“. Závěry svého nálezu Ústavní soud ČR označil jako přístup zohledňující požadavky předvídatelnosti, jasnosti a přísnosti právní úpravy a chránící soukromí více, nežli kdyby *„svým zásahem vytvořil prostor k hledání jiných, alternativních a méně transparentních cest, jak se k metadatům elektronické komunikace dostat“*. Dle názoru v odůvodnění nálezu by „*výsledkem zavržení principu data retention … byla naopak ztráta veřejnoprávních mezí a kontroly nad rozsahem uchovávání provozních a lokalizačních údajů, nad způsobem zabezpečení i jejich zpřístupňováním*“.

Autor v této souvislosti považuje za nutné připomenout výše uvedenou stručnou analýzu podstatných prvků právních úprav sousedních států – geograficky i historicky nejbližších, jak je označil Ústavní soud ČR. Promítnutí závěru Ústavního soudu ČR o jakýchsi blíže nespecifikovaných „alternativních cestách“, kterými by orgány veřejné moci v případě neexistence povinnosti Data Retention získávaly provozní a lokalizační údaje, na právní poměry těchto států by totiž naznačoval, že snad v uvedených zemích tamní orgány veřejné moci podobné alternativní cesty pravděpodobně využívají a že tyto státy paradoxně svou aktuální právní úpravou chrání právo na soukromí méně nežli ČR. Uvedené tvrzení navíc implikuje, že by orgány veřejné moci v ČR za účelem získání provozních a lokalizačních údajů v případě neexistence povinnosti Data Retention patrně byly připraveny postupovat ultra vires, když tvrzení Ústavního soudu ČR o „alternativních cestách“, kterými by tyto orgány postupovaly, lze stěží vyložit odlišně, tím spíše, že Ústavní soud ČR dodal blíže nekonkretizované hodnocení těchto „alternativních cest“ jako ve vztahu k právu na ochranu soukromí dost možná invazivnějších nežli postup v rámci povinnosti Data Retention a dokonce tyto „alternativní cesty“ výslovně označil jako „legislativní stín“. K těmto závěrům autor dospívá navzdory tomu, že Ústavní soud ČR v odůvodnění nálezu zahrnul zmínku, ve které – v rozporu s výše uvedeným – konstatuje, že *„je možné, že v případě nedostupnosti provozních a lokalizačních údajů zvolí vyšetřující orgán z hlediska ochrany soukromí invazivnější vyšetřovací metody (vždy nějakou zákonnou cestu k obstarání potřebných údajů najde)“*. Pro „zákonnou cestu“ totiž dle hodnocení autora lze pouze dosti obtížně použít termín „legislativní stín“, především však je nutno zdůraznit, že při získání údajů, byť blíže nespecifikovanou alternativní cestou, by patrně bylo zasaženo pouze právo na ochranu

soukromí dotčené osoby, nikoli plošně a bez výběru všech účastníků a uživatelů veřejně dostupných služeb elektronických komunikací.

V testu proporcionality, který Ústavní soud ČR v diskutovaném nálezu provedl, v prvním kroku zkoumal cíl napadené právní úpravy z hlediska jeho legitimity. Všechny cíle vyjádřené v případě úpravy Data Retention primárně v Trestním řádu a v důvodové zprávě k němu vyhodnotil jako sledující silný veřejný zájem a dospěl k závěru o způsobilosti napadené právní úpravy těchto cílů dosáhnout. S tímto hodnocením se autor ztotožňuje, jak rozvedeno dále, v části věnující se testu proporcionality právní úpravy Data Retention.

Ve druhém kroku testu, při zkoumání existence mírnějších, méně invazivních prostředků, schopných dosáhnout vytýčeného cíle, dospěl Ústavní soud ČR k závěru, že *„využití provozních a lokalizačních údajů skutečný ekvivalent nemá – neexistují prostředky, s nimiž by bylo možné zkoumaný nástroj porovnávat“*. Ústavní soud ČR zde v prvé řadě poměřoval Data Retention s odposlechem telekomunikačního provozu a se sledováním osob a věcí podle Trestního řádu. Dospěl přitom k závěru, že tyto dva instituty spočívají v monitorování podezřelé osoby do budoucna, na rozdíl od uchovávání provozních a lokalizačních údajů v rámci povinnosti Data Retention, které umožňuje získat informace o skutcích již nastalých. Z týchž důvodů dle Ústavního soudu ani mechanismus data freeze, uplatňovaný na Slovensku či v Německu – zde při podstatném omezení povinnosti Data Retention nelze považovat *„za adekvátní a méně invazivní náhradu“*. Napadená právní úprava tak dle hodnocení Ústavního soudu ČR splňuje druhý krok testu proporcionality.

Dle autora není z odůvodnění zřejmé, na základě čeho Ústavní soud ČR tento závěr učinil. Ústavní soud ČR se zde totiž nikterak nevypořádal se skutečností, že zmiňované právní úpravy Německy či Slovenska nejen existují, ale jsou v popsané podobě platné již delší dobu – v případě slovenské právní úpravy od 1. ledna 2016, u německé již od 10. prosince 2015. V době rozhodování Ústavního soudu tedy obě tyto zahraniční právní úpravy byly již déle než 3 roky v praxi používány, není přitom známo, že by jejich aplikace v praxi působila problémy při dosahování jejich cílů, které jsou obdobné těm v právní úpravě ČR, ostatně Ústavní soud ČR v odůvodnění nálezu neuvádí existenci žádných takovýchto překážek. Z tohoto důvodu autor nemůže souhlasit se správností provedení druhého kroku testu proporcionality a tedy ani jeho výsledku. Dle autora bylo v tomto kroku nutno, aby Ústavní soud ČR odůvodnil, z jakých důvodů tyto zahraniční právní úpravy, které přitom výslovně zmiňuje, nepovažuje za adekvátní náhradu povinnosti Data Retention. Takovýmto důvodem by dle autora mohly být například výsledky vyhodnocení dosahování cílů německé či slovenské právní úpravy, a to

výsledky neuspokojivé, zakládající pochybnosti o možnosti těchto zahraničních právních úprav dosáhnout sledovaných cílů – odhalování trestné činnosti a dalších. Takovéto neuspokojivé výsledky by byly důvodem, pro který nelze danou právní úpravu považovat za adekvátní alternativu povinnosti Data Retention. Relevantním argumentem by mohl být např. také poukaz na odlišnou míru trestné činnosti či její objasněnosti v těchto státech či na jiné úpravy vyšetřovacích postupů orgánů činných v trestním řízení apod. Nic z toho zde však Ústavní soud ČR nezkoumal, žádný takový ani jiný relevantní argument odůvodnění nálezu neobsahuje. Navíc, jak uvedeno výše, Ústavní soud SR dospěl při zkoumání tehdejší slovenské právní úpravy v nálezu sp. zn. PL.ÚS 10/2014[425] k opačnému závěru právě ve druhém kroku testu proporcionality a uzavřel, že posuzovaná právní úprava ve druhém kroku neobstojí; tehdejší slovenská právní úprava vykazovala velmi podobné základní prvky jako úprava posuzovaná v rozebíraném nálezu Ústavního soudu ČR.

Ve třetím kroku Ústavní soud ČR v prvé řadě výslovně konstatoval, že rozsah omezení práva na soukromí spočívá v případě Data Retention ve sledování elektronické komunikace *„téměř celé české populace po dobu šesti měsíců „do zásoby““*. Dále pak zkoumal, zda vymezený veřejný zájem je natolik důležitý, aby tento zásah ospravedlnil, zaměřil se proto na dobu uchování, okruh oprávněných orgánů a na dostatečnost prostředků ochrany jednotlivce v případě podezření na zneužití údajů.

U doby uchování provozních a lokalizačních údajů Ústavní soud ČR z výpovědí osob, které v řízení vyslechl, mimo jiné zjistil, že *„oprávněné orgány v případě znalosti identifikačních údajů konkrétního uživatele využívají maximální dobu, kterou jim zákon umožňuje“,* přitom však většina vyžadovaných údajů v praxi *„není starší než tři měsíce“*. Ústavní soud ČR pak v tomto bodě dospěl k závěru, že doba v délce 6 měsíců není *„dobou zjevně nepřiměřenou, což nebylo v řízení z hlediska aplikační praxe ani srovnáním s evropským standardem prokázáno“* a není proto úlohou Ústavního soudu ČR *„suplovat roli zákonodárce a určovat, že by stačila doba kratší a o kolik kratší doba by byla jediná přiměřená.“* Doplňující konstatování Ústavního soudu ČR, dle kterého jde v případě 6-timěsíční doby uchování *„o lhůtu nejkratší z rozmezí, jaké předepisovala (dnes již neplatná) směrnice o data retention, a z evropského standardu nevybočuje“* pak autor považuje za dosti nepřípadné, když odkaz na právní úpravu Data Retention Směrnice, kterou Soudní dvůr EU prohlásil za neplatnou právě pro její neslučitelnost s Listinou EU, se autorovi nejeví jako

[425] Nález Ústavného súdu SR sp. zn. PL.ÚS 10/2014 dne 29. dubna 2015.

relevantní při posuzování souladu napadené právní úpravy s ústavními zákony. Taktéž skutečnost, že délka doby uchování „nevybočuje“ z evropského standardu, autor považuje za nevypovídající o souladu napadené právní úpravy, včetně délky doby uchování, s požadavky na proporcionalitu zásahu, zejména z důvodu absentujícího zohlednění výrazně kratší (a z hlediska míry zásahu tedy výrazně méně invazivní) doby uchování dle právní úpravy Data Retention platné v Německu i zcela odlišného konceptu data freeze v platné právní úpravě Slovenska. V neposlední řadě též autor považuje za nutné v této souvislosti zdůraznit, že „evropský standard“, na který zde Ústavní soud ČR výslovně odkazuje, je tvořen právními úpravami členských států, z nichž mnohé SDEU ve svých rozsudcích reagujících na žádosti o rozhodnutí předběžné otázky shledal jako odporující požadavkům Směrnice o soukromí a elektronických komunikacích, v některých případech ještě před rozhodnutím Ústavního soudu ČR v tomto nálezu.

Při zkoumání orgánů oprávněných k vyžádání provozních a lokalizačních údajů v rámci povinnosti Data Retention a podmínek jejich přístupu k těmto údajům Ústavní soud ČR mj. zjistil, že v případě orgánů činných v trestním řízení a jejich oprávnění vymezeného v Trestním řádu umožňuje § 88a odst. 1 Trestního řádu *„využití těchto údajů pro cca 90 % skutkových podstat trestných činů“.* Toto zjištění dle hodnocení autora naznačuje, že je zde naplněna obava vyslovená ze strany SDEU v rozsudku Tele2 Sverige AB a v diskutovaném nálezu citovaná, totiž že nelze akceptovat stav, kdy z výjimky z ochrany poskytované osobním údajům se stane pravidlo, což je dle SDEU případ *„plošného a nevýběrového uchovávání velkého množství dat“*. Relevance tohoto argumentu je o to závažnější, že SDEU, jak jej cituje Ústavní soud ČR v diskutovaném nálezu *„považuje za legitimní cíl využití provozních a lokalizačních údajů v souvislosti s odhalováním trestné činnosti pouze vyšetřování „závažné trestné činnosti““*. Ústavní soud ČR však v tomto bodě konstatoval, že statistikám objasněnosti trestné činnosti z let 2010–2014, které předložila navrhovatelka, nepřikládá váhu z důvodu následného vývoje kriminality a vyšetřovacích metod a za „neprůkazné“ považuje i statistiky vykazující počet uskutečněných žádostí o výpisy telekomunikačního provozu. Následně v tomuto bodě odůvodnění nálezu Ústavní soud ČR uzavřel, že *„nadužívání provozních a lokalizačních údajů orgány činnými v trestním řízení v řízení před Ústavním soudem nebylo prokázáno“* a široké *„pojetí závažné trestné činnosti obsažené v napadeném ustanovení § 88a odst. 1 trestního řádu“* výslovně shledal přiměřeným.

Autor hodnotí jako dosti překvapivé, že Ústavní soud ČR odmítl objektivní podklady, aniž by přitom své závěry založil na jiných konkrétních zjištěních, což vzbuzuje

pochybnosti o takto učiněných závěrech. Autor na tomto místě poznamenává, že Ústavní soud ČR navíc v tomto bodě odůvodnění nálezu vyšel z informací týkajících se „záznamu telekomunikačního provozu“ [426], což je ovšem zcela odlišný právní institut od institutu Data Retention. Záznam telekomunikačního provozu upravuje trestní řád v § 88 společně s jeho odposlechem, jedná se o záznam obsahu komunikace, primárně hlasového hovoru. Oproti tomu v případě Data Retention upravuje Trestní řád v § 88a „zjištění údajů o telekomunikačním provozu“, terminologicky se zde takto označuje zjištění provozních a lokalizačních údajů. S ohledem na tento aspekt, jakož i na některé výše uvedené vnitřně kontradiktorní pasáže odůvodnění nálezu nelze dle hodnocení autora zcela vyloučit, že na straně Ústavního soudu ČR došlo v posuzovaném případě k některým nedorozuměním způsobeným technickou podstatou posuzované problematiky, která nebyla Ústavnímu soudu ČR v dostatečné míře známa.

Autor v této souvislosti podotýká, že hranice mezi záznamem telekomunikačního provozu a zjištěním údajů o telekomunikačním provozu v praxi v některých případech, s ohledem na vývoj techniky, mohou být méně zřetelné. Jak v této souvislosti upozorňuje Jiří Jelínek v komentáři k Trestnímu řádu, *„Problémem je, že zákonné souslovi „telekomunikační provoz“ již dnes nepostihuje všechny v úvahu přicházející formy elektronických komunikací uskutečňovaných v těchto sítích“* a poukazuje zejména na komunikaci uskutečňovanou prostřednictvím aplikací jak např. Facebook, Skype apod[427].

Taktéž v případě procesních záruk proti zneužití Ústavní soud ČR po provedeném řízení považoval napadenou právní úpravu za přiměřenou. Na základě textace § 88a Trestního řádu Ústavní soud ČR dovodil, že minimalizace zásahu je zde zajištěna podmínkou v tomto ustanovení obsaženou (*„nelze-li sledovaného účelu dosáhnout jinak, nebo bylo-li by jinak jeho dosažení podstatně ztížené“*), jejíž splnění bude v konkrétních případech posuzovat soudní orgán. Jako další nástroj zajišťující efektivitu záruk proti zneužití vyhodnotil Ústavní soud ČR povinnost oprávněného orgánu informovat dotčeného jednotlivce o získání jeho provozních a lokalizačních údajů obsaženou v § 88a odst. 2 Trestního řádu a navazující možnost dotčené osoby podat návrh na přezkoumání zákonnosti příkazu ke zjištění údajů o telekomunikačním provozu upravenou v Trestním řádu[428].

---

[426] Bod 106, v němž Ústavní soud ČR uvádí: *„Z výpovědi JUDr. Bradáčové vyplynulo, že z ročního nápadu trestních věcí se žádosti o záznam telekomunikačního provozu týkají 3 % případů, což nepřímo potvrdil ve své výpovědi také JUDr. Sokol z Unie obhájců.“*

[427] JELÍNEK, J. *Trestní zákoník a trestní řád s poznámkami a judikaturou - 9. aktualizované vydání.* Praha: Leges, 2022.

[428] Viz § 314l a násl. Trestního řádu.

V případech vyžádání údajů dle zákona o Policii ČR[429] sice v tomto zákoně není upravena kontrola nezávislého orgánu nad přístupem Policie ČR k uchovávaným údajům, Ústavní soud ČR však v tomto směru dovodil dostatečné záruky zejména z vázanosti Policie ČR při výkonu její činnosti zákonem o Policii ČR a také z existence interních aktů řízení, zejména několika závazných pokynů policejního prezidenta a též z vnitřní kontrolní činnosti Policie ČR.

U dalších orgánů oprávněných k vyžádání provozních a lokalizačních údajů – BIS, VZ a ČNB – Ústavní soud ČR v odůvodnění uvedl, že jelikož nebyly napadeny zvláštní právní úpravy, nepřísluší mu na tomto místě hodnotit *„přiměřenost úpravy ve vztahu k uvedeným orgánům veřejné moci“* a pouze obecně konstatoval, že pokud je v těchto případech cíl legitimní a současně jsou podmínky nastavené zvláštní právní úpravou pro přístup k provozním a lokalizačním údajům i záruky účinné ochrany jednotlivce dostatečně přísné, pak zařazení dalších orgánů mezi orgány oprávněné není co vytknout. Autor dospěl po analýze příslušných předpisů k závěru, že tyto podmínky nejsou splněny, jak uvádí dále v této práci. Závěr Ústavního soudu ČR je zde však do značné míry založen na skutečnosti uvedené výše, totiž že návrh skupiny poslanců, o kterém Ústavní soud ČR rozhodoval, směřoval proti konkrétním ustanovením ZoEK (zde § 97 odst. 3 a 4), Trestního řádu, zákona o Policii ČR a prováděcí vyhlášky k ZoEK, nikoli též proti dalším třem právním předpisům vymezujícím podmínky vyžádání a využití provozních a lokalizačních údajů ze strany BIS, ČNB a VZ. Přestože tyto tři orgány jsou v § 97 odst. 3 ZoEK výslovně uvedeny jako orgány, jimž je provozovatel sítě nebo poskytovatel služeb povinen na požádání tyto údaje bezodkladně poskytnout, obsahuje text zákona u každého z nich též omezení *„pro účely a při splnění podmínek stanovených zvláštním právním předpisem“;* posouzení splnění podmínek těchto omezení dle hodnocení autora nepřísluší poskytujícím provozovatelům sítí a poskytovatelům služeb. Ústavní soud ČR tedy byl na základě podaného návrhu oprávněn přezkoumat i samotné zařazení těchto tří orgánů mezi osoby oprávněné k vyžádání údajů, nikoli však již právní předpisy, které nebyly návrhem napadeny, jelikož by se jednalo o postup ultra petitum, který obecně není přípustný[430].

[429] Zákon č. 273/2008 Sb. o Policii ČR, ve znění pozdějších předpisů.
[430] V daném případě se nejedná o případ, kdy *„v důsledku zrušení určitého zákonného ustanovení derogačním nálezem Ústavního soudu ustanovení jiné, obsahově od předchozího odvislé, ztrácí rozumný smysl, tj. ztrácí opodstatněnost své normativní existence“* a tedy je *„dán důvod pro zrušení i tohoto zákonného ustanovení.“* Viz nález Ústavního soudu ČR sp. zn. Pl. ÚS 15/01 ze 31. října 2001.

Ústavní soud ČR rozhodoval v plénu, jediným ze soudců, který byl odlišného názoru, byla ústavní soudkyně Kateřina Šimáčková. Po analýze povinnosti Data Retention obsažené v napadených ustanoveních ZoEK a po prozkoumání závěrů Ústavního soudu ČR a jejich odůvodnění, dospěl autor k závěrům, které se v řadě aspektů shodují s odůvodněním odlišného stanoviska soudkyně Kateřiny Šimáčkové, jak rozvede dále. Dle Šimáčkové napadená právní úprava ZoEK i zákona o Policii ČR neobstojí z ústavněprávního hlediska, jelikož *„neskýtá dostatečné záruky proti úniku či zneužití dat, jejichž sbírání stát ukládá“*, v případě zákona o Policii ČR *„zasahuje do soukromí jednotlivců neproporcionálním způsobem“* a navíc je zatížena tím, že jednotlivec nemůže *„sám kontrolovat rozsah shromažďování a využití údajů o své osobě prostřednictvím „data retention“ a případně podrobit neodůvodněné zásahy do svého soukromí kontrole soudní mocí či expertním orgánem“*. Šimáčková upozorňuje na nutnost rozlišit uchovávání provozních a lokalizačních údajů a jejich předávání oprávněným orgánům, kdy *„předávání dat se děje výhradně za účelem zásahu do soukromí jednotlivce (byť sledující legitimní cíl), a představuje tak výrazně vyšší riziko z hlediska zneužití či úniku dat“*. Zásah do základních práv a svobod, který hodnotí jako zásadní, mohou dle jejího hodnocení vyvážit pouze záruky upravené v napadené úpravě výslovně a dostatečně určitě a navíc *„s možností (resp. nezbytností) jejich veřejné kontroly“*.

Autor je v prvé řadě přesvědčen, podobně jako ústavní soudkyně Šimáčková, že existence právní úpravy uchovávání provozních a lokalizačních údajů platné ve Slovenské republice a v Německu, a to existence dlouhodobá a lze tedy říci, že v praxi vyzkoušená, ba osvědčená, prokazuje reálnost alternativních řešení, která jsou v porovnání s napadenou právní úpravou v ČR výrazně méně invazivní vůči základním právům a svobodám, zde primárně vůči právu na ochranu soukromí. Soudkyně Šimáčková tuto skutečnost komentuje shodně s autorovým závěrem, tak, že existence těchto zahraničních právních úprav *„poukazuje na neudržitelnost tvrzení, že současná úprava „data retention“ v České republice nemá alternativu a je jediným vhodným a nezbytným prostředkem k dosažení příslušného legitimního cíle“*. Je to přitom samotný Ústavní soud ČR, který tyto zahraniční právní úpravy výslovně v diskutovaném nálezu zmiňuje. Autor má z tohoto důvodu za to, že Ústavní soud ČR v tomto nálezu test proporcionality neprovedl řádně, když již v jeho druhém kroku by se s existencí těchto úprav musel vypořádat, jak již uvedeno výše. Vzhledem k tomuto nedostatku dle hodnocení autora nemohl Ústavní soud ČR test proporcionality správně vyhodnotit.

Ústavní soud ČR navíc v odůvodnění nálezu shrnuje dosavadní rozsudky SDEU k otázkám Data Retention a v odůvodnění nálezu výslovně zmiňuje některé závěry Rozsudku

SDEU Digital Rights[431], včetně hlavního důvodu prohlášení Směrnice Data Retention za neplatnou: *„Přestože byla směrnice způsobilá dosáhnout sledovaného cíle (harmonizace úpravy data retention na poli boje proti závažné trestné činnosti), ani takový cíl sám o sobě nemohl odůvodnit, aby opatření týkající se všech prostředků elektronické komunikace a spočívající v uchovávání údajů téměř celé evropské populace bylo považováno za nezbytné“*. Ústavní soud ČR také výslovně uvádí požadavek SDEU obsažený v tomto rozsudku na cílenou souvislost *„mezi uchovávanými údaji a ohrožením veřejné bezpečnosti“*, dle kterého se musí jednat o *„údaje vztahující se k určitému časovému období, určité zeměpisné oblasti či okruhu určitých osob, jež mohou být jakýmkoli způsobem zapojeny do závažné trestné činnosti, anebo k osobám, které by prostřednictvím uchovávání jejich údajů mohly z jiných důvodů přispívat k boji proti závažné trestné činnosti“.* Konečně také Ústavní soud ČR v odůvodnění nálezu, v rámci prejudikatury, uvádí i rozsudek SDEU Tele2 Sverige AB a parafrázuje jeho závěr, dle kterého *„nelze akceptovat stav, kdy se z výjimky stane pravidlo, jako je tomu v případě plošného a nevýběrového uchovávání velkého množství dat“*. Přesto však Ústavní soud ČR v případě napadené právní úpravy rozhodl v rozporu se závěry této prejudikatury.

Taktéž mnohá konstatování obsažená v odůvodnění nálezu dokládají dle hodnocení autora snahu Ústavního soudu ČR soustředit se na aspekty aplikace posuzované právní úpravy v praxi, spíše nežli na posouzení souladu napadené úpravy s ústavními zákony (viz např. „*Plošné uchovávání provozních a lokalizačních údajů představuje snahu státu „neztratit v době informační společnosti krok“ a mít v rukou efektivní nástroje k plnění svých úkolů – zde zejména v oblasti bezpečnosti státu a jeho obyvatel. Principiálně proto z pohledu Ústavního soudu nelze data retention zavrhovat.“)*. Zvláště kontrastně v tomto ohledu vyznívá výše zmíněné opačné hodnocení Ústavního soudu SR, který v roce 2015 posuzoval právní úpravu Data Retention obsaženou v tehdejším slovenském zákoně o elektronických komunikáciách[432], založenou na velmi obdobných východiscích jako úprava v ZoEK. Ústavní soud SR, na rozdíl od Ústavního soudu ČR konstatoval, že *„cíle sledovaného napadenou právní úpravou…je možno dosáhnout i jinými prostředky, které představují méně intenzivní zásah do práva na soukromí, nežli je nástroj v podobě plošného a preventivního uchovávání předmětných údajů“*, jako například tzv. data freezing, napadenou právní úpravu na základě

[431] Rozsudek Soudního dvora EU (velkého senátu) z 8. dubna 2014. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner Landesregierung a další. Žádosti o rozhodnutí o předběžné otázce podané High Court (Irsko) a Verfassungsgerichtshof (Rakousko). Spojené věci C-293/12 a C-594/12.

[432] Zákon č. 351/2011 Z.z. o elektronických komunikáciách, v znení neskorších predpisov. Tento zákon byl následně nahrazen zákonem č. 452/2021 Z. z. o elektronických komunikáciách, v znení neskorších predpisov.

výsledků svého posouzení zrušil[433]. Dle hodnocení autora lze navíc pochybovat, zda závěry diskutovaného nálezu Ústavního soudu ČR mohou obstát ve světle relevantních rozsudků SDEU, zejména dále diskutovaných rozsudků ve věci C 623/17 a ve spojených věcech C-511/18, C-512/18 a C-520/18[434]. Kromě některých výše uvedených ne zcela přesvědčivě argumentačně podložených závěrů obsahuje odůvodnění nálezu též nepřesné zjednodušení věcné stránky problému ve shrnutí, a to dosti zásadního charakteru. Ústavní soud ČR v něm svůj závěr odůvodňuje mimo jiné tím, že by bylo *„nemoudré tolerovat stav, v němž by poskytovatelé služeb údaji uživatelů disponovali, a státní aparát (v odůvodněných případech) nikoli“*. Takováto situace však není nevyhnutelnou alternativou povinnosti Data Retention, jak uvádí Kateřina Šimáčková ve svém separátním votu na příkladu „zmrazovacího příkazu“ ve vztahu k datům, která provozovatelé sítí a poskytovatelé služeb v dané chvíli ke konkrétní osobě zpracovávají.

3.1.3 Posouzení splnění ústavněprávních požadavků

Na rozdíl od Ústavního soudu ČR, který v nálezu Pl. ÚS 45/17 dospěl k závěru, že *„plošný a neadresný sběr provozních a lokalizačních údajů o uskutečněné komunikaci“* není *„ve vztahu k ochraně soukromí a priori nepřiměřený“*, autor má o tomto závěru pochybnosti, především z důvodů podrobně rozebraných v relevantní judikatuře SDEU zmiňované v této práci výše[435]. Taktéž již dříve citovaný Jan Kudrna se k otázce proporcionality v případě Data Retention Směrnice, tedy k otázce plošného shromažďování provozních a lokalizačních údajů vyjádřil jednoznačně[436] tak, že tuto směrnici označil za jeden z případů *„výměny svobody za bezpečnost“*. Dle jeho hodnocení totiž *„směrnice dopadá na přibližně 500 miliónů obyvatel Evropské unie, z nichž drtivá většina nebyla a není bezpečnostním rizikem“*, a z tohoto důvodu upozorňuje, že takováto argumentace *„je pro lidská práva velmi nebezpečná“*. Data Retention Směrnice totiž dle jeho hodnocení *„vytváří prostor pro další nepřiměřené zásahy do lidských práv a svobod, aniž by tyto vedly k podstatnému omezení, nebo dokonce eliminaci bezpečnostních hrozeb“*. Kudrna již ve způsobu projednání návrhu novely ZoEK v roce

[433] Nález Ústavného súdu SR sp. zn. PL.ÚS 10/2014 dne 29. dubna 2015.
[434] Společně vyhlášené rozsudky Soudního dvora EU (velkého senátu) ze 6. října 2020 ve věci C-623/17 Privacy International a ve spojených věcech C-511/18 La Quadrature du Net a další, C-512/18 French Data Network a další a C-520/18 Ordre des barreaux francophones et germanophone a další.
[435] V tomto směru viz zejména výše zmiňované rozsudky Soudního dvora EU ve věci C 623/17 a ve spojených věcech C-511/18, C-512/18 a C-520/18.
[436] KUDRNA, Jan. 27. Pravděpodobně nejvíce porušované ustanovení Listiny (a jedna ze současných hrozeb lidským právům) in GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012 s. 277 a násl.

2008[437] spatřuje *„porušení ustanovení čl. 4 odst. 4 Listiny základních práv a svobod“*, při kterém *„podstata a smysl práva na soukromí nebyla chráněna, ale naopak byl zvolen způsob, jak se řešení tohoto problému vyhnout“*[438]. Ústavní soud ČR však dospěl k odlišnému závěru a SDEU dosud neposuzoval přímo úpravu Data Retention v právním řádu ČR, autor tak považuje za nutné zabývat se na tomto místě posouzením jejích ústavněprávních aspektů podrobně.

Test proporcionality ve vztahu k povinnosti Data Retention v právním řádu ČR provedl Ústavní soud ČR ve svých výše uvedených nálezech. Předchozí dva nálezy Ústavního soudu ČR se však týkaly verzí právní úpravy ZoEK a také Trestního řádu, které byly v mezidobí, právě v reakci na tyto nálezy, nahrazeny. Není tak relevantní se jimi zde zabývat, stejně jako posuzovat, zda byla proporcionalita zásahu vyhodnocena při přijímání ZoEK a následné Novely ZoEK. V zatím posledním nálezu Pl. ÚS 45/17 Ústavní soud ČR v roce 2019 analyzoval právní úpravu ZoEK a zákona o Policii ČR ve verzích, které v podstatných rysech odpovídají aktuálně platným a účinným verzím. Jelikož však nebyly napadeny také další právní předpisy (zákon o BIS, zákon o VZ, zákon o dohledu v oblasti kapitálového trhu), Ústavní soud ČR se jimi v tomto nálezu nezabýval. Autor má navíc výhrady k testu proporcionality provedenému v tomto nálezu ve vztahu k právní úpravě ZoEK a obecně k povinnosti Data Retention, jak již uvedeno výše.

Samotný zásah do práva na ochranu soukromí v podobě povinného plošného shromažďování osobních údajů značného množství osob je zákonem předvídaný, právní úprava ZoEK v aktuálně platném znění, na rozdíl od minulosti, v dostatečné míře splňuje kritéria přesnosti a zřetelnosti formulací a lze ji tak označit i za dostatečně předvídatelnou. Povinnost Data Retention je vymezena v aktuálně platné a účinné právní úpravě primárně v ZoEK, na něj pak navazují jednotlivé zvláštní právní předpisy, které vymezují jednotlivé oprávněné orgány a účely využití údajů. ZoEK účel využití provozních a lokalizačních údajů výslovně vymezuje pouze u Policie ČR, u ostatních oprávněných orgánů odkazuje na zvláštní právní předpisy. Zkoumání legitimnosti cíle sledovaného zákonnou úpravou a způsobilosti vytýčeného cíle dosáhnout v prvním kroku testu proporcionality je tak nutno podrobit všechny tyto právní předpisy a posoudit povinné uchovávání údajů shromažďovaných v rámci

[437] Jedná se o novelu ZoEK provedenou zákonem č. 247/2008 Sb.
[438] KUDRNA, Jan. 27. Pravděpodobně nejvíce porušované ustanovení Listiny (a jedna ze současných hrozeb lidským právům) in GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012 s. 280.

povinnosti Data Retention ve spojitosti s jejich následným vyžádáním a využitím, a to ve vztahu k jednotlivým účelům jejich použití, které se pro jednotlivé oprávněné orgány liší.

Účelu vyjádřenému opakovaně v judikatuře SDEU a také Ústavního soudu ČR[439] jako trestní řízení vedená pro zvlášť závažné trestné činy odpovídá pouze účel vymezený v Trestním řádu u orgánů činných v trestním řízení, i to jen zčásti co do kritéria závažnosti, které zde není naplněno s ohledem na široké vymezení okruhu trestných činů. Autor připomíná zjištění obsažené ve výše rozebíraném nálezu Ústavního soudu ČR Pl. ÚS 45/17, dle kterého § 88a odst. 1 Trestního řádu umožňuje využití údajů dle tohoto ustanovení *„pro cca 90 % skutkových podstat trestných činů“.* Oprávnění Policie ČR sleduje odlišnou skupinu veřejných zájmů, nicméně stále jde o zájmy, které lze považovat za natolik závažné, že mohou odůvodnit zásah do práva na ochranu soukromí, jde o účely: 1. zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, 2. zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, 3. předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu a 4. prověřování chráněné osoby[440]. Takto vymezené účely lze dle hodnocení autora považovat za ústavně aprobovaný veřejný zájem. U zpravodajských služeb – BIS a VZ by na základě dikce ZoEK měl být účel specifikován ve zvláštních právních předpisech, v zákoně o Bezpečnostní informační službě a zákoně o Vojenském zpravodajství. Ani v jednom z těchto předpisů tomu tak ovšem není, oba obsahují pouze velmi vágně formulované upřesnění oprávnění požadovat provozní a lokalizační údaje *„v rozsahu potřebném pro plnění konkrétního úkolu“*[441]. Působnost BIS i VZ je vymezena v zákoně o zpravodajských službách České republiky[442], nikoli však účel vyžádání provozních a lokalizačních údajů. Autor má proto pochybnost o ústavnosti takového řešení.

V případě ČNB je účel vymezen v zákoně o dohledu v oblasti kapitálového trhu[443] jako „výkon dohledu nad kapitálovým trhem“[444]. Samotný termín dohled nad kapitálovým trhem tento zákon nevymezuje, z jeho dalších ustanovení lze však dovodit, že ČNB při výkonu tohoto dohledu *„přispívá k ochraně investorů a rozvoji kapitálového trhu a podporuje osvětu*

---

[439] Ústavní soud ČR v nálezu Pl. ÚS 45/17 citoval svůj předchozí nález Pl. ÚS 24/10, dle kterého je nezbytné, aby zákonodárce *„omezil možnost použití uchovávaných údajů jen pro účely trestních řízení vedených pro zvlášť závažné trestné činy“*, odkázal zde i na rozsudek SDEU Digital Rights Ireland.
[440] Tyto účely jsou vyjádřeny v § 97 odst. 3 písm. b) ZoEK.
[441] Totožnou formulaci obsahuje § 8a zákona č. 154/1994 Sb. o Bezpečnostní informační službě, ve znění pozdějších předpisů i § 9 zákona č. 289/2005 Sb. o Vojenském zpravodajství.
[442] Zákon č. 153/1994 Sb. o zpravodajských službách České republiky, ve znění pozdějších předpisů.
[443] Zákon č. 15/1998 Sb. o dohledu v oblasti kapitálového trhu a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů.
[444] Viz § 8 odst. 1 písm. d) zákona o dohledu v oblasti kapitálového trhu, ve znění pozdějších předpisů.

v této oblasti“ a tím *„posiluje důvěru investorů a emitentů investičních nástrojů v kapitálový trh“*[445]. Předmětem dohledu je plnění povinností stanovených právními předpisy a vykonatelnými rozhodnutími ČNB, při jeho výkonu je ČNB oprávněna ukládat opatření a správní tresty zákonem stanovené, porušení některých z těchto povinností vymezuje tento zákon jako přestupky[446]. Provozní a lokalizační údaje je ČNB oprávněna využít pro „*odhalení přestupku na úseku podnikání nebo obchodování na kapitálovém trhu“*, což ostře kontrastuje s již výše zmíněnými požadavky relevantní judikatury na omezení i u trestních řízení pouze na ta vedená pro zvlášť závažné trestné činy, tedy nikoli pro odhalování přestupků.

Po vyhodnocení právní úpravy zákona o dohledu v oblasti kapitálového trhu dospěl autor k závěru, že účely, které jsou v tomto zákoně vymezeny, lze považovat za veřejný zájem. Jeho závažnost je však výrazně nižší nežli u účelů, pro které jsou provozní a lokalizační údaje oprávněny využít orgány činné v trestním řízení, Policie ČR a zpravodajské služby, jak dokládá i skutečnost, že porušení některých povinností, na jejichž plnění ČNB takto dohlíží, je kvalifikováno jako přestupek. Dle hodnocení autora lze uzavřít, že takto vymezené účely nenaplňují kritérium závažnosti veřejného zájmu, které je vyžadováno pro odůvodnění zásahu do základních lidských práv a svobod, jak vyplývá z rozhodovací praxe SDEU. Ta jednoznačně vyžaduje, aby se jednalo o závažnou trestnou činností nebo závažné ohrožení veřejné bezpečnosti[447].

Pro posouzení nezbytnosti a efektivity tohoto oprávnění ČNB ve vztahu ke sledovanému cíli autor vznesl k ČNB postupně 2 dotazy ohledně počtu údajů takto vyžádaných v jednotlivých letech. V první odpovědi ČNB autorovi potvrdila, že v období od 1. dubna 2006[448] do 15. května 2017 nežádala dle uvedeného ustanovení o poskytnutí provozních a lokalizačních údajů ani v jednom případě. ČNB současně ve své reakci dodala, že *„Česká národní banka nevede centrální evidenci žádostí, kdy požádala o provozní a lokalizační údaje“*[449]. Ve druhé odpovědi[450] ČNB potvrdila, že v období od 1. ledna 2017–25. dubna 2024[451] si vyžádala provozní a lokalizační údaje celkem ve 4 případech. Ze skutečnosti, že ČNB svého oprávnění v období prvních více než 10 let nevyužila ani v jednom případě a

[445] Viz § 2 zákona o dohledu v oblasti kapitálového trhu, ve znění pozdějších předpisů.
[446] Viz § 7, 7a a 9b zákona o dohledu v oblasti kapitálového trhu, ve znění pozdějších předpisů.
[447] Viz např. Rozsudek SDEU Tele2 Sverige AB.
[448] Tohoto dne nabyl účinnosti zákon č. 57/2006 Sb. o změně zákonů v souvislosti se sjednocením dohledu nad finančním trhem, který založil oprávnění ČNB žádat poskytnutí provozních a lokalizačních údajů od osob zajišťujících veřejnou komunikační síť nebo poskytujících veřejně dostupnou službu elektronických komunikací.
[449] Příloha č. 1 této práce.
[450] Příloha č. 2 této práce.
[451] Datum podání žádosti autora k ČNB.

v období následujících 7 let jej využila celkem ve 4 případech, lze usuzovat na význam této potřeby ČNB pro její činnosti dle zákona o dohledu v oblasti kapitálového trhu. Počet těchto případů dle autorova hodnocení dokládá, že toto opatření se nejeví být pro činnost ČNB při výkonu dohledu nad kapitálovým trhem nezbytným.

Připustíme-li, že oprávnění obsažené v § 58 ZoZOÚ zahrnuje též právo ÚOOÚ vyžádat si provozní a lokalizační údaje elektronických komunikací, pak v tomto případě vymezení účelu zcela absentuje. ZoZOÚ stanoví pouze velmi vágní omezení obecně pro všechny informace vyžadované na základě tohoto ustanovení, dle kterého se musí jednat o *„informace nezbytné pro plnění konkrétního úkolu“*. S poukazem na argumentaci uvedenou výše v případě ČNB tak dle hodnocení autora lze v případě ÚOOÚ dospět k obdobnému závěru, s tím, že zde navíc není účel vyjádřen a nelze tak posoudit, o jak závažný veřejný zájem se jedná. Taktéž v případě ÚOOÚ autor pro posouzení nezbytnosti a efektivity tohoto oprávnění ve vztahu ke sledovanému cíli vznesl k ÚOOÚ dotaz ohledně počtu údajů takto případně ze strany ÚOOÚ vyžádaných v jednotlivých letech. Dle odpovědi ÚOOÚ[452] takto vyžádal provozní a lokalizační údaje celkem ve 3 případech, a to v jednom případě pouze provozní a ve dvou případech provozní i lokalizační údaje elektronických komunikací. Z odpovědi ÚOOÚ není zřejmé, zda ÚOOÚ vyžádané údaje též obdržel, z její formulace však lze usuzovat, že ano. ÚOOÚ v odpovědi na autorovu žádost také doplnil, že o údaje v uvedených případech nežádal na základě § 58 ZoZOÚ, nýbrž dle čl. 58 odst. 1 písm. a), příp. d) GDPR. Jak autor uvádí výše, výklad čl. 58, který by obecně formulovanou pravomocí dozorového úřadu umožňoval prolomit zákonem specificky formulovanou ochranu informací, zde ochranu důvěrnosti komunikací, vč. provozních a lokalizačních údajů elektronických komunikací, autor považuje za nesprávný. Přesto však odpověď ÚOOÚ svědčí o tom, že v praxi v podobným případům, byť toliko ve velmi omezených počtech, dochází. Tato skutečnost nic nemění na výše uvedeném konstatování autora, že v případě ÚOOÚ není účel případného vyžádání a využití těchto údajů vyjádřen, což platí jak pro ZoZOÚ, tak i GDPR. Z vymezení ÚOOÚ jakožto ústředního správního úřadu pro oblast ochrany osobních údajů[453] ani z činností ÚOOÚ obsažených v ZoZOÚ a GDPR dle autorova hodnocení nelze dovodit žádný veřejný zájem, který by svou závažností odpovídal požadavkům vyplývajícím z rozhodovací praxe SDEU pro odůvodnění zásahu do práva na ochranu soukromí, jakožto jednoho ze základních lidských práv a svobod.

[452] Příloha č. 3 této práce.
[453] § 50 odst. 1 ZoZOÚ.

Obecně ve vztahu k výše uvedeným oprávněným orgánům platí, že všechny uvedené cíle sledují veřejný zájem a lze je považovat za legitimní, s výhradou v relevantní právní úpravě nevyjádřeného cíle v případě BIS a VZ a též s výhradou nedostatečné intenzity veřejného zájmu v případě využití údajů ze strany ČNB a ÚOOÚ, když v případě ÚOOÚ navíc účel není explicitně vyjádřen a není možno dovodit jej ani implicitně. V případě ČNB navíc autor nenalezl potřebu vyžadovat i lokalizační údaje, když, na rozdíl od provozních údajů, není podloženo v právu EU[454]. Využití těchto údajů může dle hodnocení autora oprávněným orgánům napomoci k naplnění účelů (v těch případech, kdy jsou zákonem vyjádřeny). Ne u všech zvláštních právních předpisů navazujících na ZoEK však jsou *„striktně definovány i pravomoci udělené příslušným orgánům, způsob a pravidla jejich provádění“*, jak požadoval Ústavní soud ČR v nálezu Pl. ÚS 24/10.

V případech legislativních návrhů ve prospěch Státní hygienické služby a ÚOHS byl účel těchto orgánů k vyžádání provozních a lokalizačních údajů zatím vždy vymezen tak, že nedosahoval intenzity závažného veřejného zájmu srovnatelného s vyšetřováním, odhalováním a stíháním trestných činů, a to pouze závažných, tyto účely nelze označit ani za závažné ohrožení veřejné bezpečnosti. Autorovi je známo, že aktuální slovenská úprava, která je založena na principu data freeze, zahrnuje mezi orgány oprávněné k získání údajů také Úrad verejného zdravotníctva Slovenskej republiky, to však pouze po dobu mimořádné situace nebo nouzového stavu[455], takovou limitaci však legislativní návrh v případě Státní hygienické služby neobsahoval.

Ve druhém kroku testu proporcionality, při zkoumání potřebnosti, resp. nezbytnosti zásahu do práva na ochranu soukromí ve vztahu ke sledovaným cílům je nutno porovnat vymezené právní úpravy s možnými jinými opatřeními, která by umožňovala dosažení týchž cílů, avšak při menší intenzitě zásahu do práva na ochranu soukromí. Dle autora zde nelze opomenout již výše vymezené právní úpravy platné a účinné ve Slovenské republice a také v Německu. Tyto právní úpravy jsou v praxi aplikovány již delší dobu, a to za podmínek, které lze z hlediska míry trestné činnosti a vyšetřovacích postupů orgánů činných v trestním řízení považovat za srovnatelné s podmínkami v ČR, když z dostupných informací, včetně důkazů provedených Ústavním soudem ČR v řízení zakončeném vydáním nálezu Pl. ÚS 45/17 nevyplývá, že by se podmínky v těchto zemích výrazněji odlišovaly. Obdobný závěr lze dle

[454] Nařízení Evropského parlamentu a Rady (EU) č. 596/2014.
[455] § 117 odst. 5 ve spojení s § 109 odst. 9 zákona č. 452/2021 Z.z. o elektronických komunikáciách, v znení neskorších predpisov.

autora učinit též ve vztahu k účelům sledovaným u dalších oprávněných orgánů. Z těchto skutečností tak nelze než učinit závěr, dle kterého existují alternativní postupy v podobě data freeze, případně v kombinaci se zaznamenáváním provozních a lokalizačních údajů u konkrétních osob do budoucna a také v podobě výrazně kratších dob uchovávání těchto údajů. Na rozdíl od Ústavního soudu ČR autor považuje výrazný rozdíl mezi délkou uchování údajů (jednotky týdnů oproti jednotkám měsíců) za ústavněprávně relevantní při posuzování intenzity zásahu do zkoumaného práva na ochranu soukromí. Právní úprava Data Retention ve své aktuální podobě, tedy založená na plošném uchovávání provozních a lokalizačních údajů všech účastníků a uživatelů elektronických komunikací po dobu 6 měsíců tak dle hodnocení autora nesplňuje požadavky druhého kroku testu proporcionality na potřebnost a nezbytnost.

Navzdory odlišnému názoru vyjádřenému Ústavním soudem ČR v nálezu Pl. ÚS 45/17 autor ve vztahu k nezbytnosti povinnosti Data Retention považuje za relevantní mimo jiné analýzu nevládní neziskové organizace Iuridicum Remedium, z.s.[456] zabývající se dlouhodobě právem na ochranu soukromí. Analýza na základě údajů zveřejněných Policií České republiky porovnává počet vyžádaných údajů v letech 2009–2011 se statistikami o trestné činnosti v daných letech a dochází k závěru, že míra trestné činnosti ani míra její objasněnosti nepoklesla v době od 12. dubna 2011, tedy poté kdy nález Ústavního soudu ČR zrušil právní úpravu Data Retention v ČR, a orgány činné v trestním řízení tak po relativně dlouhou dobu, až do 1. října 2012, neměly k provozním a lokalizačním údajům vůbec přístup. Podle autorovi dostupných informací odborníci z řad Policie ČR závěry zprávy kritizovali, oficiální vyjádření Policie ČR ke zprávě však autor nezaznamenal. Obdobně relevantním dokumentem je dle názoru autora studie Institutu Maxe Plancka[457] rozebíraná mj. v již zmiňovaném Nálezu Ústavního soudu SR sp. zn. PL.ÚS 10/2014.

S ohledem na tyto závěry tak již není relevantní posuzovat splnění kritérií ve třetím kroku testu proporcionality. Autor však považuje za vhodné stručně zhodnotit existenci záruk proti zneužití, ty obecně spočívají kromě již zmiňovaných požadavků na právní úpravu i v existenci účinných kontrolních mechanismů jejich dodržování. V případě Data Retention taková kontrola existuje pouze v Trestním řádu, v podobě následné informační povinnosti po

[456] VOBOŘIL, Jan. *Data Retention v (nejen) policejní praxi. Analýza postupů Policie ČR a dalších orgánů při vyžadování a využívání provozních a lokalizačních údajů o elektronických komunikacích v České republice.* Iuridicum Remedium, o.s. 25. září 2012. [online]. 2012. [cit. 24.2.2024].
[457] Max-Planck-Institut für ausländisches und internationales Strafrecht. Kriminologická studie „*Stutzlücken durch Wegfall der Vorratsdatenspeicherung?*“ [online] [cit. 15.1.2024]. Dostupné z www.grundrechte.ch.

pravomocném skončení věci a navazující možnosti podat návrh na přezkoumání zákonnosti příkazu k zjištění údajů o telekomunikačním provozu[458]. Ústavní soud ČR v nálezu Pl. ÚS 45/17 posuzoval existenci takových záruk také v zákoně o Policii ČR a konstatoval, že zde sice zákon nestanoví kontrolu nezávislého orgánu, kterou vyžaduje jak Ústavní soud ČR, ale také SDEU i ESLP, shledal však dostatečné záruky jednotlivce před zneužitím pravomoci ve vnitřní kontrolní činnosti Policie ČR a v sankcích plynoucích případnému pachateli protiprávního jednání. Autor takovéto záruky za dostatečné nepovažuje, jelikož z ustálené judikatury zejména SDEU i ESLP vyplývá jednoznačně požadavek na existenci nezávislého kontrolního orgánu a na možnost dotčené osoby obrátit se na něj a kontrolu iniciovat[459]. Takový postup zde platná právní úprava nestanoví, ačkoli mu nebrání žádná právní ani faktická překážka. V případě využití údajů ze strany BIS a VZ a také ČNB Ústavní soud ČR existenci kontrolních mechanismů v tomto nálezu neposuzoval, po analýze relevantních právních předpisů[460] lze však konstatovat, že kontrolní mechanismy v podobě srovnatelné s úpravou Trestního řádu v nich nejsou upraveny. V případě BIS a VZ může být taková neexistence dle hodnocení autora odůvodnitelná charakterem činnosti těchto zpravodajských služeb a rizikem, které by případná, byť i následná, informace mohla přinést pro veřejný zájem sledovaný činností těchto orgánů. Tento argument se však neuplatní u ČNB, kde taktéž obdobný kontrolní mechanismus v právní úpravě zcela absentuje, a pokud budeme považovat za oprávněný orgán i ÚOOÚ, pak ve vztahu k němu platí totéž. Taktéž legislativní návrhy ve vztahu ke Státní hygienické službě a ÚOHS coby oprávněným orgánům obdobný kontrolní mechanismus neobsahovaly.

3.2 Plošné zpracování osobních údajů systémy v automobilech

3.2.1 Vývoj a základní vymezení, relevantní právní úprava

Automobily jsou v současnosti vybavovány mnoha snímači a zařízeními shromažďujícími řadu údajů o vozidle, o průběhu jízdy i dalších. V posledních několika letech však byly přijaty právní úpravy, na jejichž základě jsou ke splnění různých účelů nově

[458] Povinnost je upravena v § 88a odst. 2 Trestního řádu.
[459] Takto formuloval požadavky na efektivní záruky SDEU např. v rozsudku Tele2 Sverige AB, v němž zajištění dohledu nezávislého orgánu nad dodržováním úrovně ochrany označil za jeden z nezbytných prvkem vnitrostátní úpravy, výslovně vyžadovaných článkem 8 odst. 1 a 3 Listiny EU.
[460] Zákon č. 154/1994 Sb. o Bezpečnostní informační službě, ve znění pozdějších předpisů, zákona č. 289/2005 Sb. o Vojenském zpravodajství, ve znění pozdějších předpisů, zákon č. 153/1994 Sb. o zpravodajských službách České republiky, ve znění pozdějších předpisů, zákon č. 15/1998 Sb. o dohledu v oblasti kapitálového trhu a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů.

vyráběné a do provozu uváděné automobily, především osobní a též lehké užitkové, povinně vybavovány zařízeními zaznamenávajícími některé kategorie údajů generovaných při provozu automobilů. Deaktivace těchto zařízení je v praxi velmi obtížná, případně není vůbec možná bez zásahů do systémů vozidla s negativním dopadem na technickou způsobilost vozidla k dalšímu provozu. Zařízení označované jako OBFCM (z anglického On-board Fuel and/or Energy Consumption Monitoring Device), tedy palubní zařízení pro sledování spotřeby paliva a/nebo energie, od roku 2021 zaznamenává pro účely pravidelných hlášení Evropské agentuře pro životní prostředí údaje o počtu najetých kilometrů a spotřebě každého individuálního automobilu.

Všeobecně známějším a šířeji komunikovaným je systém automatického tísňového volání eCall, jehož deklarovaným cílem je zajistit vysokou úroveň bezpečnosti silničního provozu. Taktéž tento systém je založen na povinném vybavení všech nových osobních a lehkých užitkových motorových vozidel od 31. března 2018 zařízením eCall, které automaticky aktivací palubních senzorů, případně manuálně iniciuje hlasové volání na jednotné evropské tísňové číslo 112; společně s voláním je prostřednictvím veřejných mobilních komunikačních sítí zajištěn automatický přenos standardizovaného minimálního souboru dat do centra tísňové komunikace. Autor tyto dva povinně zaváděné systémy považuje za potenciální zásah do práva na ochranu soukromí, proto je v této kapitole bude podrobněji zkoumat.

Právní úprava OBFCM

Systém zařízení OBFCM byl zaveden Prováděcím nařízením Komise (EU) 2021/392[461], které přijala Evropská komise na základě Nařízení Evropského parlamentu a Rady (EU) 2019/631[462]. Prováděcí nařízení, jak vyplývá z jeho celého názvu, zrušilo celkem čtyři dosavadní prováděcí nařízení, ta však byla založena na zpracování údajů na úrovni výrobce u každé série vozidel definované podle typu, varianty a verze[463], nikoli na zpracování

[461] Prováděcí nařízení Komise (EU) 2021/392 ze dne 4. března 2021 o sledování a hlášení údajů týkajících se emisí CO2 z osobních automobilů a lehkých užitkových vozidel podle nařízení Evropského parlamentu a Rady (EU) 2019/631 a o zrušení prováděcích nařízení Komise (EU) č. 1014/2010, (EU) č. 293/2012, (EU) 2017/1152 a (EU) 2017/1153.

[462] Nařízení Evropského parlamentu a Rady (EU) 2019/631 ze dne 17. dubna 2019, kterým se stanoví výkonnostní normy pro emise CO2 pro nové osobní automobily a pro nová lehká užitková vozidla a kterým se zrušují nařízení (ES) č. 443/2009 a (EU) č. 510/2011.

[463] Viz čl. 1 bod 3 Nařízení Komise (EU) č. 1014/2010 ze dne 10. listopadu 2010 o sledování a hlášení údajů o registraci nových osobních automobilů podle nařízení Evropského parlamentu a Rady (ES) č. 443/2009, který vymezoval „podrobné údaje ze sledování“ odkazem na tabulku obsaženou v příloze Nařízení Evropského parlamentu a Rady (ES) č. 443/2009 ze dne 23. dubna 2009, kterým se stanoví výkonnostní emisní normy pro nové osobní automobily v rámci integrovaného přístupu Společenství ke snižování emisí CO2 z lehkých

údajů jednotlivých konkrétních automobilů. Samotné nařízení (EU) 2019/631 předpokládá, že Evropská komise přijme prováděcí pravidla postupů sledování a hlášení údajů prostřednictvím prováděcích aktů, a to včetně sledování a ověřování emisí CO2 a spotřeby paliva nebo energie v reálném provozu[464]. Dle prováděcího nařízení Komise (EU) 2021/392 výrobci *„shromažďují údaje z reálného provozu spolu s čísly VIN nových osobních automobilů a nových lehkých užitkových vozidel“* registrovaných od 1. ledna 2021 a vybavených *„palubními zařízeními pro monitorování spotřeby paliva a/nebo energie“*, *„pokud majitel vozidla výslovně neodmítne tyto údaje výrobci, jeho autorizovanému prodejci nebo autorizované opravně poskytnout“*[465].

Jak vyplývá mj. z Rozsudku SDEU ve věci C-319/22[466], VIN představuje osobní údaj pro osoby, které mohou mít *„rozumně k dispozici prostředky, které jim umožní spojit VIN s identifikovanou nebo identifikovatelnou fyzickou osobou“*. Účel zpracování čísel VIN a údajů z reálného provozu shromažďovaných systémem OBFCM vymezuje Prováděcí nařízení Komise (EU) 2021/392 odkazem na nařízení (EU) 2019/631, tedy jako sledování a posuzování reprezentativnosti hodnot emisí CO2 a spotřeby paliva nebo energie, tyto údaje se *„nepoužijí k žádnému jinému účelu“*[467]. VIN lze ve výše uvedeném případě považovat ve vztahu k některým osobám zapojeným do zpracování údajů v systému OBFCM, jakými jsou autorizovaní prodejci či opravny, za osobní údaj. S ohledem na to, jakož i na skutečnost, že tyto údaje, společně s dalšími kategoriemi údajů jsou získávány a shromažďovány od všech vozidel, s výjimkou těch, u kterých majitel vozidla toto shromažďování výslovně odmítne, je dle hodnocení autora nutno toto zpracování považovat za plošné zpracování osobních údajů.

Dle Prováděcího nařízení Komise (EU) 2021/392 mají výrobci vozidel, autorizovaní prodejci, autorizované opravny a osoby či zařízení odpovědná za technické prohlídky, příp. členské státy v případě získání údajů nepřímo, zajistit splnění informační povinnosti vůči subjektům údajů – majitelům vozidel v souladu s GDPR. Doba uchování čísel VIN a údajů z reálného provozu je stanovena prováděcím nařízením, v případě výrobců, autorizovaných prodejců a opraven a osob a zařízení odpovědných za technické prohlídky je tato doba omezena předáním údajů dle právní úpravy, Evropská agentura pro životní prostředí

---

užitkových vozidel; tato tabulka předpokládá shromažďování průměrných údajů jednotlivých typů, variant a verzí automobilů, vč. průměrných specifických emisí CO2 a dalších.

[464] Viz čl. 7 odst. 7, čl. 12 odst. 4, čl. 13 odst. 4 a čl. 15 odst. 7 nařízení Evropského parlamentu a Rady (EU) 2019/631.

[465] Viz čl. 9 odst. 1 Prováděcího nařízení Komise (EU) 2021/392.

[466] Rozsudek Soudního dvora (třetího senátu) z 9. listopadu 2023 ve věci C-319/22 v řízení Gesamtverband Autoteile-Handel eV proti SCANIA CV AB.

[467] Čl. 11 odst. 4 Prováděcího nařízení Komise (EU) 2021/392, ve spojení s čl. 12 nařízení Evropského parlamentu a Rady (EU) 2019/631.

(EEA) uchovává tyto údaje po dobu 20 let[468]. Prováděcí nařízení Komise (EU) 2021/392 počítá s přezkumem shromažďování a hlášení údajů z reálného provozu, vč. potřeby trvalého sledování a hlášení údajů z reálného provozu ze strany výrobců a doby tohoto sledování a hlášení, to však na základě posouzení možného využití údajů k zajištění reprezentativnosti hodnot emisí a spotřeby v reálném provozu v průběhu času u jednotlivých výrobců, nikoli na základě vyhodnocení kritérií ochrany osobních údajů[469].

Právní úprava eCall

Celoevropský systém automatického tísňového volání eCall z vozidel předpokládala již Směrnice 2010/40/EU[470] jako jednu z prioritních akcí v rámci rozvoje inteligentních dopravních systémů. Dle Rozhodnutí Evropského parlamentu a Rady č. 585/2014/EU ze dne 15. května 2014 o zavedení interoperabilní služby eCall v celé EU členské státy na svém území zavedou nezbytnou infrastrukturu center tísňového volání služby eCall. Povinnosti výrobců vozidel zajistit vybavení nových vozidel palubním systémem eCall a související povinnosti členských států stanoví Nařízení Evropského parlamentu a Rady (EU) č. 2015/758[471]. Jako cíl zavedení systému eCall do všech vozidel a ve všech členských státech toto nařízení vymezuje bezpečnost silničního provozu. Vymezení zpracovávaných údajů, které se automaticky odesílají do centra tísňového volání služby eCall, však nařízení neobsahuje v tomto bodě odkazuje na technickou normu k e-Safety, tato norma není veřejně bezplatně dostupná[472]. Dle vymezení „minimálního souboru údajů“ zařízení eCall ve vozidle průběžně zaznamenává a aktualizuje informace o vozidle, o počtu zapnutých bezpečnostních pásů a také údaje o přesné poloze vozidla a směru jízdy; výrobci mají zajistit, aby *„údaje interní paměti palubního systému eCall … byly automaticky a systematicky odstraňovány“* a uchovávaly pouze tří poslední polohy vozidla, *„pokud je to nezbytně nutné ke stanovení stávající polohy a směru jízdy“*[473]. Nařízení vymezuje některé další záruky ochrany soukromí,

[468] Informační povinnost vymezuje Prováděcí nařízení Komise (EU) 2021/392 v čl. 11 odst. 1 a 2, dobu uchování v čl. 4 odst. 3 a v čl. 11 odst. 5.
[469] Prováděcí nařízení Komise (EU) 2021/392 vymezuje přezkum v čl. 13, s odkazem na posouzení dle čl. 12 odst. 3 nařízení (EU) 2019/631.
[470] Směrnice Evropského parlamentu a Rady 2010/40/EU ze dne 7. července 2010 o rámci pro zavedení inteligentních dopravních systémů v oblasti silniční dopravy a pro rozhraní s jinými druhy dopravy uvádí harmonizované poskytování interoperabilní služby eCall v celé EU jako jednu z prioritních akcí v čl. 3 písm. d).
[471] Nařízení Evropského parlamentu a Rady (EU) č. 2015/758 ze dne 29. dubna 2015 o požadavcích na schválení typu pro zavedení palubního systému eCall využívajícího linku tísňového volání 112 a o změně směrnice 2007/46/ES.
[472] Nařízení (EU) č. 2015/758 v definici pojmu „minimální soubor údajů“ v čl. 3 bodě 6 odkazuje na normu „Inteligentní dopravní systémy – e-Safety – Minimální soubor dat pro eCall“ (EN 15722:2011).
[473] Čl. 6 odst. 5 Nařízení (EU) č. 2015/758.

stanoví, že *„osobní údaje zpracovávané podle tohoto nařízení jsou využívány“* pouze k vyřizování vážných nehod, uchovávány jsou pouze po dobu nezbytnou k vyřizování těchto situací a jakmile přestanou být pro tento účel potřebné, jsou zcela vymazány. Výrobci vozidel mají zajistit, aby systém eCall *„nebyl vysledovatelný a nepodléhal žádnému stálému zaznamenávání“*, údaje nesmějí být dostupné mimo systém eCall nikomu před spuštěním volání eCall a technologie systému eCall musejí zamezovat sledování a zneužití, výrobci mají též poskytnout jasné a srozumitelné informace o zpracování údajů prostřednictvím systému eCall[474].

Nařízení (EU) č. 2015/758 dále umožňuje, aby vozidlo využívalo služby třetí strany zajišťující systémy eCall, namísto tohoto systému má vlastník vozidla právo kdykoliv zvolit použití systému eCall[475], naopak ovšem nikoli, systém eCall je tak pro vlastníka nově vyrobených vozidla povinným. Nařízení (EU) č. 2015/758 ukládá Evropské komisi vypracovat do 31. března 2021 hodnotící zprávu o výsledcích palubního systému eCall, včetně jeho míry rozšíření, a předložit ji Evropskému parlamentu a Radě. Tato hodnotící zpráva měla ovšem být zaměřena na možné rozšíření systému eCall na další kategorie vozidel, nikoli na vyhodnocení efektivity dosavadního využívání systému eCall[476]. Navazující nařízení Komise v přenesené pravomoci (EU) 2017/79[477] stanoví technické požadavky pro schválení typu motorových vozidel ve vztahu k palubnímu systému eCall, členské státy dle něj odmítnou udělit ES schválení typu novým typům motorových vozidel, která nesplňují stanovené požadavky, vč. vybavení systémem eCall. Jako vozidla osvobozená *„od požadavku být vybavena palubním systémem eCall“* toto nařízení definuje pouze vymezená pancéřovaná vozidla kategorií M1 a N1, pokud tato vozidla vzhledem ke svému zvláštnímu účelu nemohou splňovat stanovené požadavky[478]. Dle hodnocení autora zde tak jde o povinné, plošné zpracování osobních údajů, bez možnosti odlišné volby majitele či uživatele-řidiče vozidla.

---

[474] Viz čl. 6 Nařízení (EU) č. 2015/758.
[475] Čl. 5 odst. 3 písm. c) Nařízení (EU) č. 2015/758.
[476] Nařízení (EU) č. 2015/758 upravuje hodnotící zprávu Evropské komise v čl. 12 odst. 1, k možnému rozšíření uvádí těžká nákladní vozidla, autobusy a autokary, jednostopá motorová vozidla a zemědělské traktory, na stránkách Evropského parlamentu ani Evropské komise není k datu dokončení této práce hodnotící zpráva k nalezení.
[477] Nařízení Komise v přenesené pravomoci (EU) 2017/79 ze dne 12. září 2016, kterým se stanoví podrobné technické požadavky a zkušební postupy pro ES schválení typu motorových vozidel, pokud jde o jejich palubní systémy eCall využívající linku tísňového volání 112 a palubní samostatné technické celky a konstrukční části využívající linku tísňového volání 112, a kterým se doplňuje a mění nařízení Evropského parlamentu a Rady (EU) 2015/758, pokud jde o výjimky a použitelné normy.
[478] Viz čl. 2 a příloha IX nařízení (EU) 2017/79.

Právní úprava eCall nedefinuje žádné orgány oprávněné k využití údajů, údaje se předávají pouze do centra tísňového volání služby eCall.

S ohledem na výše uvedenou právní formu nařízení jsou v právním řádu ČR upraveny pouze některé dílčí oblasti. ZoEK upravuje tísňovou komunikaci, zahrnující i povinnost poskytovatelů služeb v případě tísňové komunikace v mobilní veřejné komunikační síti bezodkladně a bezplatně zpřístupnit centru tísňové komunikace lokalizační údaje, včetně údajů generovaných telekomunikačním koncovým zařízením[479], k automatickému vytváření a odesílání lokalizačních údajů není zapotřebí souhlas dotčené osoby. Prováděcí vyhláška[480] k ZoEK pak vymezuje některé technické podrobnosti lokalizace a identifikace volajícího při využití služby eCall a současně též automaticky přenášené základní údaje o vozidle a souvisejících okolnostech, kterými jsou: řídící informace (automatická aktivace nebo manuální aktivace a typ vozidla), identifikační číslo silničního vozidla (VIN)5), typ paliva, čas aktivace jednotky, údaje pro lokalizaci, směr jízdy, počet osob ve vozidle. Zákon o podmínkách provozu vozidel na pozemních komunikacích upravuje některé přestupky výrobců související s povinnostmi systému eCall[481].

3.2.2 Relevantní rozhodnutí soudů, stanoviska orgánů dohledu nad ochranou osobních údajů

OBFCM

K návrhu Prováděcího nařízení Komise (EU) 2021/392 byl předem konzultován Evropský inspektor ochrany údajů, ve svých připomínkách ze 14. ledna 2021[482] především upozornil, že VIN číslo[483], které je součástí shromažďovaných údajů o reálné spotřebě paliva a energie, je považováno za osobní údaj a jako takový by neměl být uchováván déle, než je nezbytné pro vymezený účel. Evropský inspektor osobních údajů ve svých formálních připomínkách konstatoval, že v návrhu prováděcího nařízení se nezdají být zcela jasné postupy, které mají dodržovat účastníci procesu, zejména způsob přímého přenosu údajů z

[479] Tísňovou komunikaci a související povinnosti upravuje ZoEK v § 33.
[480] Vyhláška č. 267/2017 Sb. o lokalizaci a identifikaci účastníka tísňové komunikace při volání na čísla tísňových volání, ve znění pozdějších předpisů, upravuje lokalizaci a identifikaci volajícího služby eCall v § 10.
[481] Zákon č. 56/2001 Sb. o podmínkách provozu vozidel na pozemních komunikacích, ve znění pozdějších předpisů, § 83a odst. 6 písm. b) a odst. 8.
[482] Evropský inspektor ochrany údajů. *EDPS formal comments on a draft Commission Implementing Regulation on the monitoring and reporting of data relating to CO2 emissions from passenger cars and light commercial vehicles pursuant to Regulation (EU) 2019/631 of the European Parliament and of the Council and repealing Implementing Regulations (EU) No 1014/2010, (EU) No 293/2012, (EU) 2017/1152 and (EU) 2017/1153.* 14 January 2021. [online] [cit. 24.2.2024]. Dostupné z: https://www.edps.europa.eu/.
[483] Vehicle identification number je 17-timístný kód jednoznačně a jedinečně identifikující vozidlo. Viz www.cebia.cz. [cit. 15.1.2024].

vozidel na výrobce a také přenosu údajů z vozidel prostřednictvím autorizovaných prodejců nebo servisů. Evropský inspektor zpochybnil také právní základ zpracování osobních údajů, kterým je dle návrhu základ dle čl. 6 odst. 1 písm. c) GDPR, tedy zpracování nezbytné pro splnění právní povinnosti, současně návrh počítá také s možností vlastníků vozidel odmítnout zpřístupnění údajů, ovšem takové právo subjektů údajů u tohoto právního základu není použitelné.

V připomínkách Evropský inspektor upozorňuje též na rozpor obsažený v návrhu, dle kterého údaje zpracovávané Evropskou komisí a Evropskou agenturou pro životní prostředí (EEA) nemají obsahovat žádné osobní údaje spojené s čísly VIN, přitom však dle návrhu má EEA uchovávat údaje VIN po dobu 20 let. Pro tak dlouhou dobu uchovávání návrh neobsahuje žádné zdůvodnění a Evropský inspektor proto požaduje buď zkrácení této doby, nebo poskytnutí přesvědčivého odůvodnění. Evropský inspektor konečně též požaduje v návrhu jasně vymezit povinnosti všech osob zúčastněných na zpracování a přenosech údajů k jejich náležitému zabezpečení, včetně použití kryptování.

eCall

Pracovní skupina WP 29 vydala již v roce 2006 pracovní dokument o ochraně údajů a důsledcích iniciativy eCall na ochranu soukromí[484]. V něm uznává sociálně-ekonomický přínos širokého zavedení služby eCall pro občany, současně však upozorňuje na důsledky nasazení služby eCall pro soukromí a ochranu údajů a na potřebu tyto důsledky zohlednit. WP 29 v dokumentu rozebírá a porovnává možnosti implementace systému eCall do vozidel na dobrovolné bázi a na bázi povinné a na základě analýzy těchto možností z hlediska ochrany osobních údajů a soukromí upřednostňuje a doporučuje dobrovolné zavedení služby eCall. V případě povinného zavedení musí být v právní úpravě zakotven systém záruk ochrany osobních údajů. WP 29 uvádí zejména potřebu zohlednit princip proporcionality v případě dalších údajů, nad rámec „minimálního souboru údajů“ přenášených při eCall volání. Tyto údaje obsažené v případném „plném souboru údajů“ musejí být v souladu s požadavky ochrany soukromí, musejí zejména zahrnovat pouze údaje, které jsou pro vymezený účel nezbytné a relevantní. Kategorie údajů zahrnuté v „plném souboru údajů“ musejí být jasně definovány a v případě, že by měly zahrnovat zdravotní či jiné citlivé údaje, je třeba věnovat zvýšenou péči jejich zpracování.

[484] WP 29. *Working document on data protection and privacy implications in eCall initiative. WP 125.* Adopted on 26th September 2006. [online]. [cit. 24.2.2024].

WP 29 na závěr dokumentu zdůrazňuje několik oblastí vyvolávajících obavy z hlediska ochrany osobních údajů. Řadí mezi ně nutnost vymezit přiměřené doby uchovávání, otázky zabezpečení údajů a také možné vytváření databází za účelem zabránění nesprávného užití či zneužití systému, ve kterých by se spojila identita majitele vozu a údaje SIM karty systému eCall; zde WP 29 zdůrazňuje, že jakékoli sekundární využití údajů, např. pro účely vymáhání plnění dopravních povinností, nemůže být povoleno. Ve vztahu ke zpracovávaným údajům WP 29 považuje možné zahrnutí VIN čísla do minimálního souboru údajů za přesahující vymezený účel. Především však WP 29 vyjadřuje znepokojení s ohledem na princip proporcionality, jelikož zavedení služby eCall nemusí být ve všech případech nezbytné s ohledem na již aktuálně existující a dobře fungující systém tísňového volání ve státech EU, který představuje reálnou alternativu k systému eCall.

Na pracovní dokument WP 29 navázal EDPB po zavedení systému eCall vydáním pokynů zaměřených šířeji na zpracování osobních údajů v souvislosti s propojenými vozidly a mobilitou[485]. EDPB obecně ve vztahu ke zpracování údajů v propojených vozidlech a aplikacích souvisejících s mobilitou, mezi něž řadí i eCall, upozorňuje na informační asymetrii a nedostatek kontroly na straně řidičů vozidel a cestujících. Tyto osoby nebudou vždy o zpracování údajů probíhajícím v propojeném vozidle nebo jeho prostřednictvím dostatečným způsobem informováni, ať již z důvodu poskytnutí informací pouze vlastníkovi, nikoli řidiči vozidla, kvůli jejich až následnému poskytnutí či z důvodu změn vlastníka či uživatele vozidla. Z těchto důvodů zde EDPB formuluje nutná omezení platná při zpracování lokalizačních údajů a připojuje své pochybností o kvalitě souhlasu poskytnutého ke zpracování. U systému eCall EDPB upozorňuje, že nařízení (EU) 2015/758 představuje právní povinnost a *„subjekt údajů nemá skutečnou nebo svobodnou volbu a nebude schopen odmítnout zpracování svých údajů“*.

3.2.3 Posouzení splnění ústavněprávních požadavků

Zpracování údajů v rámci OBFCM i v systému eCall je zpracováním osobních údajů, jak konstatovaly WP 29 i Evropský inspektor ochrany údajů. V obou případech, jak autor vyhodnotil výše, jde o zpracování plošné, které, s ohledem na vymezené cíle těchto dvou právních institutů, není zaměřeno pouze na vybrané osoby či skupiny osob relevantní ve

[485] EDPB. *Pokyny č. 01/2020 ke zpracování osobních údajů v souvislosti s propojenými vozidly a aplikacemi souvisejícími s mobilitou. Verze 2.0.* Přijato dne 9. března 2021. [cit. 24.2.2024]. Dostupné z www.edpb.europa.eu.

vztahu k těmto cílům. Obě zpracování představují zásah do práva na ochranu soukromí, v případě systému eCall zahrnující i údaje lokalizační.

Samotný zásah je v případě OBFCM i eCall vymezen v obecně závazných právních předpisech, právní úprava OBFCM dle hodnocení autora splňuje kritéria formulační přesnosti a je dostatečně předvídatelná. Právní úprava eCall je rozložena do několika vzájemně propojených předpisů s komplikovanou strukturou. Jako zarážející autor hodnotí skutečnost, že kategorie osobních údajů nepřetržitě zpracovávaných systémem eCall ve vozidle nejenže nejsou vymezeny v obecně závazném právním předpise, tento právní předpis svěřuje jejich vymezení technické normě (další technické normy, na které nařízení eCall odkazuje, v tomto případě obsahují ryze technické podrobnosti, jako jsou provozní požadavky na systém eCall[486]. Tato technická norma ovšem nejen může v čase podléhat změnám, ale těmto změnám skutečně podléhá[487], její veřejná dostupnost je navíc omezena placeným přístupem. Autor hodnotí v tomto kontextu jako zavádějící též použití termínu „minimální" v případě souboru obsahujícího osobní údaje, vč. údajů lokalizačních. Jak je zřejmé z citovaného pracovního dokumentu WP 29, jde patrně o pozůstatek úvah o možném „plném souboru údajů". Okruh orgánů, resp. osob oprávněných k využití údajů je v obou případech velmi omezený, u OBFCM je to pouze Evropská agentura pro životní prostředí (dále též jen „EEA"), u eCall jsou to pouze centra tísňového volání, podmínky pro využití údajů jsou upraveny s dostatečnou mírou podrobnosti a jednoznačnosti.

Cíle plošného zpracování osobních údajů jsou vymezeny v příslušných právních předpisech, v případě OBFCM jako sledování a posuzování reprezentativnosti hodnot emisí CO2 a spotřeby paliva nebo energie, v případě eCall je to bezpečnost silničního provozu. Lze konstatovat, že při posouzení racionality v obou případech plošná zpracování osobních údajů sledují cíle, které jsou legitimní a slouží veřejným zájmům. Celkově lze v prvním kroku testu proporcionality zkoumané právní úpravy považovat za způsobilé dosáhnout vytýčených cílů, s vážnou výhradou absentujícího vymezení zpracovávaných kategorií osobních údajů v obecně závazných předpisech v případě systému eCall. Tento nedostatek autor vnímá jako

[486] Seznam technických norem je obsažen v čl. 5 odst. 8 Nařízení (EU) č. 2015/758, který navíc v posledním bodě seznamu uvádí vágní termín *„jakékoliv další evropské normy týkající se systému eCall"*.
[487] Norma ČSN EN 15722 (018461) Inteligentní dopravní systémy – eSafety – Minimální soubor dat pro eCall, která je českou verzí evropské normy EN 15722:2011, překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví, byla účinná v době 01/2012–09/2015 (Katalogové číslo: 89813), poté byla nahrazena normou stejného číselného označení, účinnou v období 10/2015 - 01/2021 (Katalogové číslo: 97956), následně nahrazena normou stejného číselného označení, účinnou v období 02/2021 – dosud (Katalogové číslo: 511667).

závažný, a to zvláště v případě zpracování zahrnujícího mj. i lokalizační údaje[488], dle hodnocení autora je tak obtížné hodnotit právní úpravu zasahující do základního práva na ochranu soukromí z hlediska její vhodnosti k dosažení stanovených cílů.

Následně autor posuzoval, zda existují metody, které umožňují dosáhnout týchž cílů, přitom však do práva na ochranu soukromí zasahují méně intenzivně. V případě OBFCM se tak autor pokoušel v relevantní právní úpravě rozebrané výše nalézt odůvodnění nutnosti zpracovávat údaje z reálného provozu včetně čísla VIN, identifikujícího každý konkrétní automobil. Dle autora právní úprava přesvědčivé odůvodnění nutnosti shromažďovat na celounijní úrovni údaje všech jednotlivých automobilů, vč. údaje čísla VIN, neobsahuje. Potřeba takto detailní identifikace jednotlivých automobilů není zřejmá ani ve vztahu k posouzení spotřeby a emisí konkrétních typů automobilů, vč. motorizací a dalších prvků, které provádí EEA – autor v této souvislosti zkoumal zprávy zveřejňované EEA[489].

Jako srovnatelnou alternativní metodu autor hodnotí možnost anonymizace čísel VIN na úrovni výrobců, ještě před jejich předáním EEA, tuto alternativu autor považuje za možnou zvláště s ohledem na možnost odmítnout poskytnutí údajů obsaženou v právní úpravě OBFCM. Možnost odmítnout poskytnutí údajů OBFCM je však výslovně omezena pouze na „majitele vozidla“, jak ovšem upozornil EDPB[490], v případě vozidel je běžnou situace, kdy řidič není osobou vlastnící vozidlo a informovanost řidiče o probíhajícím zpracování, stejně jako možnost odmítnout zpracování, byť obecně v právní úpravě poskytnutá, je tak do značné míry limitována. Právní úprava OBFCM navíc stanoví velmi dlouho dobu uchování údajů, včetně čísel VIN na straně EEA, v délce 20 let. Ve druhém kroku testu proporcionality tak autor s ohledem na výše uvedené dospěl k závěru, že právní úprava OBFCM požadavky tohoto kroku nesplňuje.

U systému eCall autor jako alternativní možnost hodnotí stávající systém tísňového volání, který WP 29 minimálně v některých státech EU označuje za existující a dobře fungující. Současně je v tomto kroku nutno vzít v úvahu též ze strany WP 29 doporučované dobrovolné, nikoli povinné zavádění služby eCall. Oba uvedené přístupy jsou z hlediska

---

[488] EDPB v *Pokynech č. 01/2020 ke zpracování osobních údajů v souvislosti s propojenými vozidly a aplikacemi souvisejícími s mobilitou* řadí lokalizační údaje, společně s biometrickými údaji a údaji, které by mohly odhalit trestné činy nebo dopravní přestupky, mezi tři kategorie osobních údajů, které vyžadují zvláštní pozornost vzhledem ke své citlivosti a/nebo potenciálnímu dopadu na práva a zájmy subjektů údajů.

[489] Viz např. European Environment Agency. *Transport and environment report 2022.* [online]. 2022. Dostupné z www.eea.europa.eu. [cit. 8.2.2024].

[490] EDPB. *Pokyny č. 01/2020 ke zpracování osobních údajů v souvislosti s propojenými vozidly a aplikacemi souvisejícími s mobilitou. Verze 2.0,* Přijato dne 9. března 2021. [cit. 24.2.2024]. Dostupné z www.edpb.europa.eu.

zásahu do práva na ochranu soukromí méně invazivní. Z veřejně dostupných zdrojů, včetně informací zveřejňovaných Evropskou komisí, však dle hodnocení autora nelze získat dostatek informací umožňujících vyhodnotit účinnost zmiňovaných alternativních metod, druhý krok testu proporcionality není proto možno ve vztahu k systému eCall jednoznačně uzavřít. Pochybnosti ostatně v tomto směru vznesla i WP 29, jak zmíněno výše, ani WP 29 je však neuzavřela formou jednoznačného závěru.

S ohledem na výše uvedené závěry ve vztahu k OBFCM autor nepovažuje za relevantní zabývat se porovnáním závažnosti dotčených základních práv, zde zejména práva na ochranu soukromí a sledovaného veřejného zájmu ve třetím kroku testu proporcionality. Při posuzování proporcionality v užším smyslu by však nebylo možno opomenout již zmiňovanou velmi dlouhou dobu uchování údajů z reálného provozu ve spojení s číslem VIN. V případě systému eCall lze dle hodnocení autora výše uvedené argumenty o nemožnosti jednoznačného posouzení vztáhnout do jisté míry i na případné posouzení tohoto případu ve třetím kroku testu proporcionality, které navíc lze jen obtížně provést při neuzavřeném kroku předchozím. V této souvislosti je však nutno zmínit již zmiňované nevymezení zpracovávaných osobních údajů v obecně závazné právní úpravě. Tento nedostatek dle hodnocení autora koliduje s požadavky rozhodovací praxe na existenci dostatečných mechanismů bránících zneužití zásahů do základních práv.

3.3 Plošné zpracování osobních údajů leteckých cestujících

Evidence údajů osob, které překračují hranice mezi státy, v případě EU zpravidla vnější hranice Schengenského prostoru, představuje, bez ohledu na použitý dopravní prostředek, zpracování osobních údajů. Po prozkoumání těchto zpracování autor vyhodnotil jako zpracování s nejzávažnějším dopadem do ochrany soukromí zpracování údajů leteckých cestujících, mj. proto že zahrnuje i řadu kategorií údajů, které se netýkají samotné cesty, jako jsou např. údaje o platebním prostředku použitém k úhradě letenky, o zdravotních omezeních cestujícího, o stravovacích požadavcích během letu a z nich vyplývající možné informace o zdravotním stavu cestujícího apod. S ohledem na skutečnost, že cílem této práce není snaha o taxativní výčet všech plošných zpracování osobních údajů, nýbrž analýza dopadů těchto zpracování do základního práva na ochranu soukromí a jejich posouzení z ústavněprávního hlediska, omezí se autor v této kapitole na zpracování údajů leteckých cestujících.

3.3.1 Vývoj a základní vymezení, relevantní právní úprava

Plošné shromažďování a další zpracování osobních údajů cestujících v letecké dopravě zahrnuje jednak tzv. předběžné údaje o cestujících, označované též jako „údaje API" (jako zkratka z anglického termínu Advance Passanger Information) a údaje jmenné evidence cestujících, známé též pod anglickým názvem Passenger Name Records a jeho zkratkou PNR. Zatímco údaje API slouží ke zdokonalení hraničních kontrol a boje proti nedovolenému přistěhovalectví, údaje PNR představují soubory údajů z rezervačních a odbavovacích systémů leteckých dopravců, zpracovávané pro účely prevence, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti. Jak uvádí Rada Evropské unie v tiskové zprávě vydané 21. dubna 2016, „*Sytém PNR doplňuje již existující nástroje pro potírání přeshraniční trestné činnosti. Zpracování údajů PNR umožňuje donucovacím orgánům odhalit osoby, které nejsou podezřelé z trestné činnosti nebo terorismu, dříve, než specifická analýza údajů ukáže, že podezřelé být mohou.*"[491] V některých členských státech EU se navíc povinnost předávání údajů rozšířila i na železniční a pozemní dopravce a poskytovatele cestovních služeb, takto je tomu např. v Belgii[492], ke zpracování určitých, relativně omezených kategorií osobních údajů dochází také v lodní dopravě[493]. Jak již uvedeno výše, autor se zde omezí na povinné zpracování a předávání údajů v letecké dopravě, které je nejrozsáhlejším plošným zpracováním osobních údajů v oblasti hromadné dopravy, uskutečňovaným dle relevantních právních předpisů ve všech státech EU.

Vývoj plošného zpracování osobních údajů leteckých cestujících

Letecké společnosti shromažďují řadu údajů o svých cestujících, potenciálně využitelných pro účely veřejného zájmu, mezi které patří boj proti terorismu a obecněji boj proti trestné činnosti a s ohledem na to, že jde o údaje o leteckých cestujících, specificky i boj proti nelegální migraci. První snaha o takovéto využití údajů byla legislativně zakotvena v roce 2004 ve Směrnici o povinnosti dopravců předávat údaje o cestujících[494] (dále též jen „Směrnice API"). Směrnice uložila členským státům EU, aby stanovily leteckým dopravcům povinnost předávat orgánům pro provádění kontrol osob na vnějších hranicích na jejich žádost

[491] Rada Evropské unie. *Údaje o cestujících.* 21. dubna 2016. [online] [cit. 24.2.2024]. Dostupné z www.consilium.europa.eu/cs/policies/fight-against-terrorism/passenger-name-record/.
[492] Tuto skutečnost zmiňuje Rozsudek Soudního dvora (velkého senátu) ze 21. června 2022 ve věci C-817/19.
[493] Toto zpracování je založeno Nařízením Evropského parlamentu a Rady (EU) 2019/1239 ze dne 20. června 2019, kterým se zřizuje evropské prostředí jednotného námořního portálu a zrušuje směrnice 2010/65/EU.
[494] Směrnice Rady 2004/82/ES ze dne 29. dubna 2004 o povinnosti dopravců předávat údaje o cestujících.

informace o osobách vstupujících leteckou dopravou na území členských států, a to nejpozději do 5. září 2006[495]. Do právního řádu ČR provedl tuto směrnici zákon o civilním letectví[496].

Na základě dvoustranných dohod uzavíraných mezi EU na straně jedné a Spojeným královstvím a třemi mimoevropskými státy – Kanadou, Spojenými státy a Austrálií na straně druhé, měly být tyto údaje předávány do uvedených zemí. Dohody byly postupně uzavírány od roku 2005[497], zahrnovaly předávání tzv. „předběžných informací o cestujících" (Advanced Passenger Information, API) a „záznamů o knihování cestujících" (Passenger Name Record, PNR), v aktuálně používané české odborné terminologii údaje jmenné evidence cestujících. Jde vždy o údaje konkrétních fyzických osob a jedná se tedy o osobní údaje ve smyslu platné právní úpravy[498]. Rozsah takto zpracovávaných osobních údajů v mezidobí narostl a kategorie údajů PNR, které dle Dohody s Kanadou z r. 2005 letečtí dopravci provozující lety z území ES do Kanady předají příslušným kanadským orgánům, byly již podstatně širší nežli rozsah vymezený ve Směrnici 2004/82/ES a zahrnovaly např. také informace o všech způsobech platby, zúčtovací adresu, kontaktní telefonní čísla, informace související s programem pro stálé cestující – nalétané míle a adresy, číslo sedadla a další[499]. Kromě výše uvedených států je Evropská komise zmocněna vyjednat dohody PNR s Mexikem a Japonskem, v září 2023 doporučila zahájit jednání rovněž s Norskem, Islandem a Švýcarskem.

Směrnice PNR

Následně, v roce 2016, přibyla ke Směrnici API též Směrnice PNR. Ta zakládá v prvé řadě povinnost členských států zajistit, aby letečtí dopravci předávali u jednotlivých letů údaje PNR „*do databáze útvaru pro informace o cestujících toho členského státu, na jehož*

[495] Směrnice vymezila tyto povinně předávané informace: číslo a typ použitého cestovního dokladu, státní příslušnost, jméno (jména) a příjmení, datum narození, hraniční přechod vstupu na území členských států, kódové číslo letu, čas odletu a příletu, celkový počet osob přepravovaných uvedeným letem, počáteční místo nástupu na palubu.
[496] Zákon č. 49/1997 Sb., o civilním letectví, ve znění pozdějších předpisů.
[497] V případě Kanady: 2006/230/ES: Rozhodnutí Rady ze dne 18. července 2005 o uzavření Dohody mezi Evropským společenstvím a vládou Kanady o zpracovávání údajů API/PNR a následný návrh Dohody mezi Kanadou a Evropskou unií o předávání a zpracovávání údajů jmenné evidence cestujících ze 25. června 2014, 4. března 2024 Evropská komise oznámila přijetí a předložení návrhu dohody Radě Evropské unie; v případě Austrálie: Dohoda mezi Evropskou unií a Austrálií o zpracovávání údajů jmenné evidence cestujících (PNR) ze zdrojů Evropské unie leteckými dopravci a o jejich předávání Australské celní správě, uzavřená dne 30. 6. 2008 a následná Dohoda mezi Evropskou unií a Austrálií o zpracovávání údajů jmenné evidence cestujících (PNR) leteckými dopravci a o jejich předávání australské správě pro cla a ochranu hranic, datovaná dne 29. září 2011; v případě Spojených států amerických: Dohoda mezi Spojenými státy americkými a Evropskou unií o využívání jmenné evidence cestujících a o jejím předávání Ministerstvu vnitřní bezpečnosti Spojených států uzavřená v r. 2015; v případě Spojeného království uzavřená r. 2020.
[498] Čl. 4 bod 1 GDPR, resp. čl. 3 bod 1 Trestněprávní směrnice.
[499] Kategorie údajů vymezila Dohoda s Kanadou tvořící součást Rozhodnutí Rady č. 2006/230/ES z 18. července 2005 v Příloze II.

území bude let přistávat nebo z jehož území bude let zahájen“[500]. Údaje se týkají konkrétních, individuálně určených leteckých cestujících, jedná se tedy o osobní údaje. Letečtí dopravci jednotlivé kategorie těchto údajů zpracovávají pro účely zajištění letecké přepravy, nevytvářejí je tedy pro účely povinností dle právní úpravy PNR[501]. Jak dodává Policie ČR v textu Národní kontaktní bod pro terorismus, po transpozici Směrnice PNR přibylo „*využívání těchto dat orgány vymáhajícími právo*“[502].

Zákon o civilním letectví

Směrnici PNR transponovala do právního řádu ČR s účinností od 24. dubna 2019 novela zákona o civilním letectví, obsažená v tzv. změnovém zákoně[503] přijatém společně se ZoZOÚ, v souvislosti s některými úpravami právního řádu ČR v návaznosti na povinnosti vyplývající z Obecného nařízení GDPR a k provedení Trestněprávní směrnice. Tato novela vymezila v zákoně o civilním letectví právní institut jmenné evidence cestujících (PNR), podstatně rozšířila kategorie takto předávaných osobních údajů leteckých cestujících a především, vedle již existující povinnosti leteckých dopravců předávat „údaje o cestujících“ – údaje API útvaru Policie ČR příslušnému k provedení hraniční kontroly na letišti na jeho žádost, doplnila novou povinnost, zakládající automatické předávání „údajů jmenné evidence cestujících“.

V zákoně vymezené „údaje jmenné evidence cestujících“, tedy údaje PNR zahrnují též „údaje o cestujících“, tedy údaje API a řadu dalších kategorií osobních údajů, které se týkají letu *„se vzletem, mezipřistáním nebo přistáním na území České republiky“*[504]. Směrnice PNR a obdobně též zákon o civilním letectví umožňuje rozšířit povinnost leteckých dopravců k předávání údajů PNR též na lety uvnitř EU[505], takové rozšíření je nutno oznámit Evropské

[500] Viz čl. 8 odst. 1 Směrnice PNR.
[501] Dle čl. 8 odst. 1 Směrnice PNR mají letečtí dopravci tyto údaje předávat „*v rozsahu, v jakém je již shromáždili v průběhu své obvyklé činnosti*“.
[502] Policie České republiky. *Národní kontaktní bod pro terorismus.* Nedatováno. [online] [cit. 12.1.2023] Dostupné z www.policie.cz.
[503] Zákon č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.
[504] Vymezení, včetně kategorií předávaných údajů je obsaženo v zákoně č. 49/1997 Sb., o civilním letectví v § 69a odst. 5. Kategorie osobních údajů zčásti navazují na úpravu zákona o civilním letectví platnou a účinnou již před novelou provedenou zákonem č. 111/2019 Sb., i ta však v zákoně nebyla obsažena v jeho původní verzi, nýbrž do něj byla vložena s účinností od 1.7.2006 novelizací provedenou zákonem č. 225/2006 Sb., kterým se mění zákon č. 49/1997 Sb., o civilním letectví a o změně a doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů a některé další zákony.
[505] Zákon o civilním letectví toto rozšíření obsahuje v § 69a odst. 2.

komisi. Dle údajů zveřejněných v Úředním věstníku EU patří Česká republika mezi členské státy, které se rozhodly používat Směrnici PNR i na lety uvnitř EU.

Soubory předávaných údajů zahrnují poměrně široké spektrum údajů, jejich rozsah je obdobný jako v případě výše zmíněných dvoustranných dohod, nejedná se tedy pouze o informace o přepravě konkrétní fyzické osoby určitým letem. Mezi předávanými kategoriemi údajů jsou navíc např. také veškeré, nejen omezené údaje o věrnostním programu cestujícího, veškeré údaje o zavazadlech a též počet a jména a příjmení cestujících v rámci jednotlivého záznamu ve jmenné evidenci cestujících, letecký dopravce je též povinen předat výše uvedeným způsobem jakékoli změny těchto údajů. Zákon o Policii ČR počítá s možností, že údaje PNR budou zahrnovat i údaje ze zvláštních kategorií osobních údajů a stanoví pro tento případě, že Policie ČR neprodleně po přijetí vymaže *„údaje jmenné evidence cestujících, které odhalují rasový nebo etnický původ, politické názory, náboženské nebo filosofické přesvědčení, členství v odborové organizaci, zdravotní stav, sexuální chování nebo sexuální orientaci dané osoby“*[506].

Účely zpracování údajů

Účelem zpracování osobních údajů cestujících, pro který byla úprava údajů API v roce 2006 novelou vložena do zákona o civilním letectví, bylo zdokonalení hraničních kontrol a boj proti nedovolenému přistěhovalectví. V původním vládním návrhu zákona, který byl posléze Parlamentem ČR schválen jako zákon č. 225/2006 Sb., povinnost leteckých dopravců předávat osobní údaje cestujících, tedy ani vymezení kategorií předávaných údajů, obsaženy nebyly, oba tyto body byly vymezeny až v poslaneckém pozměňovacím návrhu k tomuto návrhu zákona[507], následně schváleném. Podstatným také je, že i ve znění schválených pozměňovacích návrhů nebylo povinné předávání diskutovaných údajů leteckými dopravci automatickou činností, spojenou s každým letem, nýbrž povinností předávat údaje na žádost útvaru Policie České republiky příslušného k provedení hraniční kontroly na letišti. Z hlediska časového pak původní znění zákona leteckým dopravcům uložilo povinnost předávat takto údaje *„neprodleně po doručení žádosti, nejdříve však po ukončení nástupu všech cestujících do letadla*“[508]. Toto znění je dosud platné a účinné, je

[506] Viz § 84b odst. 2 zákona o Policii ČR.
[507] Pozměňovací návrhy obsažené v usnesení Hospodářského výboru Poslanecké sněmovny Parlamentu ČR č. 383 ze dne 18. ledna 2006 (sněmovní tisk 1069/1).
[508] Viz § 69 odst. 1 zákona č. 49/1997 Sb. o civilním letectví, ve znění pozdějších předpisů.

obsaženo v § 69 zákona o civilním letectví a týká se pouze devíti základních kategorií osobních údajů[509].

Ve Směrnici PNR je účel zpracování údajů shromažďovaných dle této směrnice vymezen jako *„prevence, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti“*[510]. Směrnice PNR jej dále rozvádí tak, že zahrnuje *„posuzování cestujících před jejich plánovaným příletem do nebo odletem z členského státu za účelem identifikace osob, u kterých je vyžadováno další prověření příslušnými orgány…, vzhledem k tomu, že tyto osoby mohou být zapojeny do teroristického trestného činu nebo závažného trestného činu“*, dále též *„reakce … v konkrétních případech za účelem prevence, odhalování, vyšetřování a stíhání teroristického trestného činu nebo závažného trestného činu nebo poskytnutí výsledků tohoto zpracování příslušným orgánům a případně Europolu“* a také analýzu „*údajů PNR za účelem aktualizace nebo vytvoření nových kritérií, která mají být použita při posuzování prováděných*“[511].

Zákon č. 111/2019 Sb. v rámci transpozice PNR Směrnice kromě novely zákona o civilním letectví novelizoval též zákon o Policii ČR. Do něj tato novela doplnila nový účel zpracování osobních údajů jmenné evidence cestujících: *„posuzování cestujících, příprava kritérií, plnění konkrétního úkolu souvisejícího s trestnou činností“* uvedenou ve zvláštních právních předpisech[512]*, „u níž horní hranice trestní sazby odnětí svobody činí nejméně 3 roky, a předávání využívajícím orgánům České republiky a jiným státům pro plnění takového úkolu“*; do zákona o civilním letectví tento účel doplněn nebyl. Horní hranice trestní sazby v minimální výši 3 let představuje z hlediska rozsahu trestných činů v právním řádu ČR velmi široké vymezení. Jelikož však musejí být obě kritéria splněna kumulativně, je podstatným, že zvláštní právní předpisy, na které zákon o Policii ČR odkazuje, vymezují trestnou činnost dosti restriktivně. Konkrétně uvedená Směrnice Evropského parlamentu a Rady (EU) 2017/541 o boji proti terorismu[513] (dále též jen „Směrnice o boji proti terorismu“) vymezuje i dle svého předmětu trestné činy v oblasti teroristických trestných činů, trestných činů spojených s

[509] Tyto kategorie jsou vymezeny v § 69 odst. 2 zákona o civilním letectví, ve znění pozdějších předpisů, pod písmeny a) – i).
[510] Viz čl. 1 odst. 2 PNR Směrnice.
[511] Viz čl. 6 odst. 2 PNR Směrnice.
[512] Zákon č. 273/2008 Sb. o Policii České republiky, ve znění pozdějších předpisů, v § 84b odst. 1 výslovně uvádí a) Směrnici Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. března 2017 o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV a b) PNR Směrnici, konkrétně její Přílohu II.
[513] Směrnice Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. března 2017 o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV.

teroristickou skupinou a trestných činů spojených s teroristickými činnostmi[514], Směrnice PNR pak obsahuje taxativní seznam celkem 26 trestných činů, např. účast na zločinném spolčení, obchodování s lidmi, pohlavní vykořisťování dětí a dětská pornografie a další – tyto trestné činy jsou ve směrnici výslovně označeny jako „závažné trestné činy“[515].

Policie ČR je povinna zpracovávat údaje jmenné evidence cestujících v evidenci oddělené od jiných evidencí, při posuzování cestujících může tyto údaje porovnat s jinými evidencemi nebo mezinárodními nebo evropskými informačními systémy, pouze pokud je Policie ČR „*oprávněna tyto systémy využít pro předcházení, vyhledávání, odhalování nebo stíhání trestné činnosti*“[516].

Orgány oprávněné k vyžádání a využití údajů

Zákon o civilním letectví ukládá leteckým dopravcům předání údajů API Policii ČR, konkrétně útvaru Policie ČR příslušnému k provedení hraniční kontroly na letišti, a předání údajů jmenné evidence cestujících Policii ČR. Zákon o Policii ČR pak ukládá Policii ČR předávat *„údaje jmenné evidence cestujících, výsledky jejich požadovaného zpracování a výsledky posuzování cestujících“* tzv. „využívajícím orgánům České republiky“ a „jednotkám pro informace o cestujících“, a to i bez žádosti těchto orgánů, pokud je to potřebné pro plnění úkolu zahrnutého mezi výše uvedenými účely zpracování těchto údajů[517]. Tyto oprávněné orgány vymezuje zákon o Policii ČR tak, že využívajícími orgány České republiky se rozumí *„Celní správa České republiky, Finanční analytický úřad, Generální inspekce bezpečnostních sborů, Vojenská policie a zpravodajská služba“*, využívajícím orgánem členského státu pak takový orgán, který daný členský stát oznámil Evropské komisi a byl zveřejněn v Úředním věstníku Evropské unie. Zpravodajskými službami působícími v ČR jsou dle platné právní úpravy[518] Bezpečnostní informační služba, Úřad pro zahraniční styky a informace a Vojenské zpravodajství jako součást Ministerstva obrany, z vymezení využívajících orgánů v zákoně o civilním letectví však není zřejmé, zda mezi využívající orgány patří pouze některé ze zpravodajských služeb.

Dle Směrnice PNR je oprávněn o údaje PNR nebo o výsledek jejich zpracování od útvarů pro informace o cestujících členských států požádat také Europol, a to v mezích své

[514] Viz čl. 1 Směrnice o boji proti terorismu a vymezení konkrétních trestných činů v navazujících článcích.
[515] Čl. 3 bod 9 Směrnice o boji proti terorismu.
[516] § 84b odst. 4 a 5 zákona o Policii ČR.
[517] § 84c odst. 1 zákona o Policii ČR.
[518] Zákon č. 153/1994 o zpravodajských službách České republiky, ve znění pozdějších předpisů, vymezuje zpravodajské služby v § 3.

působnosti a za účelem plnění svých úkolů, zákon o Policii ČR předpokládá obecně zpřístupňování a předávání osobních údajů Europolu (Evropskému policejnímu orgánu)[519]. V právních předpisech upravujících činnost jednotlivých využívajících orgánů, s výjimkou zákona o Celní správě ČR, absentuje jakákoli úprava využívání údajů jmenné evidence cestujících, není v nich tedy upraven ani účel jejich využití či jakékoli další podmínky zpracování těchto údajů[520]; v případě zpravodajských služeb není z právní úpravy ani zřejmé, které ze zpravodajských služeb jsou oprávněny tyto údaje využívat. Na využití těchto údajů se tedy uplatní pouze obecná právní úprava upravující činnost jednotlivých využívajících orgánů.

Kritérium plošného zpracování

Zpracování údajů API a zejména údajů jmenné evidence cestujících a jejich předávání Policii ČR a dalším oprávněným orgánům dle právní úpravy Směrnice PNR a její národní transpozice v ČR rozebrané výše se týká všech cestujících v letecké dopravě. Jejich osobní údaje jsou předmětem zpracování a dle zákona o Policii ČR též předmětem předávání využívajícím orgánům České republiky a jednotkám pro informace o cestujících, i bez žádosti těchto orgánů; společně s výsledky posuzování cestujících takto Policie ČR předává i samotné údaje jmenné evidence cestujících[521]. K jejich zpracování dochází bez ohledu na to, zda některý z dotčených cestujících případně naplňuje jakákoli předem vymezená kritéria, která by byla stanovena v souvislosti s vymezenými účely prevence, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti. S ohledem na tuto skutečnost se dle hodnocení autora jedná o plošné zpracování osobních údajů, které se nerozlišujícím způsobem dotýká všech osob v dané kategorii či skupině osob – zde ve skupině cestujících v letecké dopravě u letů odlétajících z některého členského státu EU do třetí země nebo u letů v opačném směru, v některých případech i u letů v rámci EU.

---

[519] Čl. 10 odst. 1 Směrnice PNR, § 80a odst. 1 písm. b) zákona o Policii ČR.

[520] Zákon č. 341/2011 Sb. o Generální inspekci bezpečnostních sborů a o změně souvisejících zákonů, ve znění pozdějších předpisů, Zákon č. 300/2013 Sb. o Vojenské policii a o změně některých zákonů (zákon o Vojenské policii), ve znění pozdějších předpisů, Zákon č. 153/1994 Sb. o zpravodajských službách České republiky, ve znění pozdějších předpisů, který upravuje činnost Úřadu pro zahraniční styky a informace, stejně jako zákony upravující činnost ostatních zpravodajských služeb, tedy Zákon č. 154/1994 Sb. o Bezpečnostní informační službě, ve znění pozdějších předpisů a Zákon č. 289/2005 Sb. o Vojenském zpravodajství, ve znění pozdějších předpisů, údaje jmenné evidence cestujících nezmiňují. Obdobně je tomu v případě právních předpisů upravujících činnost a pravomoci Finančně analytického úřadu, tedy Zákona č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů a Zákona č. 69/2006 Sb. o provádění mezinárodních sankcí, ve znění pozdějších předpisů. Pouze Zákon č. 17/2012 Sb. o Celní správě České republiky, ve znění pozdějších předpisů obsahuje v § 58 odst. 5 stručnou úpravu, dle které orgány celní správy mohou údaje jmenné evidence cestujících v součinnosti s policií využívat *„pro plnění konkrétního úkolu při výkonu své působnosti“*.

[521] Jak stanoví § 84c odst. 1 zákona o Policii ČR.

Z dostupných informací vyplývá, že se jedná o údaje týkající se stovek milionů osob ročně. Dle oficiálních údajů zveřejněných Evropským parlamentem v roce 2016[522] se celkový počet cestujících přepravovaných ve 28 zemích EU pohyboval v letech 2009–2014 na úrovni sedmi až téměř devíti set milionů, při stálém plynulém nárůstu v těchto letech. Dle této statistiky tvořili 43% z těchto počtů cestující z jiné země EU, 39% ze zemí mimo EU a 18% cestujících cestovalo vnitrostátně. V roce 2018 byla přes letiště v členských státech EU přepravena téměř 1 miliarda cestujících[523]. Patrně se nejedná o počty jedinečných osob, jejichž osobní údaje byly v daném roce v rámci jmenné evidence cestujících zpracovávány, nýbrž o „celkový počet letecky přepravovaných cestujících", jak jsou celkové počty v oficiálním textu zveřejněném na stránkách Evropského parlamentu označeny. Z textu ani ze statistik, které jsou jeho součástí, to sice není zřejmé, autor však považuje za pravděpodobné, že osoby, které případně v daném roce takto letecky cestovaly vícekrát, byly také v těchto počtech započítány vícekrát. Přesto se nepochybně jedná o zpracování údajů značného množství osob, dle těchto statistik autor hodnotí zpracování osobních údajů v rámci jmenné evidence cestujících jako rozsáhlé zpracování.

Uvedené údaje se týkají naposledy roku 2018, autorovi se bohužel nepodařilo dohledat z oficiálních zdrojů, ať již na úrovni institucí a orgánů EU, tak ani na národní úrovni ČR, aktuálnější údaje z posledních let. Ani hodnotící zprávy, doporučení a návrhy rozhodnutí Evropské komise z posledních let v oblasti PNR[524] neobsahují konkrétní údaje o celkovém množství zpracovávaných údajů či o celkovém množství dotčených osob. Zpráva Evropské komise o přezkumu Směrnice PNR, vyhotovená v roce 2020, bez uvedení konkrétních počtů osob, uvádí, že analýza statistických informací, které členské státy v souladu s čl. 20 Směrnice PNR každoročně poskytují Evropské komisi o údajích PNR poskytnutých útvarům pro informace o cestujících, *„ukazuje, že pouze údaje o velmi malém zlomku cestujících jsou*

---

[522] Počet cestujících činil 753.000.000 v roce 2009 a 879.000.000 cestujících v roce 2014. Viz Evropský parlament. *Boj proti terorismu: Parlament vymezil pravidla používání údajů cestujících v letecké dopravě.* 13. dubna 2016. [online] [cit. 24.2.2024]. Dostupné z www.europarl.europa.eu/news/cs.

[523] Eurostat. *Statistika přepravy cestujících. Přes letiště v EU-27 byla v roce 2018 přepravena téměř 1 miliarda cestujících.* 7. ledna 2021. [online] [cit. 24.2.2024]. Dostupné z https://ec.europa.eu/eurostat.

[524] Např. *Report from the Commission to the European Parliament and the Council On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*. 24.7.2020, *Zpráva Komise Evropskému parlamentu a Radě o společném hodnocení Dohody mezi Spojenými státy americkými a Evropskou unií o využívání jmenné evidence cestujících a o jejím předávání Ministerstvu vnitřní bezpečnosti Spojených států*. 12. ledna 2021, *Doporučení pro Rozhodnutí Rady o zmocnění k zahájení jednání o dohodě mezi Evropskou unií a Islandem o předávání údajů jmenné evidence cestujících z EU na Island za účelem prevence, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti*. 6.9.2023, *Návrh Rozhodnutí Rady o podpisu Dohody mezi Kanadou a Evropskou unií o předávání a zpracování údajů jmenné evidence cestujících (PNR) jménem Evropské unie.* 4.3.2024. [online] [cit. 24.2.2024].

předány příslušným orgánům k dalšímu zkoumání“[525]. Tento závěr Evropské komise však dle autora pomíjí skutečnost, že jde pouze o další předání údajů PNR, tedy v případě České republiky o předání Policií ČR využívajícím orgánům ČR a jednotkám pro informace o cestujících, když letečtí dopravci dle zákona předávají Policii ČR veškeré údaje[526]. Současně též Evropská komise ve zprávě neuvádí žádnou konkrétní informaci či podklad pro své hodnocení o celkových počtech tohoto „malého zlomku cestujících“. Tato skutečnost neumožňuje závěry zprávy přezkoumat a vyhodnotit dopady aplikace Směrnice PNR na základě konkrétních údajů ani učinit závěr o míře zásahu do práva na ochranu soukromí a posoudit jeho proporcionalitu.

Ani na úrovni České republiky nejsou k dispozici oficiální statistické informace o počtech údajů API a údajů jmenné evidence cestujících. Národní kontaktní bod pro terorismus, resp. Oddělení informací o cestujících (PIU CZ) Národní centrály proti organizovanému zločinu SKPV[527] na svých stránkách, stejně jako na odkaze na stránky Ředitelství služby cizinecké policie zveřejňuje pouze obecné informace o jmenné evidenci cestujících. Z kategorií těchto informací i z doprovodného textu je dle hodnocení autora zřejmé, že nahlížejí na právní institut jmenné evidence cestujících výhradně prizmatem sledovaného veřejného zájmu (ochrany společnosti před rizikem terorismu), nikoli též jako na zásah do práva na ochranu soukromí značného množství osob, které tento právní institut bezesporu též představuje. Ačkoli je sledovaný veřejný zájem v tomto případě možno považovat za legitimní (jak autor rozebírá dále), není možno tento druhý aspekt zcela opomíjet. Jmenná evidence cestujících je zaměřena na ochranu legitimního veřejného zájmu, současně však bezesporu představuje zásah do základního lidského práva na ochranu soukromí. V důsledku absence byť i jen základních statistických informací[528] je však dle hodnocení autora fakticky znemožněna alespoň základní veřejná kontrola nad mírou využití tohoto právního institutu v praxi. Autor považuje zveřejňování statistických údajů o počtech zpracovávaných, vyžádaných a dále využitých osobních údajů nejen v případě jmenné evidence cestujících, nýbrž obecně v případech plošných zásahů do soukromí, za efektivní nástroj veřejné kontroly

[525] Report from the Commission to the European Parliament and the Council On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. 24.7.2020. [online] [cit. 24.2.2024].
[526] Viz § 69a odst. 1 zákona o civilním letectví, ve znění pozdějších předpisů a § 84c odst. 1 zákona o Policii ČR.
[527] V obou případech viz webové stránky www.policie.cz.
[528] Určitou představu si lze učinit z dílčích statistických informací zveřejňovaných Ministerstvem dopravy, dle kterých obchodní letecká přeprava cestujících zahrnující pouze české letecké dopravce činila v roce 2022 celkem 4.065.400 (statistika neuvádí použité jednotky, patrně však jde o osoby). Viz Ministerstvo dopravy. *Ročenka dopravy 2022*. [online] [cit. 15.1.2024]. Dostupné z www.sydos.cz.

a prevence zneužívání či nadužívání konkrétního právního institutu, v jehož rámci k zásahům do práva na ochranu soukromí dochází. Autor se proto tomuto aspektu věnuje podrobněji v závěru této práce, v rámci doporučení de lege ferenda.

Informace o zpracování údajů o cestujících v letecké dopravě

Zákon o civilním letectví vymezuje informační povinnost leteckých dopravců vůči subjektům údajů, to však pouze u API údajů o cestujících, nikoli též ve vztahu k PNR údajům. Letecký dopravce je takto *„povinen informovat cestující podle zvláštního právního předpisu o shromažďování a zpracování“* těchto údajů[529]. Jde pouze o obecnou informační povinnost, v podobě informačního textu určeného všem leteckým cestujícím, nikoli specificky o informování dotčených osob. Zákon o Policii ČR ukládá Policii ČR obecnou informační povinnost vztahující se na zpracovávání osobních údajů bez vědomí subjektu údajů za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech[530]. Policie ČR tak má sdělit subjektu údajů *„že pro své potřeby zpracovává jeho osobní údaje“*, a to následně, *„v okamžiku, kdy není ohroženo plnění úkolů policie“* v souvislosti s výše uvedenými účely. Výjimku však dle zákona představují situace, kdy jsou tyto údaje *„vymazány bez zbytečného odkladu po zániku uvedeného ohrožení“* a také situace, kdy by *„sdělení těchto údajů bylo spojeno s neúměrným úsilím“*, v takových případech Policie ČR dotčenou osobu informovat nemusí. S ohledem na formulaci informační povinnosti pouze ve vztahu ke zpracování osobních údajů Policií ČR „pro své potřeby“ i vzhledem k zakotvení uvedených výjimek není jednoznačné, zda se v praxi tato povinnost vztáhne na veškerá zpracování údajů PNR, zejména zda Policie ČR má povinnost informovat dotčené osoby o tom, že jejich osobní údaje PNR předala využívajícím orgánům či jednotkám pro informace o cestujících. I v případě zpracování údajů PNR sice platí, že zpracováním osobních údajů je i jejich předání[531], nejde však o zpracování pro potřeby Policie ČR a autor

[529] Informační povinnost leteckých dopravců je vymezena v § 69 odst. 3 zákona č. 49/1997 Sb. o civilním letectví, ve znění pozdějších předpisů, ustanovení § 69a upravující jmennou evidenci cestujících, takovou informační povinnost neobsahuje.
[530] Informační povinnost Policie ČR zakotvuje zákon č. 273/2008 Sb. o Policii ČR, ve znění pozdějších předpisů v § 88 ve spojení s § 79 odst. 1.
[531] Zpracování osobních údajů definuje Trestněprávní směrnice v čl. 3 bodě 2 jako jakoukoliv operaci nebo soubor operací *„s osobními údaji nebo soubory osobních údajů*“, prováděné *„pomocí či bez pomoci automatizovaných postupů*“, definice výslovně zmiňuje mimo jiné též zpřístupnění přenosem nebo jakékoliv jiné zpřístupnění.

tak uzavírá, že informační povinnost dle zákona o Policii ČR tak na tyto případy zřejmě nedopadá.

Doba uchování údajů

Zákon o civilním letectví stanoví velmi krátké doby uchovávání údajů API, a to jak pro letecké dopravce, tak rovněž pro Policii ČR[532]. Letecký dopravce tak do 24 hodin po přistání letadla přepravujícího cestující „*provede likvidaci osobních údajů o cestujících, které byly shromážděny za účelem splnění povinností"* předat údaje Policii ČR. Taktéž pro Policii ČR je stanovena velmi krátká lhůta pro výmaz takto obdržených osobních údajů – pokud je nevyužije *„k plnění jí stanoveného úkolu"*, provede likvidaci údajů „*do 24 hodin po jejich obdržení*". V případě údajů PNR však zákon o civilním letectví obdobnou povinnost nestanoví, a to ani pro letecké dopravce.

Nakládání Policie ČR s PNR údaji upravuje zákon o Policii ČR, jejich dobu uchování na straně Policie ČR vymezuje ve dvou etapách[533]. Po uplynutí šesti měsíců od přijetí údajů Policie ČR znepřístupní v evidenci vybrané kategorie údajů – jde o údaje vztahující se přímo k identitě cestujícího (jméno, příjmení, adresu a některé další)[534], ostatní údaje, vč. rezervačního kódu, údajů o stavu odbavení cestujícího a dalších, v evidenci zůstanou. PNR směrnice tento proces označuje jako „depersonalizaci", dle hodnocení autora však minimálně u některých z těchto údajů jde i nadále o osobní údaje umožňující stanovit identitu cestujícího. Po uplynutí 5 let od přijetí údajů pak Policie ČR vymaže veškeré zbývající údaje, s výjimkou údajů využívaných k plnění konkrétního úkolu souvisejícího s trestnou činností. Pro využívající orgány však zákon o civilním letectví ani zákon o Policii ČR a ani relevantní zvláštní právní předpisy upravující činnost těchto orgánů nestanoví dobu uchování údajů jmenné evidence cestujících, což platí i pro Celní správu ČR, u níž zvláštní právní předpis, na rozdíl od zvláštních právních předpisů vymezujících ostatní využívající orgány, velmi stručně využití údajů jmenné evidence cestujících zmiňuje, jak uvedeno výše. Také na dobu uchování je tedy nutno vztáhnout pouze obecnou právní úpravu upravující činnost jednotlivých využívajících orgánů, při absenci zvláštní úpravy ve vztahu k údajům jmenné evidence cestujících však toto dle hodnocení autora není dostačující.

[532] Viz § 69 odst. 4 a 6 zákona č. 49/1997 Sb. o civilním letectví, ve znění pozdějších předpisů.
[533] Viz § 84b odst. 6 zákona č. 273/2008 Sb. o Policii ČR, ve znění pozdějších předpisů.
[534] Směrnice PNR tento postup v čl. 12 označuje jako „depersonalizaci maskováním".

3.3.2 Relevantní rozhodnutí soudů, stanoviska orgánů dohledu nad ochranou osobních údajů

Evropský parlament se již v usnesení ze 20. listopadu 2008[535] vyjádřil kriticky k používání jmenné evidence cestujících pro účely vynucování práva. Konkrétně vyjádřil „*politování nad tím, že chybí přesné vymezení účelu, které představuje základní záruku při ukládání restriktivních opatření*“, a dále uvedl, že se domnívá, *„že jedná-li se o opatření tajeného sledování, má taková ochrana o to větší význam, jelikož v těchto případech hrozí větší riziko svévolného použití; domnívá se, že vzhledem k tomu, že stanovené účely a definice nejsou přesně formulované, a že by se měly striktně vymezit, aby systém PNR EU nemohl být právně napadnutelný*“[536].

Evropský inspektor ochrany údajů

Evropský inspektor ochrany údajů vyjádřil některé obavy ve vztahu k využití údajů jmenné evidence cestujících ve stanovisku z 9. prosince 2011 k návrhu dohody o předávání údajů PNR mezi EU a USA[537]. Zvláště vyjádřil potřebu jasně vymezit účel zpracování údajů PNR, jehož definice obsahují neurčité pojmy a výjimky, vyzval též ke zúžení seznamu kategorií předávaných údajů, včetně celkového zamezení zpracování citlivých údajů. Délku uchovávání až 5 let, resp. následně 10 let v „nečinné“ databázi označil za nepřiměřenou, kriticky zhodnotil též nedostatky v zajištění práv subjektů údajů a v úpravě dalšího předávání údajů.

Pracovní skupina WP 29

Pracovní skupina WP 29 se k využívání PNR údajů vyjádřila opakovaně, nejprve v roce 2010 ke Sdělení Evropské komise o globálním přístupu k předávání údajů PNR do třetích zemí[538] vyzvala především k využívání jiných prostředků, méně rušivých pro cestující, nežli je shromažďování a zpracování údajů všech cestujících, zpochybnila též užitečnost

---

[535] Evropský parlament. *Usnesení Evropského parlamentu ze dne 20. listopadu 2008 o návrhu rámcového rozhodnutí Rady o používání jmenné evidence cestujících (PNR) pro účely vynucování práva.* [online] [cit. 24.2.2024]. Dostupné z www.europarl.europa.eu.

[536] K tomuto viz též kapitola Impact on PNR systems ve studii BOEHM, Franziska, COLE, Mark D. *Data Retention after the Judgement of the Court of Justice of the European Union.* Münster/Luxembourg, 30 June 2014. [online]. 2014. [cit. 15.1.2024].

[537] Evropský inspektor ochrany údajů. *Stanovisko Evropského inspektora ochrany údajů k návrhu rozhodnutí Rady o uzavření Dohody mezi Spojenými státy americkými a Evropskou unií o využívání jmenné evidence cestujících a o jejím předávání Ministerstvu vnitřní bezpečnosti Spojených států.* 9. prosince 2011. [online] [cit. 24.2.2024]. Dostupné z https://eur-lex.europa.eu/legal-content.

[538] ARTICLE 29 – DATA PROTECTION WORKING PARTY. *Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries. WP 178.* Adopted on 12 November 2010. [online]. 2010. [cit. 24.2.2024].

profilování údajů o cestujících ve velkém měřítku. Ve stanovisku z roku 2011 se WP 29 vyjadřovala již k návrhu Směrnice o využívání údajů PNR[539]. WP 29 zde v prvé řadě zopakovala své dlouhodobé pochybnosti o potřebě a proporcionalitě PNR systému, nejasným je dle WP 29 již zamýšlený cíl, totiž zda je jím boj proti závažné nadnárodní trestné činnosti zahrnující terorismus, nebo pouze boj proti terorismu a trestným činům souvisejícím s terorismem. Analýzu dopadu připravenou Evropskou komisí hodnotí WP 29 jako nedostatečnou a zdůrazňuje, že prevence terorismu a závažné trestné činnosti jakožto účel sama o sobě neznamená naplnění požadavků nezbytnosti a proporcionality. Před zavedením PNR je dle WP 29 nutno analyzovat správné fungování stávajících systémů zavedených po zrušení hraničních kontrol mezi státy Schengenského prostoru, WP 29 zejména zdůrazňuje absenci vyhodnocení účinnosti dosavadní Směrnice API a národních právních předpisů k jejímu provedení. K naplnění principu proporcionality by boj proti terorismu a závažné trestné činnosti neměl umožňovat masové sledování a dohled všech leteckých cestujících, WP 29 proto vyjádřila vážné pochybnosti o proporcionalitě systematického porovnávání údajů všech cestujících proti předem stanoveným kritériím a nespecifikovaným databázím. Opatření, která nemohou zajistit ochranu práv a svobod cestujících, jsou přiměřená pouze, pokud jsou zavedena jako dočasná opatření v případě konkrétní hrozby, což však není případ posuzovaného návrhu. WP 29 především nezaznamenala žádné statistiky zobrazující poměr mezi počtem nevinných cestujících, jejichž údaje PNR byly shromážděny, a počtem případů vymáhání práva založených na těchto údajích PNR. Dobu uchování údajů v délce 5 let hodnotí WP 29 jako nepřiměřeně dlouhou, také maskování údajů považuje WP 29 pouze za snahu o minimalizaci údajů, nejde však o jejich anonymizaci; data osob, které nejsou podezřelé, by proto měly být vymazány. Konečně také seznam zpracovávaných údajů PNR nepovažuje WP 29 za podložený analýzou nezbytnosti, navíc obsahuje neurčité položky, jako např. „obecné poznámky“. Též ÚOOÚ zaujal již v roce 2011 k návrhu právní úpravy PNR velmi negativní stanovisko[540], argumentačně založené na obdobných obavách v oblasti ochrany osobních údajů.

[539] ARTICLE 29 – DATA PROTECTION WORKING PARTY. *Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. WP 181.* Adopted on 5 April 2011. [online]. 2011. [cit. 24.2.2024].

[540] ÚOOÚ. *Stanovisko Úřadu pro ochranu osobních údajů k Návrhu směrnice Evropského parlamentu a Rady o používání údajů jmenné evidence cestujících pro prevenci, odhalování, vyšetřování a stíhání teroristických činů a závažné trestné činnosti ze dne 9. března 2011*. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.

Soudní dvůr EU

Evropský parlament v reakci na uzavření dohody o předávání údajů PNR s Kanadou[541] požádal SDEU o posudek slučitelnosti této dohody se Smlouvou o fungování EU a s Listinou EU, jelikož dle jeho hodnocení panuje v tomto směru nejistota, zejména ve vztahu k právu jednotlivců na ochranu osobních údajů a také k právnímu základu dohody. V posudku[542] SDEU potvrdil názor Evropského parlamentu, rozhodnutí o uzavření dohody se dle hodnocení SDEU v prvé řadě přímo váže k ochraně fyzických osob při zpracovávání osobních údajů[543], ve druhé řadě se musí zakládat také na právním základě shromažďování, uchovávání, zpracovávání, analýzy a výměny příslušných informací v rámci policejní spolupráce[544]. Samotná Dohoda mezi Kanadou a EU je dle SDEU neslučitelná s články 7, 8 a 21 a čl. 52 odst. 1 Listiny EU, v rozsahu, v němž nevylučuje předávání citlivých údajů z EU do Kanady a jejich využití a uchovávání.

Pro zajištění slučitelnosti s Listinou EU musí dohoda jasně a přesně vymezit kategorie PNR údajů předávaných z EU do Kanady, založit automatizované zpracování údajů PNR na konkrétních, spolehlivých a nediskriminačních vzorcích a kritériích, při využití pouze databází provozovaných Kanadou v souvislosti s bojem proti terorismu a závažné nadnárodní trestné činnosti, také musí omezit uchovávané údaje pouze na ty cestující, u kterých existují objektivní skutečnosti zakládající domněnku o riziku těchto osob z hlediska boje proti terorismu a závažné nadnárodní trestné činnosti. Nezbytným je dle SDEU také omezení dalšího sdělování údajů PNR pouze třetím zemím se srovnatelnou úrovní ochrany či s uzavřenou adekvátní dohodou s EU a konečně též zajištění práva na individuální vyrozumění cestujících, jejichž údaje byly využity, a zavedení záruk v podobě dohledu nezávislého orgánu.

S ohledem na posudek SDEU bylo nutno návrh dohody přepracovat a teprve 4. března 2024 Evropská komise oznámila, že návrh dohody přijala a předložila Radě Evropské unie. I přes absenci dohody PNR mezi EU a Kanadou členské státy EU údaje PNR Kanadě předávají, bez právního základu EU, když předchozí dohoda byla uzavřena pouze do roku 2009[545].

[541] Dohoda byla parafována dne 6. května 2013, k podpisu došlo následně 25. června 2014.
[542] Posudek 1/15 Soudního dvora (Velkého senátu) ze 26. července 2017.
[543] Tento cíl sleduje článek 16 odst. 2 Smlouvy o fungování EU.
[544] Viz čl. 87 odst. 2 písm. a) Smlouvy o fungování EU.
[545] Tato skutečnost je zřejmá z oficiálních informací zveřejněných Evropským parlamentem. Viz European Parliament. *Transfers of passenger name records (PNR) to Canada taking place despite the absence of an EU-Canada PNR Agreement.* 24.1.2022. [online] [cit. 24.2.2024]. Dostupné z www.europarl.europa.eu.

Zásadním rozhodnutím v oblasti zpracování údajů PNR je rozsudek SDEU C-817/19[546], v němž SDEU k žádosti Ústavního soudu Belgie rozhodoval o předběžných otázkách týkajících se výkladu GDPR, Směrnice API a především Směrnice PNR. V původním řízení byl předmětem posuzování jednak zásah do práva na respektování soukromého života a práva na ochranu osobních údajů v důsledku necíleného, systematického zpracování údajů všech cestujících a jednak tvrzení, že rozšířením systému PNR na dopravu uvnitř EU dochází k nepřímému obnovení kontrol na vnitřních hranicích. SDEU v prvé řadě dospěl k závěru, že zpracování údajů dle vnitrostátních předpisů provádějících Směrnici API spadá do působnosti GDPR, zatímco zpracování dle Směrnice PNR je nutno rozdělit na zpracování prováděné útvarem pro cestující a příslušnými orgány, které spadá do působnosti Trestněprávní směrnice, a zpracování prováděné leteckými dopravci, na které se uplatní GDPR. Údaje PNR vyhodnotil SDEU jako údaje, které mohou odhalit nejen kompletní cestovní trasu a cestovní návyky, ale také vztahy mezi dvěma či více osobami či informace o finanční situaci nebo zdravotním stavu cestujících, jejich zpracování *„s sebou nese závažné zásahy do základních práv subjektů údajů“*. Po uplynutí 6 měsíců jsou sice údaje „depersonalizovány maskováním“, ovšem i poté je po dobu 5 let možno zpřístupnit úplné údaje PNR, umožňující identifikovat konkrétní osoby.

SDEU shledal určité nedostatky Směrnice PNR, zejména u některých kategorií zpracovávaných PNR údajů vymezených nejasně či u odkazu na velmi obecné kategorie trestných činů u účelu zpracování údajů PNR, tyto nedostatky lze však dle SDEU překlenout výkladem. Z tohoto důvodu SDEU neshledal důvody pro neplatnost Směrnice PNR pro její nesoulad s Listinou EU. Rozšíření povinnosti předávat údaje PNR také na všechny lety uvnitř EU však SDEU jednoznačně považuje za možné pouze v situacích, kdy členský stát na základě dostatečně konkrétních okolností zjistí, že *„čelí skutečné a aktuální či předvídatelné teroristické hrozbě“*, i v takové situaci však lze zpracování rozšířit na všechny lety uvnitř EU pouze po omezenou dobu, rozhodnutí o rozšíření navíc musí být možno podrobit účinnému přezkumu soudem či jiným nezávislým orgánem. Obdobný závěr platí dle SDEU též pro zpracování údajů o přepravě jinými prostředky nežli leteckou dopravou. Také Směrnici API je nutno vykládat tak, že se nevztahuje na lety uvnitř EU.

Účely zpracování údajů PNR jsou ve Směrnici PNR vymezeny taxativně a nelze je dle SDEU rozšiřovat vnitrostátními právními předpisy, a to ani pro činnosti zpravodajských a

[546] Rozsudek Soudního dvora (velkého senátu) ze dne 21. června 2022. Ligue des droits humains ASBL v. Conseil des ministres. C-817/19.

bezpečnostních služeb. Obdobně nelze dle SDEU údaje PNR předávat a zpracovávat pro účely zlepšení hraničních kontrol a boje proti nedovolenému přistěhovalectví. Ve vztahu k době uchovávání údajů PNR je dle SDEU nutno Směrnici PNR vykládat tak, že po uplynutí 6 měsíců lze uchovávat pouze údaje osob, u kterých předběžné posouzeni nebo případné kontroly provedené během šestiměsíční doby odhalily *„existenci objektivních skutečností, které by mohly prokázat riziko teroristických trestných činů nebo závažné trestné činnosti“*, alespoň nepřímo objektivně související s letem těchto cestujících. Směrnice PNR, vykládaná ve spojitosti s články 7, 8 a 52 odst. 1 Listiny EU, tak dle SDEU brání právním předpisům stanovícím obecnou dobu uchování údajů PNR všech cestujících bez rozdílu v délce 5 let.

EDPB

EDPB na základě tohoto rozsudku SDEU vydal prohlášení k jeho důsledkům ve vztahu k provádění Směrnice PNR v členských státech[547]. V tomto prohlášení EDPB upozornil, že SDEU v rozsudku dospěl k závěru o platnosti Směrnice PNR, současně však rozhodl, že pro zajištění souladu s Listinou EU musí být směrnice vykládána tak, že zahrnuje významná omezení zpracování osobních údajů. Z těchto omezení EDPB zdůraznil taxativní výčet účelů využití údajů PNR, použití PNR systému pouze pro teroristické činy a závažnou trestnou činnost s objektivní, alespoň nepřímou, souvislostí s leteckou přepravou cestujících, omezení aplikace směrnice na lety uvnitř EU a na jiné dopravní prostředky a nemožnost nerozlišujícího uplatňování obecné pětileté doby uchovávání údajů na všechny letecké cestující. V této souvislosti EDPB zdůraznil, že stávající systém zpracování údajů PNR v mnoha, ne-li ve většině členských států pravděpodobně není v souladu s tímto výkladem Směrnice PNR. V důsledku toho PNR systémy v celé EU dle EDPB mohou i nadále nepřiměřeně zasahovat do základních práv osob. EDPB proto vyzval členské státy k neprodlenému přijetí nezbytných kroků k zajištění souladu s Listinou EU, včetně legislativních opatření.

V mezidobí, v roce 2020, podal k SDEU celkem 3 žádosti o rozhodnutí o předběžné otázce též soud v Kolíně nad Rýnem[548]. Položené otázky se týkaly především slučitelnosti Směrnice PNR s články 7 a 8 Listiny EU, vč. dostatečné specifičnosti údajů PNR vymezených

[547] EDPB. *Statement 5/2022 on the implications of the CJEU judgement C-817/19 regarding the implementation of the Directive (EU) 2016/681 on the use of PNR in Member States.* Přijato 13. prosince 2022. [online] [cit. 24.2.2024]. Dostupné z www.edpb.europa.eu.
[548] Žádosti Amtsgericht Köln k Soudnímu dvoru EU ve věcech AC, DF a BD v. Deutsche Lufthansa AG, věci C-148/20, C-149/20 a C-150/20 ze 16., resp. 17. března 2020.

ve Směrnici PNR a paušální, jednotně stanovené doby uchovávání všech údajů PNR. Po vydání rozsudku ve věci C-817/19 se kancelář SDEU předkládajícího soudu dotázala, zda s ohledem na tento rozsudek trvá na svých žádostech o rozhodnutí o předběžné otázce, Amtsgericht Köln odpověděl, že nikoli a uvedené 3 věci tím byly ukončeny bez rozhodnutí SDEU.

3.3.3 Posouzení splnění ústavněprávních požadavků

Dle dostupných informací se Ústavní soud ČR dosud právní úpravou jmenné evidence cestujících nezabýval. SDEU však ve výše rozebíraném rozsudku C-817/19 posuzoval proporcionalitu systému PNR dle Směrnice PNR, jeho závěry je dle hodnocení autora možno využít i pro posouzení právní úpravy obsažené v právním řádu ČR v zákoně o civilním letectví a v zákoně o Policii ČR. Ve shodě se zjištěními SDEU[549] a též EDPB dle autora představuje plošné shromažďování a zpracovávání údajů jmenné evidence cestujících zásah do práva na ochranu soukromí všech leteckých cestujících z či do České republiky, vč. cestujících na letech uvnitř EU, jedná se o zpracování osobních údajů značného množství osob.

Samotný tento zásah je vymezen ve dvou výše uvedených zákonech, právní úprava dle hodnocení autora splňuje kritéria formulační přesnosti a je dostatečně předvídatelná, s dále rozvedenou výhradou vymezení využívajících orgánů v případě údajů PNR. Oprávněné orgány (tzv. využívající orgány) jsou vymezeny v zákoně o civilním letectví, a to konkrétně, s výjimkou zpravodajských služeb, jejich definice je však v dostatečné míře obsažena ve zvláštních právních předpisech. V právních předpisech upravujících činnost jednotlivých využívajících orgánů však s výjimkou Celní správy ČR není využití údajů jmenné evidence cestujících upraveno vůbec. V případě některých orgánů lze patrně na využití údajů těmito orgány do jisté míry vztáhnout obecnou úpravu využívání údajů, což však neplatí u účelu využití a dalších podmínek. Autor v tomto spatřuje nedostatek, který u těchto orgánů do určité míry narušuje výše uvedený závěr o dostatečné formulační přesnosti právní úpravy. Jedná se o nedostatek závažný, autor jej však s ohledem na celou právní úpravu zpracování údajů cestujících v letecké dopravě hodnotí pouze jako dílčí.

Cíle plošného zpracování osobních údajů leteckých cestujících, jak jsou vymezeny v zákoně o civilním letectví a v zákoně o Policii ČR, tedy zdokonalení hraničních kontrol a boj proti nedovolenému přistěhovalectví v případě údajů API a posuzování cestujících, příprava kritérií, plnění konkrétního úkolu souvisejícího s trestnou činností vymezenou

[549] Viz Rozsudek SDEU C-817/19 a též Posudek SDEU 1/15.

v zákoně o Policii ČR v případě údajů PNR sledují legitimní a obecně akceptovatelné účely sloužící veřejným zájmům. Zpracování se zde pravděpodobně týká v převážné míře osob, které neporušily žádnou právní povinnost ani nepředstavují riziko pro některý z veřejných zájmů a rovněž nepatří do kategorií osob, které vykazují vyšší míru potenciálního rizika pro některý takovýto veřejný zájem, celkově však v prvním kroku testu proporcionality lze zkoumané právní úpravy považovat za způsobilé dosáhnout vytýčených cílů.

Při zkoumání potřebnosti či nezbytnosti zásahu do práva na ochranu soukromí ve vztahu ke sledovaným, výše vymezeným cílům autor ve druhém kroku testu proporcionality zkoumal existenci alternativních postupů, umožňujících při méně intenzivním zásahu do práva na ochranu soukromí dosáhnout stejných cílů. Při vědomí dřívějších výtek WP 29 vůči shromažďování a zpracování údajů všech leteckých cestujících, kdy WP 29 upozorňovala na možnosti využívání jiných, pro cestující méně rušivých prostředků, má autor určité výhrady k naplnění kritéria potřebnosti zkoumané právní úpravy. Ani WP 29 však, s výjimkou zpracování méně invazivních údajů API, neuvedla konkrétní alternativní prostředky a postupy, tyto též nejsou autorovi známy z jiných zdrojů. S ohledem na výše uvedené autor, s jistou rezervou založenou na výše uvedených důvodech, konstatuje, že kritérium potřebnosti lze u zkoumané právní úpravy na základě dostupných informací považovat za naplněné. Při absenci byť i jen statistických údajů o míře efektivnosti zpracování a využití údajů PNR a API je však nutno upozornit na jisté pochybnosti u kritéria potřebnosti, tedy v otázce, zda se tyto systémy nestaly běžným pracovním nástrojem, využívaným nikoli toliko na základě závažných důvodů.

Ve třetím kroku testu proporcionality autor posuzoval splnění kritéria závažnosti, založeného v tomto případě na porovnání závažnosti v kolizi stojících základních práv na straně jedné a veřejných statků na straně druhé. Při tomto posouzení není možno ignorovat závěry SDEU ve výše rozebíraném rozsudku ve věci C-817/19, které je dle autora možno plně aplikovat na právní úpravu API a PNR v právním řádu ČR. Ve světle těchto závěrů je nutno konstatovat, že právní úprava ČR vykazuje některé z nedostatků, na které upozorňoval SDEU a před nimiž v návaznosti na rozsudek SDEU varoval EDPB[550]. Konkrétně lze mít pochybnosti o tom, zda účel vymezený v případě zpracování údajů PNR v zákoně o Policii ČR splňuje požadavky na míru závažnosti trestné činnosti obsažené ve Směrnici PNR a

[550] EDPB. *Statement 5/2022 on the implications of the CJEU judgement C-817/19 regarding the implementation of the Directive (EU) 2016/681 on the use of PNR in Member States.* Přijato 13. prosince 2022. [online] [cit. 24.2.2024]. Dostupné z www.edpb.europa.eu.

interpretované SDEU v uvedeném rozsudku, a to v části, v níž zákon o Policii ČR umožňuje zpracování těchto údajů v případech souvisejících s trestnou činností, *„u níž horní hranice trestní sazby odnětí svobody činí nejméně 3 roky“*[551]. Taktéž rozšíření zpracování údajů PNR na všechny lety uvnitř EU, jak je tomu v případě ČR, je v rozporu s požadavky definovanými SDEU v diskutovaném rozsudku. Konečně též doba uchování v délce 5 let se dle zákona o Policii ČR vztáhne na údaje PNR všech cestujících[552], kdy teprve po 5 letech se dále zpracovávají pouze údaje vybraných osob.

Dle ustálené judikatury je pro úspěšné naplnění kritérií proporcionality též nezbytné, aby zásahy do základních práv byly doplněny dostatečnými mechanismy účinně bránícími jejich zneužití. Nedostatečně, resp. zcela neupravené postupy ve využívání údajů PNR využívajícími orgány, jak je autor zmiňuje výše, však za takovéto záruky zneužití považovat nelze. Tyto nedostatky zkoumané právní úpravy jsou dle autorova hodnocení ve svém souhrnu natolik závažné, že znemožňují vyhodnotit tuto právní úpravu jako splňující kritérium závažnosti ve třetím kroku testu proporcionality. Nad rámec uvedeného autor upozorňuje téže na absenci veřejně dostupných informací o vyhodnocení efektivity právní úpravy PNR a též právní úpravy API v praxi, jakož i na absenci dostupných statistických údajů o míře efektivity těchto právních úprav, která do značné míry brání jak jejich vyhodnocení, tak rovněž účinné veřejné kontrole nad mechanismy API a PNR.

3.4 Plošné zpracování osobních údajů systémy dopravních kamer

Řada kamerových systémů provozovaných různými osobami, zpravidla, nikoli však výhradně, orgány veřejné moci, snímá veřejná prostranství a zaznamenává obrazový záznam, v některých případech obrazově-zvukový. Předmětem snímání jsou zpravidla osoby vyskytující se na těchto prostranstvích, v takových případech se jedná o zpracování osobních údajů. Škála účelů zpracování takovými kamerovými systémy je velmi široká a zahrnuje ochranu veřejného pořádku, bezpečnost osob, ochranu veřejného zdraví, majetku apod. Taktéž další aspekty těchto kamer jsou různorodé, v některých případech jde o zpracování nezbytná pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci či pro splnění právní povinnosti uložené správci či spravujícímu orgánu[553]. Tyto kamerové systémy navíc nejsou vždy zaměřeny na identifikaci snímaných osob.

---

[551] Viz § 84b odst. 1 zákona o Policii ČR.
[552] Viz § 84b odst. 6 zákona o Policii ČR.
[553] ÚOOÚ v Metodice k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů vydané v roce 2024 (bez bližšího časového upřesnění) řadí mezi právní předpisy připadající v takových

Jak již autor uvedl v úvodu, tato práce nemá za cíl poskytnout vyčerpávající přehled všech plošných zpracování osobních údajů, nýbrž vybrat a z ústavněprávních hledisek analyzovat dopady do práva na ochranu soukromí u těch z nich, které se jeví jak nejrozšířenější, nejzávažnější a vykazující typové rysy společné dalším obdobným zpracováním. Autor tak po analýze veřejných kamerových systémů zvolil pro další posouzení a vyhodnocení jako dostatečně reprezentativní podskupinu, kterou představují systémy dopravních kamer. Ty jsou primárně zaměřeny na snímání automobilů, zpravidla specificky na jejich identifikaci prostřednictvím SPZ. Ani tyto kamerové systémy nepředstavují zcela homogenní skupinu, jak autor ukáže dále, pro účely zkoumání zásahů do práva na ochranu soukromí jsou tak dle hodnocení autora velmi vhodným objektem.

3.4.1 Vývoj a základní vymezení, aktuální relevantní právní úprava

Jako systémy dopravních kamer autor v této práci souhrnně označuje kamerové systémy umístěné na pozemních komunikacích a snímající projíždějící vozidla, zpravidla s cílem jejich identifikace dle registrační značky (SPZ). Provozovateli těchto systémů jsou Policie ČR, obce, obecní policie, Ředitelství silnic a dálnic ČR a další osoby. Některé z těchto kamerových systémů nespadají pod působnost GDPR, nýbrž Trestněprávní směrnice, resp. ZoZOÚ, jak potvrzuje i ÚOOÚ v Metodice ke kamerovým systémům[554].

Systémy využívané Policií ČR

Oprávnění Policie ČR k využívání systémů dopravních kamer a jejich záznamů se opírá o zákon o Policii ČR, který Policii ČR opravňuje pořizovat *„zvukové, obrazové nebo jiné záznamy osob a věcí nacházejících se na místech veřejně přístupných“*, pokud je to nezbytné pro plnění jejích úkolů. Policie ČR je dle zákona obecně oprávněna v rozsahu nezbytném pro plnění svých úkolů zpracovávat informace včetně osobních údajů a dále též osobní údaje zpracovávat při plnění některých svých úkolů, *„za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech“* [555]. Zákon o Policii ČR ani jiná právní úprava nevymezuje podmínky

případech v úvahu zákon č. 273/2008 Sb., o Policii ČR, zákon č. 553/1991 Sb., o obecní policii, zákon č. 17/2012 Sb., o celní správě, zákon 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a další. ÚOOÚ. *Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů.* 2024. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.

[554] ÚOOÚ. Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů. 2024. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.

[555] § 62, § 60 a § 79 a násl. zákona č. 273/2008 Sb. o Policii ČR, ve znění pozdějších předpisů.

využívání dopravních kamerových systémů Policií ČR, konkrétní dobu uchování údajů a další, zákon o Policii ČR pouze obecně stanoví, že pokud jsou k pořizování zvukových obrazových a jiných záznamů osob a věcí na místech veřejně přístupných zřízeny *„stálé automatické technické systémy, policie informace o zřízení takových systémů vhodným způsobem uveřejní“*[556].

Policie ČR využívá systém Automatické kontroly vozidel[557], novější systém Centrální automatické kontroly vozidel (CAKV) sestávající z několika set kamer vybavených funkcí automatického rozpoznávání SPZ[558] a též některé další systémy dopravních kamer, vč. systémů měření rychlosti vozidel[559]. Zpracovávané údaje zahrnují fotografii vozidla včetně SPZ, SPZ a mezinárodní poznávací značku vozidla v textové podobě, datum, čas a místo výskytu vozidla (dle GPS souřadnic kamery), s označením směru jízdy, v případě systémů měření rychlosti též rychlost vozidla a případně i jiné údaje, například podobu osoby ve vozidle. Dle informací Policie ČR je osoba řidiče či spolujezdce zaznamenána pouze jako nahodilé zaznamenání[560], např. kamerové systémy u úsekového měření jsou však nastaveny tak, aby kromě SPZ zaznamenávaly též prostor řidiče a případně i spolujezdce. Jak potvrdil Nejvyšší správní soud, *„registrační značka silničního vozidla, jehož vlastníkem nebo provozovatelem je fyzická osoba, je osobním údajem“*[561], jako osobní údaje tak je nutno hodnotit i ostatní informace týkající se takového vozidla. Obecné oprávnění Policie ČR a též obecní policie k měření rychlosti vozidel obsahuje zákon o silničním provozu, a to za a účelem zvýšení bezpečnosti provozu na pozemních komunikacích[562].

---

[556] Viz § 62 odst. 2 zákona o Policii ČR.
[557] Policie ČR. *Automatická kontrola vozidel. Zveřejněné informace 2015*. 25. května 2015. Dostupné z www.policie.cz.
[558] Policie ČR. *Centrální automatická kontrola vozidel.* 27. září 2022. Úsekové měření rychlosti. 31. března 2022. Zveřejněné informace 2022. [online] [cit. 12.1.2023]. Dostupné z www.policie.cz.
[559] Dle Protokolu o kontrole ÚOOÚ z 15. března 2017, Čj. UOOU-09928/16-22 kontrolovaný kamerový systém Policie ČR sestával v době kontroly z několika systémů: měření úsekové rychlosti vozidel (MÚR), měření okamžité rychlosti vozidel (MOR), Systém LOOK Policie ČR, Strategické dopravní detektory (SDD), Vysokorychlostní vážení vozidel (WIM), Detekce jízdy na červenou (DTJ), Kontrolní mýtné stanice (brány) společnosti Kapsch. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
[560] Z Protokolu o kontrole ÚOOÚ z 15. března 2017, Čj. UOOU-09928/16-22 vyplývá, že *„Osoby jedoucí ve vozidle, tedy řidič a jeho spolujezdec, nejsou běžně identifikovatelné.“* [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
[561] Nejvyšší správní soud ČR takto v rozsudku sp. zn. 1 As 387/2019-56 ze 13. srpna 2020 rozhodl ve vztahu k definici osobního údaje v zákoně č. 101/2000 Sb. o ochraně osobních údajů, s ohledem na definici osobního údaje v GDPR, která je v tomto směru srovnatelná, lze z tohoto rozhodnutí i nadále vycházet. Obdobně též Agentura Evropské unie pro základní práva a Rada Evropy. *Příručka evropského práva v oblasti ochrany osobních údajů.* 2021. [online] [cit. 18.3.2024]. Dostupné z www.prd-echr.coe.in.
[562] Viz § 79a zákona č. 361/2000 Sb. o provozu na pozemních komunikacích a o změnách některých zákonů, ve znění pozdějších předpisů (zákon o silničním provozu).

Doba uchování fotografie vozidla v CAKV je dle informací zveřejněných Policií ČR šest měsíců, u dalších údajů v informačním systému CAKV jeden rok. V systému Automatická kontrola vozidel je u zařízení provozovaných Policií ČR doba uchování *„datové věty o rozpoznaných registračních značkách“* nastavena na 5 let[563]. Tyto doby uchování a jejich konkrétní délka nejsou stanoveny obecně závaznými právními předpisy. Jak vyplývá z informací zveřejněných Policií ČR, zaznamenává a uchovává Policie ČR *„i údaje o registračních značkách, u nichž v době zaznamenání nemusí být ještě známa konkrétní souvislost s úkoly tohoto bezpečnostního sboru“*, s ohledem jejich možné využití pro plnění úkolů Policie ČR[564]. Zákon o Policii ČR ukládá Policii ČR ve vztahu k pořizování záznamů povinnost vhodným způsobem uveřejnit informace o zřízení stálých automatických systémů k pořizování záznamů.

Systémy využívané dalšími osobami

Obdobně jako zákon o Policii ČR, v případě obecní policie obsahuje zákon o obecní policii velmi stručnou a dosti obecnou právní úpravu, opravňující obecní policii ke zpracovávání osobních údajů, *„které potřebuje k plnění úkolů podle tohoto nebo zvláštního zákona“* a dále též specificky k pořizování zvukových, obrazových nebo jiných záznamů z míst veřejně přístupných, je-li to potřebné pro plnění úkolů obecní policie podle zákona o obecní policii nebo podle jiného zákona, a také k poskytnutí osobních údajů *„policii, orgánům obce a dalším orgánům veřejné moci, je-li to nutné k plnění jejich úkolů“*; taktéž obecní policie je povinna vhodným způsobem uveřejnit informace o zřízení stálých automatických technických systémů k pořizování takových záznamů[565]. Zmiňovaný zákon o silničním provozu stanoví na obecné úrovni oprávnění obecní policie (spolu s oprávněním Policie ČR) měřit rychlost vozidel, pro obecní policii stanoví omezení, dle kterého obecní policie měří rychlost vozidel výhradně na místech určených Policií ČR a postupuje při tomto měření v součinnosti s Policií ČR.

Z dalších orgánů a osob zmiňovaných ve zmiňované Metodice ÚOOÚ k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů taktéž zákon o Celní správě ČR obsahuje oprávnění celníka k pořizování obrazových a dalších

[563] Policie ČR. *Rozpoznávání registračních značek. Zveřejněné informace 2015.* 26. ledna 2015. [online] [cit. 12.1.2023]. Dostupné z www.policie.cz.
[564] Policie ČR. *Automatická kontrola vozidel. Zveřejněné informace 2015.* 25. května 2015. [online] [cit. 12.1.2023]. Dostupné z www.policie.cz.
[565] Viz § 24a a § 24b zákona č. 553/1991 Sb. o obecní policii, ve znění pozdějších předpisů.

záznamů, za podmínky nezbytnosti pro plnění úkolů celníka a také oprávnění orgánů celní správy zpracovávat osobní údaje, včetně zvláštních kategorií osobních údajů nezbytných pro výkon jejich působnosti a zpracovávat osobní údaje za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů a zajištění vnitřní bezpečnosti[566]. Autor však v tomto případě nepředpokládá, že by se jednalo o dopravní kamerové systémy. Autor si taktéž není vědom dalších relevantních úprav upravujících využívání dopravních kamerových systémů.

Zařízení pro kontrolu úhrady časového poplatku za užití komunikace

Specifickým systémem dopravních kamer je systém zařízení pro kontrolu úhrady časového poplatku za užití pozemní komunikace (tento časový poplatek je běžně označován jako dálniční známka). Zákon o pozemních komunikacích obsahuje od roku 2021 vymezení Evidence vozidel v systému časového zpoplatnění a navazující právní úpravu[567], do té doby v ČR podobný systém neexistoval a „dálniční známky“, resp. časové poplatky za užití pozemní komunikace a jejich úhrady u konkrétních vozidel nebyly centrálně evidovány. Při úhradě časového poplatku se v této evidenci zaznamenají: státní poznávací značka vozidla, stát registrace vozidla, počátek a konec období uhrazeného časového poplatku, pohon vozidla zemním plynem nebo biometanem, datum a čas úhrady a adresa elektronické pošty nebo telefonní číslo, byly-li sděleny.

Původní návrh Ministerstva dopravy počítal i se zaznamenáváním dalších, velmi konkrétních důvodů osvobození, zahrnujících velmi specifické údaje pro účely evidence osvobození od zpoplatnění, vč. údajů o těžce zdravotně postižených občanech či o nezaopatřených dětech léčených pro onemocnění zhoubným nádorem nebo hemoblastosou, obsahující i jejich přesnou identifikaci, čísla a platnost průkazů ZTP nebo ZTP/P. Návrh v této podobě nebyl schválen, v zákoně jsou obsaženy pouze tyto důvody osvobození. Správcem evidence vozidel je Státní fond dopravní infrastruktury, který zajistí dálkový a nepřetržitý přístup k údajům obsaženým v evidenci taxativně vymezeným orgánům: Ministerstvu vnitra, Policii ČR, Generální inspekci bezpečnostních sborů a orgánům Celní správy České republiky[568]. Zařízení pro kontrolu úhrady časového poplatku, označovaná jako

[566] Viz § 36, § 56 a násl. a § 60 a násl. zákona č. 17/2012 Sb. o Celní správě České republiky, ve znění pozdějších předpisů.
[567] Evidence vozidel v systému časového zpoplatnění byla do zákona č. 13/1997 Sb. o pozemních komunikacích, ve znění pozdějších předpisů vložena zákonem č. 227/2019 Sb., kterým se mění zákon č. 13/1997 Sb., o pozemních komunikacích, ve znění pozdějších předpisů, a další související zákony, viz § 21c.
[568] Viz § 21c odst. 3 a 5 zákona o pozemních komunikacích, ve znění pozdějších předpisů.

„videodetekce“ zaznamenávají údaje o vozidlech projíždějících konkrétními úseky zpoplatněných komunikací.

Účely zpracování údajů

Policie ČR označuje účely dopravních kamerových systémů, které využívá, tedy i účely zpracování osobních údajů, jako plnění úkolů Policie České republiky při zajišťování veřejného pořádku, pátrání po osobách a věcech a při odhalování a objasňování trestné činnosti. U některých systémů je sledovaným účelem kontrola dodržování pravidel provozu na pozemních komunikacích (např. detekce jízdy křižovatkou či silničním úsekem při červeném signálu semaforu), obdobně též u systémů měření rychlosti projíždějících vozidel dle zákona o silničním provozu, kde zákonem vymezeným účelem je u Policie ČR i u obecní policie *„zvýšení bezpečnosti provozu na pozemních komunikacích*“[569]. Specifickým účelem je kontrola úhrady časového poplatku za užití pozemní komunikace v případě kamerových systémů a zařízení určených k této kontrole.

Orgány oprávněné vyžádání a využití údajů

Orgánem oprávněným k využití údajů ze záznamů dopravních kamerových systémů je v prvé řadě Policie ČR. Není však orgánem jediným, zákon o Policii ČR opravňuje Policii ČR předávat informace, *„které získala při plnění svých úkolů“*, záznamy kamerových systémů nevyjímaje, ostatním orgánům veřejné správy[570], bez taxativního výčtu orgánů takto oprávněných záznamy obdržet, pouze s omezením nezbytnosti pro plnění úkolů v rámci působnosti těchto orgánů[571]. Mezi tyto orgány tak patří např. i soudy, které jsou dle hodnocení Policie ČR[572] oprávněny vyžadovat od orgánů Policie ČR v rámci součinnosti všechny údaje zpracovávané v systému CAKV, a to jak pro trestní řízení, tak pro řízení dle občanského soudního řádu či zákona o zvláštních řízeních soudních, toto hodnocení lze dle autora

[569] Viz § 79a zákona o silničním provozu, ve znění pozdějších předpisů.
[570] Policie ČR. *Rozpoznávání registračních značek. Zveřejněné informace 2015.* 26. ledna 2015. Dostupné z www.policie.cz.
[571] Zákon o Policii ČR vymezuje předávání informací v několika ustanoveních, obecně v § 78 odst. 1, kde uvádí několik konkrétních orgánů, kterým Policie ČR předává informace (národní člen Eurojustu, Národní bezpečnostní úřad, Národní úřad pro kybernetickou a informační bezpečnost, zpravodajské služby České republiky, Vojenská policie, ministerstvo vnitra, Vězeňská služba České republiky, Celní správa České republiky), s dovětkem *„a dalším orgánům veřejné správy“*, bez upřesnění. Na toto ustanovení navazuje § 80 vymezující podmínky předávání osobních údajů zpracovávaných Policií ČR dle § 79 odst. 1 *„za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech.“*
[572] Policie ČR. *Centrální automatická kontrola vozidel. Zveřejněné informace 2022*. 27. září 2022. [online] [cit. 12.1.2023]. Dostupné z www.policie.cz.

vztáhnout i na další kamerové systémy; Policie ČR je vztahuje i na předávání záznamů zařízení pro kontrolu úhrady časového poplatku za užití komunikace. V případě evidence vozidel v systému časového zpoplatnění jsou orgány oprávněné k přístupu k údajům obsaženým v evidenci vymezeny taxativně v zákoně o pozemních komunikacích, jak autor uvádí výše.

Kritérium plošného zpracování

Většinu systémů dopravních kamer lze hodnotit jako systémy provádějící plošné zpracování osobních údajů značného množství osob, systémy jsou užívány ve vztahu ke všem projíždějícím vozidlům. Tento závěr potvrzuje i výše uvedená informace Policie ČR, dle které zaznamenává a uchovává i údaje o vozidlech bez jakékoli souvislosti s úkoly Policie ČR, pro možné pozdější využití[573]. Výjimkou jsou kamerové systémy měření okamžité rychlosti vozidel, které autor jako plošné zpracování osobních údajů nehodnotí. Tyto systémy totiž zaznamenávají pouze vozidla, která v konkrétním místě překročí nejvyšší povolenou rychlost, na rozdíl od kamerových systémů úsekového měření rychlosti, zaznamenávajících všechna vozidla vjíždějící do měřeného úseku a vyjíždějící z něj, pro zjištění průměrné rychlosti vozidel v měřeném úseku. Za zmínku v této souvislosti stojí situace v Německu, kde byl v letech 2018-2020 a 2021-2024 v provozu jediný testovací systém úsekového měření rychlosti ve spolkové zemi Dolní Sasko, počátkem roku 2024 byl však vypnut, z důvodu ochrany osobních údajů. Tento systém byl v Německu dlouho předmětem právních sporů, právě s ohledem na zásah do práva na informační sebeurčení[574]. Tytéž důvody vedly k existenci pouze tohoto jediného systému úsekového měření rychlosti vozidel v Německu.

3.4.2 Relevantní rozhodnutí soudů, stanoviska orgánů dohledu nad ochranou osobních údajů

ÚOOÚ

Dle dostupných informací ÚOOÚ provedl kontroly kamerových systémů měření rychlosti využívaných Policií ČR v roce 2009 a 2017. V prvním případě[575] byly předmětem kontroly systémy úsekového měření rychlosti a kamerový systém sledující průjezdy na červenou. ÚOOÚ v tomto případě ve vztahu k úsekovému měření rychlosti konstatoval, že

[573] Policie ČR. *Automatická kontrola vozidel. Zveřejněné informace 2015.* 25. května 2015. Dostupné z www.policie.cz.
[574] Německý automobilový klub ADAC k tomuto poznamenává, že *„V případě kontrol rychlosti je přechod od kontroly k monitorování plynulý.“* Viz ADAC. *Section Control eingestellt: Alle Infos zum Tempo-Messverfahren.* 16.1.2024. [online] [cit. 18.3.2024]. Dostupné z www.adac.de. (Pozn. přeloženo autorem.)
[575] ÚOOÚ. *Zpracování osobních údajů v souvislosti s měřením rychlosti vozidel*. bez uvedení data. [online] [cit. 12.1.2024]. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz, sekce Kontroly za rok 2009.

„*tento způsob měření rychlosti však současně zpracovává i osobní údaje osob, které se nedopustily přestupku, a proto je toto nepřetržité sledování všech projíždějících vozidel silným zásahem do soukromí jednotlivce*“, na základě tohoto zjištění však dospěl pouze k závěru, že *„…jeho umístění musí být podloženo skutečnou nebezpečností daného úseku vyvolávající potřebu stálého dozoru“* a uzavřel, že *„Kontrolovaný subjekt*[576] *je správcem těchto údajů a uchovává je v přiměřené lhůtě, odpovídající přestupkovému zákonu“*. Autor není přesvědčen o správnosti tohoto závěru ÚOOÚ, když v případě osobních údajů osob, které se nedopustily přestupku, není jejich zpracování odůvodněné a v souladu s platnou právní úpravou[577] by takové osobní údaje měly být neprodleně vymazány, ze zprávy o kontrole však není zřejmé, v jaké délce byla doba zpracování nastavena. ÚOOÚ v daném případě pouze uložil *„zcela odstranit obrazovou informaci o spolujezdci, a tím nahradit sporné rozmazání jeho obličeje na fotografii“*, a to definováním oblasti *„zakrytí nad maskou vozidla v levé polovině odpovídající části vozidla se spolujezdcem“*. Ve druhém případě ÚOOÚ posuzoval systémy dopravních kamer využívaných Policií ČR, včetně jejich základu v relevantních obecně závazných i interních předpisech Policie ČR, jejich zabezpečení a technicko-organizačních opatření. Dospěl přitom k závěru, že nebylo zjištěno porušení zákona.

Kromě kontrol se ÚOOÚ vyjádřil kriticky k legislativnímu procesu novely nespecifikovaného zákona týkajícího se měření rychlosti na silnicích v roce 2007, kdy ÚOOÚ nebyl konzultován a ve schváleném znění schází *„přesný popis, jak bude nakládáno se záznamy o měření rychlosti“*[578]; z informace není zřejmé, zda ÚOOÚ v této věci podnikl jakékoli další kroky.

Ústavní soud ČR

Ústavní soud ČR se zabýval úsekovým měřením rychlosti v roce 2019[579], usnesením odmítl ústavní stížnost stěžovatelky proti předchozím rozsudkům správních soudů. Ústavní soud ČR se však v této věci zabýval možným zásahem do práva vlastnit majetek a do práva na soudní ochranu, stěžovatelka nenamítala zásah do práva na ochranu soukromí, tento návrh tedy nebyl ani předmětem posuzování. Za relevantní ve vztahu k tématu této práce autor považuje, že Ústavní soud ČR se v usnesení stručně vyjádřil také k účelu sledovanému

[576] ÚOOÚ dle zjištění autora často používá pro osoby správců nepřesný termín „subjekt“, který je snadno zaměnitelný s definovaným termínem „subjekt údajů“.
[577] V době posuzovaného zpracování § 5 odst. 1 písm. e) zákona č. 101/2001 Sb. o ochraně osobních údajů, v současné době obdobně zákon č. 110/2019 Sb. o zpracování osobních údajů.
[578] ÚOOÚ. *Výroční zpráva 2007.* [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
[579] Usnesení Ústavního soudu ČR sp. zn. III.ÚS 2478/19 ze 3. září 2019.

úsekovým měřením rychlosti v posuzovaném případě, shledal, že jím bylo naplnění zájmu na zajištění bezpečnosti silničního provozu.

Význam vymezení účelu měření rychlosti Ústavní soud ČR zmínil obiter dictum také v nálezu Pl. ÚS 15/16[580], v němž uvedl, že *„Orgány veřejné moci jsou proto povinny usilovat o to, aby rozmístění automatizovaných technických prostředků skutečně bránilo vzniku škodlivých následků spojených s porušováním povinností řidiče, a aby naopak nesloužilo především naplňování obecních rozpočtů, jejichž jsou pokuty, respektive určené částky příjmem.“* Ani v tomto případě však Ústavní soud ČR neposuzoval možný zásah do práva na ochranu soukromí. Policie ČR závěry těchto dvou rozhodnutí zohlednila v Metodice určování míst pro měření rychlosti obecní policií[581], ani zde však možné zásahy do práva na ochranu soukromí nezohledňuje.

Ve vztahu k předávání údajů ze záznamů dopravních kamerových systémů využívaných Policií ČR dalším orgánům veřejné správy považuje autor za zásadní nález Ústavního soudu ČR sp. zn. IV.ÚS 2621/22[582]. V tomto případě se jednalo o možné získání kamerových záznamů z dopravních kamer správcem daně od Policie ČR a jejich využití pro potřeby řízení vedeného správcem daně ve věci nadměrného odpočtu daně z přidané hodnoty u automobilu uplatněného podnikající fyzickou osobou. Správce daně – Finanční úřad pro Ústecký kraj z důvodu pochybností v konkrétním případě požádal Policii ČR o poskytnutí informací o pohybu automobilu podnikající fyzické osoby dle záznamů dopravních kamerových systémů v časovém období specifikovaném v žádosti. Policie ČR správci daně požadované informace předala. Podnikající fyzická osoba tento postup napadla nejprve odvoláním k finančnímu ředitelství a poté ve správním soudnictví postupně u Krajského soudu v Ústí nad Labem a posléze u Nejvyššího správního soudu, které žalobu a následnou kasační stížnost zamítly[583], s odůvodněním, že neshledali žádná pochybení správce daně.

Dle hodnocení Nejvyššího správního soudu byl správce daně oprávněn požadovat od Policie ČR záznamy z dopravních kamer, jelikož *„šlo o údaje nezbytné pro správu daní a policie je subjektem povinným takové údaje správci daně na výzvu poskytnout“*. Ze stručného odůvodnění Nejvyššího správního soudu je zřejmé, že nevzal v úvahu odlišnost mezi původním účelem zpracování kamerových záznamů, kterým je zabezpečení veřejného

[580] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 15/16 ze 16. května 2018.
[581] Policie ČR. *Metodika určování míst pro měření rychlosti obecní policií podle § 79a zákona č. 361/2000 Sb.* 10. srpna 2023. [online] [cit. 12.1.2023]. Dostupné z www.policie.cz.
[582] Nález Ústavního soudu ČR ze dne 14. 2. 2023 sp. zn. IV.ÚS 2621/22.
[583] Rozsudek Krajského soudu v Ústí nad Labem ze dne 1. 6. 2020, sp. zn. 15 Af 2/2017–30, rozsudek Nejvyššího správního soudu ČR ze dne 21. července 2022 sp. zn. 9 Afs 147/2020-34.

pořádku v dopravě, a účelem, pro který záznamy vyžádal a využil správce daně, tedy účel správy daní. Původní účel stanoví Policii ČR zákon[584], dle hodnocení autora není možno jej nad rámec zákona rozšiřovat. Nejvyšší správní soud se v rozsudku nezabýval možným zásahem do práva na ochranu soukromí dotčené podnikající fyzické osoby v důsledku využití kamerových záznamů pro odlišný účel a přípustností takového zásahu, přestože to podnikatel v kasační stížnosti namítal.

Ústavní soud ČR k ústavní stížnosti dotčeného podnikatele rozhodl, že *„Nejvyšší správní soud nedostál své povinnosti náležitě odůvodnit ústavní stížností napadený rozsudek“* a rozsudkem tak *„bylo porušeno stěžovatelovo právo na soudní ochranu zaručené v čl. 36 odst. 1 a 2 Listiny základních práv a svobod.“* Ústavní soud ČR v nálezu zdůraznil, že *„stěžovatel nenamítal, že policie pořídila záznamy na výzvu správce daně, ale že je zpracovala až na jeho výzvu“*. Při použití definice zpracování, jakožto jakékoliv operace nebo soustavy operací systematicky prováděné s osobními údaji, Ústavní soud ČR konstatoval, že minimálně předání záznamů správci daně *„zjevně nemohlo být učiněno pro vlastní účely policie“*. Tuto námitku však Nejvyšší správní soud nevypořádal a Ústavní soud ČR tak jeho rozsudek zrušil pro nepřezkoumatelnost. Přitom upozornil na nutnost posoudit danou otázku komplexně, se všemi možnými dopady do ústavně zaručených práv a dodal, že *„Dospěje-li (NSS) k závěru, že takto policie může postupovat, bude třeba uvážit, zda takové oprávnění není v rozporu s některými z ústavně zaručených práv, zejména s právem na soukromí a právem na informační sebeurčení podle čl. 10 odst. 2 a 3 Listiny“*.

Nejvyšší správní soud následně rozsudkem z prosince 2023[585] zrušil rozsudek Krajského soudu v Ústí nad Labem i rozhodnutí Odvolacího finančního ředitelství a věc mu vrátil k dalšímu řízení. Nejvyšší správní soud rozhodnutí odůvodnil odkazem na § 78 zákona o Policii ČR, který umožňuje předávání informací jiným orgánům veřejné správy, *„je-li to nezbytné pro plnění úkolů v rámci jejich působnosti“*, a na § 80 téhož zákona obsahujícího speciální právní úpravu předávání a zpřístupňování osobních údajů, kterými mohou být i kamerové záznamy, u nichž právní úprava v § 80 odst. 1 písm. a) váže předávání na podmínku „stanoví-li tak zákon“. Správa daní dle Nejvyššího správního soudu *„spadá do působnosti orgánů finanční správy jako správců daně“*[586], přičemž podle daňového řádu[587] *„mají*

[584] § 60 odst. 1 v návaznosti na § 62 odst. 1 zákona č. 273/2008 Sb. o Policii ČR, ve znění pozdějších předpisů.
[585] Rozsudek Nejvyššího správního soudu ČR ze dne 14. prosince 2023 sp. zn. 9 Afs 147/2020–87.
[586] Dle § 10 odst. 1 zákona č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů, a § 1 odst. 1 zákona č. 456/2011 Sb., o Finanční správě České republiky, ve znění pozdějších předpisů.
[587] § 57 odst. 1 písm. d) zákona č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů.

povinnost poskytnout údaje na základě vyžádání správce daně […] orgány veřejné moci a osoby, které […] zpracovávají jiné údaje nezbytné pro správu daní", mezi které patří i Policie ČR. Jak zákon o Policii ČR, tak i daňový řád však dle obsahují *„podmínku nezbytnosti údajů pro správu daní"*[588] a jelikož již samotné poskytnutí těchto údajů *„potenciálně představuje zásah do práva na soukromí, příp. též práva na informační sebeurčení",* je třeba, aby *„takový zásah obstál v testu proporcionality"*. Dle Nejvyššího správního soudu *„Použití kamerových záznamů o pohybu vozidla daňového subjektu jistě může být vhodné ve vztahu ke správnému zjištění a stanovení daně v tom ohledu, že je způsobilé ověřit užívání vozidla daňovým subjektem"*, není však pro správu daní nezbytné. Nejvyšší správní soud proto konstatoval, že *„správce daně nebyl oprávněn záznamy od Policie ČR vyžadovat a použít je jako důkazní prostředek v daňovém řízení"*, výslovně tyto záznamy označil za nezákonně získané. Jelikož dle Nejvyššího správního soudu postup správce daně neobstojí v posouzení nezbytnosti, soud se již nezabýval otázkou přiměřenosti v užším smyslu ve třetím kroku testu proporcionality.

Německo – Vrchní správní soud Dolního Saska, Spolkový ústavní soud Německa

S ohledem na zvláštní pozornost, kterou kamerovým systémům úsekových měření rychlosti vozidel věnují příslušné orgány v Německu, zvláště s ohledem na problematiku ochrany osobních údajů, autor považuje za vhodné na tomto místě zmínit relevantní soudní rozhodnutí německých soudů v této oblasti, zejména Spolkového ústavního soudu Německa.

V rámci přípravy výše zmiňovaného testovacího provozu systému úsekového měření v Německu, ve spolkové zemi Dolní Sasko byl již v roce 2014 v této věci konzultován i zemský pověřenec pro ochranu osobních údajů Dolního Saska[589]. Ten formuloval základní zásady ochrany osobních údajů, které musí takovýto systém splňovat[590], autor je považuje za aplikovatelné i ve vztahu k podobným zařízením v ČR. Zařízení smí být v prvé řadě využíváno pouze pro účely zjišťování překročení rychlosti, získané údaje nesmějí být využity pro žádný jiný účel. Určení, zda se jedná o přestupek překročení rychlosti, musí být provedeno okamžitě, musí přitom být technicky zajištěno, že v případech, kdy dle výpočtu průměrné rychlosti nedošlo k překročení rychlostního limitu, jsou údaje okamžitě vymazány beze stopy a bez možnosti zjištění vazby na konkrétní osoby. Pro splnění požadavků ochrany osobních údajů byl poté systém v Dolním Sasku nastaven tak, že pokud výpočet průměrné rychlosti mezi

[588] § 78 zákona o Policii ČR i 57 odst. 1 písm. d) daňového řádu.
[589] Landesbeauftragte für den Datenschutz Niedersachsen.
[590] Viz Niedersächsisches Ministerium für Inneres und Sport. *Verkehrsüberwachung durch Abschnittskontrolle.* 8. 12. 2020. [online] [cit. 18.3.2024]. Dostupné z www.innenministerkonferenz.de.

měřícími body neukázal překročení povolené rychlosti, byly údaje okamžitě vymazány, aby z nich nebylo možno vyvozovat žádné závěry o vozidle nebo řidiči. Systém úsekového měření v Dolním Sasku byl též předmětem rozhodování správních soudů, v první instanci soud rozhodl, že se jedná o zásah do základního práva na informační sebeurčení, toto rozhodnutí však následně zvrátil Vrchní soud Dolního Saska, který žalobu zamítl[591] a potvrdil, že relevantní obecně závazný právní předpis je v daném případě dostatečným právním základem. Spolkový ústavní soud Německa zamítl následnou ústavní stížnost v této věci[592].

Spolkový ústavní soud Německa se možnými zásahy do práva na ochranu soukromí, resp. do práva na informační sebeurčení prostřednictvím dopravních kamerových systémů zabýval v několika případech, ve třech rozhodnutích z 18. prosince 2018[593] posuzoval z těchto aspektů kamerové systémy automatického rozpoznávání SPZ. V nálezu BvR 142/15 Spolkový ústavní soud Německa především rozhodl, že *„automatické rozpoznávání registračních značek představuje zásah do základního práva na informační sebeurčení každé osoby, jejíž registrační značky jsou automaticky zaznamenány, a to i v případě, že výsledkem je "žádná shoda" a údaje jsou okamžitě vymazány“*. Automatické rozpoznávání registračních značek automobilů pak soud z hlediska závažnosti zásahu do základních práv považuje za srovnatelné s policejními opatřeními při prohlídce osob nebo věcí, musí tedy sloužit k ochraně srovnatelně závažných veřejných zájmů. Automatické rozpoznávání registračních značek používané na bázi náhodných prohlídek vyžaduje dle Spolkového ústavního soudu zvláštní odůvodnění. V případě boje proti trestné činnosti, kterou usnadňuje neexistence kontrol na vnitřních hranicích EU, jsou podmínky takového zvláštního odůvodnění naplněny, pokud opatření automatického rozpoznávání registračních značek mají jasnou věcnou i prostorovou souvislost se státní hranicí.

Ve dvou navazujících nálezech sp. zn. 1 BvR 2795/09 a 1 BvR 3187/10 Spolkový ústavní soud Německa z výše uvedených důvodů prohlásil za protiústavní a neplatné některé části právních předpisů spolkových zemí Hesensko a Bádensko-Württembersko, především v částech, ve kterých tyto předpisy neomezují kontrolu registračních značek na ochranu právních zájmů přinejmenším značné váhy, místa pro provádění kontrol nejsou dostatečně

[591] Rozsudek 12. senátu Vrchního správního soudu Dolního Saska sp. zn. 12 LC 79/19 ze dne 13. listopadu 2019, předchozí rozsudek Správního soudu v Hannoveru sp. zn. 7 A 849/19ze dne 12. března 2019. Podrobně viz tisková zpráva Vrchního správního soudu Dolního Saska. *Verkehrsüberwachung mittels „Abschnittskontrolle“ (= Section Control) auf der B 6 ist rechtmäßig*. 14. listopadu 2019.
[592] Spolkový ústavní soud Německa. 1 BvR 2356/20 z 11. ledna 2021.
[593] Spolkový ústavní soud Německa. Nálezy prvního senátu sp. zn. BvR 142/15, 1 BvR 2795/09 a 1 BvR 3187/10 z 18. prosince 2018.

určitě omezena ve vztahu ke státním hranicím a neomezují zpracování registračních značek pro další účely na ochranu právních zájmů přinejmenším značné váhy nebo srovnatelně důležitého veřejného zájmu.

3.4.3 Posouzení splnění ústavněprávních požadavků

Výše v této kapitole autor dospěl k závěru, že zpracování osobních údajů prováděné většinou dopravních kamerových systémů lze hodnotit jako plošné zpracování, které se uplatní u všech projíždějících vozidel a představuje zásah do práva na ochranu soukromí značného množství osob. V rámci posouzení splnění ústavněprávních požadavků autor v prvé řadě zkoumal, zda tento zásah je zákonem předvídaný. Právní základ zpracování osobních údajů dopravními kamerovými systémy je obsažen v zákoně o Policii ČR, v zákoně o obecní policii a specificky u zařízení pro kontrolu úhrady časového poplatku za užití komunikace v zákoně o pozemních komunikacích. S výjimkou zákona o pozemních komunikacích se však jedná o právní úpravy velmi stručné, které využívání kamerových systémů upravují dosti obecným způsobem, absentuje v nich podrobnější vymezení podmínek využití záznamů těchto kamer, doby uchování a dalších podmínek zpracování osobních údajů, včetně podmínek předání zpracovávaných údajů dalším orgánům a osobám a účelů takového předání. Jak je přitom zřejmé z výše uvedených informací zveřejněných Policií ČR, tyto systémy v některých případech zpracovávají též údaje osob, které nemají konkrétní souvislost s úkoly Policie ČR, důvodem je jejich možné budoucí využití[594], což však v případě dopravních kamerových systémů představuje zpracování osobních údajů pro neurčitý účel. Navíc je nutno vzít v úvahu, že záznamy kamerových systémů dopravních kamer zpravidla obsahují mimo jiné též údaje o výskytu konkrétního vozidla identifikovaného na základě SPZ v určitém místě a čase, z nichž lze v řadě případů dovodit lokalizační údaje určité osoby.

<u>Dopravní kamerové systémy dle zákona o Policii ČR a zákona o obecní policii</u>

S ohledem na výše uvedené dle hodnocení autora relevantní právní úprava zákona o Policii ČR a zákona o obecní policii splňuje kritéria přesnosti a zřetelnosti formulací kladená Ústavním soudem ČR na právní úpravy umožňující zásahy do základních práv pouze u vymezení účelu využití údajů přímo Policií ČR, resp. obecní policií. Tato kritéria však právní úprava nesplňuje v případě dalších aspektů, tyto právní předpisy nelze označit za dostatečně

[594] Policie ČR. *Automatická kontrola vozidel. Zveřejněné informace 2015.* 25. května 2015. Dostupné z www.policie.cz.

předvídatelné ve vztahu k samotnému vymezení některých kamerových systémů, jako jsou systémy úsekového měření, ve vztahu k době uchovávání údajů, k vymezení orgánů oprávněných zpracovávané údaje využít a též k účelům předání údajů těmto dalším orgánům a jejich využití.

Autor v této souvislosti považuje za významné, že orgány finanční správy, jejichž zpracováním kamerových záznamů se ve výše uvedených rozsudcích zabýval Nejvyšší správní soud i Ústavní soud ČR, jsou tak orgány, které v praxi minimálně v posuzovaném případě údaje ze záznamů kamerových systémů vyžádaly a využily. Orgány finanční správy přitom však nejsou obsaženy v příkladmém výčtu orgánů v zákoně o Policii ČR[595], jimž Policie ČR předává osobní údaje, vč. kamerových záznamů dopravních kamer. Tyto orgány se tak řadí pod neurčitou množinu „dalších orgánů veřejné správy" a společně s orgány finanční správy tak mezi oprávněné orgány v případě údajů dopravních kamerových systémů patří též další nespecifikované orgány. V případě orgánů finanční správy je však zřejmé, že nejde pouze o hypotetickou možnost vyžádání a využití kamerových záznamů. Tento nedostatek autor považuje za zásadní, nevymezení oprávněných orgánů brání provedení testu proporcionality ve vztahu k nespecifikovaným orgánům veřejné správy. V tomto bodě lze poukázat na výše uvedený požadavek zemského pověřence pro ochranu osobních údajů Dolního Saska, aby zařízení smělo být využíváno pouze pro účely zjišťování překročení rychlosti, pro žádný jiný účel nesmějí být získané údaje využity; takový požadavek je dle hodnocení autora plně uplatnitelný i v právním řádu ČR.

Autor tedy přistoupil k provedení testu proporcionality zpracování záznamů dopravních kamerových systémů pouze 1. ve vztahu k jejich využití Policií ČR a obecní policií, i přes výše uvedenou výhradu vůči nedostatečnému vymezení některých specifických kamerových systémů, a též 2. ve vztahu k údajům zpracovávaným v evidenci vozidel v systému časového zpoplatnění. V prvním kroku testu autor dospěl k závěru, že zpracování těchto záznamů pro vlastní účely Policie ČR a obdobně též obecní policie splňuje kritéria vhodnosti. Záznamy dopravních kamerových systémů jsou dle hodnocení autora způsobilé dosáhnout cíl, kterým jsou úkoly Policie ČR k ochraně bezpečnosti osob a majetku a veřejného pořádku a úkoly na úseku bezpečnosti, resp. úkoly obecní policie při zabezpečování místních

[595] § 78 odst. 1 zákona o Policii ČR.

záležitostí veřejného pořádku v rámci působnosti obce a plnění dalších úkolů stanovených zákonem[596].

Ve druhém kroku testu proporcionality autor zkoumal nezbytnost zásahu do základního práva, zde práva na ochranu soukromí, ve vztahu ke sledovaným cílům a analyzoval možnost dosáhnout těchto cílů jinými opatřeními, méně zasahujícími do práva na ochranu soukromí. Obecně v případě dopravních kamerových systémů využívaných Policií ČR a obecní policií se na základě autorovi dostupných informací jeví být požadavky nezbytnosti naplněny, obdobně je tomu v případě zpracování údajů pro účely výběru a kontroly úhrady časového poplatku. V případě kamerových systémů úsekového měření rychlosti však existuje alternativní postup, který je výrazně šetrnější z hlediska zásahu do práva na ochranu soukromí. Tento postup byl v praxi reálně využit v systému provozovaném v Dolním Sasku v případě popisovaném výše a lze jej tak považovat za v praxi realizovatelný. Spočívá v nastavení systému tak, že v případech, kdy dle výpočtu průměrné rychlosti konkrétní vozidlo nepřekročilo nejvyšší rychlost povolenou v daném úseku, systém údaje okamžitě vymaže, bez možnosti jejich dalšího uchování, tento výpočet též musí být prováděn neprodleně. V důsledku toho nejsou zpracovávány údaje osob, u kterých neexistuje podezření z překročení povolené rychlosti a není u nich tedy naplněn účel zpracování údajů. Jak uvedeno výše, systémy využívané Policií ČR však dle dostupných informací takto nastaveny nejsou a zaznamenávají a uchovávají i údaje o vozidlech, která rychlostní limit nepřekročila a tyto údaje tak nemají žádnou souvislost s úkoly Policie ČR. Autorovi nejsou známy přesné informace o systémech využívaných obecní policií, jelikož tyto informace nejsou z veřejně dostupných zdrojů snadno zjistitelné. Pokud jsou však systémy obecní policie nastaveny obdobně, platí ve vztahu k nim tentýž závěr. V tomto směru tedy právní úprava zákona o Policii ČR a obdobně též zákona o obecní policii, které takovéto mechanismy nezakotvují, dle hodnocení autora nesplňují požadavky druhého kroku testu proporcionality.

Navíc nelze pominout skutečnost, že údaje úsekového měření uchovávají též jednotlivé obce, na jejichž území jsou systémy provozovány. Přesné údaje se autorovi nepodařilo z veřejně dostupných zdrojů dohledat, dle autorových odhadů je však takových obcí v současnosti velké množství, mnohdy lze mít pochybnosti o nastavení zabezpečení

[596] Zákon o Policii ČR opravňuje v § 62 odst. 1 Policii ČR pořizovat obrazové a další záznamy nezbytné *„pro plnění jejích úkolů“*, úkoly Policie ČR jsou vymezeny v § 2 téhož předpisu; zákon o obecní policii obsahuje obdobné oprávnění obecní policie potřebné pro plnění jejích úkolů v § 24b odst. 1, úkoly obecní policie pak vymezuje v § 1 odst. 2.

použitých systémů[597], doba uchování údajů taktéž není stanovena jednotně a mnohdy nejsou ani veřejně dostupné informace o provozování kamerových systémů v dostatečné míře. Z informací o již zmiňovaném pilotním provozu v Dolním Sasku vyplývá, že Policejní ředitelství v Hannoveru poskytovalo v době pilotního provozu na svých internetových stránkách informace ke zpracování osobních údajů tímto kamerovým systémem[598]. Na stránkách Policie ČR se autorovi nepodařilo nalézt souhrnnou informaci k měření rychlosti, resp. k úsekovému měření, jediné informace k této oblasti zveřejňuje Policie ČR v sekci Zveřejněné informace na svých internetových stránkách, v rámci odpovědí poskytnutých žadatelům o informace v konkrétních případech. Dle autorových poznatků není tedy možno bez vznesení dotazu zjistit informace o tomto zpracování osobních údajů, zejména zda a po jakou dobu jsou uchovávány údaje o vozidlech, která byla kamerovými systémy využívanými Policií ČR zachycena v konkrétním místě, avšak nebylo zjištěno překročení nejvyšší povolené rychlosti ani jiný přestupek. Právní úprava požadující po Policii ČR a po obecní policii „vhodným způsobem uveřejnit" informace o zřízení stálých automatických technických systémů se nejeví jako dostačující, a to tím spíše že v praxi dle hodnocení autora mnohdy není naplňována.

Splnění kritérií třetího kroku testu proporcionality je obecně možno posoudit pouze ve vztahu k právní úpravě, která splnila požadavky předchozích dvou kroků. V případě, kdy tyto požadavky splňují pouze některé části právní úpravy, je takový postup dle hodnocení autora možný za podmínky, že se jedná o části právní úpravy, které jsou oddělitelné a lze je tak samostatně posoudit. Platnou a účinnou právní úpravu je nutno v testu proporcionality posuzovat jako celek a nelze tak dospět k závěru, že některé její části v testu proporcionality obstojí a jiné nikoli. Kamerové systémy úsekového měření rychlosti, které dle hodnocení autora nesplnily kritéria druhého kroku testu proporcionality, nejsou upraveny v oddělené právní úpravě a zákon o Policii ČR, resp. zákon o obecní policii, neobsahují ve vztahu k těmto systémům specifickou úpravu, odlišnou a oddělenou od dopravních kamerových systémů využívaných Policií ČR a obecní policií.

---

[597] Jak ukazuje případ z roku 2016, kdy neznámé osoby úspěšně napadly systém zaznamenávající fotografie z kamer úsekového měření a SPZ i zachycené fotografie řidičů nahradili symbolem Alza. Viz např. FTV Prima. *Hackeři ovládli měření na D1. Pokuty můžete zahodit*. Dostupné z https://cool.iprima.cz/porady/autosalon/hackeri-ovladli-mereni-na-d1-pokuty-muzete-zahodit.

[598] Viz Niedersächsisches Ministerium für Inneres und Sport. *Rechtsgrundlage zur Abschnittskontrolle „Section Control" bestätigt: Nach OVG-Beschluss wird der Betrieb an der B 6 bei Hannover kurzfristig wieder aufgenommen.* 14. 11. 2019. [online] [cit. 18.3.2024]. Dostupné z https://www.mi.niedersachsen.de.

Autor však dospěl k závěru, že tyto systémy představují dostatečně specifický druh dopravních kamerových systémů a lze proto ve třetím kroku testu proporcionality vyhodnotit právní úpravu zákona o Policii ČR a zákona o obecní policii ve vztahu k ostatním, běžným dopravním kamerovým systémům. Při porovnání závažnosti základního práva na ochranu soukromí a veřejných statků stojících v kolizi s ním, zde tedy veřejných zájmů vymezených výše, se požadavky tohoto kroku jeví být v případě posuzovaných úprav naplněny, avšak s výhradou uvedenou výše ve vztahu k systémům úsekového měření rychlosti. Autor má v případě úpravy dopravních kamerových systémů v těchto právních úpravách pochybnosti také ohledně existence efektivních kontrolních mechanismů, které by bránily zneužití zásahů. Mezi základní předpoklady takovýchto mechanismů totiž dle hodnocení autora patří dostupné informace o používaných systémech, tento požadavek zde ovšem není splněn, jak uvedeno výše, relevantní právní úpravy jej, s ohledem na svou stručnost v dostatečné míře neupravují. Taktéž bez jednoznačného vymezení oprávněných orgánů a účelů předání a využití těmito orgány, na jejichž nedostatečnost ukázal výše uvedený případ řešený Ústavním soudem ČR v nálezu sp. zn. IV.ÚS 2621/22, a bez jednoznačně upravené doby uchování nelze dle autorova hodnocení považovat požadavek na záruky a kontrolní mechanismy za splněný. Právní úprava zákona o Policii ČR i zákona o obecní policii tak v případě dopravních kamerových systémů ve třetím kroku testu proporcionality nesplňuje jeho požadavky.

Evidence vozidel v systému časového zpoplatnění

Právní úpravu zákona o pozemních komunikacích autor považuje za splňující kritéria přesnosti formulací a též za dostatečně předvídatelnou, avšak s výhradou vůči době uchování údajů, která v této úpravě není obsažena dostatečným způsobem. Zákon o pozemních komunikacích v případě evidence vozidel v systému časového zpoplatnění vymezuje dobu uchování pouze u údajů o vozidlech, pro která byl uhrazen časový poplatek, a to v délce *„2 let od konce období, pro které byl uhrazen časový poplatek“*[599], v případě údajů zaznamenávaných technickými zařízeními ke kontrole úhrady časového poplatku za užití pozemní komunikace však dobu uchování nevymezuje.

Zpracování údajů evidence vozidel v systému časového zpoplatnění a následné zpracování údajů v rámci kontroly úhrady časového poplatku jsou dle hodnocení autora způsobilé k dosažení cílů vyplývajících ze zákona o pozemních komunikacích jako výběr časového poplatku zajišťovaný Státním fondem dopravní infrastruktury a kontrola úhrady

[599] § 21 odst. 6 zákona č. 13/1997 Sb. o pozemních komunikacích, ve znění pozdějších předpisů.

tohoto poplatku[600]. Zájem na dosažení výše uvedených cílů lze hodnotit jako ústavně aprobovaný veřejný zájem.

V případě evidence vozidel v systému časového zpoplatnění v zákoně o pozemních komunikacích autor ve druhém kroku testu proporcionality vyhodnotil zásah do práva na ochranu soukromí jako nezbytný ve vztahu ke sledovaným cílům. Možnost dosažení týchž cílů opatřeními šetrnějšími a méně zasahujícími do práva na ochranu soukromí zde sice existuje, v podobě ještě donedávna v praxi užívaných označení úhrady prostřednictvím nálepek na čelním skle vozidla, tato možnost se však nejeví jako po technické stránce zcela srovnatelná a též zahraniční zkušenosti ukazují na v současnosti již spíše ojedinělý charakter tohoto řešení.

Při aplikaci požadavků třetího kroku testu proporcionality na právní úpravu evidence vozidel v systému časového zpoplatnění v zákoně o pozemních komunikacích autor porovnával závažnost základního práva na ochranu soukromí na straně jedné a veřejných statků stojících v kolizi s ním, zde tedy veřejných zájmů vymezených výše. Konkrétně jde o zájem na úhradě časového poplatku za užití pozemní komunikace a na kontrole této úhrady, který je zjevně zájmem nižší závažnosti v porovnání s veřejnými statky vymezenými u jiných typových zásahů posuzovaných v této práci. Autor ovšem po porovnání vyhodnotil požadavky tohoto kroku jako splněné. I zde má však autor určité pochybnosti o dostatečnosti záruk bránících zneužití, mimo jiné i s ohledem na nedostatečně upravenou dobu uchování.

3.5 Zpracování údajů o zdravotním stavu

Osobní údaje, které vypovídají o zdravotním stavu fyzické osoby, řadí GDPR do zvláštních kategorií osobních údajů a na rozdíl od běžných osobních údajů jejich zpracování obecně zakazuje, nejsou-li naplněny podmínky některé z taxativně stanovených výjimek; GDPR tímto konzistentně navazuje na předchozí právní úpravu[601]. Zpracování osobních údajů vypovídajících o zdravotním stavu značného množství osob proto dle hodnocení autora mohou představovat závažný zásah do práva na ochranu soukromí.

Při identifikaci typových situací, v nichž jsou na základě povinností uložených právní úpravou zpracovávány údaje o zdravotním stavu, se autor zaměřil v prvé řadě na

[600] Tyto cíle vyplývají z § 21c, resp. § 13 písm. j) zákona o pozemních komunikacích, ve znění pozdějších předpisů.
[601] Zvláštní kategorie osobních údajů a podmínky jejich zpracování vymezuje GDPR v čl. 9, předchozí právní úprava Směrnice 95/46/ES, resp. zákona č. 101/2001 Sb. o ochraně osobních údajů, který v § 4 písm. b) údaje o zdravotním stavu řadil do kategorie tzv. citlivých údajů, v § 9 pak stanovil velmi přísné podmínky pro jejich zpracování.

zpracování údajů v Národních zdravotních registrech. Tato povinná zpracování osobních údajů autor s ohledem na zaměření této práce vyhodnotil pro jejich celkový rozsah a pro závažnost kategorií osobních údajů v registrech obsažených jako velmi vhodný předmět pro další zkoumání v této práci. Autor zkoumal též zpracování osobních údajů, která byla prováděna v rámci boje proti onemocnění COVID-19; v oblasti zpracování údajů o zdravotním stavu lze tyto typové případy považovat rovněž za zásadní. Přestože se jednalo o zpracování jednorázová, byť probíhající po delší časový úsek, svým charakterem i rozsahem neměla tato zpracování dosud v právním řádu ČR obdoby, mnohá z nich lze označit za zpracování plošná, týkající se značného množství osob vymezených na základě obecných kritérií. Tato zpracování v některých případech, nikoli však vždy (např. zpracování údajů o návštěvě restaurace), zahrnovala též údaje o zdravotním stavu, vedle nich se týkala též dalších kategorií osobních údajů, v některých případech i údajů lokalizačních, kromě práva na ochranu soukromí zasahovala tato zpracování též do některých další základních práv, jako např. práva na svobodu pohybu.

Po tomto předběžném posouzení se autor, především z důvodů komplexnosti povinných zpracování osobních údajů v rámci boje proti COVID-19, rozhodl zabývat se v rámci podrobné analýzy zpracování údajů o zdravotním stavu v této kapitole pouze výše uvedenými Národními zdravotními registry. Zpracování v těchto registrech autor považuje z hlediska zásahu do práva na ochranu soukromí za velmi reprezentativní, přitom zahrnující všechny typické aspekty zásahů založených zpracováním osobních údajů trvalého charakteru, dotýkajících se značného množství osob. Autor v tomto směru přihlédl též k již výše zdůrazňovanému záměru této práce, kterým není snaha o taxativní výčet a vyčerpávající popis všech případů zásahů do práva na ochranu soukromí, nýbrž analýza typových zásahů z ústavněprávního hlediska.

3.5.1 Vývoj a základní vymezení, aktuální relevantní právní úprava

Národní zdravotní registry vymezuje zákon o zdravotních službách[602] a transplantační zákon[603], včetně kategorií údajů, které jsou v nich obsaženy. V každém

[602] Zákon č. 372/2011 Sb. o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů v § 72 a násl. řadí Národní zdravotní registry do Národního zdravotnického systému jako jeho součást, Příloha k tomuto zákonu pak obsahuje vymezení jednotlivých registrů. Národní zdravotní registry obsahoval již předchozí zákon č. 20/1966 Sb. o péči o zdraví lidu, ve znění pozdějších předpisů.

[603] Zákon č. 285/2002 Sb. o darování, odběrech a transplantacích tkání a orgánů a o změně některých zákonů (transplantační zákon), ve znění pozdějších předpisů.

z registrů jsou evidovány identifikační údaje jednotlivých fyzických osob, ve většině případů pacientů (v některých registrech údaje těhotných žen či osob vyloučených z dárcovství krve) a též údaje o konkrétním onemocnění, osobní a rodinné anamnézy, údaje o léčbě daných osob a řadu dalších údajů, kromě pacientů jsou v registrech zpracovávány též údaje zdravotnických pracovníků. Národní zdravotní registry jsou součástí Národního zdravotnického informačního systému (dále též jen „NZIS"), jeho správcem je Ústav zdravotnických informací a statistiky České republiky zřízený Ministerstvem zdravotnictví[604] (dále též jen „ÚZIS"). Ministerstvo vnitra, Policie ČR či Český statistický úřad poskytují ÚZIS v rámci součinnosti velmi rozsáhlou řadu osobních údajů, včetně údajů ze základního registru obyvatel a z evidence obyvatel zahrnujících např. i údaje o státních občanstvích, informace o číslech a druzích elektronicky čitelných identifikačních dokladů, typu a identifikátoru datové schránky, rodinném stavu, například i včetně data a místa vzniku registrovaného partnerství a osobních údajů registrovaného partnera, údajů o osvojenci, vč. stupně osvojení a mnohé další[605].

Národní zdravotní registry jsou zřízeny na základě zákona a osobní údaje pacientů a dalších osob do nich poskytovatelé zdravotních a sociálních služeb, zdravotní pojišťovny a další osoby předávají bez souhlasu pacientů, součinnost poskytuje i Ministerstvo vnitra a Policie ČR; prováděcí vyhláška stanoví okruh poskytovatelů a dalších osob předávajících údaje do registrů, periodicitu a lhůty pro jejich předávání[606]. Pro vedení registrů lze využívat údaje z informačních systémů veřejné správy, tyto registry vytvářejí vzájemně propojenou soustavu, údaje v nich uvedené lze sdružovat[607], to však pouze pro účely vymezené v zákoně pro vedení registrů. Dobu uchování vymezuje zákon o zdravotních službách samostatně pro každý z registrů, zpravidla je vázána až na úmrtí pacienta a je tedy vymezena jako určitý počet let po úmrtí; v některých případech je vázána na nahlášení údajů nebo vznik hlášené skutečnosti, v takovém případě činí minimálně 25 let od této skutečnosti, zpravidla ještě déle, po uplynutí doby uchovávání se údaje dle zákona anonymizují[608]. Doba uchování je tedy velmi dlouhá a zpravidla pokrývá podstatnou část života dané osoby. Z hlediska práva osobních údajů je v této souvislosti relevantní, že po úmrtí dané osoby se již údaje k této osobě se

[604] Transplantační zákon v 18 odst. 3 označuje Ústav zdravotnických informací a statistiky České republiky terminologií zpracování osobních údajů za zpracovatele osobních údajů.
[605] Viz § 71 zákona o zdravotních službách.
[606] Vyhláška č. 373/2016 Sb. o předávání údajů do Národního zdravotnického informačního systému, ve znění pozdějších předpisů.
[607] Viz § 45 odst. 2 písm m) ve spojení s § 70 odst. 2, § 72 odst. 2 zákona o zdravotních službách.
[608] Zákon o zdravotních službách stanoví doby uchování v Příloze č. 1 pro každý z Národních zdravotních registrů.

vztahující nepovažují za osobní údaje[609]. Transplantační zákon dobu uchování pro údaje v národních zdravotních registrech upravených v tomto zákoně nestanoví, obecně v otázkách nakládání s údaji v registrech odkazuje na zvláštní právní předpis[610], kterým je zákon o zdravotních službách a ZoZOÚ, ty však v případech registrů zvláštní dobu uchovávání neupravují, uplatní se tedy povinnost správce uchovávat osobní údaje pouze po dobu nezbytnou s ohledem na vymezený účel zpracování.

Účely zpracování

Zákon o zdravotních službách vymezuje „účely zdravotních registrů“, které je dle hodnocení autora nutno považovat za účely zpracování osobních údajů v těchto registrech. Těmito účely jsou v případě osobních údajů pacientů a osob v obdobném postavení zákonem uvedeny zejména *„sběr informací k hodnocení zdravotního stavu obyvatelstva a jeho vývoje“*, sledování společensky závažných a dalších nemocí a jejich důsledků, vč. jejich incidence, okolností vzniku a šíření, *„evidence a sledování pacientů s vybranými společensky závažnými nemocemi“* a zpracování údajů registrů *„s cílem zlepšovat zdraví populace“* a některé další účely vymezené zákonem[611]. Některé z těchto účelů nejsou vymezeny zcela jednoznačně a srozumitelně, např. v případě sběru informací jako účelu registru[612] by samotná činnost měla být sama sobě účelem. Transplantační zákon zvláštní účely zpracování nedefinuje.

Orgány oprávněné k využití údajů

Přístup k údajům zpracovávaným v Národních zdravotních registrech má dle zákona o zdravotních službách kromě správce zdravotnického registru též jeho provozovatel a jejich pracovníci, v zákonem vymezených případech poskytovatelé zdravotních služeb, Koordinační středisko transplantací a orgán ochrany veřejného zdraví a dále též *„instituce, která má ze zákona právo využívat data určeného zdravotnického registru pro svoji činnost*“. K údajům Národního registru hrazených zdravotních služeb má přístup též zdravotní pojišťovna, v rozsahu údajů, které jako zdravotní služby uhradila[613], v případě registru

[609] Tuto skutečnost lze dovodit z vymezení osobního údaje v čl. 4 bod 1 GDPR, tato skutečnost je výslovně zmíněna v recitále GDPR, viz recitál 27 a 158. ZoZOÚ nestanovil v tomto směru odlišnou úpravu.
[610] Viz § 18 odst. 2 transplantačního zákona.
[611] Viz § 73 odst. 1 zákona o zdravotních službách.
[612] Iuridicum Remedium o.s. v podání pro Ústavní soud ČR účely takto vymezené v zákoně o zdravotních službách kritizuje, když účelem registru nemůže být sama jeho existence, nýbrž řešení nějakého problému. Iuridicum Remedium o.s. *Stanovisko občanského sdružení Iuridicum Remedium k ústavní konformitě úpravy národních zdravotních registrů v zákoně o zdravotních službách (vypracované jako součást dopisu AMICUS CURIAE pro Ústavní soud ČR ve věci sp. zn. Pl. ÚS 1/12).* [online] [cit. 15.1.2024]. Dostupné z www.iure.org.
[613] Viz § 73 odst. 2 a 77a odst. 5 zákona o zdravotních službách.

zdravotnických pracovníků zahrnují oprávněné osoby též vzdělávací zařízení, profesní komory a další. Pokud jde o uvedené oprávnění „provozovatele“ k přístupu k registrům, zákon o zdravotních službách ani transplantační zákon pojem „provozovatel“ v aktuální verzi nepoužívají (používají pouze odlišný termín „správce“ NZIS) a tato množina je tak dle hodnocení autora prázdná. Taktéž v případě uvedené „instituce“ s právem využití dat ze zákona ani jeden z obou relevantních zákonů výslovně neposkytuje konkrétním institucím právo využívat údaje ze zdravotních registrů pro svou činnost, v jiných předpisech autor jednoznačné vymezení takovéhoto oprávnění také nenalezl.

Kritérium plošného zpracování

Celkové počty subjektů údajů zahrnutých do Národních zdravotních registrů nejsou dostupné, ze statistik zveřejněných na stránkách ÚZIS[614] je však zřejmé, že jednotlivé registry zpracovávají údaje stovek tisíc až milionů osob. Autor však vyhodnotil, že v tomto případě se nejedná o plošné zpracování týkající se všech osob bez výběru dle konkrétních, předem specifikovaných kritérií, nýbrž o zpracování zaměřené vždy pouze na vybrané osoby splňující kritéria relevantní ve vztahu k účelům zpracování údajů v jednotlivých registrech, zpravidla je tímto kritériem výskyt konkrétního onemocnění či jiného zdravotního stavu dané osoby.

3.5.2 Relevantní rozhodnutí soudů, stanoviska orgánů dohledu nad ochranou osobních údajů

ÚOOÚ

ÚOOÚ provedl v ÚZIS v roce 2007 kontrolu zpracování zdravotnických informací a vedení národních zdravotních registrů, ve zveřejněné informaci ÚOOÚ označuje tuto kontrolu jako velmi závažnou. ÚZIS je dle ÚOOÚ z hlediska rozsahu spravovaných údajů *„zřejmě největším správcem citlivých údajů“* v ČR, když v Národních zdravotních registrech vede ÚZIS *„citlivé osobní údaje o značné části obyvatel České republiky“*. Primárním předmětem kontroly bylo zabezpečení a ochrana zpracovávaných osobních údajů proti zneužití, ÚOOÚ v tomto směru neshledal pochybení[615]. Dle následného vyjádření předsedy ÚOOÚ je však právní úprava NZIS *„v příkrém rozporu s evropskými standardy ochrany dat ve zdravotnictví“,* předseda doporučoval, aby informace o zdravotním stavu byly zpracovávány v anonymní podobě, k novelizaci právní úpravy však nedošlo[616].

[614] Viz ÚZIS. *Souhrnné reporty*. [online]. [cit. 23.2.2024]. Dostupné z www.uzis.cz.
[615] ÚOOÚ. *Kontroly za rok 2007. Zdravotnictví.* [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
[616] ČT24. *Ochránci dat řeší zdravotní registry i úniky ze spisů*. 24.9.2008. [online] [cit. 15.1.2024]. Dostupné z www.ct24.ceskatelevize.cz.

Ústavní soud ČR

Ústavní soud ČR zpracování osobních údajů v Národních zdravotních registrech posuzoval celkem ve 3 nálezech relevantních vzhledem k tématu práce. V nálezu Pl. ÚS 1/12[617] Ústavní soud ČR k návrhu skupiny poslanců zkoumal více právních předpisů, v samotném zákoně o zdravotních službách se zabýval několika oblastmi, v rámci Národních zdravotních registrů zde však posuzoval pouze právní úpravu Národního registru zdravotnických pracovníků, většinu této právní úpravy Ústavní soud ČR tímto nálezem zrušil. Skupina senátorů[618] navrhovala zrušit celou úpravu NZIS z důvodu neurčitého a velmi vágního účelu této databáze a nepřípustného rozsahu zveřejňovaných osobních údajů zdravotnických pracovníků, jejichž seznamy jsou navíc duplicitní k seznamům vedeným profesními komorami. Napadený Registr zdravotnických pracovníků byl dle zákona o zdravotních službách v převážné části veřejně přístupný.

Dle vyjádření předkladatele napadené právní úpravy, Ministerstva zdravotnictví, v případě zdravotních registrů převáží veřejný zájem na ochraně veřejného zdraví a právo konkrétních osob na ochranu zdraví nad právem na ochranu soukromí, když údaje zpracovávané v registrech slouží mj. zdravotnickému výzkumu, vč. epidemiologických studií. ÚOOÚ upozornil, že v legislativním procesu s ním právní úprava zdravotních registrů nebyla projednána ani nebylo připraveno vyhodnocení jejích dopadů do soukromí osob. ÚOOÚ ve svém vyjádření kritizoval též sloučení některých dosavadních registrů, dlouhou dobu uchování údajů a především nejasně vymezený účel vedení registrů, upozornil také na zkušenosti jiných evropských států, v nichž k dosažení stejného účelu postačují databáze klinických studií, vedené buď na základě souhlasu pacientů či v anonymní podobě. Národní registr zdravotnických pracovníků považuje ÚOOÚ za nepřiměřený.

Ústavní soud ČR vyhodnotil návrh skupiny senátorů na zrušení celého NZIS jako obecný, nespecifikující, zda navrhovatelé zpochybňují všechny dílčí registry či pouze některé z nich. Z tohoto důvodu se dále podrobně zabýval pouze Národním registrem zdravotnických pracovníků. V jeho případě Ústavní soud ČR akceptoval, že účel zajištění přístupu veřejnosti k údajům o zdravotnických pracovnících je v zákoně vymezen pouze implicitně. V následném

[617] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 1/12 ze dne 27. listopadu 2012.

[618] V průběhu řízení zahájeného na základě návrhu skupiny poslanců obdržel Ústavní soud ČR další dva návrhy skupiny senátorů, resp, skupiny poslanců směřující proti zákonu o zdravotních službách, z důvodu již zahájeného řízení o zrušení tohoto zákona jako celku Ústavní soud ČR tyto návrhy odmítl (usnesení sp. zn. Pl. ÚS 2/12 ze dne 24.1.2021 a sp. zn. Pl. ÚS 7/12 ze dne 6.3.2021), ovšem v původně zahájeném řízení podrobil napadený zákon přezkumu též v rozsahu námitek obsažených v obou odmítnutých návrzích.

testu proporcionality však dospěl k závěru, že v případě některých kategorií údajů, konkrétně data a místa narození, státního občanství a údajů o ztrátě oprávnění k výkonu zdravotnického povolání, ztrátě zdravotní způsobilosti či bezúhonnosti, veřejný přístup neobstojí ve druhém kroku testu proporcionality, tedy v posouzení potřebnosti těchto údajů pro dosažení sledovaného cíle, způsobů jejich získání a následného nakládání s nimi. Ústavní soud ČR zde přitom nemohl vycházet z jiných účelů nežli těch vymezených zákonem nebo alespoň z jeho textu implicitně jednoznačně dovoditelných. Výhrady zde Ústavní soud ČR vyjádřil i k celkové době zveřejnění a uchovávání údajů, která není dostatečně určitě vymezena, a též k úpravě rozsahu přístupu oprávněných osob k údajům registru. Ústavní soud ČR se v tomto případě zabýval pouze Národním registrem zdravotnických pracovníků, nepřezkoumával tedy ústavnost právní úpravy celého NZIS. Výslovně upozornil, že *„shromažďování a zpracovávání osobních údajů o zdravotním stavu pacientů bez jejich souhlasu představuje velmi intenzivní zásah do jejich základních práv“.* Na právní úpravu, zejména na stanovení účelů shromažďování a zpracování údajů, včetně rozsahu údajů, na okruh osob oprávněných k přístupu k údajům a účel přístupu, dobu uchování, zabezpečení a kontrolu nakládání s údaji, je proto nutno klást zvláště přísné požadavky.

Nálezem Pl. ÚS 33/16[619] plénum Ústavního soudu ČR zamítlo návrh skupiny senátorů na zrušení celé právní úpravy NZIS v zákoně o zdravotních službách, odůvodněný především jejím rozporem s právem každého na ochranu před neoprávněným shromažďováním, zveřejňováním a jiným zneužíváním údajů o své osobě, zaručeným v čl. 10 odst. 3 Listiny. Ústavní soud ČR vyhodnotil, že dotčeným základním právem zde je primárně právo na ochranu osobních údajů, jehož součástí je právo na informační sebeurčení. Tato práva mohou kolidovat s právem každého na ochranu zdraví, taktéž zaručeným Listinou v čl. 31, proto Ústavní soud ČR posuzoval respektování zásady přiměřenosti zákonodárcem a tedy dosažení spravedlivé rovnováhy mezi soupeřícími zájmy. V rámci testu proporcionality se Ústavní soud ČR v jeho druhém kroku, při posuzování potřebnosti, zvláště zaměřil na rozsah údajů v napadených registrech a na okruh osob oprávněných k přístupu k údajům v nich. U žádné ze zpracovávaných kategorií údajů obsažených v jednotlivých registrech přitom Ústavní soud ČR nedospěl k závěru o její nadbytečnosti či nedůvodnosti, přestože rodné číslo zde Ústavní soud ČR považoval za problematické. Případný užší rozsah zpracovávaných údajů by však dle jeho hodnocení nemusel představovat plnohodnotnou alternativu ve vztahu k cílům

[619] Nález Ústavního soudu ČR ze dne 18. listopadu 2020 sp. zn. Pl. ÚS 33/16.

vymezeným zákonodárcem. Obecně přitom případné řešení šetrnější vůči dotčeným základním právům, které je posuzováno v testu proporcionality, musí být schopno dosáhnout sledovaných legitimních cílů minimálně ve srovnatelné míře. V rámci třetího kroku testu proporcionality Ústavní soud ČR konstatoval, že *„shromažďování osobních údajů ve zdravotnických registrech“* patří mezi případy přesahující právní sféru jednotlivce a je tak u něj *„s určitými striktními výjimkami založena povinnost státu chránit zdraví i proti vůli dotčených osob“*. Neústavnost zde proto Ústavní soud ČR neshledal v absenci souhlasu či v nemožnosti požádat na základě opt-out principu o výmaz údajů. Povahu práva na ochranu zdraví totiž Ústavní soud ČR považoval za určující, právo na ochranu osobních údajů mu tak v tomto případě musí přiměřeným způsobem ustoupit. Podstatným aspektem posuzovaných registrů je dle Ústavního soudu ČR jejich neveřejný charakter. Posuzovaný zákon sice neobsahuje dostatečné záruky bezpečnosti zpracovávaných údajů, ty však dle Ústavního soudu ČR vyplývají z právního řádu, resp. z právních aktů unijního práva.

Po vyhodnocení testu proporcionality tak Ústavní soud ČR dospěl k závěru, že napadená ustanovení zákona o zdravotních službách v něm obstojí, konstatoval přitom, že tato právní úprava není založena na plošném sběru všech údajů ve všech registrech, nýbrž spočívá pouze v dílčích záznamech konkrétních registrů. Celkem čtyři ústavní soudci uplatnili k nálezu odlišné stanovisko. Podle Ivana Davida nastavení NZIS nemělo v ústavním přezkumu obstát, nálezu vytýká zejména bezvýhradnou akceptaci legitimního cíle právní úpravy, založenou na tezi, dle které efektivita informačního systému a jeho přínos pro sledovaný účel narůstá s množstvím zpracovávaných údajů, tato teze však dle Davida není zcela podložena vyjádřeními předloženými v řízení. Obdobně také dle tří dalších ústavních soudců Ústavní soud ČR v nálezu místo správného pečlivého zkoumání jednotlivých kategorií osobních údajů obsažených v registrech provedl test proporcionality povrchním způsobem ve vztahu ke všem údajům najednou. Nález také neobsahuje vysvětlení závěru o nemožnosti dosáhnout sledovaného cíle šetrnějším způsobem. Soudci v odlišném stanovisku upozornili též na existenci možnosti vyslovit vůči systému registrů právo opt-out v řadě evropských zemí, zpochybnili také důvodnost potřeby identifikovat konkrétní pacienty a varovali i před možnou zneužitelností celého systému registrů, zvláště při neexistenci dostatečných záruk.

Zatím poslední relevantní nález Pl. ÚS 25/21[620] se k návrhu Městského soudu v Praze zabýval problematikou poskytování informací z NZIS, ochrany soukromí se týkal

[620] Nález Ústavního soudu ČR sp. zn. Pl. ÚS 25/21 ze dne 17. ledna 2023.

pouze částečně. Právní úprava v této části dle navrhovatele v rozporu s ústavním pořádkem omezuje právo na svobodný přístup k informacím, když stanoví, že ÚZIS *„poskytne na základě žádosti podle zákona o svobodném přístupu k informacím, pokud se jedná o údaje v Národním zdravotnickém informačním systému, pouze informace o struktuře dat“*[621]. Ústavní soud ČR zde posuzoval zásah do práva na svobodu projevu dle čl. 17 Listiny, zahrnujícího též právo na svobodné vyhledávání informací. V odůvodnění konstatoval, že poskytnutím informací z NZIS by zcela jistě mohlo být *„zasaženo do soukromého a rodinného života či do práva na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě“*, zákonná výluka ovšem kromě těchto údajů dopadá na veškeré informace obsažené v NZIS. Ústavní soud ČR však dospěl k závěru o možném ústavně souladném výkladu zákonných výluk z informační povinnosti a návrh zamítl.

3.5.3 Posouzení splnění ústavněprávních požadavků

Dle autorova závěru výše se v případě zpracování údajů v Národních zdravotních registrech nejedná o plošné zpracování osobních údajů, jde však o shromažďování a zpracování údajů značného množství osob, z podstatné části údajů o zdravotním stavu zařazených do zvláštních kategorií osobních údajů[622], toto zpracování tak představuje zásah do práva na ochranu soukromí. Autor tak u něj považuje za potřebné vyhodnotit splnění ústavněprávních požadavků. Zásah do práva na ochranu soukromí v podobě zpracování údajů v Národních zdravotních registrech je zákonem předvídaný, právní úpravu zákona o zdravotních službách a na něj navazujícího transplantačního zákona, kteréžto zákony tento zásah zakládají, autor vyhodnotil jako splňující kritéria formulační přesnosti a v dostatečné míře předvídatelné.

Autor dále posuzoval účely zpracování vymezené v relevantní právní úpravě, zvláště s ohledem na pochybnosti vyjádřené v tomto směru ze strany Iuridicum Remedium, jak zmiňováno výše. Autor zaznamenal, že Ústavní soud ČR v nálezu Pl. ÚS 33/16 účely zpracování převzal ze zákona o zdravotních službách, aniž by se k jejich vymezení kriticky vyjádřil. Jak již autor vyjádřil výše, nepovažuje vymezení některých z těchto účelů za zcela jednoznačné a srozumitelné. Po prozkoumání textu zákona však autor dospěl k závěru, že tyto nejednoznačnosti a částečné nesrozumitelnosti lze překlenout výkladem a účely vymezené v zákoně o zdravotních službách tedy je možno považovat z ústavněprávního hlediska za

[621] Viz § 73 odst. 7 zákona o zdravotních službách.
[622] Viz výše zmiňovaný závěr ÚOOÚ o největším správci citlivých údajů obsažený v informaci o kontrole zpracování v ÚZIS.

dostatečně splňující požadavky na určitost. Ostatně, Ústavní soud ČR v otázce vymezení účelů v právní úpravě připouští i jejich implicitní vyjádření[623]. Lze tak přistoupit ke zkoumání legitimnosti sledovaných cílů vytýčených právní úpravou a způsobilosti dosažení těchto cílů v prvním kroku testu proporcionality. Ve shodě se závěry Ústavního soudu ČR v nálezu Pl. ÚS 33/16 autor účely posuzovaných registrů vyhodnotil jako legitimní cíle, směřující ke zlepšení podmínek pro poskytování zdravotní péče. Končený cíl právní úpravy tak lze vyjádřit jako ochranu zdraví, takto vymezený cíl je dle hodnocení autora veřejným zájmem, který je nutno považovat za ústavně aprobovaný. Autor se však neztotožňuje s hodnocením Ústavního soudu ČR obsaženým tamtéž, dle kterého je efektivita informačního systému a přínos takového systému pro sledovaný účel přímo úměrná množství dat obsažených v informačním systému, a to přestože Ústavní soud ČR tvrdí, že tento závěr (který nepřesně označuje za „skutečnost“) nelze v obecné rovině zpochybnit.

Autor tak při zkoumání nezbytnosti zásahu ve vztahu ke sledovaným cílům a při porovnání zkoumané právní úpravy s jinými do úvahy připadajícími opatřeními, která by při méně intenzivním zásahu do práva na ochranu soukromí umožňovala dosažení týchž cílů, ve druhém kroku testu proporcionality považoval za nutné zaměřit se především na rozsah osobních údajů zpracovávaných dle zkoumané právní úpravy. Autor v tomto směru hodnotil jako relevantní některé výtky obsažené v odlišných stanoviscích ústavních soudců k nálezu Ústavního soudu ČR Pl. ÚS 33/16. Na rozdíl od přístupu Ústavního soudu ČR nezabývat se *„izolovaně ústavností každého jednotlivého údaje obsaženého ve zdravotnických registrech“* autor naopak považoval za nutné zabývat se kategoriemi zpracovávaných osobních údajů podrobně. Po jejich prozkoumání autor dospěl k závěru, že některé z nich nevyhovují požadavkům nezbytnosti ve vztahu ke sledovaným cílům. Dle hodnocení autora tak konkrétně údaje o osvojení, místu uzavření manželství či vzniku registrovaného partnerství nebo o státním občanství nejsou nezbytnými pro dosažení cíle vymezeného právní úpravou jako zlepšení podmínek pro poskytování zdravotní péče. Zkoumaná právní úprava tak v této části neobstojí ve druhém kroku testu proporcionality, jedná se však pouze o část právní úpravy, o konkrétní kategorie zpracovávaných údajů. Také doba uchovávání údajů v neanonymizované podobě, před jejich anonymizací, se v případech některých registrů jeví být velmi dlouhá a otázka alternativního, vůči právu na ochranu soukromí méně invazivního, řešení v podobě jejího zkrácení, případně v kombinaci s anonymizací údajů či alespoň jejich pseudonymizací

[623] Viz např. Nález Ústavního soudu ČR sp. zn. Pl. ÚS 1/12 ze dne 27. listopadu 2012.

po uplynutí určité, v právní úpravě jednoznačně vymezené doby, je dle autora relevantní. Autor nemá dostatek informací k tomu, aby mohl posoudit, zda alternativní řešení v podobě registrů založených na režimu opt-out (umožňujícím vyslovit účinně nesouhlas pacienta se zpracováním údajů), případně řešení spojené s anonymizací zpracovávaných údajů je možným a způsobilým dosáhnout stanovených cílů; informace k takovému posouzení autor nenalezl ani v citovaném nálezu Ústavního soudu ČR Pl. ÚS 33/16, byť dle hodnocení autora se Ústavní soud ČR ve zmiňovaném případě měl právě takovému posouzení věnovat. V otázce podmínek přístupu oprávněných osob k údajům obsaženým v registrech vymezených v zákoně o zdravotních službách[624] se autor neztotožnil s výhradami disentujících ústavních soudců, podmínky přístupu i jeho šíři autor vyhodnotil jako upravené dostatečným způsobem.

Ve třetím kroku testu proporcionality, při porovnání závažnosti práva na ochranu soukromí a v kolizi s ním stojícího práva na ochranu zdraví, autor vyhodnotil požadavky na závažnost právní úpravy představující zkoumaný zásah do základních práv jako naplněné, pochopitelně s výhradou částí zákona o zdravotních službách vymezujících kategorie osobních údajů, které dle hodnocení autora neobstály již ve druhém kroku testu proporcionality. Tyto části však autor považuje za oddělitelné, bez vlivu na zbývající části posuzované právní úpravy, kategorie osobních údajů nevyhovujících posouzení nezbytnosti představují menší část osobních údajů celkově zpracovávaných dle dané právní úpravy. Ve třetím kroku je však dle autora nezbytné vyhodnotit též existenci záruk proti zneužití posuzované právní úpravy, resp. dle této právní úpravy zpracovávaných osobních údajů, zvláště se zřetelem na zařazení některých kategorií těchto údajů mezi „zvláštní kategorie“ ve smyslu právní úpravy GDPR[625]. Za potenciálně zneužitelný nástroj označilo ve svých odlišných stanoviscích soubory informací obsažených v posuzovaných registrech též několik ústavních soudců, autor s jejich hodnocením souhlasí. Záruky proti zneužití spočívají obecně v kvalitativních požadavcích na právní úpravu zakládající posuzovaný zásah a také v účinných kontrolních mechanismech bránících zneužití možností této právní úpravy a v posuzovaném případě i zneužití zpracovávaných osobních údajů.

Posuzovaná právní úprava dle hodnocení autora splňuje ústavněprávní požadavky na vymezení zpracovávaných údajů, podmínek přístupu k nim a oprávněných orgánů, některé z kategorií osobních údajů dle této právní úpravy však neobstojí v posouzení nezbytnosti, jak

---

[624] Osoby oprávněné k přístupu ke zpracovávaným údajům a podmínky přístupu vymezuje zákon o zdravotních službách v § 73 odst. 2 a 3.
[625] Čl. 9 GDPR.

rozebráno výše. Dalším nedostatkem posuzované právní úpravy jsou absentující jednoznačné požadavky na zabezpečení zpracovávaných údajů. Autor na rozdíl od Ústavního soudu ČR nepovažuje za dostatečnou existenci takových požadavků v obecné právní úpravě ochrany osobních údajů. Konečně, právní úprava Národních zdravotních registrů též nevymezuje dostatečně kontrolní mechanismy dodržování povinností a omezení, které by bylo možno považovat za účinně bránící zásahům.

4 Závěry vyplývající z rozboru zkoumaných typových případů

4.1 Obecné závěry vyplývající z rozhodovací a výkladové praxe

Autor v předchozím textu zkoumal několik vybraných typových případů zásahů do práva na ochranu soukromí. V rámci toho autor analyzoval též dostupná rozhodnutí soudů a stanoviska a doporučení orgánů dozoru a dalších relevantních orgánů, zejména Pracovní skupiny WP 29 a EDPB či Evropského inspektora ochrany údajů. Z vyhodnocení vyplynuly některé obecné závěry, které se netýkají toliko konkrétního posuzovaného zpracování, nýbrž je dle hodnocení autora lze zobecnit a aplikovat je na případy podobných zásahů do základních lidských práv, primárně práva na ochranu soukromí a práv souvisejících, k nimž dochází či k nimž v budoucnu může dojít.

Zejména lze dle hodnocení autora na základě zkoumaných případů vymezit hlavní prvky a podstatu společnou zásahům spočívajícím v plošném shromažďování osobních údajů, jakož i dotčená základní práva. Ze zkoumaných materiálů vyplývají též faktory relevantní pro hodnocení míry zásahů, včetně prvků, které jejich intenzitu zvyšují; autor tyto faktory rozebral u jednotlivých případů zkoumaných zásahů.

Autor považuje za významné, že některá ze zkoumaných rozhodnutí a dalších materiálů upozorňovala též na riziko vyplývající z možné kombinace zásahů a vzájemného propojení údajů shromážděných na základě jednotlivých právních úprav[626]. Jednalo se však zpravidla pouze o upozornění poznamenaná v soudních rozhodnutích obiter dictum či o obecné úvahy ve stanoviscích některých orgánů; soudy ani orgány dozoru v žádném z dostupných a autorovi známých rozhodnutí neposuzovaly možnou kombinací zásahů, resp. možné propojení údajů a jejich databází získaných z různých zdrojů a shromážděných na základě různých právních předpisů. Tato skutečnost vyplývá z omezení, dle kterých jak Ústavní soud ČR, tak rovněž další, v této práci uváděné soudy posuzující tvrzené zásahy do práv a návrhy na zrušení právních předpisů jsou zpravidla, na rozdíl od dozorových orgánů v oblasti ochrany osobních údajů, v řízení vázány rozsahem podaného návrhu a nejsou tak oprávněny kromě napadeného právního předpisu posuzovat i předpisy jiné[627].

---

[626] Např. Ústavní soud ČR v nálezu Pl. ÚS 24/10 upozornil, že *„ve virtuálním prostoru informačních technologií a elektronické komunikace (v tzv. kyberprostoru) jsou, zejména díky rozvoji internetu a mobilní komunikace, každou minutou zaznamenávány, shromažďovány a fakticky zpřístupněny tisíce, ba miliony dat, údajů a informací, které zasahují i do soukromé (osobnostní) sféry každého jednotlivce, ačkoliv on sám do ní vědomě nikoho vpustit nechtěl“*.

[627] Jak konstatoval Ústavní soud ČR v usnesení sp. zn. I.ÚS 2369/21 ze dne 12. října 2021: *„Podle ustáleného názoru Ústavního soudu je však Ústavní soud ve svém rozhodování vázán rozsahem a obsahem podaného návrhu a ve svém rozhodnutí z jeho hranic (ultra petitum) vykročit nemůže.“* Obdobně viz také usnesení Ústavního soudu

Na základě analýzy jednotlivých typových případů zásahů do práva na ochranu soukromí povinným, ve většině případů plošným, zpracováním osobních údajů provedené v této práci autor dospěl k závěru o nutnosti zajistit efektivní kontrolní mechanismy, s cílem eliminovat neproporcionální zásahy do tohoto práva a také v relevantních právních úpravách zahrnout a též v praxi aplikovat záruky bránící možnému zneužití zásahů. Takovéto kontrolní mechanismy lze dle hodnocení autora do značné míry zobecnit pro většinu zkoumaných zásahů, jak autor ukáže v následujícím textu.

4.1.1 Zásady zabezpečení zpracovávaných údajů

Kromě dále rozebraných kontrolních mechanismů a záruk autor považuje za potřebné vymezit v právních úpravách zakládajících jednotlivé zásahy též základní zásady zabezpečení zpracovávaných osobních údajů. Otázka zabezpečení zpracovávaných osobních údajů sice bezprostředně nepatří mezi kontrolní mechanismy, je ovšem velmi relevantní zvláště v případě plošných shromažďování a zpracování osobních údajů, která jsou uložena jako povinnost, a to často nejen orgánům veřejné moci, ale i dalším osobám. Právě na tento aspekt výstižně poukázal Ústavní soud ČR v nálezu Pl. ÚS 24/10, již výše rozebíraném, když - sice pouze obiter dictum, v závěru svého nálezu, přesto však jednoznačně – vyjádřil pochybnosti nad tím, „*zda je vůbec žádoucí, aby soukromé osoby (poskytovatelé služeb v oblasti internetu a telefonní a mobilní komunikace, zejm. mobilní operátoři a obchodní společnosti zajišťující připojení k internetu) byly nadány oprávněním uchovávat veškeré údaje o jimi poskytované komunikaci i o zákaznících, jimž jsou jejich služby poskytovány (tzn. údaje jdoucí i nad rozsah údajů, jež jsou dle napadené právní úpravy povinny uchovávat)*“[628].

Problematika zabezpečení zpracovávaných osobních údajů je však významná též v případech, kdy zpracování provádí či má provádět orgán veřejné moci. I zde je nutno posoudit, zda takový orgán je dostatečně personálně i odborně a organizačně vybaven k danému zpracování, zda má dostatečné a jednoznačně definované procesy, při nichž má

ČR sp. zn. IV.ÚS 335/07 ze dne 19. března 2007, sp. zn. Pl. ÚS 16/94 ze dne 21. července 1994 či sp. zn. II.ÚS 1276/16 ze dne 25. října 2016.

[628] Viz nález Ústavního soudu ČR Pl. ÚS 24/10 ze dne 22. března 2011, bod 57. Za zmínku stojí též to, že Ústavní soud ČR zde své sdělení doplňuje mylným závěrem, dle kterého poskytovatelé služeb s takto shromažďovanými údaji volně disponují „*za účelem vymáhání pohledávek, rozvoje obchodní činnosti a marketingu*“. Tento závěr vychází patrně z nedorozumění, když k takovýmto činnostem nepochybně poskytovatelé služeb elektronických komunikací nejsou oprávněni údaje shromažďované v rámci povinnosti Data Retention využívat, ani z dostupných informací o kontrolách provedených ze strany ÚOOÚ u těchto poskytovatelů po dobu existence povinnosti Data Retention nevyplývá jakékoli podezření z takovéhoto využívání. Navíc samotný Ústavní soud ČR tento svůj závěr v odůvodnění nálezu neopírá o žádné konkrétní zjištění a není tak zřejmé, na základě čeho k tomuto dosti závažnému varování dospěl.

docházet k plošnému zpracování osobních údajů, a zda se technická a organizační opatření v případě konkrétního orgánu jeví jako dostatečná k předejití možnému porušení zabezpečení zpracovávaných osobních údajů či jejich využití pro jiný než zákonem vymezený účel. Takto tomu zřejmě nebylo např. v případě návrhu novely zákona o ochraně veřejného zdraví[629], kterou do legislativního procesu předložilo Ministerstvo zdravotnictví v závěru roku 2020. Tato novela předpokládala mj. jednotné řízení státního zdravotního dozoru a vytvoření Státní hygienické služby jakožto ústředního orgánu, který se měl stát nástupcem stávajících krajských hygienických stanic, s cílem „*zvýšit efektivitu a vyšší úroveň koordinace všech zainteresovaných subjektů při výkonu státního zdravotního dozoru*“, deklarovaným v důvodové zprávě k návrhu. Navíc však měla Státní hygienická služba takto získat některé zcela nové pravomoci, včetně oprávnění vyžádat si lokalizační údaje účastníků a uživatelů sítí a služeb elektronických komunikací. Tato novela zůstala ve stadiu návrhu, který kvůli silné kritice nebyl předložen Parlamentu ČR, stále však zůstává v oficiálním systému legislativního procesu. Pomineme-li hodnocení proporcionality navrhované úpravy, je nutno zdůraznit, že nynější krajské hygienické stanice dle hodnocení autora nejsou vybaveny takovými technickými a organizačními opatřeními, aby byly způsobilé bez rizika zpracovávat lokalizační údaje značného množství osob; dle dostupných informací by tomu patrně nebylo jinak ani u zamýšlené Státní hygienické služby.

4.2 Doporučení de lege ferenda

4.2.1 Obecně ke kontrolním mechanismům a zárukám

Jak autor ukázal na rozboru několika typových případů nejzávažnějších zásahů do práva na ochranu soukromí popisovaných v této práci, přibývá takových zásahů do tohoto základního práva, které jsou založeny na konkrétní právní úpravě a představují plošné shromažďování a další zpracování osobních údajů velkého množství osob, bez omezení na konkrétní skupinu osob, definovanou jednoznačně a na základě vymezeného účelu zpracování. Nic také nenasvědčuje tomu, že by takovéto zásahy měly z jakýchkoli důvodů ustat, naopak, z vývoje posledních několik let[630] lze usuzovat, že obdobných zásahů opírajících se o platnou

[629] Dostupné v elektronické knihovně připravované legislativy eKlep pod č.j. MZDR 53739/2020.

[630] Jen v posledních několika letech byla zahájena plošná zpracování osobních údajů ve třech z případů rozebíraných v této práci – povinnost leteckých dopravců shromažďovat údaje jmenné evidence cestujících dle Směrnice PNR byla promítnuta do zákona o civilním letectví novelou účinnou od 24. dubna 2019, Nařízení eCall ukládá výrobcům povinnost instalace systému eCall do nově vyrobených automobilů od 31. března 2018, novela zákona o pozemních komunikacích od roku 2021 zavedla elektronické dálniční známky a s nimi související zpracování osobních údajů.

právní úpravu bude do budoucna přibývat. Autor je proto na základě uvedeného přesvědčen o potřebě vymezit opatření, která by měla být aplikována jak pro existující zásahy do práva na ochranu soukromí, tak rovněž de lege ferenda pro zásahy založené na právních úpravách, které v budoucnu mohou být přijaty a které budou vykazovat typové znaky plošných zpracování popsaných v této práci.

Jak autor podrobně rozebral v předchozím textu, v případech právních předpisů zakládajících zásahy do soukromí za účelem naplnění určitých veřejných zájmů či pro zajištění základních práv jiných osob patří mezi zásadní a nezbytné předpoklady zajištění ústavnosti též dostatečné kontrolní mechanismy. Tyto mechanismy slouží jako prevence před zneužitím oprávnění určených k zajištění cílů vymezených právní úpravou. Ústavní soud ČR takovéto mechanismy považuje za nezbytný předpoklad toho, aby zásah do základních práv obstál v testu proporcionality, jak zdůraznil např. v nálezu Pl. ÚS 3/14. V tomto nálezu Ústavní soud ČR takovéto potřebné mechanismy označil za účinné záruky *„ústavněprávní ochrany proti zneužití“*, v posuzovaném případě konkrétně záruky proti zneužití získaných informací. Obecně jde o záruky před svévolnou aplikací omezení základního práva, resp. šířeji o záruky přiměřenosti zásahů do soukromí.

Doporučení se týkají v prvé řadě kontrolních mechanismů, které by měly být zakotveny v takových předpisech, které z některého z důvodů výše uvedených, zásah do práva na ochranu soukromí zakládají. Na základě relevantní judikatury soudů v oblasti konkrétních zásahů do práva na ochranu soukromí, společně se stanovisky orgánů dozoru a dalších orgánů, které autor rozebíral výše, u jednotlivých typových zásahů do tohoto práva, lze dle hodnocení autora učinit několik obecných závěrů ve vztahu ke kontrolním mechanismům, které by měly být zakotveny v právních úpravách zakotvujících právní instituty, které představují zásah do práva na ochranu soukromí a do práv souvisejících. To platí zvláště v případech, kdy jde o zásahy plošné a nerozlišující, to samozřejmě za podmínky, že takovýto plošný zásah v konkrétním případě, resp. samotná právní úprava zásah zakotvující, splňuje kritéria proporcionality a nejde tak o zásah odporující ústavněprávním požadavkům, jak tyto vyplývá z relevantní rozhodovací praxe rozebírané v této práci, a tedy o zásah nepřípustný.

Je zřejmé, že existují jak obecné kontrolní mechanismy, které lze aplikovat ve většině případů zásahů do práva na ochranu soukromí rozebíraných v této práci a ideálně též v případech obdobných budoucích zásahů, tak rovněž konkrétní mechanismy, týkající se pouze některých zde diskutovaných případů. U některých ze zásahů do práva na ochranu soukromí, o nichž autor pojednal výše, byly již v současnosti určité kontrolní mechanismy

stanoveny relevantní právní úpravou specificky pro konkrétní zásah, s cílem eliminovat možnost zneužití, nadměrného užívání konkrétního zásahu či jeho využívání v situaci, kdy nejsou splněny pro tento zásah zákonem stanovené podmínky. Některé z nich byly přijaty společně s právní úpravou, která vymezuje povinné plošné shromažďování osobních údajů, jiné se vyvinuly teprve následně, v průběhu aplikace takovéto právní úpravy, zejména v důsledku rozhodovací praxe soudů[631]. U každého z nich je nutno posoudit a vyhodnotit, nakolik jde o mechanismus efektivní, a především, zda je v praxi dosažitelný pro dotčené osoby – subjekty údajů a zda je též skutečně v dostatečné míře využíván, jak na to autor poukázal u některých výše rozebíraných případů či zda takovémuto využívání v praxi brání existující překážky právního či faktického charakteru. Tímto se autor zabýval u jednotlivých, výše rozebíraných, konkrétních případů zásahů do práva na ochranu soukromí. Cílem této práce je však závěry učiněné takto v konkrétních případech zobecnit a navrhnout jejich aplikaci i pro futuro, v případech budoucích zásahů.

S ohledem na výše uvedené autor v následujícím textu popisuje konkrétní kontrolní mechanismy, které v této práci identifikoval jako relevantní a způsobilé zajistit ochranu ústavnosti a specificky ochranu základního lidského práva na ochranu soukromí v případě zásahů do tohoto práva v podobě zákonem založeného plošného shromažďování osobních údajů. U kontrolních mechanismů již existujících, tedy již zakotvených v současné právní úpravě, se autor zaměřuje na zhodnocení jejich efektivity v praxi, včetně případných návrhů na jejich úpravy de lege ferenda, s cílem maximálního zajištění proporcionality ve vztahu mezi zamýšleným účelem právní úpravy a zásahem do práva na ochranu soukromí, který tato právní úprava zakládá. Autor považuje za zásadní cíl svého vyhodnocení kontrolních mechanismů možnost zobecnění těchto závěrů a možnost vztáhnout doporučení týkající se kontrolních mechanismů jak na případy popsané v této práci, tak rovněž na případy budoucích zásahů do práva na ochranu soukromí, k nimž patrně bude i nadále docházet v důsledku nových právních úprav, které však aktuálně nelze identifikovat. Z tohoto důvodu se autor pokusí dále své závěry s ohledem na tento cíl zobecnit.

[631] Takto tomu bylo např. u zvláštního řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu a příkazu k zjištění údajů o telekomunikačním provozu upraveného mezi zvláštními způsoby řízení v § 314l – § 314n Trestního řádu.

4.2.2 Kontrolní mechanismy v rámci legislativního procesu – legislativní pravidla a legislativní DPIA analýza, konzultace s dozorovým orgánem

Jak autor ukázal v této práci, mnohá velmi závažná plošná shromažďování a další zpracování osobních údajů značných množství osob jsou založena na obecně závazných právních předpisech, které takováto plošná shromažďování ukládají jako povinnost – z případů analyzovaných v této práci je tomu tak u povinného uchovávání provozních a lokalizačních údajů elektronických komunikací, zpracování osobních údajů systémy v automobilech, osobních údajů leteckých cestujících či údajů o zdravotním stavu. Primární kontrolu naplnění požadavků na proporcionalitu zásahu je tedy nutno zajistit ještě dříve, než k zásahu samotnému dojde, již ve fázi legislativního procesu příslušné právní úpravy, a to jak co do samotné potřebnosti zásahu jako takového, tak rovněž ve vztahu k šíři a intenzitě zásahu.

Procesy a pravidla, která se uplatňují již v rámci legislativního procesu, patří mezi záruky ústavnosti. Především jsou však z časového hlediska prvními kontrolními mechanismy, které se uplatní již při přípravě legislativního návrhu. Legislativní pravidla vlády[632] stanoví pro všechny vládní legislativní návrhy obsahové a formální požadavky aplikované na připravované právní předpisy a pravidla, podle nichž postupují ministerstva a jiné ústřední orgány státní správy při tvorbě a projednání připravovaných právních předpisů. Dle těchto pravidel v prvé řadě musí přípravě každého právního předpisu „*předcházet podrobná analýza právního a skutkového stavu*“, jejíž součástí je i „*zhodnocení nezbytnosti změny právního stavu*“ (viz čl. 2 odst, 1). Legislativní pravidla zahrnují mj. i povinnost vyhodnotit, mezi jinými aspekty, též dopady do soukromí. Konkrétně již ve fázi věcného záměru ukládají legislativní pravidla povinnost vypracovat „*zhodnocení současného stavu a dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů, které musí obsahovat vysvětlení účelu navrhovaného zpracování osobních údajů a popis návaznosti na stávající nebo již připravovaná zpracování osobních údajů, posouzení navrhovaného řešení zpracování z hlediska nezbytnosti a přiměřenosti ve vztahu k jím sledovanému účelu a posouzení rizik pro práva a svobody fyzických osob a možných opatření k jejich snížení*“ (viz čl. 4 odst. 1 písm. h). Obdobně též následně důvodová zpráva, která je součástí návrhu každého zákona, obsahuje v obecné části rovněž „*zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů*“ (viz čl. 9 odst. 2 písm. i). Tyto povinnosti se neomezují pouze na návrhy zákonů, čl. 14 Legislativních pravidel vlády ukládá obdobné povinné

[632] Vláda ČR. *Legislativní pravidla vlády.* [online]. [cit. 23.2.2024]. Dostupné z www.vlada.gov.cz.

náležitosti též pro odůvodnění návrhu nařízení vlády a dle čl. 16 odst. 4 se vztáhnou obdobně též na odůvodnění návrhu vyhlášky. Tato pravidla platí pro všechny vládní legislativní návrhy bez rozdílu, neuplatňují se tak specificky pouze u návrhů, které dle předběžného vyhodnocení zahrnují mj. zásah do práva na ochranu soukromí.

V rámci těchto obecných povinností je ochrana soukromí, resp. ochrana osobních údajů jednou z oblastí, které je nutno vyhodnotit. Legislativní pravidla, zahrnující i „Metodiku hodnocení dopadů regulace na administrativní zátěž občanů, včetně dopadů na soukromí", která tvoří metodický podpůrný nástroj k Obecným zásadám RIA, jsou takto nastavena dlouhodobě[633]. Vedle těchto obecných povinností existuje též specifický kontrolní mechanismus, který vstoupil v účinnost relativně nedávno a jeho praktická aplikace tak ještě neprobíhá zcela automaticky. Je jím povinnost konzultace s dozorovým úřadem, kterou ukládá členským státům GDPR v čl. 36 odst. 4 u všech „návrhů legislativních opatření", která „*má přijmout vnitrostátní parlament*" a též u každého návrhu „*regulačního opatření založeného na takovém legislativním opatření, jež souvisí se zpracováním*". Použije se tedy až od účinnosti GDPR, ode dne 25. května 2018[634]. Tento mechanismus má za cíl již v rámci legislativního procesu zabránit nadměrným, nepřiměřeným a nevyváženým zásahům do práva na ochranu soukromí, uplatňuje se tedy ve vztahu ke všem takovýmto zásahům, ke kterým dochází na základě právní úpravy, bez ohledu na konkrétní právní úpravu umožňující zásah. Jde o mechanismus preventivního charakteru, určený k využití před samotným zásahem.

Jedná se o povinnost obdobnou té, kterou ukládá GDPR v témže článku 36 každému správci v případech, kdy určitý druh zpracování osobních údajů bude mít pravděpodobně za následek vysoké riziko pro práva a svobody fyzických osob a z posouzení vlivu na ochranu osobních údajů (analýzy DPIA) vyplynulo, že by takový následek v podobě vysokého rizika nastal v případě, že by „*správce nepřijal opatření ke zmírnění tohoto rizika*"[635]. Konzultační

---

[633] Samotná Legislativní pravidla vlády byla schválená usnesením vlády ze dne 19. března 1998 č. 188 a následně postupně upravována a doplňována v dalších letech, Metodika hodnocení dopadů regulace na administrativní zátěž občanů, včetně dopadů na soukromí, byla vydána v červnu 2015, Obecné zásady pro hodnocení dopadů regulace (RIA) v aktuální podobě nabyly účinnosti 3. února 2016. Všechny tři uvedené dokumenty dostupné z www.vlada.gov.cz.

[634] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, která předcházela Obecnému nařízení GDPR, zakotvovala v čl. 20 mechanismus předběžné kontroly, v jehož rámci prováděly orgány dozoru předběžná šetření, zpravidla na základě oznámení od správce. Čl. 20 pak v odst. 3 stanovil specifickou možnost členských států „*přistoupit k tomuto šetření rovněž v rámci vypracování opatření přijatého vnitrostátním parlamentem nebo opatření založeného na tomto legislativním opatření, které vymezuje povahu zpracování a stanoví vhodná ochranná opatření*". Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, jakožto národní právní předpis pro oblast ochrany osobních údajů, ani jiný relevantní právní předpis však takovýto proces neupravoval a v praxi tak v ČR u legislativních opatření nebyla prováděna předběžná šetření.

[635] Viz čl. 35 odst. 1 ve spojení s čl. 36 odst. 1 GDPR.

povinnost uložená členským státům dle čl. 36 odst. 4 se však aplikuje bez ohledu na to, zda přetrvává vysoké riziko. Pokud jde o šíři dopadu, autor považuje za plně odůvodněný názor vyslovený v Komentáři ke GDPR[636], který pojem „regulační opatření" obsažený v tomto ustanovení, vykládá dosti široce. Autoři komentáře k tomu uvádějí: „*Podle našeho názoru se jimi rozumějí nejen podzákonné právní předpisy, například vládní nařízení či vyhlášky ministerstva, ale jakákoliv obecná opatření orgánů veřejné správy přijímaná na základě právních předpisů, tedy i ohledně zpracování založených na právním základu podle čl. 6 odst. 1 písm. e).*" Současně je však z gramatického výkladu tohoto ustanovení zřejmá limitace, uváděná i autory komentáře: „*Tato konzultační povinnost se však vztahuje pouze na legislativu přijímanou přímo parlamentem nebo opatření přijímaná na jejím základě. Nevztahuje se tedy na právní předpisy v oblasti samosprávy, jako jsou vyhlášky obcí v samostatné působnosti.*" Je však nutno brát v úvahu, že z textu čl., 36 odst. 4 GDPR ani ze ZoZOÚ nevyplývá konkrétní navazující povinnost předkladatele návrhu konzultovaného právního předpisu zohlednit výsledky takovéto konzultace. Autor plně souhlasí s názorem autorů citovaného komentáře, dle kterého by měl „*předkladatel návrhu výstupy takové konzultace vždy brát v úvahu*".

Obdobně jako v případě správců, též u předkladatelů návrhů legislativních opatření je nezbytným předpokladem konzultace předchozí vypracování DPIA analýzy, v těchto případech legislativní DPIA analýzy, tedy analýzy posouzení vlivu návrhů právních předpisů na ochranu osobních údajů. Legislativní DPIA má svůj základ již v usnesení Vlády ČR z roku 2012[637]. Bohužel však stále v praxi předkladatelé mnohdy přistupují k přípravě DPIA analýzy formalisticky, jak upozornil ÚOOÚ v materiálech „Nová úprava DPIA" a „Návod k posouzení vlivu na ochranu osobních údajů u návrhů právních předpisů (DPIA)"[638], publikovaných v rámci přípravy a veřejné konzultace k návrhu upravené metodiky legislativní DPIA analýzy. Dle zkušeností ÚOOÚ bývá v některých případech na zpracování řádné legislativní DPIA analýzy a její vyhodnocení nedostatek času. V důsledku toho pak „*posouzení vlivu na ochranu osobních údajů je redukováno na prosté konstatování, že předloha je v souladu se zákonem či GDPR*", zcela však schází popis zpracování osobních údajů, které návrh právní úpravy předpokládá. Následně tedy nelze určit, zda je zamýšlené zpracování osobních údajů legální a

---

[636] Viz UŘIČAŘ, Miroslav, RÁMIŠ, Vladan a kol. *Obecné nařízení o ochraně osobních údajů. Komentář. 1. vydání.* Praha: C. H. Beck, 2021. s. 832 a násl.

[637] Vláda ČR v usnesení č. 820 ze dne 14. listopadu 2012 o změně Legislativních pravidel vlády schválila s účinností od 1. ledna 2013 změny Legislativních pravidel vlády, zahrnující mj. i zavedení legislativní DPIA.

[638] ÚOOÚ. *Nová úprava DPIA*. Publikováno 9.2.2023. *Návod k posouzení vlivu na ochranu osobních údajů u návrhů právních předpisů (DPIA).* 3. ledna 2019. [online] [cit. 12.1.2024]. Oba materiály dostupné z www.uoou.gov.cz.

legitimní. Konstatování souladu legislativního návrhu se zákonem však dle ÚOOÚ „*součástí legislativního DPIA ani být nemá, protože se rozumí samo sebou*“[639].

Dle autora lze z těchto varovných konstatování ÚOOÚ učinit závěr, že se ÚOOÚ s takto zásadní bagatelizací provedení legislativní DPIA nesetkává v praxi pouze ojediněle. V opačném případě by patrně ÚOOÚ nepovažoval tento přístup za problém, který je nutno řešit systémově, úpravami metodiky legislativní DPIA analýzy. To však dle hodnocení autora naznačuje, že se jedná nikoli pouze o individuální lidské selhání v konkrétních případech, nýbrž dosti možná o systémový problém. Je totiž pouze obtížně představitelné, že by situace, kdy se legislativní DPIA omezí na konstatování souladu posuzovaného návrhu právního předpisu se zákonem, byla pouhým důsledkem časového tlaku na předkladatele návrhu právního předpisu. Patrně se v takových případech jedná o problém hlubší, spočívající v tom, že takto ryze formalisticky zpracovaná legislativní DPIA analýza není v rámci legislativního procesu shledána zjevně nedostatečnou, kdy jako jednoznačný důsledek by celý takovýto návrh právního předpisu měl být vrácen k přepracování. Legislativní DPIA analýza totiž dle hodnocení autora není samostatným dokumentem, který lze k návrhu právního předpisu doplnit až následně. Pokud má obsahovat mj. posouzení nezbytnosti a přiměřenosti právního předpisu se zaměřením na zamýšlené zpracování, musí se naopak právní předpis přizpůsobit výsledkům a závěrům analýzy. Také právní úprava ZoZOÚ vychází z předpokladu, že právní předpis, který stanoví povinné zpracování osobních údajů, byl připraven se zohledněním rizik pro práva fyzických osob – subjektů údajů, a proto správce není v takovém případě povinen vypracovat vlastní DPIA analýzu[640].

Právě tyto nedostatky v oblasti ochrany osobních údajů, které ÚOOÚ v praxi u legislativních návrhů shledával, se staly důvodem, pro který ÚOOÚ připravil metodické doporučení pro posouzení dopadů na ochranu osobních údajů u předloh právních předpisů. Novela legislativních pravidel vlády účinná od 1. dubna 2023[641] změnila mimo jiné pravidla pro zpracování posouzení vlivu na ochranu osobních údajů a vymezila požadavky na legislativní DPIA analýzu, včetně nezbytné náležitosti v podobě popisu návaznosti

---

[639] Viz ÚOOÚ. *Zahájena veřejná konzultace k metodice legislativního DPIA*. Publikováno 8.3.2023. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.

[640] Viz Výjimka z povinnosti posouzení vlivu zpracování osobních údajů na ochranu osobních údajů obsažená v § 10 ZoZOÚ, dle které „*Správce nemusí provádět posouzení vlivu zpracování na ochranu osobních údajů před jeho zahájením, pokud mu právní předpis stanoví povinnost takové zpracování osobních údajů provést*“.

[641] Návrh změn Legislativních pravidel vlády, Obecných zásad pro hodnocení dopadů regulace (RIA) a Jednacího řádu vlády čj. 1508/22 – bod 32 schůze vlády konané dne 21. 12. 2022, předložený ministrem pro legislativu a předsedou Legislativní rady vlády, byl na jednání vlády konaném 11. ledna 2023 schválen se změnou. Schválené znění dostupné z https://www.odok.cz/portal/zvlady/jednani-detail/2023-01-11/.

navrhovaného zpracování osobních údajů „*na stávající nebo již připravovaná zpracování osobních údajů*“ a především „*posouzení navrhovaného řešení zpracování z hlediska nezbytnosti a přiměřenosti ve vztahu k jím sledovanému účelu a posouzení rizik pro práva a svobody fyzických osob a možných opatření k jejich snížení*“. ÚOOÚ proto v návaznosti na tyto změny připravil metodické doporučení, které má nahradit dosavadní Návod k posouzení vlivu na ochranu osobních údajů u návrhů právních předpisů (DPIA)[642].

V době přípravy této práce není k dispozici finální znění metodického doporučení ÚOOÚ. Autor však obecně tento krok ÚOOÚ hodnotí jako pozitivní, a to ve dvou směrech – v prvé řadě tím úřad signalizuje zvýšený důraz na aspekty ochrany osobních údajů v rámci prací na legislativních návrzích, což by se v praxi mělo dotknout především těch návrhů, které mají potenciál zasáhnout do práva na ochranu soukromí, ve druhé řadě je pozitivní, že ÚOOÚ v rámci své působnosti dozorového orgánu sleduje a hodnotí vývoj i v rovině legislativní a na identifikované nedostatky reaguje úpravami pravidel. Lze tedy očekávat, že tyto kroky do budoucna mohou přinést pozitivní dopady, mj. i v případech, které se budou týkat dalších zásahů do ochrany osobních údajů, resp. do práva na ochranu soukromí. Současně je však dle hodnocení autora v této chvíli předčasné hodnotit očekávané dopady takovýchto kroků v praxi. Jednak je otázkou, zda předkladatelé, kteří dosud k přípravě legislativních DPIA analýz přistupovali dle pozorování ÚOOÚ formalisticky, změní svou praxi pouze v důsledku novely Legislativních pravidel vlády a navazujícího metodického doporučení ÚOOÚ. Dále lze zatím stěží předvídat, zda kvalitnější DPIA analýza v konkrétních případech skutečně povede k eliminaci zásahů do soukromí či alespoň ke snížení jejich četnosti a intenzity a zkvalitnění efektivních kontrolních mechanismů a dostatečných záruk.

Autor si je vědom skutečnosti, že uplatnění výše popsaného kontrolního mechanismu v podobě obsažené v Legislativních pravidlech vlády, společně s povinností provést legislativní DPIA analýzu je v praxi v mnoha případech do značné míry limitováno faktem, že legislativní návrh je pouze implementací právní úpravy unijního práva – takto tomu bylo např. u povinnosti Data Retention dle Data Retention Směrnice[643], u povinného zpracování údajů jmenné evidence cestujících - PNR či u povinného zavádění systému eCall. I v těchto případech však má jak předkladatel, tak rovněž zákonodárce zpravidla určitou

[642] ÚOOÚ. *Návod k posouzení vlivu na ochranu osobních údajů u návrhů právních předpisů (DPIA)*. 3. ledna 2019. Dostupné z www.uoou.gov.cz .

[643] V případě povinnosti Data Retention Evropská komise v praxi uplatňovala právní kroky vůči členským státům EU, které neprovedly transpozici této povinnosti dle Data Retention Směrnice – tak tomu bylo v případě Německa, Rakouska či Švédska.

možnost volby, byť nikoli ohledně samotného provedení transpozice a tím méně u adaptace právního řádu pro zajištění aplikace nařízení, nýbrž ve vztahu k šíři implementace unijního práva. Implementaci předpisů Evropské unie do právního řádu ČR i celkovou implementaci těchto předpisů, tedy zajištění náležité aplikace adekvátních opatření, vč. následného účinného vymáhání práv a povinností založených takovou právní úpravou, je totiž obecně možno provést buďto způsobem, který splňuje minimální požadavky stanovené v konkrétním případě implementovaným předpisem Evropské unie, nebo je provést formou „neminimalistické implementace“[644], tedy přijetím takových požadavků v právním řádu ČR, které jsou nad rámec minimálních požadavků stanovených předpisy Evropské unie, např. využitím rozšiřující výjimky, tedy využitím „*ustanovení implementovaného předpisu Evropské unie, které stanoví možnost odchýlit se od obecné úpravy obsažené v tomto předpisu Evropské unie, a to v rozšiřujícím směru*“, nevyužitím zužující výjimky, která v implementovaném předpisu Evropské unie umožňuje odchýlit se od obecné úpravy obsažené v tomto předpisu ve zužujícím smyslu, případně tím, že předkladatel právního předpisu zvolí takovou z variant obsažených v implementovaném předpise, která je nejméně zatěžující. Pokud se takováto volba týká aspektů, které zahrnují zásahy do základního práva na ochranu soukromí, pak učinění příslušné volby by mělo být provedeno způsobem, který je založen na principu proporcionality a je plně v souladu s ním.

V praxi tomu tak ovšem vždy nemusí být, jak uvádí mj. rovněž Jan Kudrna ve svém textu „Pravděpodobně nejvíce porušované ustanovení Listiny (a jedna ze současných hrozeb lidským právům)“[645] a dokládá tuto skutečnost právě příkladem týkajícím se zásahu do práva na ochranu soukromí v podobě plošného shromažďování provozních a lokalizačních údajů. Jak pisatel následně upozorňuje, v případě, který ve svém textu popisuje, tedy u novely zákona o elektronických komunikacích týkající se povinného plošného uchovávání provozních a lokalizačních údajů, neproběhla v Poslanecké sněmovně v rámci legislativního procesu k této novele diskuse o jádru problému. Místo toho v průběhu legislativního procesu spíše zaznívaly

---

[644] Dle Metodických pokynů pro zajišťování prací při plnění legislativních závazků vyplývajících z členství České republiky v Evropské unii, schválených usnesením vlády ze dne 12. října 2005 č. 1304 a změněných usnesením vlády ze dne 26. října 2009 č. 1344, usnesením vlády ze dne 3. ledna 2018 č. 19 a usnesením vlády ze dne 27. února 2018 č. 138, platí, že „*neminimalistickou implementací se rozumí stanovení požadavků v právním řádu České republiky nad rámec minimálních požadavků stanovených předpisy Evropské unie*“. Podrobné vymezení „neminimalistické implementace“ obsahuje též Metodická pomůcka pro prevenci nadbytečné regulatorní zátěže při implementaci práva EU, na niž odkazují Obecné zásady pro hodnocení dopadů regulace (RIA) schválené usnesením Vlády ČR č. 922 ze dne 14. prosince 2011.

[645] KUDRNA, Jan. Pravděpodobně nejvíce porušované ustanovení Listiny (a jedna ze současných hrozeb lidským právům) in GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012 s. 275 a násl.

zavádějící informace a „*ani při projednávání ve výborech neproběhla diskuse o podstatě problému, tedy zda a případně v jakém rozsahu shromažďovat údaje, jak je chránit proti zneužití, aby bylo zachováno soukromí jednotlivců*“.

Kudrna ovšem v této souvislosti upozorňuje i na legislativní proces na straně evropského zákonodárce u Data Retention Směrnice, u které dle jeho komentáře neproběhla zralá úvaha o tomto omezení lidských práv, kteréžto úvaze měla předcházet kvalifikovaná diskuse o problému a možných řešeních, včetně zhodnocení, „*zda nebezpečí skutečně existuje, zda je odstranitelné či minimalizovatelné, případně jakým způsobem a zda přijímané řešení tuto roli může vůbec sehrát“*. Na základě výše uvedeného pak závěrem výslovně uvádí, že příprava a schválení Data Retention Směrnice „*je velmi často kritizována právě z toho důvodu, že uvedené požadavky splněny nebyly a že naopak směrnice ve své stávající podobě vytváří prostor pro další nepřiměřené zásahy do lidských práv a svobod, aniž by tyto vedly k podstatnému omezení, nebo dokonce eliminaci bezpečnostních hrozeb*“. Navíc ohledně samotného legislativního návrhu novely zákona o elektronických komunikací Kudrna uvádí, že „*v mnoha směrech šla česká právní úprava vysoko nad rámec opatření obsažených ve směrnici*“.

Dle hodnocení autora popisovaná situace představuje problém, který je systémově řešitelný pouze částečně. Kvalitu těch fází legislativního procesu, které následují po přípravě vládního návrhu zákona a při kterých je návrh zákona projednáván zákonodárným sborem, lze ovlivnit pouze nepřímo a navíc jen do jisté míry, stanovením pravidel aplikovaných již v předchozích fázích tohoto procesu, tedy pravidel pro přípravu návrhu zákona předkladatelem. Toto je cílem zmiňovaných Legislativních pravidel vlády, která se aplikují v procesu přípravy vládních návrhů. V následujících fázích legislativního procesu však již dle hodnocení autora obecně neexistuje možnost ingerence ze strany moci výkonné či soudní přímo do legislativního procesu konkrétního právního předpisu v jeho průběhu. Totéž platí obdobně též v případě legislativních návrhů, které nebyly předloženy jako vládní návrh, typicky u poslaneckých zákonodárných iniciativ. ÚOOÚ sice v textu „Metodika pro legislativní DPIA“[646] doporučuje „*vložit legislativní DPIA rovněž do důvodové zprávy iniciativního návrhu nebo do odůvodnění věcných pozměňovacích návrhů*“, autor má však pochybnosti o tom, zda se navrhovatelé budou takovýmto doporučením skutečně v praxi řídit.

[646] ÚOOÚ. *Metodika pro legislativní DPIA*. Bez uvedení data publikace. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.

Také autoři Komentáře ke GDPR[647] se zabývali mj. otázkou, jaká je reálná možnost aplikace ustanovení čl. 36 odst. 4 GDPR ukládajícího členským státům povinnost konzultace s dozorovým úřadem během přípravy návrhu legislativního opatření „*v případě legislativních návrhů připravených mimo vládu ČR, tedy v případě návrhů zákonů předkládaných dalšími osobami se zákonodárnou iniciativou (poslanec, skupina poslanců. Senát či zastupitelstvo vyššího územního samosprávného celku)*“. Dospěli k závěru, dle kterého „z textace odstavce 4 („*Členské státy konzultují s dozorovým úřadem během přípravy návrhu legislativního opatření, které má přijmout vnitrostátní parlament…“) je zřejmé, že se povinnost takové konzultace vztahuje na všechna legislativní opatření přijímaná vnitrostátním parlamentem, a přikláníme se tak k tomu, že i v případě návrhů legislativních opatření, které nevypracovala vláda, je praktické, aby k takovéto konzultaci byla povinna vláda ČR, když dle § 87 odst. 2 JŘPS platí, že „Pokud není navrhovatelem vláda, předseda Sněmovny ji požádá, aby se do 30 dnů od doručení žádosti k návrhu svým stanoviskem vyjádřila*“. Obecně pak je dle hodnocení autora v této souvislosti nutno pečlivě zvážit míru, s jakou může moc výkonná zasahovat do oblasti legislativního procesu. Aleš Gerloch označil otázku „*extenzí mezi exekutivou a legislativou, převážně expanze exekutivy do legislativy*“ již v současné podobě za jednu ze slabin ústavního prostředí České republiky. Ústava podle jeho hodnocení „*tyto extenze sice uznává, ale současně se dostávají do rozporu s oním klasickým označením – moc zákonodárná, moc výkonná*“[648].

Uvedené pochybnosti však dle autora neznamenají, že by bylo nutno rezignovat na kvalitu legislativních pravidel, právě naopak. Tato pravidla se uplatňují na předkladatele vládních legislativních návrhů – právě právní předpisy navržené jakožto vládní návrhy přitom zpravidla zakládají typové příklady zásahů do práva na ochranu soukromí diskutované v této práci. Navíc u návrhů právních předpisů či u věcných pozměňovacích návrhů si poslanec-zpravodaj projednávaného návrhu může vyžádat stanovisko relevantního ministerstva, které v něm může zohlednit, kromě dalších podstatných otázek, též problematiku ochrany osobních údajů. Nedostatky legislativního procesu, vč. konkrétních doporučení ke zlepšení se podrobně zabýval Aleš Gerloch, který upozornil mj. na vysoké tempo přijímání nových právních předpisů a jejich celkové množství a též na otázky formy a obsahu pozměňovacích a doplňujících poslaneckých návrhů[649]. Aleš Gerloch upozornil také na časté změny a

[647] UŘIČAŘ, Miroslav, RÁMIŠ, Vladan a kol. *Obecné nařízení o ochraně osobních údajů. Komentář. 1. vydání.* Praha: C. H. Beck, 2021. s. 833.
[648] GERLOCH, Aleš. *Ústava a ústavnost v České republice.* Soudce 11/2016. s. 56.
[649] K tomu viz GERLOCH, Aleš a kol. *Teorie a praxe tvorby práva.* Praha: ASPI, 2008. s. 362 a násl.

novelizace právních předpisů, jakožto jeden z ne příliš pozitivních projevů západní civilizace[650].

Někteří ústavní odborníci v této souvislosti uvažují o možných omezeních a doplnění povinností pro poslanecké zákonodárné iniciativy a pozměňovací návrhy, v zájmu zvýšení jejich legislativní kvality. Boris Balog takto např. navrhuje ústavní omezení práva zákonodárné iniciativy zavedením minimálního počtu poslanců oprávněných podat návrh zákona a také povinné odůvodňování pozměňovacích návrhů, vč, hodnocení jejich dopadů do konkrétních oblastí[651]. Tyto návrhy se sice týkají primárně Slovenské republiky a jejího právního řádu, mohou však být relevantní i ve vztahu k ČR. Současně však autor považuje za zásadní pečlivé posouzení jakýchkoli návrhů, které by představovaly zásah do legislativního procesu, jak je v aktuální podobě zakotven v Ústavě ČR. Obdobně také např. Aleš Gerloch uvažuje o možnostech změny okruhů subjektů zákonodárné iniciativy v Ústavě ČR tak, že návrh zákona byla oprávněna podat pouze skupina poslanců, nikoli jednotlivý poslanec[652].

Jak již uvedeno výše, plošné shromažďování a zpracování osobních údajů značného množství osob je v praxi v řadě případů založeno na normách práva EU, které jsou do právního řádu ČR následně implementovány, je proto namístě, zahrnout do tohoto posouzení též legislativní proces přijímání norem práva EU. Dle hodnocení autora lze mnohé ze zde uvedených výhrad konstatovat obdobně též ve vztahu k legislativnímu procesu přijímání norem práva EU, jako např. u již diskutované Data Retention Směrnice. Právě tato směrnice může být v tomto směru velmi vhodným příkladem. Také Jan Kudrna v již zmiňovaném textu[653] kritizuje tuto směrnici jako „*jeden z případů, kdy má dojít k výměně „svobody za bezpečnost“,* a upozorňuje v této souvislosti na to, že „*argumentace, v níž převažují emoce, je pro lidská práva velmi nebezpečná*“. Pisatel též uvádí, že tato směrnice „*vytváří prostor pro další nepřiměřené zásahy do lidských práv a svobod, aniž by tyto vedly k podstatnému omezení, nebo dokonce eliminaci bezpečnostních hrozeb*“.

---

[650] Viz úvaha v textu Nový dualismus práva: *„Ale u zákona už je představa úplně opačná, než byla v devatenáctém století. Tehdy se zákon bral jako něco, co má platit po desetiletí, ne-li po staletí jako jasné pravidlo. Teď? Zákon byl schválen a je třeba ho co nejdříve novelizovat nebo pokud možno zrušit a nahradit jinou úpravou. To je bohužel jeden z určitých typických projevů západní civilizace.“* GERLOCH, Aleš. *Nový dualismus práva.* Soudce 7/2014. s. 32.

[651] K tomu viz BALOG, Boris. Inovačné výzvy pre Ústavu z oblasti legislatívy alebo o legislatívnej smršti a iných (nielen meteorologických) poverách v slovenskej legislatíve. In *INOVAČNÉ VÝZVY PRE ÚSTAVY A ÚSTAVNÉ SYSTÉMY V GLOBALIZOVANEJ EURÓPE. Bratislavské právnické fórum 2013. Zborník príspevkov z medzinárodnej vedeckej konferencie.* Bratislava: Univerzita Komenského, 2013. s. 660 a násl.

[652] GERLOCH, Aleš a kol. *Teorie a praxe tvorby práva.* Praha: ASPI, 2008. s. 364.

[653] KUDRNA, Jan. Pravděpodobně nejvíce porušované ustanovení Listiny (a jedna ze současných hrozeb lidským právům) in GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012 s. 277–278.

V případě Data Retention Směrnice navíc dle autora existuje zásadní a neodůvodněný rozpor v důvodech deklarovaných ze strany Evropské komise při přijetí této směrnice a v následné reakci Evropské komise na prohlášení směrnice za neplatnou SDEU. Důvody pro přijetí směrnice jako evropské právní úpravy, obsažené též v recitálech samotné směrnice, velmi jednoznačně formulovaly potřebu přijetí takovéto právní úpravy, a to jednak významem provozních a lokalizačních údajů pro vyšetřování, odhalování a stíhání trestných činů a z toho vyplývající nutností zajistit na evropské úrovni jejich uchování po určitou dobu[654] a též harmonizací povinností poskytovatelů uchovávat tyto údaje, které „*nemůže být uspokojivě dosaženo na úrovni členských států*“[655]. Data Retention Směrnice byla přijata 15. března 2006 a v době jejího prohlášení za neplatnou 8. dubna 2014 tak od jejího přijetí uplynulo pouze 8 let, lze tedy předpokládat, že důvody pro její přijetí uváděné výše se v mezidobí výrazně nezměnily. Přesto však Evropská komise v reakci na prohlášení neplatnosti této směrnice bez dalšího konstatovala, že „*Komise nepřichází s žádnými novými iniciativami v oblasti Data Retention*“ a dokonce toto své konstatování zdůraznila slovy, dle kterých tento závěr již Komise velmi jasně uvedla[656], aniž by přitom jakkoli odůvodnila, proč k takto zásadní změně došlo, zda se dle hodnocení Evropské komise změnila faktická stránka - vyšetřování, odhalování a stíhání trestných činů či potřeba harmonizace povinnosti uchovávání provozních a lokalizačních údajů. Ani v následujících letech Evropská komise tento postoj nezměnila ani jej nijak blíže neodůvodnila. Tato změna dle hodnocení autora zpochybňuje závažnost důvodů deklarovaných při přijetí směrnice.

Klíčovou však je dle autora především otázka možného řešení naznačených nedostatků legislativního procesu u evropského zákonodárce. Logickým by bylo začlenění povinnosti legislativní DPIA analýzy též u návrhů právních předpisů práva EU, a to tím spíše, že nařízení GDPR, v němž byla tato povinnost uložena členským státům, schválil právě

---

[654] Viz bod 11 recitálu Data Retention Směrnice: „*Vzhledem k významu provozních a lokalizačních údajů pro vyšetřování, odhalování a stíhání trestných činnů, jak názorně dosvědčují výzkum i praktické zkušenosti několika členských států, je nutné na evropské úrovni zajistit, aby se po určitou dobu a za podmínek stanovených v této směrnici uchovávaly údaje vytvářené a zpracovávané poskytovateli veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí při poskytování komunikačních služeb.“*

[655] Viz bod 21 recitálu Data Retention Směrnice: *„Jelikož cílů této směrnice, totiž harmonizace povinností poskytovatelů uchovávat určité údaje a zajistit jejich dostupnost pro účely vyšetřování, odhalování a stíhání závažných trestných činů, jak jsou vymezeny každým členským státem v jeho vnitrostátních právních předpisech, nemůže být uspokojivě dosaženo na úrovni členských států, a proto jich z důvodu rozsahu a účinků této směrnice může být lépe dosaženo na úrovni Společenství, může Společenství přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje tato směrnice rámec toho, co je nezbytné k dosažení těchto cílů.“*

[656] European Commission. *European Commission statement on national data retention laws*. Brussels, 16 September 2015. [online] [cit. 03.05.2024]. V anglickém originále „*We have been very clear that the Commission is not coming forward with any new initiatives on Data Retention.*“, přeloženo autorem.

evropský zákonodárce. Bylo by tedy možno očekávat, že evropský zákonodárce, při vědomí skutečnosti, že řada případů zpracování osobních údajů uložených právními předpisy nepramení bezprostředně z národního práva členských států EU, nýbrž je pouze implementací normy práva EU, vyvine snahu regulovat též vlastní legislativní činnost, obdobně jako to činí u legislativního procesu členských států. V praxi tomu tak ovšem není a autor považuje změnu v tomto směru za obtížně realizovatelnou. Prakticky jedinou efektivní možností je tak dle hodnocení autora oprávnění ÚOOÚ, jakožto dozorového orgánu, upozorňovat v konkrétních případech na tyto nedostatky, a to zejména v rámci svého členství v EDPB. Tento sbor byl zřízen čl. 68 GDPR *„jako subjekt Unie s právní subjektivitou"* a sestává z vedoucích každého dozorového úřadu z jednotlivých členských států EU a z Evropského inspektora ochrany údajů nebo jejich zástupců. Evropská komise má právo účastnit se činností a schůzek sboru, bez hlasovacího práva. GDPR v čl. 69 zaručuje EDPB nezávislost při plnění úkolů a výkonu pravomocí, včetně výslovného zakotvení jedné ze složek nezávislosti EDPB v čl. 69 odst. 2, dle kterého „*sbor při plnění svých úkolů nebo výkonu svých pravomocí od nikoho nevyžaduje ani nepřijímá pokyny*". EDPB v rámci svých úkolů vymezených demonstrativním výčtem v čl. 70 GDPR mj. též „*poskytuje poradenství Komisi ve veškerých záležitostech souvisejících s ochranou osobních údajů v Unii*", obdobné oprávnění EDPB vymezuje mezi jeho úkoly též Trestněprávní směrnice. Tyto předpisy uvedené poradenství EDPB nekonkretizují ani jej neformalizují, jak však uvádějí autoři Komentáře ke GDPR, „*Evropská komise by měla doporučení EDPB řádně zohlednit při své činnosti*"[657].

Za možný prostředek k zajištění nápravy výše popsaných situací považuje autor do jisté míry též oprávnění národních soudů obrátit se na Ústavní soud ČR či na SDEU se žádostí o rozhodnutí o předběžné otázce. Možnost tohoto postupu je však omezena pouze na případy stanovené platnou právní úpravou. K předložení věci Ústavnímu soudu ČR je v souladu s čl. 95 odst. 2 Ústavy ČR oprávněn soud, pokud dojde „*k závěru, že zákon, jehož má být při řešení věci použito, je v rozporu s ústavním pořádkem*". Řízení před SDEU o rozhodnutí o předběžné otázce týkající se výkladu Smlouvy o fungování Evropské unie a Smlouvy o Evropské unii či platnosti a výkladu aktů přijatých orgány, institucemi nebo jinými subjekty Unie jsou v souladu s čl. 267 Smlouvy o fungování Evropské unie oprávněny iniciovat soudy členského státu, které považují rozhodnutí o takové otázce za „*nezbytné k vynesení svého rozsudku*", resp. v případě soudu, *„jehož rozhodnutí nelze napadnout opravnými prostředky podle*

[657] UŘIČAŘ, Miroslav, RÁMIŠ, Vladan a kol. *Obecné nařízení o ochraně osobních údajů. Komentář. 1. vydání.* Praha: C. H. Beck, 2021. s. 1132.

vnitrostátního práva“, jde o povinnost obrátit se v této věci na Soudní dvůr EU. Obě tyto možnosti samozřejmě připadají v úvahu až po ukončení legislativního procesu na úrovni EU a zpravidla též na národní úrovni, ve fázi konkrétní aplikace právního předpisu.

Dílčí závěry

Autor shledává výše popsané kontrolní mechanismy v rámci legislativního procesu, tedy mechanismy vyplývající z Legislativních pravidel vlády a též povinnost vypracovat legislativní DPIA analýzu a povinnou konzultaci s ÚOOÚ, jako mechanismy, které jsou obecně způsobilé dosáhnout vymezeného účelu, totiž zajistit dodržování požadavků ústavnosti, vč. záruk práva na ochranu soukromí a práv souvisejících, v legislativním procesu při přípravě právních předpisů, z nichž může vyplývat zásah do těchto práv. Praktickým nedostatkem těchto kontrolních mechanismů je však mnohdy nedodržování povinností uložených právní úpravou ze strany předkladatelů právních předpisů, jak o něm hovoří ÚOOÚ, a to bez jakékoli negativní konsekvence takovéhoto postupu pro předkladatele.

Na základě výše uvedeného se jako logické nabízí řešení v podobě změny právní úpravy, která by předkladatelům právních předpisů jednoznačně uložila povinnost konzultace s ÚOOÚ a povinnost provedení legislativní DPIA analýzy. Takováto změna je proveditelná novelou ZoZOÚ, bez nutnosti zásahu do textu GDPR. V této souvislosti je však nutno uvažovat též o otázce možných negativních konsekvencí v případě nesplnění těchto povinností předkladatelem, kdy jejich absence v praxi do značné míry limituje dopad tohoto opatření. Hypotetická možnost sankcionovat nedodržování povinností či jejich pouhé formální plnění, která by byla zakotvena v obecně závazném právním předpise, se autorovi jeví jako problematická, a to jak v rovině právní, tak rovněž v rovině praktického provedení. Problematickým se dle hodnocení autora jeví možné rozhodování o sankcích a jejich ukládání předkladatelům, pokud by k němu měl být oprávněn dozorový orgán v oblasti ochrany osobních údajů, ÚOOÚ. Takovéto rozhodování by se totiž týkalo činnosti ministerstev a Vlády ČR v oblasti legislativní, vč. jisté míry hodnocení legislativních prací na návrzích právních předpisů ze strany ÚOOÚ. Autor má silné pochybnosti o legislativní proveditelnosti takovéto varianty a nepovažuje ji za reálnou; podrobněji se jí tedy dále nezabýval.

Z tohoto důvodu autor považuje za vhodnější, aby změny de lege ferenda, místo snahy o definici následků porušení povinností a o ukládání sankcí za taková porušení, byly zaměřeny ve dvou rovinách – jednak na přesné vymezení samotné povinnosti a konečně též na posílení úlohy ÚOOÚ jakožto orgánu dozoru v oblasti ochrany osobních údajů. Konkrétně autor považuje v prvé řadě za vhodné precizovat jak povinnost konzultace předkladatele

právního předpisu s ÚOOÚ a následnou povinnost zohlednit připomínky ÚOOÚ v legislativním návrhu, tak rovněž povinnost provedení legislativní DPIA analýzy. Obě tyto povinnosti jsou totiž uloženy ve stávajícím znění GDPR v podobě dosti vágní[658], když v textu nejsou jednoznačně vymezeni ani adresáti povinnosti (členské státy) ani povinnost samotná (během přípravy návrhu legislativního opatření nebo návrhu regulačního opatření založeného na takovém legislativním opatření). Takovéto upřesnění by dle autora mohlo být zakotveno v ZoZOÚ, jakožto v zákoně, mezi jehož hlavní cíle patří adaptace vnitrostátní právní úpravy na Obecné nařízení GDPR; současně by toto upřesnění dle hodnocení autora plně zapadalo do předmětu úpravy ZoZOÚ, jak je vymezen v § 1 tohoto právního předpisu[659]. Upřesnění by jednoznačně vymezilo předkladatele vládních návrhů zákonů jako adresáty obou povinností – konzultace s ÚOOÚ i legislativní DPIA. Současně by takováto změna mohla zahrnovat též povinnost předkladatelů legislativních návrhů zohlednit ve svém vyjádření předkládaném na žádost k jiným než vládním návrhům právních předpisů mimo jiné rovněž otázky ochrany osobních údajů a práva na ochranu soukromí. Takové vyjádření pochopitelně nemůže nahradit DPIA analýzu, autorovi se však požadavek na vypracování DPIA analýzy u jiných než vládních legislativních návrhů jeví v praxi jako fakticky nerealizovatelný, zejména kvůli nevynutitelnosti, a to přestože ÚOOÚ ve svém dokumentu Metodika pro legislativní DPIA[660] uvádí, že „*s ohledem na článek 35 odst. 10 a článek 36 odst. 4 GDPR však lze doporučit zohlednit i při postupu podle zákona č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny, nebo podle zákona č. 107/1999 Sb., o jednacím řádu Senátu, tuto pomůcku použít a vložit legislativní DPIA rovněž do důvodové zprávy iniciativního návrhu nebo do odůvodnění věcných pozměňovacích návrhů*“.

Pokud jde o úlohu ÚOOÚ, autorovi se jeví jako velmi vhodné, aby ÚOOÚ v případech, kdy zjistí nedostatečné naplnění uvedených povinností, na tyto zjištěné nedostatky upozornil předkladatele právního předpisu, byť i formou upozornění učiněného ex post, případně i po přijetí právního předpisu a současně tato svá zjištění transparentně zveřejnil. Takovéto aktivity by ÚOOÚ byl dle autorova hodnocení oprávněn činit bez nutnosti

---

[658] Srov. text čl. 36 odst. 4 GDPR: *„Členské státy konzultují s dozorovým úřadem během přípravy návrhu legislativního opatření, které má přijmout vnitrostátní parlament, nebo návrhu regulačního opatření založeného na takovém legislativním opatření, jež souvisí se zpracováním.“.*

[659] ZoZOÚ v § 1 stanoví, že *„Tento zákon zapracovává příslušné předpisy Evropské unie, zároveň navazuje na přímo použitelný předpis Evropské unie a k naplnění práva každého na ochranu soukromí upravuje práva a povinnosti při zpracování osobních údajů.“*

[660] ÚOOÚ. *Metodika pro legislativní DPIA*. Bez uvedení data publikace. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.

změny právní úpravy vymezující ÚOOÚ a jeho působnost, tedy právní úpravy Části první Hlavy V ZoZOÚ. Navíc již dle současného znění ZoZOÚ je ÚOOÚ oprávněn poskytovat „*Parlamentu vyjádření k návrhu právního předpisu, který upravuje zpracování osobních údajů*“, a to i bez předchozí žádosti[661]. Diskutované kroky dozorového úřadu sice nebudou (a ani nemohou) mít za následek bezprostřední negativní konsekvence pro předkladatele právního předpisu či pro jakýkoli jiný orgán či osobu, současně však mohou být jistým vodítkem jak pro osoby, které by se cítily dotčeny takovýmto právním předpisem a uvažovaly by o jeho napadení, tak rovněž případně pro obecné soudy a zvláště Ústavní soud ČR v případě posuzování takovéhoto právního předpisu. Ústavní soud ČR by si tak v případném řízení o zrušení zákonů a jiných právních předpisů byl v takovém případě vědom toho, že v rámci přípravy návrhu posuzovaného zákona nebyly dodrženy konkrétní povinnosti stanovené platnou právní úpravou.

Autor hodnotí obě navržené změny – jak precizaci povinnosti ukládané předkladatelům právních předpisů, tak rovněž popsané důsledné kroky ze strany ÚOOÚ – jako proveditelné jak po stránce právní, tak rovněž v rovině jejich praktické aplikace. Současně by však bylo plně namístě usilovat o obdobné změny rovněž v legislativním procesu evropského zákonodárce, při přijímání norem unijního práva, včetně posílení role EDPB v legislativního procesu a zajištění adekvátních reakcí na upozornění a doporučen obsažená ve stanoviscích EDPB k návrhům norem unijního práva. Zde autor spatřuje roli EDPB a především Evropské komise, konkrétní návrhy v tomto směru však nezaznamenal.

4.2.3 Pravidelné vyhodnocování efektivity opatření

Analýzou výše v této práci rozebraných typových případů zásahů do práva na ochranu soukromí a práv souvisejících dospěl autor k závěru o nezbytnosti podrobovat účel, který konkrétní právní úpravy sledují, pravidelnému přezkumu. V případech plošného shromažďování osobních údajů značného množství osob by tedy nemělo postačovat vymezení sledovaného veřejného zájmu provedené v právní úpravě v okamžiku přípravy jejího návrhu. Jednak může v legislativním procesu, typicky při projednávání návrhu zákona oběma komorami Parlamentu ČR, dojít, ostatně v praxi také často dochází, k různým úpravám a změnám oproti původnímu textu právního předpisu, k němuž byla ve fázi návrhu vypracována analýza dopadu a případně též legislativní DPIA analýza. Může se jednat jak o úpravy přímo v základních parametrech, které byly takto posuzovány, jako např. účel zpracování, rozsah

[661] Viz § 54 odst. 3 písm. c) ZoZOÚ.

kategorií údajů, rozsah dotčených osob, doba uchovávání apod., tak rovněž o úpravy týkající se v návrhu definovaných kontrolních mechanismů, případně i o úpravy jiné, které ve svém důsledku např. některý z kontrolních mechanismů učiní neefektivní či zcela nefunkční. Kromě toho však může též následně, při aplikaci zákona v praxi dojít k posunům, které budou mít obdobné důsledky, vyloučeny také nejsou faktické změny, v jejichž důsledku se zpracování, které původně nevykazovalo charakteristiky plošného zpracování, takovým stane, dojde k výraznému rozšíření počtu dotčených osob proti původním předpokladům, naruší se původně splněná kritéria proporcionality zásahu apod.

Jako typický příklad dle hodnocení autora může sloužit povinné zpracování provozních a lokalizačních údajů elektronických komunikací. Jak autor dovodil v analýze této povinnosti dříve v této práci, v tomto případě došlo – a v legislativní praxi ČR stále dochází – k postupnému doplňování dalších účelů zpracování, spolu s přidáváním dalších orgánů oprávněných využít tyto osobní údaje. Vedle toho dochází též k výraznému nárůstu míry využití provozních a lokalizačních údajů ze strany oprávněných orgánů, jak autor ukázal v kapitole věnované povinnosti Data Retention porovnáním souhrnných údajů zveřejňovaných ČTÚ za jednotlivé roky[662].

Částečný mechanismus vyhodnocování efektivity obsahovala Data Retention směrnice. Členským státům ukládala povinnost zajistit Evropské komisi pravidelně jednou ročně statistiky zahrnující informace o případech poskytnutí informací příslušným orgánům, o čase ode dne uchování údajů do dne žádosti příslušného orgánu a o případech, kdy nebylo možné žádosti o poskytnutí údajů vyhovět; Evropská komise však měla ve směrnici pouze jednorázovou povinnost předložit do 15. září 2010 Evropskému parlamentu a Radě hodnocení používání směrnice a jejího dopadu na hospodářské subjekty a spotřebitele a toto hodnocení též zveřejnit[663]. I tento mechanismus umožňující vyhodnocování souhrnných údajů však po prohlášení neplatnosti Data Retention směrnice zanikl, jelikož se nepřenesl do národních právních řádů členských států EU, přestože povinné uchovávání provozních a lokalizačních údajů v nich zpravidla zůstalo; Evropská komise náhradu neplatné směrnice nenavrhla.

Právní úpravy zakládající další typové zásahy do práva na ochranu soukromí v podobě plošného shromažďování a zpracování osobních údajů dle hodnocení autora takový mechanismus zpravidla neobsahují. Takto např. u zpracování údajů jmenné evidence

---

[662] Již výše zmiňované přehledy zveřejňované ČTÚ ukazují nárůst případů vyžádaných provozních a lokalizačních údajů mobilních sítí mezi roky 2013 a 2018 na dvojnásobek, ze 173.087 v roce 2013 na 332.892 v roce 2018.

[663] Viz čl. 10 a 15 Data Retention směrnice.

cestujících v letecké dopravě vypracovává Evropská komise zprávy o jejich hodnocení, většinou ve vztahu ke konkrétní dohodě uzavřené v této věci se třetím státem, tyto zprávy jsou však zpravidla pouze velmi obecným textem, který neobsahuje ani celkové počty osob dotčených tímto povinným zpracováním osobních údajů ani celkové počty případů, v nichž byly údaje jmenné evidence cestujících předávané dle konkrétní dohody využity k úspěšné eliminaci konkrétní hrozby (např. hrozba teroristického útoku)[664]. Tato absence fakticky znemožňuje učinit jakýkoli závěr o efektivitě a v důsledku toho i o reálné potřebnosti povinně vedené jmenné evidence cestujících.

Dílčí závěry

Ze shora popsaných důvodů považuje autor za nutné, aby právní úpravy zakládající zásah do základních práv a svobod, zde do práva na ochranu soukromí plošným shromažďováním a zpracováním osobních údajů, obsahovaly též povinnost pravidelného hodnocení celkového využití údajů a efektivity přijatých opatření v praxi. Tato povinnost je dle autorova hodnocení důležitá ve všech případech zásahů rozebíraných v této práci, zásadní je však v situacích, kdy narůstá okruh oprávněných orgánů a také míra využití daného právního institutu, jako je tomu např. u využívání provozních a lokalizačních údajů elektronických komunikací, avšak nejen u nich. Nositel této povinnosti musí být v právní úpravě jednoznačně vymezen, měl by jím být předkladatel právní úpravy, případně si lze představit uložení takové povinnosti ÚOOÚ, což by mohlo zaručit jednotný přístup ke splnění povinnosti a vzájemnou porovnatelnost hodnocení vypracovaných v jednotlivých, vzájemně odlišných oblastech.

4.2.4 Zveřejňování statistických údajů

Jako jeden z efektivních kontrolních mechanismů autor hodnotí shromažďování a zveřejňování statistických údajů o počtech žádostí oprávněných orgánů o údaje, resp. o počtech využití údajů, případně doplněné o související informace. V případě Data Retention

[664] Report from the Commission to the European Parliament and the Council On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. 24.7.2020, Zpráva Komise Evropskému parlamentu a Radě o společném hodnocení Dohody mezi Spojenými státy americkými a Evropskou unií o využívání jmenné evidence cestujících a o jejím předávání Ministerstvu vnitřní bezpečnosti Spojených států. 12. ledna 2021, Doporučení pro Rozhodnutí Rady o zmocnění k zahájení jednání o dohodě mezi Evropskou unií a Islandem o předávání údajů jmenné evidence cestujících z EU na Island za účelem prevence, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti. 6.9.2023, Návrh Rozhodnutí Rady o podpisu Dohody mezi Kanadou a Evropskou unií o předávání a zpracování údajů jmenné evidence cestujících (PNR) jménem Evropské unie. 4.3.2024. [online] [cit. 24.2.2024].

bylo dlouhou dobu povinností uloženou v ZoEK provozovatelům sítí a poskytovatelům služeb elektronických komunikací shromažďovat tyto statistické údaje na základě povinnosti uložené jim v ZoEK[665] a pravidelně je předávat ČTÚ[666], ten je pak na souhrnné bázi předával Evropské komisi a vedle toho také, již bez jednoznačného zakotvení v zákoně, pravidelně, na roční bázi v souhrnné podobě zveřejňoval[667]. Tyto statistiky představovaly dle hodnocení autora významný kontrolní prvek umožňující veřejnou kontrolu rozsahu provozních a lokalizačních údajů vyžádaných oprávněnými orgány v jednotlivých letech. S ohledem na jejich dlouhodobé zveřejňování současně umožňovaly sledovat změny v rozsahu těchto údajů a tedy v rozsahu zásahů do soukromí dotčených osob v jednotlivých letech a tyto celkové počty porovnávat se statistikami trestné činnosti za dané období i s mírou její objasněnosti.

Povinnosti provozovatelů sítí a poskytovatelů služeb shromažďovat a předávat tyto údaje ČTÚ byly do ZoEK vloženy novelou provedenou zákonem č. 247/2008 Sb.[668], která do právního řádu ČR transponovala Data Retention Směrnici, ke splnění povinnosti uložené členským státům v Data Retention Směrnici[669]. Jak samotné shromažďování těchto statistických údajů provozovateli sítí a poskytovateli služeb elektronických komunikací i ČTÚ, tak rovněž jejich zveřejňování ze strany ČTÚ nebylo způsobilé nijak zasahovat do

---

[665] ZoEK obsahoval v § 97 ve znění účinném do 1.11.2021:
- odst. 10, dle kterého *„Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna vést evidenci*
a) počtu případů, ve kterých na základě žádosti poskytla provozní a lokalizační údaje orgánům oprávněným k jejich vyžádání,
b) doby, která v jednotlivých případech uplynula ode dne, kdy zahájila uchovávání provozních a lokalizačních údajů do dne, kdy o tyto údaje oprávněný orgán požádal, a
c) počtu případů, kdy nemohla žádosti o poskytnutí provozních a lokalizačních údajů vyhovět.“,
- *odst. 11, dle kterého „Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna předávat Úřadu evidenci uvedenou v odstavci 10 souhrnně vždy za uplynulý kalendářní rok, a to v elektronické formě, nejpozději do 31. ledna následujícího kalendářního roku. Předávaná evidence nesmí obsahovat osobní a identifikační údaje. Úřad souhrn obdržených evidencí neprodleně předá Komisi.“*
- a odst. 12: *„Formu evidence předávané podle odstavce 11 a způsob jejího předávání Úřadu stanoví prováděcí právní předpis.“*

[666] Podrobnosti členění těchto přehledů stanovila vyhláška č. 318/2010 Sb., kterou se stanoví forma evidence provozních a lokalizačních údajů a způsob jejího předávání Českému telekomunikačnímu úřadu

[667] Přehledy za předchozí roky jsou stále dostupné na internetových stránkách ČTÚ, v rubrice Tiskové zprávy. Viz Český telekomunikační úřad. *Přehledy poskytnutých provozních a lokalizačních údajů*. Dostupné z www.ctu.gov.cz. [cit. 8.2.2024].

[668] Zákon č. 247/2008 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

[669] Dle čl. 10 odst. 1 a 2 Data Retention Směrnice:
„1. Členské státy zajistí, aby Komise dostávala jednou ročně statistiky o uchovávání údajů vytvořených nebo zpracovaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí. Statistika zahrne: případy, kdy byly příslušným orgánům poskytnuty informace v souladu s použitelnými vnitrostátními právními předpisy, čas, který uplynul ode dne uchování údajů do dne, kdy příslušný orgán požádal o předání údajů, případy, kdy nebylo možné žádosti o poskytnutí údajů vyhovět.
2. Tyto statistiky neobsahují osobní údaje.“

činnosti oprávněných orgánů či tyto orgány jakkoli omezovat a představovalo tak velmi specifický, přitom však v mnoha ohledech velmi účinný kontrolní mechanismus. V souladu se závěry ústavní soudkyně Kateřiny Šimáčkové obsaženými v jejím separátním votu k nálezu Ústavního soudu Pl. ÚS 45/17[670] lze dle autora říci, že toto shromažďování a zveřejňování statistických údajů bylo naplněním požadavku na možnost veřejné kontroly záruk týkajících se povinnosti Data Retention a upravených v právní úpravě ZoEK.

Tyto povinnosti však byly zrušeny novelou ZoEK provedenou zákonem č. 374/2021 Sb.[671], společně se zrušením uvedené prováděcí vyhlášky, aniž by byl zřejmý důvod těchto změn. Předkladatel novely, Ministerstvo průmyslu a obchodu, k tomu v důvodové zprávě k vládnímu návrhu této novely uvedl, že tato ustanovení a vyhláška byly zrušeny „v souvislosti se zrušením Data Retention Směrnice", jelikož zrušením této směrnice dle předkladatele *„vzniká potřeba odpovídající změny zákona"* i potřeba zrušení prováděcí vyhlášky. Autor se s tímto odůvodněním neztotožňuje, naopak, je přesvědčen, že takováto změna nebyla nejen potřebná, ale ani účelná. V souvislosti se zrušením Data Retention Směrnice odpadlo předávání souhrnných statistických údajů ze strany ČTÚ Evropské komisi. Spojovat však s tím odstranění efektivního kontrolního mechanismu se jeví jako velmi nevhodné a lze v tom spatřovat zásadní neporozumění důvodům jeho existence. Klíčovým je, že zrušením Data Retention Směrnice nedošlo ke zrušení samotné povinnosti Data Retention v právním řádu ČR a nebyl tedy relevantní důvod odstraňovat mechanismus, jehož jediným účelem bylo zajistit přehled o míře využívání institutu Data Retention a tedy kontrolu nad ním.

Ústavní soud ČR přitom v nálezu Pl. ÚS 45/17 povinnost provozovatelů sítí a poskytovatelů služeb *„vést evidenci případů zpřístupnění provozních a lokalizačních údajů a pravidelně ji „reportovat" Českému telekomunikačnímu úřadu"* dle § 97 odst. 10 a 11 ZoEK výslovně zmiňuje jako jeden z prvků zabezpečení uchovávaných provozních a lokalizačních údajů a záruk proti jejich zneužití, zejména ve formě neoprávněného či svévolného přístupu k těmto údajům[672]. Také v dalších zásadních soudních rozhodnutích, která autor zmiňuje výše, soudy při svém rozhodování vycházely mimo jiné rovněž ze zveřejňovaných statistických

[670] Ústavní soudkyně Šimáčková ve svém odlišném stanovisku k nálezu Ústavního soudu ČR sp. zn. Pl. ÚS 45/17 ze 14. května 2019 zdůraznila, vedle nutnosti záruk výslovně a dostatečně určitě upravených v právní úpravě zakládající takto zásadní zásah do základních práv a svobod, též nezbytnost existence veřejné kontroly takových záruk.

[671] Zákon č. 374/2021 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony.

[672] Viz Nález Ústavního soudu ČR sp. zn. Pl. ÚS 45/17 ze 14. května 2019, bod 95.

údajů, zejména v případě rozhodování o povinném zpracovávání provozních a lokalizačních údajů elektronických komunikací, v některých případech soudy na základě těchto souhrnných údajů dospěly k podezření o nadužívání zkoumaného institutu vyžádání těchto údajů[673].

Dílčí závěry

Autor je přesvědčen, že transparentní zveřejňování souhrnných statistických údajů o počtech vyžádání či využití osobních údajů v rámci jednotlivých právních institutů zkoumaných v této práci je významným kontrolním prvkem využitelným nejen ve výše zmiňovaném případě provozních a lokalizačních údajů elektronických komunikací. Jak již autor uvedl výše, v případě jednoho z případů zásahů do práva na ochranu soukromí v podobě povinného zpracování údajů jmenné evidence cestujících jsou k dispozici pouze oficiální statistické údaje staré téměř 10 let, a i to pouze na úrovni celé EU; oficiální informace týkající se České republiky pak nejsou k dispozici vůbec. Právě souhrnné údaje přitom umožňují ověřit míru využití údajů a také porovnat ji v jednotlivých letech, především však lze na jejich základě vyhodnotit využití údajů ve vztahu k zákonem vymezeným účelům. Zveřejněné statistiky tak umožňují veřejnou kontrolu nad využitím jednotlivých právních institutů umožňujících zásahy do práva na ochranu soukromí. Současně statistické údaje v případech plošných zpracování osobních údajů nemohou být zpravidla nositelem informací, u nichž by byla dána potřeba jejich utajení.

Autor tak má za to, že povinné zveřejňování statistických údajů by mělo být součástí právních úprav zakládajících plošná zpracování osobních údajů zasahujících do práva na ochranu soukromí. Jako nositele této povinnosti by měla právní úprava souhrnně určit jeden z orgánů veřejné moci dané údaje využívajících, případně lze uložit povinnost takto statistické údaje shromažďovat a zveřejňovat orgánu, který je dozorovým orgánem pro danou oblast, jako tomu bylo v případě ČTÚ u provozních a lokalizačních údajů elektronických komunikací.

4.2.5 Nepřípustnost využívání údajů pro odlišný účel

Jedním ze základních pravidel platných obecně pro zpracování osobních údajů je omezení zpracování ve vztahu k vymezenému účelu – tzv. zásada účelového omezení je

[673] Ústavní soud ČR v nálezu sp. zn. Pl. ÚS 24/10 či v nálezu sp. zn. Pl. ÚS 24/11, kde právě veřejně přístupné statistické údaj dke hodnocení Ústavního soudu ČR „*nasvědčují závěru, že nástroj v podobě vyžádání si a použití uchovávaných údajů (včetně údajů o neuskutečněných hovorech, na které napadené ustanovení vůbec nepamatuje) je orgány činnými v trestním řízení využíván ve značném rozsahu, a to i pro účely vyšetřování běžné, tj. méně závažné trestné činnosti.*“ Ústavní soud Slovenské republiky v nálezu sp. zn. PL.ÚS 10/2014 na základě souhrnných statistických údajů vyhodnotil využívání tohoto nástroje „*ako bežného alebo rutinného prostriedku na vyšetrovanie aj menej závažnej trestnej činnosti“.*

v GDPR zahrnuta mezi základní zásady zpracování osobních údajů, taktéž Trestněprávní směrnice a k jejímu provedení ZoZOÚ tuto zásadu formuluje obdobně[674]. V případě zpracování založeného na povinnosti uložené právním předpisem pak je nezbytné dodržení striktního omezení využívání údajů pouze pro účel vymezený touto právní úpravou a tedy nemožnost volně rozšiřovat zpracování osobních údajů pro jiné účely, v rozporu s uvedenými omezeními. V opačném případě by nejen kontrolní mechanismy rozebírané v této práci v rámci úvah de lege ferenda, ale i mnohé z existujících kontrolních mechanismů měly velmi omezenou účinnosti, některé by dokonce byly zcela neúčinné a v praxi by tak nemohla být garantována ústavnost postupů, které zasahují do základních lidských práv, zde práva na ochranu soukromí a práv souvisejících.

Autor považoval tuto zásadu za natolik jednoznačnou a v praxi v zásadě respektovanou, že měl za téměř nadbytečné podrobněji rozebírat její znaky a podmínky naplnění v praxi. Nedávný případ popisovaný výše v této práci, v němž správce daně vyžádal a získal údaje z dopravního kamerového systému Policie ČR a tyto údaje v konkrétním případě též využil pro účely správy daní, resp. pro účely kontroly oprávněnosti uplatněného nároku na daňový odpočet, však autora vede k nutnosti rozebrat zde tuto zásadu a především její limity a výjimky z její aplikace podrobněji. Potřebu formulovat tuto zásadu jako jeden z kontrolních mechanismů zdůraznila skutečnost, že soudy, včetně Nejvyššího správního soudu, v následném soudním přezkumu rozhodnutí správce daně při svém rozhodování vyhodnotily celý případ odlišně. Výjimkou je pouze následné rozhodování Ústavního soud ČR. Jak rozebráno v této práci výše, případem se zabýval nejprve Krajský soud v Ústí nad Labem, následně tento postup správce daně posuzoval Nejvyšší správní soud na základě kasační stížnosti podané dotčenou osobou, tuto stížnost však zamítl, když se neztotožnil s argumenty,

---

[674] Viz čl. 5 odst. 1 písm. b) GDPR, dle kterého osobní údaje musí být *„shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný“*, další zpracování osobních údajů GDPR ve vymezení této zásady výslovně připouští pouze *„pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely“*, zpracování splňující tato kritéria se *„nepovažuje za neslučitelné s původními účely“*. Trestněprávní směrnice v obdobně formulovaném ustanovení čl. 4 odst. 1 písm. b) ukládá členským státům zajistit, aby byly osobní údaje *„shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nebyly zpracovávány způsobem, který je s těmito účely neslučitelný“*; v čl. 4 odst. 2 pak Trestněprávní směrnice připouští výjimku, dle které *„Zpracování stejným nebo jiným správcem pro kterýkoli účel uvedený v čl. 1 odst. 1 jiný než účel, pro nějž byly osobní údaje shromážděny, je přípustné“* za současného splnění dvou podmínek: 1. správce musí být *„oprávněn zpracovávat takové osobní údaje pro takový účel v souladu s právem Unie či členského státu“* a současně 2. zpracování pro tento jiný účel musí být *„nezbytné a přiměřené v souladu s právem Unie či členského státu“*. ZoZOÚ tuto zásadu reflektuje v § 25 odst. 2, dle kterého *„Pro účel nesouvisející s plněním úkolu uvedeného v § 24 odst. 1 lze osobní údaje zpracovávat, pouze pokud je k tomu spravující orgán oprávněn a tento účel není neslučitelný se stanoveným konkrétním účelem jejich zpracování“*.

o které byla kasační stížnost opřena[675]. Jak již autor také uvedl výše v této práci, v dané věci znovu rozhodoval Nejvyšší správní soud, poté co Ústavní soud ČR[676] zrušil jeho předchozí rozhodnutí a ve výroku svého nálezu výslovně konstatoval, že rozsudkem Nejvyššího správního soudu bylo porušeno stěžovatelovo právo na soudní ochranu. V novém rozhodnutí Nejvyšší správní soud aplikoval na postup správce daně test proporcionality, se závěrem že tento postup neobstojí při posouzení nezbytnosti, když využití údajů kamerových systémů není pro správu daní nezbytné. Nejvyšší správní soud proto s těmito závěry zrušil rozsudek Krajského soudu v Ústí nad Labem i rozhodnutí Odvolacího finančního ředitelství a věc mu vrátil k dalšímu řízení[677]. Z posuzovaného konkrétního případu není zřejmé, zda správci daně obdobně postupovali běžně a pouze jejich postup nebyl předmětem přezkumu, nebo zda se jedná pouze o tento ojedinělý případ.

Autor vnímá popsaný konkrétní případ obecněji, v širším kontextu, nikoli pouze ve vztahu k využití záznamů z kamerového systému Policie ČR. V obecné rovině jde dle autora o problém pramenící z využití údajů některým z orgánů veřejné moci k účelu odlišnému od účelu, k němuž byly dané údaje původně shromážděny a zpracovávány, když takto byl účel jejich uchovávání navíc vymezen relevantní právní úpravou. Vedle skutečnosti, že se v daném případě jednalo specificky o lokalizační údaje, jejichž ochranu autor rozebírá dále v závěrech této práce, zde tedy v obecnější rovině jde o otázku oprávnění orgánů veřejné moci vyžádat si a využít při své činnosti některé osobní údaje, bez ohledu na původní účel jejich shromáždění a zpracování. K takovému původnímu účelu se přitom obecně vztahují výše rozebírané kontrolní mechanismy v rámci legislativního procesu, včetně případné legislativní DPIA analýzy či konzultace s dozorovým orgánem. Právní úprava regulující činnost řady orgánů veřejné moci neobsahuje v tomto směru jasně a výslovně formulované limity a oprávnění těchto orgánů k přístupu k informacím vymezuje dosti široce, v některých případech zahrnuje také obecně formulovanou povinnost každého poskytnout danému orgánu informace, kterými disponuje, to vše zpravidla pouze s výjimkou údajů chráněných zvláštní povinností mlčenlivosti. Jako takto oprávněné orgány připadají v úvahu zejména Policie ČR a též některé dozorové orgány – typicky ÚOHS, ČNB či ÚOOÚ, ale též orgány finanční správy a některé další. Jak autor ukazuje výše, v případě žádostí o poskytnutí provozních a lokalizačních údajů elektronických komunikací, paradoxně právě ÚOOÚ, jakožto ústřední správní úřad pro oblast

[675] Viz Rozsudek Nejvyššího správního soudu sp. zn. 9 Afs 147/2020–34 ze dne 21. července 2022.
[676] Viz nález Ústavního soudu ČR sp. zn. IV. ÚS 2621/22 ze dne 14. února 2023.
[677] Rozsudek Nejvyššího správního soudu ČR ze dne 14. prosince 2023 sp. zn. 9 Afs 147/2020–87.

ochrany osobních údajů, považoval opakovaně, v několika případech za potřebné vyžádat si tyto údaje, včetně údajů lokalizačních, navzdory tomu, že právní úprava i relevantní rozhodovací praxe Ústavního soudu ČR, SDEU i ESLP jejich využití omezuje pouze na případy splňující kritéria vysoké závažnosti, jako je tomu u vyšetřování závažné trestné činnosti.

S ohledem na výše uvedené pak v rámci zásahů do práva na ochranu soukromí ze strany veřejné moci spočívajících ve shromažďování a zpracování osobních údajů autor považuje za zvláště nebezpečné možné propojování databází obsahujících osobní údaje shromážděné k rozdílným účelům a možnost kombinace osobních údajů z různých zdrojů. Takovéto zpracování osobních údajů dle hodnocení autora platná právní úprava v obecné rovině neumožňuje, resp. je přímo zakazuje, nestanoví-li zvláštní zákon jinak. V praxi však není vyloučeno, aby k takovémuto vzájemnému propojení došlo na straně některých orgánů oprávněných vyžádat si konkrétní údaje, a to s odkazem na zvláštní právní úpravy regulující činnost oprávněných orgánů, s odůvodněním na základě těchto právních úprav, resp. oprávnění z nich vyplývajících. Před riziky vyplývajícími ze shromažďování a dalšího zpracování mnoha údajů týkajících se podstatné části občanů EU v enormních databázích varoval např. také generální advokát SDEU, Pedro Cruz Villalón v již výše zmiňovaném stanovisku k věci C-293-12.

Nejasný a vágně vymezený účel pro použití některých technických i legislativních prostředků oprávněnými orgány může také vést k překročení přípustných mezí zásahu do soukromí. Vladimír Smejkal takto v rámci úvah a prognóz dalšího vývoje kybernetické kriminality varuje před možností, že *„některé aktivity orgánů státu, OČVTŘ nevyjímaje“* již mohou směřovat k porušování základních lidských práv. Zvláště v tomto směru upozorňuje na software Galileo RCS využívaného podle některých zdrojů Policií ČR. Tento software údajně umožňuje *„infiltrovat elektronická zařízení, využít je ke sledování jejich obsahu, odposlouchávání a pozměňování jejich softwarového vybavení a obsahu datových souborů“* a další[678].

Dílčí závěry

V některých právních předpisech zákonodárce či evropský zákonodárce použil řešení v podobě výslovného omezení účelu zpracování údajů či zákazu jejich využití pro odlišný účel. Takto je tomu např. v nařízení eCall, které stanoví, že *„osobní údaje*

[678] SMEJKAL, Vladimír. *Kybernetická kriminalita. 3. vyd.* Plzeň: Aleš Čeněk, 2022. s. 680 a násl., s. 918 a násl.

zpracovávané podle tohoto nařízení jsou využívány pouze k vyřizování situací" vážných nehod zaznamenaných *„prostřednictvím aktivace jednoho či více senzorů nebo procesorů ve vozidle"*[679]. Na základě rozboru výše však toto řešení autor nepovažuje za plně funkční a efektivní ve vztahu k orgánům veřejné moci, když brání pouze standardnímu využití pro jiný účel. Patrně by však na základě tohoto ustanovení nebylo možno odmítnout poskytnutí údajů k žádosti některého z orgánů veřejné moci, jako tomu bylo například u výše rozebíraného správce daně.

Jediným skutečně efektivním řešením je dle hodnocení autora přesné a taxativní vymezení orgánů oprávněných vyžádat si osobní údaje, včetně účelu jejich využití těmito orgány a dalších podmínek jejich zpracování. Takovéto vymezení musí být obsaženo přímo v právní úpravě, která zakládá konkrétní zásah do práva na ochranu soukromí, v mnoha případech rozebíraných v této práci tomu tak ovšem není, jak autor ukázal výše. Jako vzor v tomto směru může sloužit právní úprava provozních a lokalizačních údajů elektronických komunikací v ZoEK rozebraná výše, ostatně také tato úprava neobsahovala takto jednoznačné vymezení od počátku, vyvinulo se teprve v reakci na rozhodnutí Ústavního soudu ČR.

4.2.6 Zajištění informovanosti dotčených subjektů

Základním kontrolním mechanismem v případě zpracování osobních údajů je dle hodnocení autora informovanost dotčených subjektů údajů o prováděném zpracování, která je nezbytnou podmínkou pro to, aby dané osoby měly nad svými osobními údaji kontrolu a především aby mohly ve vztahu k prováděnému zpracování vykonávat svá práva. V případech zkoumaných v této práci se bude zpravidla jednat o informaci poskytnutou dotčené osobě následně, poté co již její poskytnutí nebude moci ohrozit vyšetřování či jiný postup oprávněného orgánu.

Informace o prováděném zpracování

Základní zásadou zpracování osobních údajů dle GDPR je zásada zákonnosti, korektnosti a transparentnosti[680], dle které musejí být osobní údaje ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem. Tato zásada zejména v požadavku transparentnosti zahrnuje i kontrolní prvek, jelikož transparentnost, jak je dále rozvedena v textu GDPR[681], vyžaduje od správců poskytnutí transparentních informací

[679] Čl. 6 odst. 2 ve spojení s čl. 5 odst. 2 nařízení eCall.
[680] Čl. 5 odst. 1 GDPR.
[681] Čl. 12 a nás. GDPR.

subjektům údajů o prováděném zpracování. Informace takto získané jsou pro subjekty údajů nezbytnou podmínkou pro kontrolu nad svými osobními údaji a také pro výkon práv subjektu údajů ve vztahu k prováděnému zpracování[682][683]. Taktéž Trestněprávní směrnice uvádí mezi základními zásadami zpracování osobních údajů zásadu zákonnosti a korektnosti[684], na rozdíl od GDPR zde nezahrnuje požadavek transparentnosti. Tento požadavek je v Trestněprávní směrnici zmíněn pouze v recitálu[685], a to i ve vztahu k provádění činností, jakými jsou skryté vyšetřování nebo dohled pomocí videokamer. V judikatuře k povinnosti Data Retention se vyvinul požadavek povinného dodatečného informování dotčené osoby o přístupu k jejím provozním a lokalizačním údajům a o jejich využití alespoň následně, poté, co pomine nebezpečí narušení vyšetřování či jiné činnosti oprávněného orgánu. Soudy tuto informační povinnost označují za nástroj k zajištění efektivních záruk proti zneužití institutu Data Retention[686], promítl se také do Trestního řádu[687].

Informovanost dotčených subjektů údajů – fyzických osob o tom, že se tyto osoby staly předmětem zásahu, je u některých zde rozebíraných kontrolních mechanismů s významnými reálnými dopady nezbytnou podmínkou uplatnění těchto mechanismů v praxi. Taková informovanost může být v některých situacích zajištěna až následně, po proběhnuvším zásahu. Tak tomu bude typicky v situacích, kdy dřívější předání informace dotčené fyzické osoby by mohlo zmařit účel takového využití údajů o soukromí ze strany orgánů veřejné moci. Bez této informace, byť následně získané, totiž zpravidla dotčená osoba nemá reálnou možnost využít procesně-právních institutů zakotvených právní úpravou v podobě umožňující přezkum zásahu v konkrétním případě, z podnětu osoby zásahem dotčené[688].

Jak zdůraznil již ESLP v rozhodnutí Malone v. UK, citovaném v této práci výše, pokud se dotčená osoba nedozví ani o samotné existenci sledování, k němuž dochází tajně, může tato skutečnost vést až k situaci, kterou ESLP označil za „*nicotnost*“ článku 8 Evropské

---

[682] K tomuto podrobně viz Pracovní skupina zřízená podle článku 29. *Pokyny k transparentnosti podle nařízení 2016/679,* přijaty dne 29. listopadu 2017, ve znění naposledy revidovaném a přijatém dne 11. dubna 2018. WP260 rev.01.

[683] Spojitost mezi informací poskytnutou subjektu údajů a možností výkonu práv formulovat např. generální advokát SDEU, Pedro Cruz Villalón ve stanovisku ze dne 9. července 2015 k případu Smaranda Bara a další proti Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală (ANAF): *„…požadavek informování subjektů dotčených zpracováním jejich osobních údajů, který zaručuje transparentnost veškerého zpracování, je o to důležitější, že vytváří předpoklady pro to, aby dotyčné osoby mohly vykonat své právo na přístup ke zpracovávaným údajům“*.

[684] Čl. 4 odst. 1 písm. a) Trestněprávní směrnice.

[685] Viz recitál bod 26 Trestněprávní směrnice.

[686] Viz např. nálezy Ústavního soudu ČR Pl. ÚS 24/11 či Pl. ÚS 45/17.

[687] Viz § 88a odst. 2 Trestního řádu.

[688] Příkladem může být institut přezkumu příkazu k zjištění údajů o telekomunikačním provozu dle § 314l a násl. Trestního řádu, jehož využití je bez informovanosti dotčené osoby o proběhnuvším zásahu prakticky nemožné.

úmluvy. Jelikož tento článek stanoví právo každého na respektování rodinného a soukromého života a odpovídající zákaz pro státní orgány zasahovat do výkonu tohoto práva, s výjimkou případů v souladu se zákonem a nezbytných v demokratické společnosti pro vymezené účely, může dle ESLP v důsledku toho být s jednotlivcem zacházeno způsobem odporujícím tomuto článku a může být dokonce zbaven práva tímto článkem přiznaného. Právě z tohoto důvodu je zcela zásadní vědomost dotčené osoby o provedeném zásahu; samotné využití prostředků ochrany před proběhnuvší zásahem je pak na rozhodnutí dané osoby. Tento závěr dle hodnocení autora neplatí pouze ve vztahu k čl. 8 Evropské úmluvy, lze jej zobecnit. Aby byl v praxi proces informování dotčené osoby skutečně zaručen a probíhal efektivním a pro dotčenou osobu využitelným způsobem (zejména z hlediska časového i z hlediska obsahového), musí být zakotven obecně závazným právním předpisem, a to v podobě jednoznačně vymezené a efektivně vynutitelné povinnosti uložené osobám, resp. zpravidla orgánům veřejné moci, které zásah do práva na ochranu soukromí uskutečňují.

Také Ústavní soud ČR v nálezech Pl. ÚS 24/10 a Pl. ÚS 24/11 zdůraznil nezbytnost povinnosti informovat, byť následně dotčenou osobu o využití údajů pro naplnění požadavků testu proporcionality a pro účinnou ochranu před nezákonným zásahem do základních práv a svobod těchto osob. Právě vědomost osoby, do jejíchž základních práv bylo zasaženo, o provedeném zásahu je nezbytným předpokladem pro faktickou možnost této osoby iniciovat přezkum provedeného zásahu v konkrétním případě nezávislým orgánem zmocněným k takovému přezkumu právní úpravou. Obdobně též generální advokát Soudního dvora EU ve svém stanovisku ve spojených věcech C 293/12 a C 594/12[689] upozornil, že „*Unijní zákonodárce měl stanovit zásadu povinnosti orgánů oprávněných přistupovat k údajům tyto údaje vymazat, jakmile jejich potřeba pomine, a informovat dotyčné osoby o takovém přístupu alespoň a posteriori, jakmile pomine nebezpečí, že toto informování naruší efektivitu opatření odůvodňujících využití daných údajů.*“ Soudní dvůr EU pak v rozsudku v těchto spojených věcech na upozornění generálního advokáta navázal a dodal, že „*Okolnost, že k uchovávání údajů a jejich následnému využití dochází bez informování účastníka nebo registrovaného uživatele, může navíc v dotyčných osobách vyvolávat dojem – jak uvedl generální advokát v bodech 52 a 72 svého stanoviska – že jejich soukromí je pod neustálým dohledem.*“.

[689] Stanovisko generálního advokáta Pedra Cruz Villalóna ve věci C-293/12 a ve věci C-594/12 přednesené dne 12. prosince 2013.

Dílčí závěry

Autor má na základě analýz platné právní úpravy zkoumaných případů, jakož i rozhodovací a výkladové praxe za to, že ve většině případů by v relevantní právní úpravě obecně bylo možno uložit povinnost orgánu, který si informace o dané osobě vyžádal, informovat tuto osobu, v odůvodněných případech až následně. Tímto krokem získá dotčená osoba informaci o zásahu do jejího práva na ochranu soukromí a bude na jejím zvážení, zda tento zásah a jeho důvodnost napadne právní cestou.

V jednotlivých relevantních právních úpravách by měl být současně nastaven proces přezkumu daného zásahu z podnětu dotčené osoby, obdobně jako je tomu v případě výše uváděného řízení o přezkumu příkazu k odposlechu a záznamu telekomunikačního provozu a příkazu k zjištění údajů o telekomunikačním provozu, upraveného v Trestním řádu[690] Podmínkou efektivity tohoto mechanismu je, aby povinnost byla uložena konkrétní povinné osobě – orgánu, který si informace oprávněně vyžádal. Povinnost musí být formulována jednoznačným a v praxi vynutitelným způsobem, což je ostatně obecný požadavek tykající se právních předpisů v širší míře.

Tento kontrolní mechanismus může být dle názoru autora v praxi velmi účinnou zárukou ústavnosti zásahů do práva na ochranu soukromí. Tento efekt přitom může mít již samotné zakotvení povinnosti informovat dotčenou osobu a související existence institutu přezkumu zásahu. Na druhou stranu je však nutno brát na zřetel, že se bude vždy jednat o kontrolní mechanismus aplikovatelný pouze v případech konkrétních zásahů. Je proto nutné, aby byl doplňkem dalších, v této práci rozebraných kontrolních mechanismů, nikoli jejich náhradou.

4.2.7 Kontrola ze strany nezávislého orgánu

Dalším kontrolním mechanismem uplatnitelným obecně, ve vztahu k zásahům do práva na ochranu soukromí, je kontrola ze strany nezávislého orgánu vybaveného oprávněním dozoru, zde nad oblastí ochrany osobních údajů. Dle Ústavního soudu ČR platí, že „*přípustnost omezení práva na ochranu osobních údajů podle čl. 10 Listiny, čl. 8 Listiny EU i čl. 8 Úmluvy*“ je vázána „*na účinnou kontrolu dodržování s tím spjatých povinností nezávislým orgánem*“. Požadavek účinné kontroly zahrnuje nezbytně i existenci citelných sankcí v relevantní právní úpravě pro případ porušení povinností, jak vyplývá z již výše rozebíraného

[690] Viz § 314l a násl. Trestního řádu.

nálezu Pl. ÚS 3/14. Dle názoru autora z tohoto závěru Ústavního soudu ČR vyplývá, jak velmi významná je nejen samotná existence sankcí za porušení povinností stanovených za účelem zajištění práva na ochranu soukromí, tedy jejich zakotvení v platné právní úpravě, ale také skutečnost, zda a nakolik efektivně jsou tyto sankce v případech zjištěných porušení v praxi skutečně uplatňovány. Uvedený závěr autor považuje ve vztahu k tématu této práce za velmi relevantní. Pokud u zásahů do práva na ochranu soukromí, které byly v obecné rovině, při splnění zákonem vymezených podmínek, vyhodnoceny jako přípustné, neexistuje kontrola dodržování těchto podmínek ze strany nezávislého orgánu buď vůbec či sice existuje, ovšem není „*doprovázena citelnými sankcemi*“ při zjištění porušení těchto povinností, lze důvodně pochybovat o obecné přípustnosti zásahu jako takového[691].

Autor má za to, že efektivní kontrola dodržování povinností stanovených právě za účelem udržení zásahu do základního lidského práva – zde práva na ochranu soukromí – v mezích, které umožňují považovat zásah za přípustný, patří ke klíčovým aspektům ochrany základních lidských práv, resp. ochrany ústavnosti. Obecně však lze vážně pochybovat o efektivní kontrole tehdy, pokud dozorový orgán není v případech zjištěných porušení oprávněn uložit žádné sankce. Dle ZoZOÚ ovšem ve vztahu k přestupkům dle tohoto zákona, které projednává ÚOOÚ, platí, že „*Pokud spáchá přestupek podle § 62 zákona č. 110/2019 Sb. orgán veřejné moci nebo veřejný subjekt, Úřad podle § 62 odst. 5 tohoto zákona od uložení správního trestu upustí*“ [692] [693]. Jak nezávislí odborníci, tak rovněž samotný ÚOOÚ tuto legislativní úpravu kritizuje, když např. v prvním případě, v němž byl v praxi nucen toto ustanovení aplikovat, konstatoval, že „*Úřad zmiňovanou právní úpravou přišel o možnost ukládat pokuty orgánům veřejné moci a veřejným subjektům, tedy například ministerstvům, různým správním úřadům, městům či obcím za přestupky související s ochranou osobních údajů. Přestože si je Úřad plně vědom skutečnosti, že zákonodárcem zvolené řešení zakládá*

[691] Ústavní soud ČR ve zmiňovaném nálezu Pl. ÚS 3/14 tento závěr výslovně vztahuje k dodržování povinností spojených se specifickou, v nálezu posuzovanou právní úpravou, konkrétně povinností spojených s ochranou informací z „nejintimnější osobní sféry jednotlivce a dále s ochranou zvlášť zranitelných osob („*Napadené ustanovení zákona o archivnictví nezbavuje stát povinnosti ochránit informace z nejintimnější osobní sféry jednotlivce (sexualita, stigmatizující informace o zdravotním stavu či utrpěné újmě) a zvlášť zranitelné osoby (děti, osoby se zdravotním postižením). Na účinnou kontrolu dodržování s tím spjatých povinností nezávislým orgánem, doprovázenou citelnými sankcemi v případě jejich porušení, je vázána přípustnost omezení práva na ochranu osobních údajů podle čl. 10 Listiny, čl. 8 Listiny EU i čl. 8 Úmluvy.“*). Autor má však za to, že tento závěr lze zobecnit výše uvedeným způsobem, aniž by se takové zobecnění dostalo do rozporu s argumentací, kterou Ústavní soud ČR v daném případě použil.

[692] Viz ÚOOÚ. *Porušení povinností při zpracování osobních údajů.* [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.

[693] Viz § 62 odst. 5 ZoZOÚ, dle kterého *„Úřad upustí od uložení správního trestu také tehdy, jde-li o správce a zpracovatele uvedené v čl. 83 odst. 7 nařízení Evropského parlamentu a Rady (EU) 2016/679.“*

rozdílné postavení různých skupin správců a zpracovatelů osobních údajů, je při své rozhodovací činnosti plně vázán zákonem. Může však orgánům veřejné moci a veřejným subjektům i nadále ukládat nápravná opatření.“[694] Toto ustanovení ZoZOÚ je založeno na možnosti, kterou poskytuje GDPR v čl. 83 odst. 7[695]. Způsob, jakým český zákonodárce toto oprávnění GDPR využil, bývá často terčem kritiky ze strany odborníků[696], taktéž ÚOOÚ v této souvislosti poukazuje na to, že zákonodárcem „*zvolené řešení zakládá rozdílné postavení různých skupin správců a zpracovatelů osobních údajů*“[697].

Výše rozebíraný požadavek kontroly zahrnuje také prvek nezávislosti orgánu, který je kontrolou pověřen a tuto kontrolu vykonává. V oblasti ochrany osobních údajů je v České republice takovým orgánem ÚOOÚ, který je „*ústředním správním úřadem pro oblast ochrany osobních údajů*“. V zájmu zajištění jeho nezávislosti, kterou výslovně vyžaduje též Obecné nařízení GDPR[698], současně platí, že do jeho činnosti „*lze zasahovat jen na základě zákona*“[699]. Jak v této souvislosti konstatuje Ústavní soud ČR v nálezu Pl. ÚS 3/14, „*Tuto kontrolní úlohu plní v první řadě Úřad pro ochranu osobních údajů výkonem dozorové činnosti a uplatňováním pokut za přestupky*“. Samotnou kontrolní úlohu Úřadu, byť zakotvenou v zákoně a ve spojení s vymezením požadavků na nezávislost postavení dozorových úřadů obsažených v GDPR[700], však bez dalšího není možno považovat za dostatečnou záruku proti zneužití institutu umožňujícího zásah do základních práv a svobod v případech, které jsou předmětem této práce. V tomto směru lze poukázat na nález Pl. ÚS 24/10, v němž Ústavní soud ČR hodnotí dostatečnost, resp. samotnou existenci „*možnosti dotčených jednotlivců domáhat se efektivní ochrany proti případnému zneužití, svévoli či nesplnění stanovených povinností*“. Dospěl zde k závěru, který se sice týkal právní úpravy zákona o elektronických komunikacích[701], posuzované v tomto nálezu, dle hodnocení autora

---

[694] Viz ÚOOÚ. *ÚOOÚ nemohl udělit pokutu ministerstvu, neumožňuje mu to zákon.* Publikováno 9.8.2019. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
[695] Dle tohoto ustanovení *„Aniž jsou dotčeny nápravné pravomoci dozorových úřadů podle čl. 58 odst. 2, může každý členský stát stanovit pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě.“*.
[696] Viz např. *ÚOOÚ nemohl udělit pokutu ministerstvu vnitra, neumožňuje mu to zákon*. Advokátní deník online. 29. 8. 2019. [online] [cit. 12.1.2024]. Dostupné z www.advokatnidenik.cz.
[697] ÚOOÚ. *ÚOOÚ nemohl udělit pokutu ministerstvu, neumožňuje mu to zákon*. 9.8.2019. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
[698] Viz čl. 51 a následující GDPR.
[699] Viz § 50 a 51 zákona č. 110/2019 Sb. o zpracování osobních údajů. Jako ústřední orgán státní správy vymezuje Úřad pro ochranu osobních údajů též zákon č. 2/1969 Sb. o zřízení ministerstev a jiných ústředních orgánů státní správy České socialistické republiky, ve znění pozdějších předpisů.
[700] Čl. 51 a násl. GDPR.
[701] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

se však jedná o závěr, který nemá bezprostřední vazbu pouze na posuzovaný právní předpis, není tedy závislý na textaci tohoto předpisu a lze jej zobecnit a vztáhnout i k dalším obdobným případům, proto jej autor uvádí v těchto obecných závěrech.

Dle tohoto závěru Ústavního soudu ČR *„dozor Úřadu pro ochranu osobních údajů nad dodržováním povinností při zpracování osobních údajů"* předvídaný zákonem a *„vymezené nástroje jeho činnosti a kontroly nelze považovat za adekvátní a efektivní prostředek k ochraně základních práv dotčených jednotlivců, neboť tento nástroj neovládají sami“*. Autor toto hodnocení Ústavního soudu ČR vykládá tak, že Ústavní soud ČR nepovažuje samotný dozor ÚOOÚ, vč. nástrojů činnosti a kontrol tohoto úřadu za neefektivní v obecné rovině, pouze hodnotil jeho efektivitu a především přiměřenost ve vztahu k ochraně základních práv osob, které jsou dotčeny plošným zpracováním provozních a lokalizačních údajů dle posuzované právní úpravy ZoEK. Závěr učiněný v tomto nálezu pak specificky akcentuje skutečnost, že dotčené osoby nástroj v podobě dozoru ÚOOÚ neovládají, a to tím spíše, že tyto osoby navíc mnohdy ani následně nezískají informaci o proběhnuvším zásahu do jejich základního práva v podobě práva na informační sebeurčení. O významu informování subjektu údajů o provedeném zásahu pojednává autor výše.

V právní úpravě posuzované Ústavním soudem ČR nebyla v dané době zakotvena odpovídající právní povinnost orgánů oprávněných k získání uchovávaných provozních a lokalizačních údajů informovat, byť i následně, dotčené osoby. Ústavní soud ČR proto v nálezu Pl. ÚS 24/10 uzavřel, že v daném případě „*úkony, představující očividný zásah do základního práva jednotlivců na soukromí v podobě práva na informační sebeurčení (ve smyslu čl. 10 odst. 3 a čl. 13 Listiny), se tak vlivem nedostatečné a shora uvedeným ústavněprávním požadavkům neodpovídající právní úpravy ocitají mimo jakoukoliv bezprostřední, byť i následnou kontrolu, zejména pak kontrolu soudní, k jejíž nezbytnosti se vyjádřil i ESLP v citovaném rozhodnutí Camenzind v. Švýcarsko*“[702]. Ústavní soud ČR nad rámec výše uvedeného navíc v daném nálezu dodává, že k obdobným závěrům dospěly při posuzování ústavnosti obdobných právních úprav v národních právních řadech jiných států Evropy ústavní soudy daných států a jako příklad uvádí Německo, Rumunsko, Bulharsko či Kypr, výslovně zmiňuje také obdobné závěry Soudního dvora EU obsažené v rozhodnutí

[702] Rozsudek ESLP ve věci Camenzind proti Švýcarsku (no. 21353/93) ze dne 16. 12. 1997.

vydaném v řízení o předběžné otázce ve spojených věcech C-92/09 a C-93/09 z 9. listopadu 2010[703].

Roli orgánu dozoru plní do jisté míry též Stálá komise Poslanecké sněmovny Parlamentu ČR pro kontrolu použití odposlechu a záznamu telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací (dále též jen „Stálá komise PSP ČR"), to však pouze ve vztahu k odposlechu a záznamu telekomunikačního provozu[704]. Tato komise má kontrolní oprávnění výhradně ve vztahu k odposlechu a záznamu telekomunikačního provozu, nikoli též k vyžádání provozních a lokalizačních údajů, navíc se jedná o kontrolní orgán pouze ve vztahu k jednomu ze zásahů do práva na ochranu soukromí, a to zásahu dosti specifickému, byť z hlediska počtu případů velmi četnému. Stálá komise PSP ČR tak dle hodnocení autora není orgánem, který by mohl být považován za obecný kontrolní orgán v případech zásahů rozebíraných v této práci.

Dílčí závěry

Autor na základě výše uvedeného dospěl k závěru o nutnosti jednoznačně vymezit dozorové oprávnění ÚOOÚ v případech zásahů do práva na ochranu soukromí v podobě plošného shromažďování osobních údajů, jejichž typové případy autor rozebral výše v této práci. Předpokladem efektivní možnosti kontroly ÚOOÚ či jiného orgánu je však obecně informovanost dotčených subjektů údajů o proběhnuvším zásahu, jak autor upozornil v předchozím bodě. Současně se jako nezbytné jeví též odstranění zákonné překážky ukládající ÚOOÚ upustit od uložení správního trestu v případech, kdy se přestupku v oblasti ochrany osobních údajů dopustí orgán veřejné moci nebo veřejný subjekt[705].

4.2.8 Zvláštní ochrana lokalizačních údajů

Analýzou typových případů plošného zpracování údajů obsažených v této práci autor dospěl k závěru, že plošná zpracování lokalizačních údajů značného množství osob představují zásah do práva na ochranu soukromí s vysokou intenzitou. Dle hodnocení autora je tato intenzita výrazně vyšší, nežli je tomu u řady jiných kategorií osobních údajů. Lokalizační údaje totiž umožňuji fakticky monitorovat dotčené osoby zpětně, sledovat jejich pohyb a vyvozovat též další závěry, které na první pohled nemusejí být zcela zřejmé, včetně

[703] Rozhodnutí Soudního dvora EU v řízení o předběžné otázce ze dne 9. 11. 2010 ve spojených věcech Volker und Markus Schecke GbR GbR a Hartmut Eifert v. Land Hessen (C-92/09 a C-93/09).
[704] Existenci této kontroly předpokládá zákon o Policii ČR v § 98 Kontrola použití odposlechu a záznamu telekomunikačního provozu, použití sledování osob a věcí a rušení provozu elektronických komunikací.
[705] Viz § 62 odst. 5 ZoZOÚ.

informací o vzájemném vysoce pravděpodobném kontaktu dotčených osob v důsledku jejich výskytu ve stejný čas na stejném místě (případně ve spojení s informací o opakovaném takovémto společném výskytu zjištěném z analýzy lokalizačních údajů) či včetně predikce budoucího pohybu dotčených osob na základě analýzy jejich dosavadních vzorců chování apod. Zvláštní význam těchto údajů dovodil i generální advokát Soudního dvora EU ve svém, již výše zmiňovaném, stanovisku ve spojených věcech C 293/12 a C 594/12[706], které se týkaly posouzení Data Retention Směrnice, zakládající povinné zpracování provozních a lokalizačních údajů. Generální advokát Pedro Cruz Villalón označil tyto dvě kategorie osobních údajů za „kvalifikované", na rozdíl od „osobních údajů v tradičním smyslu" a upozornil na možné přesné a úplné zmapování chování konkrétní osoby či vytvoření obrazu soukromé identity takovéto osoby.

Osobní údaje v současné době v obecné rovině vymezuje GDPR, kromě obecných osobních údajů rozlišuje GDPR též osobní údaje ze zvláštních kategorií, lokalizační údaje však mezi ně nezařazuje a jejich úpravu ponechává zvláštnímu právnímu předpisu. Tím je Směrnice o soukromí a elektronických komunikacích a v právním řádu ČR ZoEK. Tyto předpisy se však uplatní pouze v oblasti elektronických komunikací, ostatně oba jsou ryze předpisy práva elektronických komunikací. Obdobné omezení výslovně předpokládá též návrh nařízení ePrivacy, jak autor popsal výše[707]. Lokalizační údaje udávající zeměpisnou polohu konkrétní fyzické osoby a také průběžné změny této polohy v čase (tedy „dynamické" lokalizační údaje, jak je autor vymezil v této práci výše) dlouhou dobu generovala téměř výhradně koncová zařízení elektronických komunikací (ZoEK používá termín telekomunikační koncová zařízení[708]) v mobilních komunikačních sítích. I v současnosti jde dle autora o typický případ vzniku lokalizačních údajů, ve významu výše vymezených dynamických lokalizačních údajů. Tato skutečnost vyplývá ze způsobu používání koncového zařízení – mobilního telefonního přístroje. Ten je často předmětem, který fyzická osoba nosí při sobě. Uvedený závěr však v současnosti již neplatí pouze pro koncová zařízení elektronických komunikací, údaje odpovídající výše vymezeným „dynamickým lokalizačním údajům" vznikají a k jejich zpracování dochází i v některých dalších oblastech.

---

[706] Stanovisko generálního advokáta Pedra Cruz Villalóna ve věci C-293/12 a ve věci C-594/12 přednesené dne 12. prosince 2013.

[707] Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích).

[708] ZoEK v tomto směru není zcela konzistentní, termín telekomunikační koncové zařízení používá např. v § 33 odst. 5 či 73 odst. 1, na jiných místech hovoří ve stejném významu pouze o koncovém zařízení.

Ve vztahu k tématu této práce považuje autor tuto skutečnost za velmi významnou, z případů plošného zpracovávání osobních údajů zkoumaných v této práci je tomu tak především u dopravních kamerových systémů, včetně systémů ke kontrole úhrady elektronických dálničních známek[709] a systémů dopravních kamer pro měření rychlosti vozidel či u zpracování údajů systémy v automobilech, zejména systémem eCall. Ve všech těchto zmiňovaných případech se jedná o lokalizační údaje, které lze současně považovat za osobní údaje, navíc se ve všech těchto případech jedná současně o lokalizační údaje, které jsou v čase proměnné a lze z nich tedy zjistit pohyb konkrétní fyzické osoby. Z případů v této práci neuvedených je to dále též např. využívání bezhotovostních platebních prostředků, jakými jsou platební karty či aplikace umožňující provedení platební transakce. Případů, v nichž jsou ve značném rozsahu, v některých případech i plošně, zpracovávány lokalizační údaje, přitom v praxi přibývá, jak autor ukázal výše v této práci. O to zásadnější je dle autora absence obecné úpravy lokalizačních údajů, mimo oblast elektronických komunikací. V popsaných případech totiž není ochrana lokalizačních údajů v relevantní právní úpravě upravena buď vůbec či pouze obecně, společně s jinými kategoriemi údajů, přičemž lokalizační údaje v ní nejsou specificky zmíněny, není tak specificky upravena ani jejich ochrana. Ta v důsledku toho není srovnatelná s ochranou poskytovanou lokalizačním údajům v rámci institutu důvěrnosti komunikací obsaženého v ZoEK (byť i ten je omezen pouze na údaje v rámci veřejně dostupných služeb elektronických komunikací či veřejných komunikačních sítí, jak autor rozebírá výše). Výše uvedený deficit ochrany je dle hodnocení autora důsledkem absence zakotvení úpravy lokalizačních údajů a jejich ochrany v obecné právní úpravě, bez vazby na elektronické komunikace. V úvahu přichází úprava ochrany osobních údajů či jiný právní předpis.

Snahy o využití těchto „netelekomunikačních“ lokalizačních údajů, které lze zaznamenat v praxi, svědčí o tom, že se nejedná pouze o teoretické úvahy. Jde např. o výše v této práci rozebírané situace využití údajů kamerového systému na silnicích ze strany správce daně pro účely kontroly správnosti nároku na daňový odpočet či snahy orgánů veřejné moci (vč. orgánů státní správy v oblasti ochrany veřejného zdraví) o využití údajů o lokalitě provedených platebních transakcí v případech karanténních omezení pohybu aplikovaných v souvislosti s výskytem onemocnění COVID-19[710]. Oba tyto případy svědčí dle autora

[709] Zákon č. 13/1997 Sb. o pozemních komunikacích, ve znění pozdějších předpisů, používá pro elektronické dálniční známky termín „časový poplatek za užití pozemní komunikace“, viz § 13 písm. j) a další ustanovení tohoto zákona.
[710] Viz např. Vláda ČR. *Chytrá karanténa nahradí dosavadní plošná opatření proti koronaviru*. 7.5.2020. [online]. [cit. 23.2.2024]. Dostupné z www.vlada.gov.cz.

jednoznačně o snaze orgánů veřejné moci využít takovéto lokalizační údaje k monitorování pohybu konkrétních fyzických osob.

Dílčí závěry

S ohledem na výše uvedené považuje autor za relevantní zvážit uplatnění specifické ochrany poskytované aktuálně lokalizačním údajům v právní úpravě elektronických komunikací, jakožto součásti důvěrnosti komunikací[711], de lege ferenda i na lokalizační údaje vznikající a uchovávané též v jiných oblastech nežli v elektronických komunikacích. Tato potřeba platí dle autora zvláště, jsou-li údaje uchovávány povinně, tento aspekt však není podmínkou zvýšené ochrany. Jak autor dovodil výše, důvod ke specifickému režimu ochrany lokalizačních údajů není dán pouze v případech, kdy jsou tyto údaje součástí komunikace dotčených osob či doprovodnými údaji takové komunikace. I ze samotných lokalizačních údajů, bez přístupu k dalším údajům o komunikaci a obsahu komunikace, lze totiž dovodit množství závěrů týkajících se osobních aspektů a charakteristik dotčené osoby, jejího soukromí, osob, s nimiž se stýká, predikce chování dotčených osob v budoucnu a dalších, to vše navíc i automatizovaným způsobem.

Bylo by tedy namístě, aby vymezení lokalizačních údajů, které vypovídají o lokalitě konkrétní fyzické osoby a umožňují monitorovat pohyb takové osoby, zejména „dynamických lokalizačních údajů“, bylo obsaženo v obecné právní úpravě ochrany osobních údajů, jakožto speciální kategorie osobních údajů. Takové vymezení by mělo především všem lokalizačním údajům zajišťovat stejnou míru ochrany, jakou aktuálně požívají lokalizační údaje generované v oblasti elektronických komunikací. Autor totiž nenachází relevantní argumenty pro zajištění ochrany těmto údajům pouze v závislosti na oblasti, ve které vznikají, jak je tomu v současné právní úpravě. V tomto směru autor považuje za relevantní též již výše zmiňované pochybnosti Jana Kudrny ohledně správnosti zařazení ochrany provozních a lokalizačních údajů pod ochranu poskytovanou čl. 13 Listiny.

Dle hodnocení autora je možným řešením výše popsaného problému specifická úprava ochrany lokalizačních údajů, jakožto zvláštní kategorie osobních údajů, v obecné právní úpravě ochrany osobních údajů, která by zahrnovala i případy, kdy tyto údaje nebyly získány v rámci poskytování služeb elektronických komunikací. Alternativním řešením by byla specifická ochrana zajištěná lokalizačním údajům v jednotlivých relevantních právních

[711] ZoEK používá v § 87 a násl. termín Ochrana osobních, provozních a lokalizačních údajů a důvěrnost komunikací, zatímco Listina setrvává v čl. 13 u formulace „*tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením*“.

úpravách týkajících se oblastí, v nichž lokalizační údaje vznikají – jako možné příklady lze uvést zákon o pozemních komunikacích zavádějící systém monitorování úhrady elektronických dálničních známek – Evidenci vozidel v systému časového zpoplatnění či zákon o platebním styku[712] upravující podmínky poskytování platebních služeb a provádění platebních transakcí. Jednalo by se tak ovšem vždy pouze o vzájemně nepropojené právní úpravy. Obecná ochrana by také mohla být obsažena v nařízení ePrivacy, dle autorovi dostupných informací s tím ovšem tento právní předpis nepočítá. Navíc je v současnosti ve stadiu návrhu diskutován již více než 10 let, když původním záměrem evropského zákonodárce bylo jeho přijetí společně s GDPR již v roce 2016. S ohledem na tyto skutečnosti autor považuje za vhodnější, minimálně v současné době, zařadit tuto ochranu přímo v právním řádu ČR, v ZoZOÚ.

Součástí této obecné ochrany by v souladu se závěry obsaženými ve výše rozebírané rozhodovací praxi k zásahům do práva na ochranu soukromí, zejména Ústavního soudu ČR a SDEU, měly být jak odpovídající povinnosti k ochraně takovýchto osobních údajů, tak rovněž omezení pro přístup k těmto údajům a pro jejich využití, obdobná omezením v úpravě provozních a lokalizačních údajů v ZoEK. V současné době existující ochrana poskytovaná lokalizačním údajům v ZoEK se mj. i v důsledku výše rozebíraných omezení nejeví jako zcela systémová. Obecná ochrana důvěrnosti komunikací, která vyplývá přímo z Listiny a z trestního zákoníku[713], nestanoví a s ohledem na zařazení a charakteristiky těchto dvou právních předpisů a ochrany v ní vymezené ani není způsobilá stanovit konkrétní pravidla zvýšené ochrany takových kategorií údajů.

[712] Zákon č. 13/1997 Sb. o pozemních komunikacích, ve znění pozdějších předpisů, zákon č. 370/2017 Sb. o platebním styku, ve znění pozdějších předpisů.
[713] Porušení tajemství dopravovaných zpráv vymezuje zákon č. 40/2009 Sb. trestní zákoník, ve znění pozdějších předpisů, v § 182 odst. 2.

5 Závěr, zhodnocení naplnění v úvodu vytyčených cílů

Autor pro podrobný rozbor v této práci vybral typové případy zpracování osobních údajů značného množství osob, zpravidla plošného charakteru. Jde o případy, které jsou založeny převážně na povinnosti zpracování osobních údajů buď přímo orgány veřejné moci či jinými osobami, avšak pro využití orgány veřejné moci, případně jde o zpracování právní úpravou v této podobě a ve značném rozsahu předpokládaná. Jako případy ke zkoumání v této práci autor vybral takové případy, u kterých na základě dostupných informací bylo možno předpokládat nejzávažnější dopad do soukromé sféry fyzických osob. Následně autor tyto vybrané případy analyzoval, za účelem identifikace cíle jednotlivých právních úprav, v podobě sledovaného veřejného zájmu a posouzení, zda a nakolik zkoumané právní úpravy naplňují ústavněprávní požadavky vyplývající z dostupné relevantní výkladové a rozhodovací praxe, zejména z rozhodovací činnosti Ústavního soudu ČR a Soudního dvora EU.

V úvodu práce si autor vytkl cíl posoudit na základě této analýzy dostatečnost omezení, kontrolních opatření a záruk bránících zneužití jednotlivých typových případů a v případě zjištěných nedostatků identifikovat opatření, která by de lege ferenda měla být přijata za účelem zajištění efektivních kontrolních opatření a ústavněprávních záruk. Autor se při návrzích těchto opatření zaměřil především na jejich obecnou využitelnost nejen v případech v této práci zkoumaných, nýbrž i v případě možných budoucích nových zásahů do práva na ochranu soukromí a práv souvisejících. Současně autor usiloval o maximální praktickou proveditelnost navržených opatření, ve snaze vyhnout se pouhým teoretickým úvahám, jejichž uplatnění v praxi by se jevilo jako spíše nepravděpodobné. Přitom autor samozřejmě připouští, že mnohá z navržených opatření bude v praxi obtížné prosadit, zvláště pokud by mělo dojít ke změnám v postupech orgánů veřejné moci, byť jsou mnohé z těchto změn předpokládány již platnou právní úpravou.

Dle hodnocení autora umožnují dílčí rozbory obsažené v této práci a jejich následná syntéza provedená v závěru práce učinit ve vztahu k navrženým obecným kontrolním mechanismům u zásahů do práva na ochranu soukromí následující shrnující závěry. V prvé řadě je nutno zdůraznit, že kontrolní mechanismy diskutované výše představují nikoli vzájemné substituty či alternativní mechanismy, které by se navzájem nahrazovaly, nýbrž naopak prvky, které by měly být aplikovány paralelně. Každý z výše představených kontrolních mechanismů se totiž dle názoru autora dotýká buď odlišné fáze legislativního procesu právních úprav zakládajících zásah do práva na ochranu soukromí, nebo vzájemně odlišných aspektů těchto zásahů.

Bohužel však dle autorova pozorování, jehož dílčí závěry rovněž představil výše, dochází z hlediska vývoje nikoli k postupné aplikaci jednotlivých kontrolních mechanismů a k posilování jejich uplatnění v praxi, nýbrž právě naopak – autor vnímá minimálně v případě některých kontrolních mechanismů zde diskutovaných spíše oslabování jejich faktické existence. Tak např. zveřejňování statistických údajů se u jmenné evidence cestujících v praxi omezilo pouze na okamžik přijetí dané právní úpravy, poté již oficiální celkové údaje publikovány nejsou; taktéž v případě povinnosti Data Retention přestal ČTÚ již před několika lety nejen zveřejňovat celkové statistické údaje o počtech případů, v nichž byly tyto údaje oprávněnými orgány vyžádány, ale přestal tyto údaje od povinných osob – poskytovatelů služeb a provozovatelů sítí elektronických komunikací v rámci pravidelných regulačních výkazů vyžadovat. V současnosti je tedy již nemá k dispozici, přičemž jejich shromažďování od jednotlivých povinných osob nepřevzal po ČTÚ ani jiný orgán. Důvodem byla v tomto případě změna právní úpravy, v důsledku které již shromažďování údajů od poskytovatelů služeb a provozovatelů sítí elektronických komunikací není vyžadováno.

Obecně též lze bohužel pozorovat trend k nárůstu množství závažných zásahů do soukromé sféry značného množství osob, jakož i ke zvyšování intenzity takových zásahů. Současně autor zaznamenává též postupně přibývající případy povinně shromažďovaných osobních údajů, zpravidla na plošném a nerozlišujícím základě, jak bylo ukázáno v této práci. Znepokojivé jsou taktéž narůstající snahy o využívání povinně zpracovávaných údajů pro účely odlišné od účelů původně vymezených, včetně snah o rozšiřování orgánů oprávněných k využívání takovýchto údajů, ať již cestou legislativních návrhů, jak autor ukázal výše v případě provozních a lokalizačních údajů elektronických komunikací a jejich možného budoucího využití ze strany ÚOHS a Státní hygienické služby, či dokonce cestou „faktickou“, beze změny právní úpravy, jak bylo dokladováno v této práci též ve vztahu k provozním i lokalizačním údajům elektronických komunikací, a to paradoxně ze strany ÚOOÚ. Příkladem budiž také případ získání záznamu údajů dopravních kamerových systémů Policie ČR a jejich využití v praxi ze strany správce daně.

Současně je z rozboru uvedených případů zřejmé, že uplatnění některých navržených kontrolních mechanismů je v praxi v mnoha případech do značné míry limitováno faktem, že právní úpravy zakládající závažné zásahy do práva na ochranu soukromí a do práv souvisejících jsou mnohdy založeny na implementaci právní úpravy unijního práva. Tento limitující faktor se z povahy věci projevuje zejména, nikoli však toliko, v případě výše

diskutované povinnosti provést legislativní DPIA analýzu v podobě obsažené v Legislativních pravidlech vlády.

Jak však uvedeno výše, i v takových situacích existuje pro předkladatele a také pro zákonodárce mnohdy určitá možnost volby prostředků, zejména v případě transpozice směrnic unijního práva. Především je ovšem do budoucna namístě zaměřit se na kvalitativní zlepšení legislativního procesu přijímání norem práva EU, počínaje již samotným návrhem a jeho odůvodněním. Příkladem budiž diskutovaná Data Retention Směrnice, která byla původně navržena a evropským zákonodárcem schválena jako *„opatření k odstranění překážek a narušení na vnitřním trhu EU“*, přestože od počátku existovaly silné pochybnosti o tom, že skutečným účelem této právní úpravy byla místo toho harmonizace uchovávání údajů elektronických komunikací pro usnadnění aktivit v oblasti trestního práva v členských státech EU. Navíc, po prohlášení této směrnice za neplatnou rozhodnutím Soudního dvora EU, kdy bylo možno očekávat na úrovni EU návrh nové právní úpravy, která by reagovala na nedostatky vytýkané Soudním dvorem EU, Evropská komise rozhodla takový návrh nepřipravit, jak také veřejně vyhlásila. Důsledkem toho je situace faktického rozporu mezi závěry Rozsudku Digital Rights a realitou v mnoha členských státech EU, Soudní dvůr EU se z tohoto důvodu problematikou Data Retention i nadále opakovaně zabývá k žádostem národních soudů o rozhodnutí předběžných otázek ve vztahu k relevantním národním úpravám.

Jako zásadní pro řešení tohoto problému se proto jeví zařazení adekvátní legislativní DPIA analýzy při přijímání unijního práva, včetně relevantního zapojení EDPB do legislativního procesu a tedy celkové posílení jeho role a především náležitá reakce na upozornění a doporučení EDPB v průběhu přijímání norem unijního práva. Právě v tomto ohledu považuje autor změny za dosti obtížně realizovatelné, nikoli však nemožné.

Současně však autor považuje mnohé další kontrolní mechanismy navržené na obecné úrovni v závěrech této práce za plně aplikovatelné a pro eliminaci následků zásahů do práva na ochranu soukromí velmi potřebné, když např. zajištění informovanosti dotčených osob, pravidelné vyhodnocování efektivity opatření či nemožnost využití shromažďovaných a dále zpracovávaných osobních údajů pro účel odlišný od účelu původního patří mezi opatření proveditelná zpravidla bez závislosti na normách unijního práva. Jedná se přitom o mechanismy a záruky, které při náležitém využití mohou být velmi efektivní.

S ohledem na výše uvedené autor hodnotí cíle vytýčené v úvodu práce jako naplněné, zejména v podobě výběru typových případů nejzávažnějších zásahů do práva na

ochranu soukromí, jejich důkladné analýzy s důrazem na ústavněprávní hlediska a následného návrhu obecných opatření k zajištění záruk ústavnosti zásahů do práva na ochranu soukromí a práv souvisejících.

6 Přílohy

Příloha č. 1 Odpověď ČNB z 15.5.2017 k žádosti autora ve věci žádostí o provozní a lokalizační údaje

Příloha č. 2 Odpověď ČNB ze 25.4.2024 k žádosti autora ve věci žádostí o provozní a lokalizační údaje

Příloha č. 3 Odpověď ÚOOÚ ze 22.5.2024 k žádosti autora ve věci žádostí o provozní a lokalizační údaje

7 Seznam použitých zdrojů, vč. citovaných rozhodnutí

7.1 Seznam citované literatury

1. BALOG, Boris. Inovačné výzvy pre Ústavu z oblasti legislatívy alebo o legislatívnej smršti a iných (nielen meteorologických) poverách v slovenskej legislatíve. In *INOVAČNÉ VÝZVY PRE ÚSTAVY A ÚSTAVNÉ SYSTÉMY V GLOBALIZOVANEJ EURÓPE. Bratislavské právnické fórum 2013. Zborník príspevkov z medzinárodnej vedeckej konferencie.* Bratislava: Univerzita Komenského, 2013, s. 660–674. ISBN 9788071603658.
2. BARAK, Aharon. *Proportionality. Constitutional Rights and their Limitations.* Cambridge: Cambridge University Press, 2012. 638 p. ISBN 9781107008588.
3. BENDOR, Ariel L., SELA, Tal. *How proportional is proportionality?* International Journal of Constitutional Law, Volume 13, Issue 2, April 2015, Pages 530–544. ISSN 1474-2640.
4. BOBEK, Michal, KOMÁREK, Jan, PASSER, Jan M., GILLIS, Mark. *Předběžná otázka v komunitárním právu.* Praha: Linde Praha, a.s., 2005. 522 s. ISBN 80-7201-513-3.
5. EAGLE, Nathan, PENTLAND, Alex. *Reality mining: sensing complex social systems.* Massachusetts Institut of Technology. MIT Media Laboratory. 3. November 2005. Personal and ubiquitous computing. 2006. ISSN 1617-4917.
6. EHMANN, Eugen, SELMAYR, Martin. *Datenschutz-Grundverordnung: DS-GVO. 3. Auflage.* München: C.H.BECK Verlag, 2024. 1486 s. ISBN 978-3-406-79777-4.
7. GERLOCH, Aleš. *Nový dualismus práva.* Soudce 7/2014. s. 32. ISSN 2788-3795.
8. GERLOCH, Aleš a kol. *Teorie a praxe tvorby práva*. Praha: ASPI, 2008. 424 s. ISBN 978-80-7357-362-1.
9. GERLOCH, Aleš. *Teorie práva, 8. vyd.* Plzeň: Aleš Čeněk, 2021. 352 s. ISBN 978-80-7380-838-9.
10. GERLOCH, Aleš. *Ústava a ústavnost v České republice.* Soudce 11/2016. s. 56. ISSN 2788-3795.
11. GERLOCH, Aleš, ŠTURMA, Pavel (eds.) *Ochrana základních práv a svobod v proměnách práva na počátku 21. století v českém, evropském a mezinárodním kontextu*. Praha: Auditorium, 2012. 536 s. ISBN 978-80-87284-23-0.
12. GŘIVNA, Tomáš, POLČÁK, Radim (eds.) *Kyberkriminalita a právo.* Praha: Auditorium s.r.o., 2008. 220 s. ISBN 978-80-903786-7-4.

13. HARAŠTA, Jakub, MÍŠEK, Jakub. IP adresy v kybernetické bezpečnosti. *Revue pro právo a technologie.* 2015, roč. 6, č. 12. ISSN: 1804-5383.
14. HOLUBÁŘ Adam, MOHELSKÝ Michal, SEBORSKÝ Jaroslav. *Data retention a lokalizační údaje v boji s pandemií onemocnění Covid-19.* Advokátní deník. 26.3.2020. ISSN 2571-3558.
15. CHUDOMELOVÁ, Zuzana, BERAN, Marek, JADRNÝ, Vratislav, NĚMEČKOVÁ, Šárka, NOVÁK, Jaromír. *Zákon o elektronických komunikacích*. *Komentář*. Praha: Wolters Kluwer ČR, 2016. 508 s. ISBN 978-80-7552-100-2.
16. JELÍNEK, Jiří. *Trestní zákoník a trestní řád s poznámkami a judikaturou - 9. aktualizované vydání.* Praha: Leges, 2022. 1424 s. ISBN 978-80-7502-637-8.
17. KMEC, Jiří, KOSAŘ, David, KRATOCHVÍL, Jan, BOBEK, Michal. *Evropská úmluva o lidských právech. Komentář. 1. vyd.* Praha: C.H. Beck, 2012, 1696 s. ISBN 978-80-7400-365-3.
18. KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, z.s.p.o., 2016. 524 s. ISBN 978-80-88168-15-7.
19. KRAUSOVÁ, Alžběta. *Zásada autonomie vůle v ochraně soukromí: Možnosti a limity v rozhodování o vlastních biometrických údajích.* Právní rozhledy. Roč. 26, č. 6 (2018), s. 191-197. ISSN 1210-6410.
20. KÜHLING, Jürgen, BUCHNER, Benedikt. *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG. Kommentar. 4. Auflage.* München: C.H.BECK Verlag, 2024. 2140 s. ISBN 978-3-406-80263-8.
21. KUSCHEWSKY, Monika. *Data Protection & Privacy, Jurisdictional comparisons.* Second Edition 2014. London : Thomson Reuters (Professional) UK Limited. ISBN ISBN 978-1908239143.
22. MADEJ, Martin. *Meze základních práv v České republice.* Praha: Leges, 2018. 240 s. ISBN 978-80-7502-294-3.
23. ONDŘEJEK, Pavel. *Princip proporcionality a jeho role při interpretaci základních práv a svobod*. Praha: Leges, 2012. 232 s. ISBN 978-80-87576-31-1.
24. POLČÁK, Radim. *Internet a proměny práva.* Praha: Auditorium s.r.o., 2012. 392 s. ISBN 978-80-87284-22-3.
25. RYCHETSKÝ, Pavel, LANGÁŠEK, Tomáš, HERC, Tomáš, MLSNA, Petr a kolektiv. *Ústava České republiky. Zákon o bezpečnosti České republiky. Komentář.* Praha: Wolters Kluwer (ČR) 2015. 1224 s. ISBN 978-80-7478-809-3.
26. SCHELLE, Karel, TAUCHEN, Jaromír (eds). *Encyklopedie českých právních dějin. XVIII. svazek Ta-Ty.* Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2019. 890 s. ISBN 978-80-7380-779-5 v koedici s Ostrava: KEY Publishing s.r.o. 2019. ISBN 978-80-7418-322-5.
27. SMEJKAL, Vladimír. *Kybernetická kriminalita. 3. vyd.* Plzeň: Aleš Čeněk, 2022. 1166 s. ISBN 978-80-7380-849-5.
28. SMEJKAL, Vladimír a kol. *Právo informačních a telekomunikačních systémů.* 1. vydání. Praha : C.H.Beck, 2001. 770 s. ISBN 80-7179-765-0.
29. SVOBODOVÁ, Magdaléna. *Nahrazování směrnic nařízeními v právu Evropské unie. Habilitační přednáška.* Právník 5/2022. s. 469-472. ISSN 0231-6625.
30. ŠIŠKOVÁ, Naděžda. *Evropská unijní ochrana lidských práv (Charta a další instrumenty ochrany lidských práv v EU).* Praha: Linde Praha a.s, 2001. 217 s. ISBN 80-7201-278-9.

31. ŠTURMA, Pavel. *Mezinárodní a evropské kontrolní mechanismy v oblasti lidských práv. 3. doplněné vydání.* Praha: C.H.Beck, 2010. 164 s. ISBN 978-80-7400-961-7.
32. TOMÁŠEK, Michal, ŠMEJKAL, Václav a kol. *Smlouva o fungování EU. Smlouva o EU. Listina základních práv EU. Komentář.* Praha: C.H.Beck, 2022. 1696 s. ISBN 978-80-7676-508-5.
33. UŘIČAŘ, Miroslav, RÁMIŠ, Vladan a kol. *Obecné nařízení o ochraně osobních údajů. Komentář. 1. vydání.* Praha: C. H. Beck, 2021. 1414 s. ISBN 978-80-7400-815-3.
34. VOBOŘIL, Jan. Využívání provozních a lokalizačních údajů ze strany oprávněných orgánů, zejména Policie ČR. DATA RETENTION RELOADED: ZKUŠENOSTI, PROBLÉMY A APLIKAČNÍ PRAXE. In: *Sborník z workshopu konaného dne 23.4.2013 v Brně*. 1. vyd. Řada teoretická, Ed. S, č. 464. Brno : Masarykova univerzita, Právnická fakulta, 2013, 232 s. ISBN 9788021067226.
35. VOBOŘIL, Jan. *Data Retention v (nejen) policejní praxi. Analýza postupů Policie ČR a dalších orgánů při vyžadování a využívání provozních a lokalizačních údajů o elektronických komunikacích v České republice.* Iuridicum Remedium, o.s. 25. září 2012. [online]. 2012. [cit. 24.2.2024].
36. WAGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch, LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer, 2012, 1076 s. ISBN 978-80-7676-747-8.
37. ZUCCA, Lorenzo. *Constitutional Dilemmas: Conflicts of Fundamental Legal Rights in Europe and the USA.* Oxford: Oxford University Press, 2008. 206 p. ISBN 978-0199552184.
38. ŽÁK KRZYŽANKOVÁ, Katarzyna, KÜHN, Zdeněk et al. (eds.) *Právo jako multidimenzionální fenomén. Pocta Aleši Gerlochovi k 65. narozeninám.* Plzeň: Aleš Čeněk, 2020. 800 s. ISBN 978-80-7380-797-9.

7.2 Seznam použitých internetových zdrojů

1. ADAC. *Section Control eingestellt: Alle Infos zum Tempo-Messverfahren.* 16.1.2024. [online] [cit. 18.3.2024]. Dostupné z www.adac.de.
2. Agentura Evropské unie pro základní práva a Rada Evropy. *Příručka evropského práva v oblasti ochrany osobních údajů.* 2021. [online] [cit. 18.3.2024]. Dostupné z www.prd-echr.coe.in.
3. ARTICLE 29 – DATA PROTECTION WORKING PARTY. *Opinion 10/2001 on the need for a balanced approach in the fight against terrorism. WP 53.* Adopted on 14 December 2001. [online]. 2001. [cit. 24.2.2024].
4. ARTICLE 29 – DATA PROTECTION WORKING PARTY. *Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005). WP 113.* Adopted on 21st October 2005. [online]. 2005. [cit. 24.2.2024].
5. ARTICLE 29 – DATA PROTECTION WORKING PARTY. *Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the Retention of data generated or processed in connection with the provision of publicly availabe electronic communications services or of public communications networks and amending Directive 2002/58/EC. WP 119.* Adopted on 25 March 2006. [online]. 2006. [cit. 24.2.2024].

6. ARTICLE 29 – DATA PROTECTION WORKING PARTY. *Working document on data protection and privacy implications in eCall initiative. WP 125.* Adopted on 26th September 2006. [online]. 2006. [cit. 24.2.2024].
7. ARTICLE 29 – DATA PROTECTION WORKING PARTY. *Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries. WP 178.* Adopted on 12 November 2010. [online]. 2010. [cit. 24.2.2024].
8. ARTICLE 29 – DATA PROTECTION WORKING PARTY. *Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. WP 181.* Adopted on 5 April 2011. [online] [cit. 24.2.2024].
9. BOEHM, Franziska, COLE, Mark D. *Data Retention after the Judgement of the Court of Justice of the European Union*. Münster/Luxembourg, 30 June 2014. [online] [cit. 15.1.2024]. Dostupné z https://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf .
10. CEBIA. Vehicle identification number. [online] [cit. 15.1.2024]. Dostupné z www.cebia.cz.
11. Česká advokátní komora. *ÚOOÚ nemohl udělit pokutu ministerstvu vnitra, neumožňuje mu to zákon*. Advokátní deník online. 29. 8. 2019. [online] [cit. 12.1.2024]. Dostupné z www.advokatnidenik.cz.
12. Česká advokátní komora. *Připomínky k návrhu zákona, kterým se mění zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a další související zákony.* Č.j.: 07.32-000005/20, nedatováno. [online] [cit. 12.1.2024]. Dostupné z www.cak.cz.
13. Český telekomunikační úřad. *Tisková zpráva. Operátoři předali ČTÚ výkaz o poskytnutých provozních a lokalizačních údajích.* 19.3.2014. [online] [cit. 8.2.2024]. Dostupné z www.ctu.gov.cz.
14. Český telekomunikační úřad. *Tisková zpráva. Operátoři v roce 2018 na žádost oprávněných orgánů předali 332 tisíc provozních a lokalizačních údajů.* 25.3.2019. [online] [cit. 8.2.2024] Dostupné z www.ctu.gov.cz.
15. Český telekomunikační úřad. *Přehledy poskytnutých provozních a lokalizačních údajů*. [online] [cit. 8.2.2024] Dostupné z www.ctu.gov.cz.
16. Český telekomunikační úřad. *Výroční zpráva Českého telekomunikačního úřadu za rok 2022*. [online] [cit. 8.2.2024]. Dostupné z www.ctu.gov.cz.
17. ČT24. *Ochránci dat řeší zdravotní registry i úniky ze spisů*. 24.9.2008. [online] [cit. 15.1.2024]. Dostupné z www.ct24.ceskatelevize.cz.
18. European Data Protection Board. *Pokyny č. 01/2020 ke zpracování osobních údajů v souvislosti s propojenými vozidly a aplikacemi souvisejícími s mobilitou. Verze 2.0.* Přijato dne 9. března 2021. [online] [cit. 24.2.2024]. Dostupné z www.edpb.europa.eu.
19. European Data Protection Board. *Statement 5/2022 on the implications of the CJEU judgement C-817/19 regarding the implementation of the Directive (EU) 2016/681 on the use of PNR in Member States.* Přijato 13. prosince 2022. [online] [cit. 24.2.2024]. Dostupné z www.edpb.europa.eu.

20. European Council. *Evropská bezpečnostní strategie*. 12. prosince 2003 [online]. [cit. 12.1.2023].
21. European Council. *Declaration on Combating Terrorism.* 25 March 2004 [online] [cit. 12.1.2023]. Dostupné z www.consilium.europa.eu.
22. European Council. *Document of the Council 8958/04 of 28 April 2004.* [online] [cit. 12.1.2023]. Dostupné z www.consilium.europa.eu.
23. European Council. *Council Declaration on the EU response to the London bombings.* 13 July 2005. [online] [cit. 12.1.2023]. Dostupné z www.consilium.europa.eu.
24. European Council. *Press Release, 2709th Council Meeting, Justice and Home Affairs* [online] [cit. 12.1.2023]. Dostupné z www.consilium.europa.eu.
25. European Council. *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union´s Foreign and Security Policy*. 2008. [online] [cit. 12.1.2023]. Dostupné z www.consilium.europa.eu.
26. European Commission. *Memo Frequently Asked Qestions: The Data Retention Questions.* 8 April 2014. [online] [cit. 24.2.2024]. Dostupné z www.ec.europa.eu.
27. European Commission. *European Commision statement on national data retention laws*. Brussels, 16 September 2015. [online] [cit. 3.5.2024]. Dostupné z www.ec.europa.eu.
28. European Commission. *Report from the Commission to the European Parliament and the Council On the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*. 24.7.2020. [online] [cit. 24.2.2024]. Dostupné z www.ec.europa.eu.
29. Evropská komise. *Zpráva Komise Evropskému parlamentu a Radě o společném hodnocení Dohody mezi Spojenými státy americkými a Evropskou unií o využívání jmenné evidence cestujících a o jejím předávání Ministerstvu vnitřní bezpečnosti Spojených států*. 12. ledna 2021. [online] [cit. 24.2.2024]. Dostupné z www.ec.europa.eu.
30. Evropská komise. *Doporučení pro Rozhodnutí Rady o zmocnění k zahájení jednání o dohodě mezi Evropskou unií a Islandem o předávání údajů jmenné evidence cestujících z EU na Island za účelem prevence, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti*. 6.9.2023. [online] [cit. 24.2.2024]. Dostupné z www.ec.europa.eu.
31. Evropská komise. *Návrh Rozhodnutí Rady o podpisu Dohody mezi Kanadou a Evropskou unií o předávání a zpracování údajů jmenné evidence cestujících (PNR) jménem Evropské unie.* 4.3.2024. [online] [cit. 24.2.2024]. Dostupné z www.ec.europa.eu.
32. European Environment Agency. *Transport and environment report 2022.* [online]. 2022. Dostupné z www.eea.europa.eu. [cit. 8.2.2024].
33. European Parliament. *Transfers of passenger name records (PNR) to Canada taking place despite the absence of an EU-Canada PNR Agreement.* 24.1.2022. Dostupné z www.europarl.europa.eu. [online] [cit. 24.2.2024].
34. Evropský parlament. *Usnesení Evropského parlamentu ze dne 20. listopadu 2008 o návrhu rámcového rozhodnutí Rady o používání jmenné evidence cestujících (PNR) pro účely vynucování práva.* [online] [cit. 24.2.2024]. Dostupné z www.europarl.europa.eu.
35. Evropský parlament. *Boj proti terorismu: Parlament vymezil pravidla používání údajů cestujících v letecké dopravě.* 13. dubna 2016. [online] [cit. 24.2.2024]. Dostupné z www.europarl.europa.eu.
36. Eurostat. *Statistika přepravy cestujících. Přes letiště v EU-27 byla v roce 2018 přepravena téměř 1 miliarda cestujících.* 7. ledna 2021. [online] [cit. 24.2.2024]. Dostupné z https://ec.europa.eu/eurostat.

37. Evropský inspektor ochrany údajů. *Stanovisko Evropského inspektora ochrany údajů k návrhu rozhodnutí Rady o uzavření Dohody mezi Spojenými státy americkými a Evropskou unií o využívání jmenné evidence cestujících a o jejím předávání Ministerstvu vnitřní bezpečnosti Spojených států.* 9. prosince 2011. [online] [cit. 24.2.2024]. Dostupné z https://eur-lex.europa.eu/legal-content.
38. Evropský inspektor ochrany údajů. *EDPS formal comments on a draft Commission Implementing Regulation on the monitoring and reporting of data relating to CO2 emissions from passenger cars and light commercial vehicles pursuant to Regulation (EU) 2019/631 of the European Parliament and of the Council and repealing Implementing Regulations (EU) No 1014/2010, (EU) No 293/2012, (EU) 2017/1152 and (EU) 2017/1153.* 14 January 2021. [online] [cit. 24.2.2024]. Dostupné z https://www.edps.europa.eu/.
39. FTV Prima. *Hackeři ovládli měření na D1. Pokuty můžete zahodit*. 1.8.2016. [online] [cit. 15.1.2024]. Dostupné z https://cool.iprima.cz/porady/autosalon/hackeri-ovladli-mereni-na-d1-pokuty-muzete-zahodit.
40. Iuridicum Remedium o.s. *Stanovisko občanského sdružení Iuridicum Remedium k ústavní konformitě úpravy národních zdravotních registrů v zákoně o zdravotních službách (vypracované jako součást dopisu AMICUS CURIAE pro Ústavní soud ČR ve věci sp. zn. Pl. ÚS 1/12).* [online] [cit. 15.1.2024]. Dostupné z www.iure.org.
41. Max-Planck-Institut für ausländisches und internationales Strafrecht. Kriminologická studie „*Stutzlücken durch Wegfall der Vorratsdatenspeicherung?*“. 2012. [online] [cit. 15.1.2024]. Dostupné z www.grundrechte.ch.
42. Ministerstvo dopravy ČR. *Ročenka dopravy 2022.* [online] [cit. 15.1.2024]. Dostupné z www.sydos.cz.
43. Ministerstvo průmyslu a obchodu. *Metodická pracovní pomůcka. Metodické doporučení Ministerstva pro místní rozvoj a Ministerstva průmyslu a obchodu.* 5. června 2019. [online] [cit. 15.1.2024]. Dostupné z www.mpo.gov.cz.
44. Moravskoslezské datové centrum, příspěvková organizace. *Vysokorychlostní datová síť Moravskoslezského kraje, etapa I.* [online] [cit. 15.1.2024]. Dostupné z Portálu pro vhodné uveřejnění https://www.vhodne-uverejneni.cz/.
45. Nejvyšší soud ČR. Tisková zpráva ze dne 28. července 2016. *Reakce Nejvyššího soudu na titulní článek deníku Právo ze dne 28.7.2016.* Dostupné z www.nsoud.cz. [online] [cit. 27.6.2017].
46. Niedersächsisches Ministerium für Inneres und Sport. *Rechtsgrundlage zur Abschnittskontrolle „Section Control“ bestätigt: Nach OVG-Beschluss wird der Betrieb an der B 6 bei Hannover kurzfristig wieder aufgenommen.* 14. 11. 2019. [online] [cit. 18.3.2024]. Dostupné z https://www.mi.niedersachsen.de.
47. Niedersächsisches Ministerium für Inneres und Sport. *Verkehrsüberwachung durch Abschnittskontrolle.* 8. 12. 2020. [online] [cit. 18.3.2024]. Dostupné z www.innenministerkonferenz.de.
48. Policie ČR. *Automatická kontrola vozidel. Zveřejněné informace 2015*. 25. května 2015. [online] [cit. 12.1.2023]. Dostupné z www.policie.cz.
49. Policie ČR. *Rozpoznávání registračních značek. Zveřejněné informace 2015.* 26. ledna 2015. [online] [cit. 12.1.2023]. Dostupné z www.policie.cz.
50. Policie ČR. *Spuštění lokalizačních SMS na mobilních telefonech.* 12. února 2020. [online] [cit. 12.1.2023] Dostupné z www.policie.cz.

51. Policie České republiky. *Národní kontaktní bod pro terorismus.* Nedatováno. [online] [cit. 12.1.2023] Dostupné z www.policie.cz.
52. Policie ČR. *Centrální automatická kontrola vozidel. Zveřejněné informace 2022.* 27. září 2022. [online] [cit. 12.1.2023]. Dostupné z www.policie.cz.
53. Policie ČR. *Úsekové měření rychlosti. Zveřejněné informace 2022.* 31. března 2022. [online] [cit. 12.1.2023]. Dostupné z www.policie.cz.
54. Policie ČR. *Metodika určování míst pro měření rychlosti obecní policií podle § 79a zákona č. 361/2000 Sb.* 10. srpna 2023. [online] [cit. 12.1.2023]. Dostupné z www.policie.cz.
55. Pracovní skupina WP 29. *Stanovisko 1/2014 k uplatňování pojmů nezbytnosti a proporcionality a ochrany údajů v oblasti vymáhání práva, přijato 27. února 2014.* [online] [cit. 24.2.2024]. Dostupné z https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation.
56. Pracovní skupina WP 29. *Pokyny týkající se pověřenců pro ochranu osobních údajů WP 243 rev.01.* Přijaté dne 13. prosince 2016 a naposledy revidované a přijaté dne 5. dubna 2017. [online] [cit. 24.2.2024]. Dostupné z www.uoou.gov.cz.
57. Pracovní skupina WP 29. *Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko" pro účely nařízení 2016/679 WP 248 rev.01.* Přijaté dne 4. dubna 2017. Naposledy revidované a přijaté dne 4. října 2017 v aktualizovaném znění. [online] [cit. 24.2.2024]. Dostupné z www.uoou.gov.cz.
58. Pracovní skupina zřízená podle článku 29. *Pokyny k transparentnosti podle nařízení 2016/679.* Přijaté dne 29. listopadu 2017, ve znění naposledy revidovaném a přijatém dne 11. dubna 2018. WP260 rev.01. [online] [cit. 24.2.2024]. Dostupné z www.uoou.gov.cz.
59. Rada Evropské unie. *Údaje o cestujících.* 21. dubna 2016. [online] [cit. 24.2.2024]. Dostupné z www.consilium.europa.eu/cs/policies/fight-against-terrorism/passenger-name-record/.
60. Úřad pro ochranu hospodářské soutěže. *Úřad předložil řadu legislativních návrhů pro větší efektivitu v oblasti hospodářské soutěže.* [online] [cit. 18.3.2024]. Dostupné z www.uohs.gov.cz.
61. Úřad pro ochranu osobních údajů. *Rada Evropy.* [online] [cit. 18.3.2024]. Dostupné z www.uoou.gov.cz.
62. Úřad pro ochranu osobních údajů. *Desatero omylů*. Nedatováno. [online] [cit. 18.3.2024]. Dostupné z www.uoou.gov.cz.
63. Úřad pro ochranu osobních údajů. *Lhůty pro uchovávání dat by se měly pro různé subjekty stanovovat individuálně.* 14.1.2021. [online] [cit. 18.3.2024]. Dostupné z www.uoou.gov.cz.
64. Úřad pro ochranu osobních údajů. *Připomínky k návrhu zákona, kterým se mění zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a další související zákony.* Nedatováno. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
65. Úřad pro ochranu osobních údajů. *Stanovisko Úřadu pro ochranu osobních údajů k Návrhu směrnice Evropského parlamentu a Rady o používání údajů jmenné evidence cestujících pro prevenci, odhalování, vyšetřování a stíhání teroristických činů a závažné trestné činnosti ze dne 9. března 2011*. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.

66. Úřad pro ochranu osobních údajů. *Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů.* 2024. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
67. Úřad pro ochranu osobních údajů. Protokol o kontrole ÚOOÚ z 15. března 2017. Čj. UOOU-09928/16-22. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
68. Úřad pro ochranu osobních údajů. *Výroční zpráva 2007.* [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
69. Úřad pro ochranu osobních údajů. *Zpracování osobních údajů v souvislosti s měřením rychlosti vozidel*. bez uvedení data. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz, sekce Kontroly za rok 2009.
70. Úřad pro ochranu osobních údajů. *Kontroly za rok 2007. Zdravotnictví.* [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
71. Úřad pro ochranu osobních údajů. *Nová úprava DPIA*. 9.2.2023. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
72. Úřad pro ochranu osobních údajů. *Návod k posouzení vlivu na ochranu osobních údajů u návrhů právních předpisů (DPIA).* 3. ledna 2019. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
73. Úřad pro ochranu osobních údajů. *Zahájena veřejná konzultace k metodice legislativního DPIA*. 8.3.2023. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
74. Úřad pro ochranu osobních údajů. *Metodika pro legislativní DPIA*. Bez uvedení data publikace. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
75. Úřad pro ochranu osobních údajů. *Porušení povinností při zpracování osobních údajů.* [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
76. Úřad pro ochranu osobních údajů. *ÚOOÚ nemohl udělit pokutu ministerstvu, neumožňuje mu to zákon.* Publikováno 9.8.2019. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
77. Úřad pro ochranu osobních údajů. *K povinnosti provádět posouzení vlivu na ochranu osobních údajů (DPIA)*. Nedatováno, zveřejněno 7. února 2018. [online] [cit. 12.1.2024]. Dostupné z www.uoou.gov.cz.
78. Úřad pro ochranu osobních údajů. *Uchování údajů – prováděcí vyhláška*. Č.j. UOOU-11928/15-8. 3.listopadu 2015. [online]. [cit. 24.2.2024]. Dostupné z www.uoou.gov.cz.
79. Ústav zdravotnických informací a statistiky ČR. *Souhrnné reporty.* [online]. [cit. 23.2.2024]. Dostupné z www.uzis.cz.
80. Vláda ČR. *Legislativní pravidla vlády.* [online]. [cit. 23.2.2024]. Dostupné z www.vlada.gov.cz.
81. Vláda ČR. *Metodika hodnocení dopadů regulace na administrativní zátěž občanů, včetně dopadů na soukromí*. Červen 2015. [online]. [cit. 23.2.2024]. Dostupné z www.vlada.gov.cz.
82. Vláda ČR. *Obecné zásady pro hodnocení dopadů regulace (RIA).* 3. února 2016. [online]. [cit. 23.2.2024]. Dostupné z www.vlada.gov.cz.
83. Vláda ČR. *Usnesení č. 820 ze dne 14. listopadu 2012 o změně Legislativních pravidel vlády*. [online]. [cit. 23.2.2024]. Dostupné z www.vlada.gov.cz
84. Vláda ČR. *Návrh změn Legislativních pravidel vlády, Obecných zásad pro hodnocení dopadů regulace (RIA) a Jednacího řádu vlády.* Předloženy ministrem pro legislativu a předsedou Legislativní rady vlády. Č.j. 1508/22. Bod 32 schůze vlády konané dne 21. 12. 2022. [online]. [cit. 23.2.2024]. Dostupné z www.odok.cz.

85. Vláda ČR. *Metodické pokyny pro zajišťování prací při plnění legislativních závazků vyplývajících z členství České republiky v Evropské unii, schválené usnesením vlády ze dne 12. října 2005 č. 1304 a změněné usnesením vlády ze dne 26. října 2009 č. 1344, usnesením vlády ze dne 3. ledna 2018 č. 19 a usnesením vlády ze dne 27. února 2018 č. 138.* [online]. [cit. 23.2.2024]. Dostupné z www.vlada.gov.cz.
86. Vláda ČR. *Metodická pomůcka pro prevenci nadbytečné regulatorní zátěže při implementaci práva EU.* [online]. [cit. 23.2.2024]. Dostupné z www.vlada.gov.cz.
87. Vláda ČR. *Chytrá karanténa nahradí dosavadní plošná opatření proti koronaviru*. 7.5.2020. [online]. [cit. 23.2.2024]. Dostupné z www.vlada.gov.cz

7.3 Seznam použitých právních předpisů (včetně návrhů právních předpisů)

1. Návrh Nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích).
2. Návrh Data Retention Směrnice Evropského parlamentu a Rady o uchovávání údajů zpracovávaných v souvislosti s poskytováním veřejných služeb v odvětví elektronických komunikací, kterou se mění směrnice 2002/58/ES ze dne 21. září 2005, COM (2005) 438 final.
3. Návrh zákona, kterým se mění zákon č. 258/2000 Sb., o ochraně veřejného zdraví a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a další související zákony. Č.j. MZDR 53739/2020.
4. Návrh zákona o elektronických komunikacích. Sněmovní tisk Poslanecké sněmovny Parlamentu České republiky č. 768/4.
5. Návrh novely Vyhlášky Ministerstva průmyslu a obchodu č. 357/2012 Sb. ze dne 17. října 2012 o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.
6. Listina základních práv a svobod, ve znění pozdějších změn.
7. Listina základních práv Evropské unie (2016/C 202/02; Úř. věst. C 202, 7.6.2016, s. 389–405)
8. Nařízení Evropského parlamentu a Rady (ES) č. 443/2009 ze dne 23. dubna 2009, kterým se stanoví výkonnostní emisní normy pro nové osobní automobily v rámci integrovaného přístupu Společenství ke snižování emisí CO2 z lehkých užitkových vozidel.
9. Nařízení Komise (EU) č. 1014/2010 ze dne 10. listopadu 2010 o sledování a hlášení údajů o registraci nových osobních automobilů podle nařízení Evropského parlamentu a Rady (ES) č. 443/2009.
10. Nařízení Evropského Parlamentu a Rady (EU) č. 596/2014 ze dne 16. dubna 2014 o zneužívání trhu (nařízení o zneužívání trhu) a o zrušení směrnice Evropského parlamentu a Rady 2003/6/ES a směrnic Komise 2003/124/ES, 2003/125/ES a 2004/72/ES.
11. Nařízení Evropského parlamentu a Rady (EU) 2015/758 ze dne 29. dubna 2015 o požadavcích na schválení typu pro zavedení palubního systému eCall využívajícího linku tísňového volání 112 a o změně směrnice 2007/46/ES
12. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení Směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
13. Nařízení Komise v přenesené pravomoci (EU) 2017/79 ze dne 12. září 2016, kterým se stanoví podrobné technické požadavky a zkušební postupy pro ES schválení typu motorových vozidel, pokud jde o jejich palubní systémy eCall využívající linku tísňového volání 112 a palubní samostatné technické celky a konstrukční části využívající linku

tísňového volání 112, a kterým se doplňuje a mění nařízení Evropského parlamentu a Rady (EU) 2015/758, pokud jde o výjimky a použitelné normy.
14. Nařízení Evropského parlamentu a Rady (EU) 2019/631 ze dne 17. dubna 2019, kterým se stanoví výkonnostní normy pro emise CO2 pro nové osobní automobily a pro nová lehká užitková vozidla a kterým se zrušují nařízení (ES) č. 443/2009 a (EU) č. 510/2011.
15. Nařízení Evropského parlamentu a Rady (EU) 2019/1239 ze dne 20. června 2019, kterým se zřizuje evropské prostředí jednotného námořního portálu a zrušuje směrnice 2010/65/EU.
16. Prováděcí nařízení Komise (EU) 2021/392 ze dne 4. března 2021 o sledování a hlášení údajů týkajících se emisí CO2 z osobních automobilů a lehkých užitkových vozidel podle nařízení Evropského parlamentu a Rady (EU) 2019/631 a o zrušení prováděcích nařízení Komise (EU) č. 1014/2010, (EU) č. 293/2012, (EU) 2017/1152 a (EU) 2017/1153.
17. Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Úř. věst. L 281, 23.11.1995, s. 31).
18. Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice).
19. Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích), ve znění pozdějších předpisů.
20. Směrnice Rady 2004/82/ES ze dne 29. dubna 2004 o povinnosti dopravců předávat údaje o cestujících.
21. Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES.
22. Směrnice Evropského parlamentu a Rady 2010/40/EU ze dne 7. července 2010 o rámci pro zavedení inteligentních dopravních systémů v oblasti silniční dopravy a pro rozhraní s jinými druhy dopravy.
23. Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.
24. Směrnice Evropského parlamentu a Rady (EU) 2016/681 ze dne 27. dubna 2016 o používání údajů jmenné evidence cestujících (PNR) pro prevenci, odhalování, vyšetřování a stíhání teroristických trestných činů a závažné trestné činnosti.
25. Směrnice Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. března 2017 o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV.
26. Smlouva o fungování Evropské unie ze dne 13. prosince 2007 – konsolidované znění (Úř. věst. C 202, 7.6.2016, s. 47–360).
27. Řád telegrafní, vyhlášen nařízením obchodního ministeria ze dne 18. dubna 1905, na základě Nejvyššího rozhodnutí ze dne 10. dubna 1905 a uvádějíc ve skutek dekret dvorní kanceláře ze dne 25. ledna 1847, č. 2581, sb. z. pol. č. 9.
28. Ústavní listina Československé republiky, uvozená zákonem 121/1920 Sb.

29. Ústavní zákon č. 1/1993 Sb. Ústava České republiky, ve znění pozdějších změn.
30. Základní zákon státní č. 142/1867 ř.z. o obecných právech občanů státních v královstvích a zemích v radě říšské zastoupených.
31. Zákon č. 60/1923 Sb. o telegrafech.
32. Zákon č. 72/1950 Sb. o telekomunikacích, ve znění pozdějších předpisů.
33. Zákon č. 141/1961 Sb. o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.
34. Zákon č. 110/1964 Sb. o telekomunikacích, ve znění pozdějších předpisů.
35. Zákon č. 20/1966 Sb. o péči o zdraví lidu, ve znění pozdějších předpisů.
36. Zákon č. 71/1967 Sb. o správním řízení (správní řád), ve znění pozdějších předpisů.
37. Zákon č. 178/1990, kterým se mění a doplňuje trestní řád.
38. Zákon č. 283/1991 Sb. o Policii České republiky ve znění k 1.7.2000.
39. Zákon č. 553/1991 Sb. o obecní policii, ve znění pozdějších předpisů.
40. Zákon č. 563/1991 Sb. o účetnictví, ve znění pozdějších předpisů.
41. Zákon č. 67/1992 Sb. o Vojenském obranném zpravodajství ve znění účinném k 1.7.2000.
42. Zákon č. 153/1994 Sb. o zpravodajských službách České republiky, ve znění pozdějších předpisů.
43. Zákon č. 154/1994 Sb. o Bezpečnostní informační službě, ve znění pozdějších předpisů.
44. Zákon č. 13/1997 Sb., o pozemních komunikacích, ve znění pozdějších předpisů.
45. Zákon č. 49/1997 Sb., o civilním letectví, ve znění pozdějších předpisů.
46. Zákon č. 15/1998 Sb. o dohledu v oblasti kapitálového trhu a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů.
47. Zákon č. 56/2001 Sb. o podmínkách provozu vozidel na pozemních komunikacích, ve znění pozdějších předpisů.
48. Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.
49. Zákon č. 150/2021 Sb., kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony.
50. Zákon č. 151/2000 Sb. o telekomunikacích a o změně dalších zákonů, ve znění pozdějších předpisů.
51. Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.
52. Zákon č. 361/2000 Sb. o provozu na pozemních komunikacích a o změnách některých zákonů (zákon o silničním provozu), ve znění pozdějších předpisů.
53. Zákon č. 137/2001 Sb. o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb. občanský soudní řád, ve znění pozdějších předpisů.
54. Zákon č. 265/2001 Sb., kterým se mění zákon č. 141/1961 Sb. o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů, zákon č. 140/1961 Sb. trestní zákon, ve znění pozdějších předpisů, a některé další zákony.
55. Zákon č. 285/2002 Sb. o darování, odběrech a transplantacích tkání a orgánů a o změně některých zákonů (transplantační zákon), ve znění pozdějších předpisů.
56. Zákon č. 499/2004 Sb., o archivnictví a spisové službě, ve znění účinném do dne 30. 6. 2009.

57. Zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.
58. Zákon č. 289/2005 Sb. o Vojenském zpravodajství, ve znění pozdějších předpisů.
59. Zákon č. 57/2006 Sb. o změně zákonů v souvislosti se sjednocením dohledu nad finančním trhem.
60. Zákon č. 69/2006 Sb. o provádění mezinárodních sankcí, ve znění pozdějších předpisů.
61. Zákon č. 225/2006 Sb., kterým se mění zákon č. 49/1997 Sb., o civilním letectví a o změně a doplnění zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů a některé další zákony.
62. Zákon č. 57/2008 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.
63. Zákon č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů.
64. Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.
65. Zákon č. 247/2008 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.
66. Zákon č. 40/2009 Sb. trestní zákoník, ve znění pozdějších předpisů.
67. Zákon č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů.
68. Zákon č. 207/2011 Sb., kterým se mění zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.
69. Zákon č. 341/2011 Sb. o Generální inspekci bezpečnostních sborů a o změně souvisejících zákonů, ve znění pozdějších předpisů.
70. Zákon č. 372/2011 Sb. o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů.
71. Zákon č. 456/2011 Sb., o Finanční správě České republiky, ve znění pozdějších předpisů.
72. Zákon č. 17/2012 Sb. o Celní správě České republiky, ve znění pozdějších předpisů.
73. Zákon č. 273/2012 Sb., kterým se mění zákon č. 127/2005 Sb. o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a některé další zákony.
74. Zákon č. 300/2013 Sb. o Vojenské policii a o změně některých zákonů (zákon o Vojenské policii), ve znění pozdějších předpisů.
75. Zákon č. 110/2019 Sb. o zpracování osobních údajů.
76. Zákon č. 111/2019, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů.
77. Zákon č. 227/2019 Sb. kterým se mění zákon č. 13/1997 Sb., o pozemních komunikacích, ve znění pozdějších předpisů, a další související zákony.
78. Zákon č. 374/2021 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony.
79. Vyhláška Ministerstva vnitra ČR č. 336/2005 Sb. ze dne 29. srpna 2005 o formě a rozsahu informací poskytovaných z databáze účastníků veřejně dostupné telefonní služby a o technických a provozních podmínkách a bodech pro připojení koncového telekomunikačního zařízení pro odposlech a záznam zpráv.

80. Vyhláška č. 485/2005 Sb. o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání, ve znění pozdějších předpisů.
81. Vyhláška č. 357/2012 Sb. o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.
82. Vyhláška Českého telekomunikačního úřadu č. 462/2013 Sb. ze dne 19. prosince 2013 o stanovení výše a způsobu úhrady efektivně vynaložených nákladů na odposlech a záznam zpráv, na uchovávání a poskytování provozních a lokalizačních údajů a na poskytování informací z databáze účastníků veřejně dostupné telefonní služby, ve znění pozdějších předpisů.
83. Vyhláška č. 373/2016 Sb. o předávání údajů do Národního zdravotnického informačního systému, ve znění pozdějších předpisů.
84. Vyhláška č. 267/2017 Sb. o lokalizaci a identifikaci účastníka tísňové komunikace při volání na čísla tísňových volání, ve znění pozdějších předpisů.
85. Mezinárodní pakt o občanských a politických právech. Vyhláška ministra zahraničních věcí č. 120/1976 Sb. o Mezinárodním paktu o občanských a politických právech a Mezinárodním paktu o hospodářských, sociálních a kulturních právech.
86. Úmluva o ochraně lidských práv a základních svobod, společně s Dodatkovým protokolem a Protokoly č. 2, 4, 6 a 7.
87. Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat, vyhlášena jako Sdělení ministerstva zahraničních věcí č. 115/2001 Sb. m. s., ve znění pozdějších dodatkových protokolů.
88. Všeobecná deklarace lidských práv vyhlášená Usnesením č. DE 01/48 Valného shromáždění OSN ze dne 10. prosince 1948.

Zdroje úzce související s právními předpisy

89. Důvodová zpráva k novele Trestního řádu provedené zákonem č. 265/2001 Sb.
90. Důvodová zpráva k návrhu zákona č. 57/2006 Sb. o změně zákonů v souvislosti se sjednocením dohledu nad finančním trhem.
91. Důvodová zpráva k návrhu novely zákona o elektronických komunikacích. Sněmovní tisk 1084. Poslanecká sněmovna, 8. období, 2017–2021.
92. Usnesení Ústavně právního výboru Poslanecké sněmovny Parlamentu ČR ze 74. schůze 14. a 15. března 2001. Pozměňovací návrh k novele Trestního řádu (sněmovní tisk 785/1).
93. Usnesení Hospodářského výboru Poslanecké sněmovny Parlamentu ČR č. 383 ze dne 18. ledna 2006 (sněmovní tisk 1069/1).

Spolková republika Německo.

94. Hessisches Datenschutzgesetz vom 7. Oktober 1970 GVBl. I S. 625.
95. Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Daten bei der Datenverarbeitung vom 27 Januar 1977.
96. Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten (VerkDSpG k.a.Abk.) vom 10.Dezember 2015.
97. Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBI. I S.1190).

Slovenská republika

98. Zákon č. 301/2005 Z.z. Trestný poriadok v znení neskorších predpisov.
99. Zákon č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov.
100. Zákon č. 397/2015 Z.z., ktorým sa na účely Trestného zákona ustanovuje zoznam látok s anabolickým alebo iným hormonálnym účinkom a ktorým sa menia a dopĺňajú niektoré zákony.
101. Zákon č. 452/2021 Z. z. o elektronických komunikáciách, v znení neskorších predpisov.

7.4 Seznam použité judikatury

Krajské soudy

1. Rozsudek Krajského soudu v Ústí nad Labem ze dne 1. 6. 2020, sp. zn. 15 Af 2/2017–30.

Nejvyšší soud ČR

2. Rozsudek Nejvyššího soudu ČR sp. zn. 4 Tdo 630/2005 ze dne 8. června 2005.
3. Rozsudek Nejvyššího soudu ČR sp. zn. 4 Tdo 1346/2014 ze 29. října 2014.

Nejvyšší správní soud ČR

4. Rozsudek Nejvyššího správního soudu ČR sp. zn. 1 As 387/2019-56 ze 13. srpna 2020.
5. Rozsudek Nejvyššího správního soudu sp. zn. 9 Afs 147/2020–34 ze dne 21. července 2022.
6. Rozsudek Nejvyššího správního soudu ČR ze dne 14. prosince 2023 sp. zn. 9 Afs 147/2020–87.

Ústavní soud ČR

7. Nález Ústavního soudu ČR sp. zn. Pl.ÚS 4/94 ze dne 12. října 1994.
8. Nález Ústavního soudu ČR sp. zn. Pl. ÚS 15/96 ze dne 9. října 1996.
9. Nález Ústavního soudu ČR sp. zn. II.ÚS 485/98 ze dne 30. listopadu 1999.
10. Nález Ústavního soudu ČR sp. zn. I.ÚS 22/99 ze dne 2. února 2000.
11. Nález Ústavního soudu ČR sp. zn. II. ÚS 517/99 ze dne 1. března 2000.
12. Nález Ústavního soudu ČR sp. zn. I. ÚS 653/99 ze dne 29. srpna 2000.
13. Nález Ústavního soudu ČR sp. zn. II. ÚS 502/2000 ze dne 22. ledna 2001.
14. Nález Ústavního soudu ČR sp. zn. IV. ÚS 536/2000 ze dne 13. února 2001.
15. Nález Ústavního soudu ČR sp. zn. IV. ÚS 78/01 ze dne 27. srpna 2001.
16. Nález Ústavního soudu ČR sp. zn. Pl. ÚS 15/01 ze dne 31. října 2001.
17. Nález Ústavního soudu ČR sp. zn. III ÚS 256/01 ze 21. března 2002.
18. Nález Ústavního soudu ČR sp. zn. I. ÚS 512/02 ze 20. listopadu 2002.
19. Nález Ústavního soudu ČR sp. zn. Pl. ÚS 41/02 ze dne 28.ledna 2004.
20. Nález Ústavního soudu ČR sp. zn. I.ÚS 453/03 ze dne 11. listopadu 2005.

21. Nález Ústavního soudu ČR sp. zn. IV. ÚS 412/04 ze dne 7. prosince 2005.
22. Nález Ústavního soudu ČR sp. zn. I. ÚS 191/05 ze dne 18. září 2006.
23. Nález Ústavního soudu sp. zn. ČR I. ÚS 321/06 ze dne 18. prosince 2006.
24. Usnesení Ústavního soudu ČR sp. zn. IV.ÚS 335/07 ze dne 19. března 2007.
25. Nález Ústavního soudu ČR sp. zn. II. ÚS 615/06 ze dne 23. května 2007.
26. Nález Ústavního soudu ČR sp. zn. IV. ÚS 23/05 ze dne 17. července 2007.
27. Nález Ústavního soudu ČR sp. zn. II. ÚS 789/06 ze dne 27. září 2007.
28. Nález Ústavního soudu ČR sp. zn. II.ÚS 2268/07 ze dne 29. února 2008.
29. Nález Ústavního soudu ČR sp. zn. I.ÚS 3038/07 ze dne 29. února 2008.
30. Nález Ústavního soudu ČR sp. zn. Pl. ÚS 13/06 ze dne 8. července 2008.
31. Nález Ústavního soudu ČR sp. zn. I. ÚS 705/06 ze dne 1. prosince 2008.
32. Nález Ústavního soudu ČR sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011.
33. Nález Ústavního soudu ČR sp. zn. Pl. ÚS 24/11 ze dne 20. prosince 2011.
34. Nález Ústavního soudu ČR sp. zn. Pl. ÚS 1/12 ze dne 27. listopadu 2012.
35. Nález Ústavního soudu ČR Pl. ÚS 3/14 ze dne 20. prosince 2016.
36. Nález Ústavního soudu ČR sp. zn. Pl. ÚS 15/16 ze dne 16. května 2018.
37. Nález Ústavního soudu ČR sp. zn. Pl. ÚS 45/17 ze dne 14. května 2019.
38. Usnesení Ústavního soudu ČR sp. zn. III.ÚS 2478/19 ze dne 3. září 2019.
39. Nález Ústavního soudu ČR Pl. ÚS 10/17 ze dne 3. listopadu 2020.
40. Nález Ústavního soudu ČR ze dne 18. listopadu 2020 sp. zn. Pl. ÚS 33/16.
41. Usnesení Ústavního soudu ČR sp. zn. Pl. ÚS 2/12 ze dne 24. ledna 2021.
42. Usnesení Ústavního soudu ČR sp. zn. Pl. ÚS 7/12 ze dne 6. března 2021.
43. Usnesení Ústavního soudu ČR sp. zn. I.ÚS 2369/21 ze dne 12. října 2021.
44. Nález Ústavního soudu ČR sp. zn. Pl. ÚS 25/21 ze dne 17. ledna 2023.
45. Nález Ústavního soudu ČR sp. zn. IV.ÚS 2621/22 ze dne 14. února 2023.
46. Usnesení Ústavního soudu ČR sp. zn. Pl. ÚS 16/94 ze dne 21. července 1994.
47. Usnesení Ústavního soudu ČR sp. zn. II.ÚS 1276/16 ze dne 25. října 2016.
48. Zpráva Ústavního soudu k nálezu Pl. ÚS 45/17. Ústavní soud ČR. TZ 60/2019. 22. května 2019.

Soudní dvůr EU

49. Rozsudek Soudního dvora EU (velkého senátu) C-301/06 Ireland v European Parliament and Council z 10. února 2009.
50. Rozsudek Soudního dvora EU (velkého senátu) ze dne 9. listopadu 2010. Volker und Markus Schecke GbR (C-92/09) a Hartumt Eifert (C-93/09) proti Land Hessen. Žádosti o rozhodnutí o předběžné otázce: Verwaltungsgericht Wiesbaden – Německo. Spojené věci C 92/09 a C 93/09.
51. Rozsudek Soudního dvora EU (třetího senátu) ze 17. února 2011. The Number (UK) Ltd, Conduit Enterprises Ltd proti Office of Communications, British Telecommunications plc. Věc C-16/10.
52. Rozsudek Soudního dvora EU (třetího senátu) ze 22. listopadu 2012 Josef Probst v. mr.nexnet GmbH. Žádost o rozhodnutí o předběžné otázce podaná Bundesgerichtshof. Věc C-119/12.
53. Rozsudek Soudního dvora EU (velkého senátu) z 8. dubna 2014. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další a Kärntner

Landesregierung a další. Žádosti o rozhodnutí o předběžné otázce podané High Court (Irsko) a Verfassungsgerichtshof (Rakousko). Spojené věci C-293/12 a C-594/12.
54. Rozsudek Soudního dvora EU (velkého senátu) ze 21. prosince 2016. Tele2 Sverige AB v. Post – och telestyrelsen (C-203/15) a Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis, za přítomnosti Open Rights Group, Privacy International, The Law Society of England and Wales (C-698/15). Žádosti o rozhodnutí o předběžné otázce podané rozhodnutím Kammarrätten i Stockholm (správní odvolací soud ve Stockholmu, Švédsko) a rozhodnutím Court of Appeal (England & Wales) (Civil Division) [odvolací soud pro Anglii a Wales, občanskoprávní oddělení, Spojené království]. Spojené věci C-203/15 a C-698/15.
55. Rozsudek Soudního dvora EU (velkého senátu) ze 6. října 2020. Privacy International v. Secretary of State for Foreign and Commonwealth Affairs, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service. Žádost o rozhodnutí o předběžné otázce podaná rozhodnutím Investigatory Powers Tribunal (tribunál pro kontrolu vyšetřovacích pravomocí, Spojené království). Věc C-623/17.
56. Rozsudek Soudního dvora EU (velkého senátu) ze 6. října 2020 ve spojených věcech C-511/18 La Quadrature du Net a další, C-512/18 French Data Network a další a C-520/18 Ordre des barreaux francophones et germanophone a další.
57. Rozsudek Soudního dvora EU (velkého senátu) ze 2. března 2021 ve věci C-746/18.
58. Rozsudek Soudního dvora EU (velkého senátu) z 5. dubna 2022 ve věci C-140/20.
59. Rozsudek Soudního dvora EU (velkého senátu) ze 21. června 2022 ve věci C-817/19.
60. Rozsudek Soudního dvora EU (velkého senátu) ze 20. září 2022. Bundesrepublik Deutschland, zastoupená Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen v. SpaceNet AG a Telekom Deutschland GmbH. Žádosti o rozhodnutí o předběžné otázce podané rozhodnutími Bundesverwaltungsgericht (Spolkový správní soud, Německo). Spojené věci C 793/19 a C 794/19.
61. Rozsudek Soudního dvora EU (třetího senátu) z 9. listopadu 2023 ve věci C-319/22 v řízení Gesamtverband Autoteile-Handel eV proti SCANIA CV AB.
62. Posudek 1/15 Soudního dvora (Velkého senátu) ze dne 26. července 2017.
63. Řízení pro nesplnění povinnosti podle čl. 258 a násl. Smlouvy o fungování Evropské unie. Evropská komise v. Švédské království, věc C-185/09 a C-270/11, Evropská komise v. Rakouská republika, věc C-189/09 a Evropská komise v. Německo, věc C-329/12.
64. Stanovisko Generálního advokáta Soudního dvora EU, Pedro Cruz Villalóna přednesené 12. prosince 2013 ve věci C-293/12.
65. Stanovisko Generálního advokáta Soudního dvora EU, Henrika Saugmandsgaard Oe, ze dne 19. července 2016 ve spojených věcech C-203/15 a C-698/15.
66. Žádosti Amtsgericht Köln k Soudnímu dvoru EU ve věcech AC, DF a BD v. Deutsche Lufthansa AG, věci C-148/20, C-149/20 a C-150/20 ze 16., resp. 17. března 2020.

Evropský soud pro lidská práva

67. Rozsudek ESLP ve věci Klass a další proti Německu č. 5029/71 ze dne 6. září 1978.
68. Rozsudek ESLP ve věci Malone v. The United Kingdom č. 8691/79 ze dne 2. srpna 1984. Judgment of the European Court of Human Rights, dated 2 August 1984. Case of Malone v. The United Kingdom (Application no. 8691/79).

69. Rozsudek ESLP ve věci Leander v. Švédsko č. 9248/81 ze dne 26. března 1987.
70. Rozsudek ESLP ve věci Kruslin v. Francie č. 11801/85 ze dne 24. dubna 1990.
71. Rozsudek ESLP ve věci Niemietz proti Německu (no. 13710/88) ze dne 16. prosince 1992.
72. Rozsudek ESLP ve věci Z. proti Finsku, č. 22009/93, rozsudek ze dne 25. února 1997.
73. Rozsudek ESLP ve věci Camenzind proti Švýcarsku (no. 21353/93) ze dne 16. prosince 1997.
74. Rozsudek ESLP ve věci Kopp v. Švýcarsko č. 23224/94 ze dne 25. března 1998.
75. Rozsudek ESLP ve věci Valenzuela Contreras v. Španělsko č. 58/1997/842/1048 ze dne 30. července 1998.
76. Rozsudek ESLP ve věci Amann proti Švýcarsku (no. 27798/95) ze dne 16. února 2000.
77. Rozsudek ESLP ve věci Rotaru proti Rumunsku č. 28341/95 ze dne 4. května 2000.
78. Rozsudek ESLP ve věci P. G. a J. H. proti UK (no. 44787/98) ze dne 25. září 2001.
79. Rozsudek ESLP ve věci Peck proti Velké Británii, č. 44647/98, rozsudek ze dne 28. ledna 2003.
80. Judgment of the European Court of Human Rights, dated 29 June 2006. Case of Gabriele Weber and Cesar Richard Saravia against Germany (Application no. 54934/00).
81. Judgment of the European Court of Human Rights, dated 1 July 2008. Case of Liberty and others v. The United Kingdom (Application no. 58243/00).
82. Rozsudek ESLP ve věci S. a Marper proti UK (no. 30562/04 a 30566/04) ze dne 4. prosince 2008.
83. Rozsudek ESLP ve věci Gillan a Quinton proti Spojenému království, rozsudek č. 4158/05 ze dne 12. ledna 2010.
84. Judgment of the European Court of Human Rights, dated 4 December 2015. Case of Roman Zakharov v. Russia (Application no. 47143/06).
85. Rozsudek ESLP ve věcech č. 58170/13, 62322/14 a 24960/15 – Big Brother Watch a ostatní proti Spojenému království ze dne 13. září 2018.

Slovenská republika

86. Uznesenie Ústavného súdu Slovenskej republiky sp.zn. PL. ÚS 10/2014 z 23. apríla 2014.
87. Nález Ústavného súdu Slovenskej republiky sp.zn. PL. ÚS 10/2014 ze 29. apríla 2015.

Německo

88. Rozhodnutí Spolkového ústavního soudu Německa ze dne 15. 12. 1983, BVerfGE 65, 1 (Volkszählungsurteil).
89. Bundesverfassungsgericht - BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83, Rn. 1-215.
90. Bundesverfassungsgericht. Urteil vom 2. März 2010. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.
91. Rozhodnutí Spolkového ústavního soudu Německa. Bundesverfassungsgericht 1 BvR 668/04. Urteil vom 27. Juli 2005 (Vorbeugende Telekommunikationsüberwachung) a Bundesverfassungsgericht. 1 BvR 370/07, 1 BvR 595/07. Urteil vom 27. Februar 2008 (Grundrecht auf Computerschutz).

92. Bundesverfassungsgericht - BVerfG, Urteil des Ersten Senats vom 4. April 2006 - 1 BvR 518/02.
93. Rozhodnutí Spolkového ústavního soudu Německa. Bundesverfassungsgericht 1 BvR 256/08, 1 BvR 263/08 a 1 BvR 586/08. Urteil des Ersten Senats vom 2. März 2010.
94. Nálezy prvního senátu Spolkového ústavního soudu Německa sp. zn. BvR 142/15, 1 BvR 2795/09 a 1 BvR 3187/10 z 18. prosince 2018.
95. Rozsudek Správního soudu v Hannoveru sp. zn. 7 A 849/19ze dne 12. března 2019.
96. Rozsudek 12. senátu Vrchního správního soudu Dolního Saska sp. zn. 12 LC 79/19 ze dne 13. listopadu 2019.
97. Rozhodnutí Spolkového ústavního soudu Německa. 1 BvR 2356/20 z 11. ledna 2021.
98. Tisková zpráva Vrchního správního soudu Dolního Saska. *Verkehrsüberwachung mittels „Abschnittskontrolle“ (= Section Control) auf der B 6 ist rechtmäßig*. 14. listopadu 2019.

Další členské státy EU

99. Rozhodnutí Ústavního soudu Belgie č. 84/2015 z 11. června 2015.
100. Rozhodnutí Nevyššího správního soudu Bulharska ze dne 17. prosince 2008.
101. Rozhodnutí Ústavního soudu Bulharska č. 8/2014 ze 12. března 2015.
102. Rozhodnutí oblastního soudu v Haagu č.C/09/ 009/KG ZA 14/1575 ze dne 11.března 2015.
103. Rozhodnutí Nejvyššího soudu Kypru z února 2011.
104. Rozhodnutí Ústavního soudu Polska (Trybunal Konstytucyjny) ze 30. července 2014 sp. zn. K 23/11. Wyrok Trybunalu Konstytucyjnego Sygn. akt K 23/11 z dnia 30 lipca 2014 r.
105. Rozhodnutí Ústavního soudu Rakouska. Verfassungsgerichtshof. Urteil vom 27. Juni 2014. G-47/2012-49. [online]. 2014.
106. Rozhodnutí Ústavního soudu Rumunska č. 1258/2009 ze dne 8. října 2009 v kauze Dragotoniu a Militaru-Pidhorni v. Romania, 2007, publikováno v Monitorul Oficial al Romaniei (v anglickém překladu Official Gazette of Romania) no. 798 ze dne 23, října 2009.
107. Rozhodnutí Ústavního soudu Republiky Slovinsko č. U-I-65/13-19 ze 3.7.2014. Viz Slovenia / Constitutional Court / U-I-65/13-19. 3.7.2014.

Spojené státy americké

108. Rozhodnutí Nejvyššího soudu Spojených států amerických. Olmstead et al. v. United States. Green et al. v. United States McInnis v. United States sp. zn. 277 U.S. 438 48 S. Ct. 564; 67 L. Ed. 785; 1923 U.S. LEXIS 2588; 24 A.L.R. 1238 ze 20. a 21. února 1928.

7.5 Seznam ostatních zdrojů

1. Norma ČSN EN 15722 Inteligentní dopravní systémy – eSafety – Minimální soubor dat pro eCall, ve verzích: Katalogové číslo 89913 (Účinnost od 1.12.2011), Katalogové číslo 97956 (Účinnost od 1.9.2015), Katalogové číslo 511667 (Účinnost od 1.1.2021).
2. Rozhodnutí Rady č. 2006/230/ES ze dne 18. července 2005 o uzavření Dohody mezi Evropským společenstvím a vládou Kanady o zpracovávání údajů API/PNR. Dostupné z www.data.consilium.europa.eu.

3. Návrh Dohody mezi Kanadou a Evropskou unií o předávání a zpracovávání údajů jmenné evidence cestujících ze 25. června 2014. Dostupné z www.data.consilium.europa.eu.
4. Dohoda mezi Evropskou unií a Austrálií o zpracovávání údajů jmenné evidence cestujících (PNR) ze zdrojů Evropské unie leteckými dopravci a o jejich předávání Australské celní správě, uzavřená dne 30. 6. 2008. Dostupné z www.data.consilium.europa.eu.
5. Dohoda mezi Evropskou unií a Austrálií o zpracovávání údajů jmenné evidence cestujících (PNR) leteckými dopravci a o jejich předávání australské správě pro cla a ochranu hranic, datovaná dne 29. září 2011. Dostupné z www.data.consilium.europa.eu.
6. Dohoda mezi Spojenými státy americkými a Evropskou unií o využívání jmenné evidence cestujících a o jejím předávání Ministerstvu vnitřní bezpečnosti Spojených států uzavřená v r. 2015. Dostupné z www.data.consilium.europa.eu.
7. Dohoda mezi Spojeným královstvím a Evropskou unií o využívání jmenné evidence cestujících uzavřená r. 2020. Dostupné z www.data.consilium.europa.eu.

8 Abstrakt, klíčová slova

8.1 Abstrakt

Zásahy do práva na ochranu soukromí ze strany orgánů veřejné moci

Předmětem této práce je posouzení vybraných typových zásahů do práva na ochranu soukromí z hlediska splnění požadavků ústavnosti. Autor se zaměřil na případy plošného shromažďování osobních údajů značného množství osob a jejich dalšího zpracování pro účely orgánů veřejné moci. Posuzovaná zpracování jsou založena na konkrétních právních úpravách, zpravidla jako zpracování povinná, bez možnosti dotčených osob zpracování svých osobních údajů se vyhnout, jelikož jednotlivé relevantní právní úpravy upravují zpracování osobních údajů vždy za účelem naplnění určitého veřejného zájmu.

Na základě předběžné analýzy autor pro další zkoumání v této práci vyhodnotil případy, které se jeví jako nejzávažnější z hlediska míry zásahu do práva na ochranu soukromí, zejména s ohledem na množství dotčených osob a na celkové množství zpracovávaných osobních údajů. Konkrétně jde o: 1. plošné zpracování provozních a lokalizačních údajů elektronických komunikací, 2. plošné zpracování osobních údajů systémy v automobilech, 3. plošné zpracování osobních údajů leteckých cestujících, 4. plošné zpracování osobních údajů systémy dopravních kamer a 5. zpracování údajů o zdravotním stavu.

V těchto vybraných případech autor vždy identifikoval právní úpravu zakládající předmětné zpracování a posoudil vymezení jednotlivých prvků zpracování v právní úpravě. Součástí této části práce je také analýza relevantních stanovisek a rozhodnutí orgánů dozoru nad ochranou osobních údajů a soudů a na jejich základě následně u každé ze zkoumaných úprav posouzení splnění ústavněprávních požadavků a vyhodnocení případných nedostatků.

Výsledkem této práce je zobecnění závěrů, ke kterým autor dospěl při posuzování jednotlivých zkoumaných případů, a návrh opatření de lege ferenda uplatnitelných jak u existujících, tak rovněž u možných budoucích obdobných případů zásahů do práva na ochranu soukromí. Tato opatření zahrnují i návrhy dostatečných a efektivních kontrolních mechanismů, které v souladu s ustálenou rozhodovací praxí Ústavního soudu ČR patří u právních úprav zakládajících zásah do některých ze základních lidských práv a svobod mezi základní předpoklady zajištění ústavnosti dané právní úpravy.

8.2 Klíčová slova

právo na ochranu soukromí, právo na informační sebeurčení, osobní údaj, lokalizační údaj, DPIA analýza

8.3 Abstract

Interference with the Right to Privacy by Public Authorities

The subject of this thesis is the assessment of selected types of interference with the right to privacy in terms of meeting the requirements of constitutionality. The author focused on cases of flat collection of personal data of a significant number of persons and their further processing for the purposes of public authorities. The considered processing are based on specific legal regulations, usually as mandatory processing, without the possibility for the persons concerned to avoid the processing of their personal data, since the individual relevant legal regulations always regulate the processing of personal data for the purpose of fulfilling a certain public interest.

On the basis of a preliminary analysis, the author has evaluated the cases that appear to be the most serious in terms of the degree of interference with the right to privacy, in particular with regard to the number of persons concerned and the total amount of personal data processed, for further examination in this thesis. Specifically, these are: 1. the blanket processing of electronic communications traffic and location data, 2. the blanket processing of personal data by in-car systems, 3. the blanket processing of personal data of air passengers, 4. the blanket processing of personal data by traffic camera systems and 5. the processing of health data.

In these selected cases, the author has always identified the legislation establishing the processing in question and assessed the definition of the individual elements of processing in the legislation. This part of the thesis also includes an analysis of relevant opinions and decisions of the data protection supervisory authorities and courts and, on the basis of these, an assessment of compliance with constitutional requirements and an evaluation of possible shortcomings for each of the examined regulations.

The outcome of this thesis is a generalisation of the conclusions reached by the author when assessing the individual cases examined and a proposal of de lege ferenda measures applicable to both existing and possible future similar cases of interference with the right to privacy. These measures also include proposals for sufficient and effective control mechanisms, which, in accordance with the established decision-making practice of the Constitutional Court of the Czech Republic, are among the basic prerequisites for ensuring the constitutionality of a given legal regulation when it constitutes an interference with some of the fundamental human rights and freedoms.

8.4 Keywords

right to privacy, right to informational self-determination, personal data, location data, Data Protection Impact Assessment