POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra veřejnoprávních disciplín

Aktuální otázky Data Retention

Bakalářská práce

Current issues of Data Retention

Bachelor thesis

VEDOUCÍ PRÁCE
Mgr.et Mgr. Bohumil Peterka

AUTOR PRÁCE
Erich Mika

PRAHA

2022

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Teplicích, dne 13. 8. 2021

……..

Erich Mika

ANOTACE

Tato bakalářská práce se zabývá problematikou aktuálních otázek Data Retention (volně přeloženo jako provozní a lokalizační údaje) v České republice a použitím těchto údajů pro potřeby Policie ČR. Je zde obsažena minulost Data Retention a současná situace, a to v Evropské Unii a České republice. V úvodní části bakalářské práce je více rozvedena definice Data Retention, důvody vzniku a také listovní tajemství, jako předchůdce provozních a lokalizačních údajů. Ve druhé části se pak zaměřuji na právní předpisy, týkající se uchovávání provozních a lokalizačních údajů a také subjekty, které mohou o tyto údaje žádat. Třetí část je pak samotná zavedení praxe při zajišťování těchto údajů. V další části této práce se pak zaměřuji na dosud nejaktuálnější téma v oblasti data retention a tím je COVID-19.

KLÍČOVÁ SLOVA

Data retention * provozní a lokalizační údaje * listovní tajemství * právo na soukromí * COVID-19

ANNOTATION

This bachelor's thesis deals with the current issues of Data Retention in the Czech Republic and the use of this data for the needs of the Police of the Czech Republic. Both the past of Data Retention and the current situation in the European Union and the Czech Republic are included here. In the introductory part of the bachelor's thesis, the definition of Data Retention, the reasons for its origin, and also privacy of correspondence, as a precursor to data retention, are more elaborated. In the second part, there is a focus on legal regulations regarding the handling of data retention, as well as legal entities that can request this data. The third part is the very introduction of practice in securing this data. In the next part of this work, I focus on the most current topic of data retention, and that is COVID-19.

KEYWORDS

Data retention * privacy of correspondece * privacy rights * COVID-19

Poděkování

Rád bych touto cestou poděkoval Mgr. et Mgr. Bohumilu PETERKOVI, za odborné vedení práce a podnětné rady, které mi byly velkým přínosem.

Dále bych rád poděkoval své rodině za jejich podporu během celé doby mého bakalářského studia.

OBSAH

ÚVOD

Data retention, do češtiny volně přeloženo „ukládání provozních a lokalizačních údajů“ bylo předmětem diskuzí nejen v minulosti, ale na síle nabírá i v současné době a to nejen ve světě, ale i v České Republice. V posledních dvou letech je toto téma probírané v mnohem větší míře, než kdykoliv předtím a to hlavně kvůli vypuknutí celosvětové pandemie COVID-19. Vzhledem k rychlému šíření nemoci COVID-19 a obav z následků, které by tato nemoc mohla způsobit, přistoupila Vláda ČR k vyhlášení nouzového stavu. Ten byl vyhlášen v souladu s čl. 5 a čl. 6 ústavního zákona č. 110/1998 Sb., o bezpečnosti ČR.

V této souvislosti byly následně zveřejněny informace o tom, že velké procento osob nedodržuje nařízenou karanténu, ačkoliv zákon tuto povinnost ukládá. Tyto informace byly získány mimo jiné z údajů o platbách bankovními kartami.

V tomto ohledu se můžeme bavit jak o lidské nezodpovědnosti, tak současně o tom, jaké prostředky je stát oprávněn použít k předcházení a následnému postižení takových jednání, neboť vedle omezení svobody pohybu, pobytu a shromažďování, majících za úkol zpomalení šíření viru, je také nutné přistoupit k efektivní kontrole dodržovaní těchto omezení fyzickými osobami, jakož i ke sledování potenciálního šíření nemoci z důvodu jejich nerespektování.

V první kapitole této práce se zaměřuji na problematiku Data retention ze zákonodárného hlediska a také na to, na jaké osoby se pravidla uchovávání lokalizačních a provozních údajů vztahuje. Také v této kapitole nastiňuji historii Data retention a to jak v Evropské unii tak v České republice.

Další otázkou je pak technická stránka Data retention. Příkladem může být pak počet uskutečněných hovorů, odeslaných SMS nebo datový provoz. Za všechny příklady pak mluví data ze Štědrého dne. V roce 2021 bylo na Štědrý den spojeno 11 870 917 hovorů, což představuje nárust o 11 % oproti předchozímu roku, bylo odesláno 7 391 511 SMS, což představuje pokles o 21 % oproti předchozímu roku a bylo spotřebováno 1 035 TB dat, což představuje nárůst o 34 %. V tomto smyslu pak mluvíme o obrovské objemy dat, které musí být uchovávány.

V další části bakalářské práce se pak zaměřuji na praxi při vyžadování uchovávaných dat, se zaměřením zejména na praxi u Policie ČR. V této souvislosti přináším statistiky, jak byly údaje v uplynulých letech využívány.

V této souvislosti narážíme na fakt, že ne vždy uchovávané informace obsahují jen metadata[1] proběhlé komunikace, v některých případech je možní zjistit i její obsah. Ochránci lidských práv pak poukazují na porušování lidských práv, zanesených v Listině základních práv a svobod. Policii však tato data mohou napomoci při odhalování trestných činů nebo při pátrání po nezvěstných osobách.

Dále se v této části zaměřím na to, jaká je praxe při vyžadování lokalizačních údajů, jak policista získává provozní a lokalizační údaje nebo také na to, jak často policie o tato data žádá.

[1] Metadata (z řeckého meta = mezi a latinského data = to, co je dáno) jsou data, která poskytují informace o jiných datech

1 DATA RETENTION

V dnešní době to vypadá, že se veškerý svět přesouvá prostřednictvím internetu do digitální podoby. Toto prostřední je bezpochyby vhodné k uchovávání a shromažďování osobních informací. Toto uchovávání je pak na denním pořádku, přičemž objem dat, takto uchovaných je obrovský. To, jak je následně s těmito daty nakládáno je pak v režii správců informačních systémů. Tento sběr dat pak musí podléhat zákonu o ochraně osobních údajů. V dnešní době člověk podepisuje souhlas s nakládáním s osobními údaji skoro každé firmě, u které má nějaký produkt, například poskytovatelům elektřiny. Souhlas je také vyžadován u většiny internetových stránek, které člověk navštíví. Poskytovatelé internetových služeb uchovávají například webovou historii, oblíbená nebo shlédnutá videa na určitých platformách, aktuální polohu uživatele nebo často vyhledávaná slovní spojení. Na oplátku pak uživateli poskytují komfort v podobě doporučení zajímavých webů, doporučují další videa ke shlédnutí, články na internetu, o kterých si poskytovatel služeb myslí, že by mohly být pro uživatele zajímavé. Toto vše na základě uchovaných dat, s jejímž uchováním musí uživatel souhlasit.

Tento proces nese název data mining[2] a je hojně využíván například na sociálních sítích jako je Facebook, Twitter nebo Instagram. Výhodou tohoto procesu je pak komfortnější práce na internetu nebo na samotné sociální síti, kdy je uživateli navrhován obsah, který mu je blízký. Někdo pak může namítat to, že nevýhodou je cílená reklama na uživatele. Tato reklama je zobrazována na základě nashromážděných dat. Konspirační teoretik pak může namítnout, že data by mohla být získána i na základě odposlechu z mikrofonu na zařízení, na kterém se reklama zobrazuje.

Na internetu jsou sdílena videa či články o tom, jak uživatel, který chce vyzkoušet tuto teorii začne v blízkosti svého mobilního telefonu, který je připojený k internetu mluvit o nějakém produktu, který před tím nikdy na svém zařízení nevyhledával, nebo o něm dokonce nikdy nemluvil. Často je jako cíl konverzace mezi uživatelem

[2] Data mining, (angl. Dolování z data či vytěžování dat) je analytická metodologie získávání netriviálních skrytých a potenciálně užitečných informací z dat.

a telefonem vybrán objekt, který uživatel nezná, nebo nepotřebuje. Jako příklad můžeme uvést krmení pro psy pro uživatele, který doma psa nemá, a proto krmení nepotřebuje. Následně uživatel navštíví internetové stránky, nebo sociální síť, na které jsou zobrazovány reklamy a reklamy následně nabízí uživateli krmení pro psy různých společností. Tento pokus je možno samozřejmě provést v domácích podmínkách. Cílená reklama tak nemusí být každému sympatická, lidé pak nabývají dojmu, že dochází porušení hranic soukromí. Proto se v tomto případě mluví o Data retention pro naše pohodlí, ovšem za cenu zásahu do soukromí.

Samotné Data retention pak funguje na bázi preventivního a celoplošného sběru dat každého, kdo je připojen k internetu na jakémkoliv zařízení, ať už se jedná o mobilní telefon, počítač nebo tablet, kdo používá mobilní telefon nebo pevnou linku. Data následně archivuje poskytovatel služeb elektronických komunikací, a to dle stanovených předpisů po dobu 6-24 měsíců podle toho, jakou si daný stát Evropské unie zvolil hranici. Pokud dojde k trestnému činu, je možnost takto data vyžádat tak, aby pomohla při objasnění skutečnostní důležitých pro trestní řízení. Provozní a lokalizační údaje je pak možné využít také mimo trestní řízení, a to v případě zahájení pátrání po konkrétní hledané nebo pohřešované osobě, za účelem zjištění totožnosti osoby neznáme totožnosti nebo totožnosti nalezené mrtvoly.

1.1 Co je Data retention

Data retention je anglický výraz. Najít pro toto slovní spojení konkrétní český výraz není jednoduché. Ze zákona je tento výraz definován jako *„povinnost osob zajišťujících veřejnou komunikační síť nebo poskytujících veřejně dostupnou službu elektronických komunikací uchovávat provozní a lokalizační údaje, které jsou vytvářeny, nebo zpracovávány při zajišťování jejich veřejných komunikačních sítí a při poskytování jejich veřejně dostupných služeb elektronických komunikací“*[3].

[3] zákon č. 127/2005 Sb., Zákon o elektronických komunikacích a o změně některých souvisejících zákonů.

Tuto definici jsem následně zkrátil na pojem „uchovávání provozních a lokalizačních údajů“. Toto slovní spojení následně používám dále v textu této práce.

Data retention plní v první řadě preventivní roli. To, jestli budou data někdy použita není nikdy dopředu známo. Co se týče technických a organizačních opatření, jsou údaje uchovávány ve speciálním režimu tak, aby k nim měly přístup pouze zvláště zmocněné osoby. Každý stát si tyto orgány určuje sám. Také financování si každý stát určuje dle svého zvážení.

Evropská unie vyžaduje uchovávání těchto dat po všech členských státech, přičemž při nedodržení směrnic pak může vést až k sankcím, uděleným Evropskou unií pro konkrétní stát. Tato povinnost pak vychází ze Směrnice Evropského parlamentu a Rady 2006/24/ES[4]. Uchovávána jsou pak veškerá data, jak mobilní, tak internetová, která využívá každý člověk, který komunikuje prostřednictvím operátorů a poskytovatelů služeb, působících na území Evropské unie.

V České republice jsou pak „provozní údaje“ a „lokalizační údaje“ uvedeny v zákoně č. 127/2005 Sb. v ust. §90 a ust. §91 odst. 1) takto:

„Provozními údaji se rozumí jakékoliv údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování.“

„Lokalizačními údaji se rozumí jakékoliv údaje zpracovávané v síti elektronicích komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací.“

Historickým předchůdcem provozních a lokalizačních údajů je pak listovní tajemství.

[4] Směrnice Evropského parlamentu a Rady 2006/24/ES o uchování údajů vytvořených nebo zpracovaných při poskytování veřejně dostupných služeb v odvětví elektronických komunikací nebo veřejných komunikačních sítí, kterou se mění směrnice 2002/58/ES

1.2 Listovní tajemství

Listovní tajemství je jedno ze základních lidských práv a svobod přiznaných v České republice Listinou základních práv a svobod a to článkem 13. Ekvivalentem tohoto práva na půdě Evropské Unie je pak článek 8 Evropské úmluvy o lidských právech. Dle ust. §182 z.č. 40/2009 Sb. pak nesmí být porušeno listovní tajemství, které se vztahuje i na datové, textové, hlasové, zvukové či obrazové zprávy, posílané prostřednictvím sítě elektronických komunikací.

Snahy o ochranu obsahu přenášených zpráv před neoprávněnými osobami v různých podobách, lze zaznamenat dávno předtím, než se začala postupně uplatňovat ochrana listovního tajemství používané v právních řádech různých zemí.

Jako takové bylo zaručeno již v době Rakouska-Uherska, a to v roce 1867. To zajišťovala v té době rakousko-uherská ústava, která stanovila, že *„Listovní tajemství nesmí být porušeno, zbavení dopisu smí nastat v případě zákonného zatčení, či domovní prohlídky.“*[5] V době První republiky pak listovní tajemství zajišťoval Ústavní zákon 293/1920 Sb. Následně i poválečné ústavy např. z roku 1948 nebo pak socialistická ústava, ústavní zákon č. 100/1960 Sb. Toto právo bylo za socialismu porušováno kontrolou vybrané korespondence. Dle pramenů poštovního muzea bylo před podpisem Charty 77[6] prověřeno sedm set tisíc zásilek a pod podpisu Charty 77 dokonce až sedm desítek milionů zásilek. Tyto byly kontrolovány agenty StB.

1.2.1 Subjekt ochrany listovního tajemství

Dle čl. 13 Listiny základních práv a svobod a čl. 8 Evropské úmluvy o lidských právech se za subjekt chráněný těmito články považuje kdokoliv. Ani jeden z výše uvedených článků neobsahuje speciální subjekt. Ochrana je poskytnuta každému. Nezáleží na státní příslušnosti nebo zvláštní funkci. Tato ochrana je současně

[5] zákon č. 142/1867 Ústava Rakouska-Uherska z 21.12 1867

[6] Charta 77 byla neformální československá občanská iniciativa, která kritizovala politickou i státní moc za nedodržování lidských a občanských práv, k jejichž dodržování se ČSSR zavázala při podpisu Závěrečného aktu Konference o bezpečnosti a spolupráci v Evropě v Helsinkách.

poskytována jak příjemci, tak odesílateli zprávy. Není také rozdíl mezi tím, jestli se jedná o fyzickou nebo právnickou osobu.

Stejně tak je také nahlíženo na narušitele listovního tajemství. I tím může být kdokoliv. Z toho vyplývá, že narušitelem nesmí být fyzická ani právnická osoba, dokonce ani stát zastoupený orgány veřejné moci.

1.2.2 Předmět ochrany listovního tajemství

Ochrana listovního tajemství se vztahuje na jakékoliv listiny, které jsou uchovávány v soukromí a jsou zasílány poštou nebo jiným způsobem. A to bez ohledu na to, jestli se jedná o listinu soukromou nebo veřejnou. Ochrana tajemství jiných písemností se uplatňuje na text, který je zachycený na jakémkoliv podkladu. Dalším subjektem, zmíněným v čl. 13 Listiny základních práv a svobod, který je tímto článkem chráněný jsou záznamy. Z trestního zákoníku pak vyplývá, že za záznam se se považuje například film nebo jiný záznam, fotografie, ale také například počítačová data.

Ústavní soud České republiky a také ústavní soudy jiných evropských zemí se zabývaly otázkou, jestli listovní tajemství chrání pouze samotný obsah odesílaných zpráv, nebo také další parametry samotných zpráv. A to především identita účastníků, čas a místo nebo způsob komunikace. Touto otázkou se zabývá směrnice Evropského soudu 2006/24/ES. Hlavním důvodem přijetí této směrnice byly teroristické útoky v New Yorku v roce 2001 a Madridu v roce 2004. Zde se potkává otázka listovního tajemství a uchovávání provozních a lokalizačních údajů.

1.2.3 Listovní tajemství a jeho ukotvení v jednotlivých zákonech

Jak již bylo popsáno, listovní tajemství je základním právem dle čl. 13 Listiny základních práv a svobod. Toto právo však není neomezené a již v samotném článku odkazuje na výjimky, stanovené dalším zákonem. Zásah do tohoto práva je možný na základě zákona. Stejně tak je na tom výklad čl. 8 Evropské úmluvy o ochraně lidských práv.

V trestním řádu je možno zasahovat do listovního tajemství dle ust. § 78 – povinnost k vydání věci. Toto ustanovení stanovuje povinnost vydat na vyzvání

hmotnou věc. Za hmotnou věc je považována i listina, která je uchovávána v soukromí a spadá pod ochranu ust. Čl. 13 Listiny. Věc se v tomto případě vydává soudu, státnímu zástupci nebo policejnímu orgánu.

Dalším je pak ust. § 79 trestního řádu – odnětí věci. K odnětí věci je potřeba předchozího souhlasu státního zástupce, nesnese-li věc odkladu. Státní zástupce vydá příkaz k odnětí věci na žádost soudu, státního zástupce, policejního orgánu nebo také předsedy senátu.

K zadržení zásilky dle ust. § 86 trestního řádu není nutné předchozího zahájení trestního stíhání. V tomto případě se může jednat o neodkladný nebo neopakovatelný úkon.

Dalším stupněm zásahu do důvěrnosti korespondence je pak navazující ust. § 87 trestního řádu, kterým je otevření zásilky. Nejen, že jsou zde uvedeny informace o odesílateli a příjemci zásilky, ale dochází také k narušení samotného obsahu zásilky. Takto zadrženou zásilku může otevřít pouze předseda senátu, státní zástupce nebo policejní orgán při splnění dalších podmínek.

Omezení práva na ochranu listovního tajemství můžeme také nalézt v zákoníku práce. Zaměstnanci je možno zasahovat do jeho práva z důvodu ochrany majetku a oprávněných zájmů zaměstnavatele. Nejedná se zde o snahu zajišťovat důkazy v trestním řízení nebo o prevenci před páchání trestné činnosti. Tato právní úprava je pak zakotvena v ust. § 316 odst. 2 a 3 zákoníku práce[7]. Ve druhém odstavci je uveden zákaz narušení soukromí zaměstnance, například formou odposlechu telefonických hovorů nebo kontrolou listovní nebo elektronické korespondence, pokud k tomu nemá zaměstnavatel závažný důvod spočívající ve zvláštní povaze jeho činnosti. Kontrolní mechanismy zaměstnavatele jsou pak uvedeny ve třetím odstavci. Zaměstnanec musí být informován o rozsahu i způsobu kontroly. Následně je zaměstnavatel oprávněn provádět skryté či otevřené sledování, odposlechy a záznamy telefonických hovorů nebo kontrolovat listovní zásilky či elektronickou poštu adresovanou zaměstnanci.

[7] z.č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů

Omezení práva na ochranu listovního tajemství můžeme také nalézt v zákoně o výkonu trestu odnětí svobody[8], zákoně o výkonu vazby[9], zákoně o vojenském zpravodajství[10] nebo například v zákoně o poštovních službách[11] a některých dalších.

Subjekty dotčené narušením práva na ochranu listovního tajemství mají možnost se svého práva domáhat. K porušování tohoto práva dochází ať už úmyslně (hackerské skupiny), či neúmyslně, a to především z neznalosti či nepochopení právních předpisů. Jedním ze způsobů řešení následků porušení listovního tajemství je například náhrada nemajetkové újmy. To stanoví ust. § 2956 občanského zákoníku[12], vznikne-li škůdci povinnost odčinit člověku újmu na jeho přirozeném právu chráněném ustanoveními první části občanského zákoníku, nahradí škodu i nemajetkovou újmu, kterou tím způsobil.

1.3 Důvody vzniku Data retention

Jako hlavní důvody vzniku Data retention jsou uváděny teroristické útoky. A to především z roku 2001 v New Yorku, USA, 2004 Madridu, Španělsko a 2005 v Londýně, Velká Británie. Hrozba toho, že by mohly následovat další útoky, přispěla k rychlejšímu zavedení pravidel pro uchovávání provozních a lokalizačních údajů. Tato pravidla pak měla také sloužit je sjednocení podmínek v jednotlivých státech Evropské unie.

1.4 Data Retention v ČR

1.4.1 Historie

Česká republika patřila v oblasti uchovávání provozních a lokalizačních údajů mezi nejvyspělejší státy Evropské unie. A to díky zákonu č. 127/2005 Sb., který vešel v platnost 1.května 2005. O rok později pak Evropská unie vydala směrnici

[8] z.č. 169/1999 Sb., zákon o výkonu trestu odnětí svobody a o změně některých souvisejících zákonů
[9] z.č. 293/1993 Sb., zákon o výkonu vazby
[10] z.č. 150/2001 Sb., zákon o Vojenském zpravodajství
[11] z.č. 29/2000 Sb., zákon o poštovních službách a o změně některých zákonů
[12] z.č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

2006/24/ES. Po vydání této směrnice nastala situace, kdy většina států Evropské unie požádala o možnost zavedení směrnice ve více etapách tak, aby vše stihly. Česká republika pak požádala o opak, tedy o urychlení celého procesu. Toto bylo použito pro telefonní komunikace, co se týče oblasti internetu, tam bylo zažádáno, stejně jako v jiných evropských státech, o odklad implementace. V české právní úpravě navíc byly zaneseny požadavky, které byly nad rámec unijní směrnice, např. informace o šifrování nebo vztah mezi SIM kartou a IMEI mobilního telefonu. V roce 2008 byla následně přijata novela zákona, která přidala povinnost veškeré komunikaci, internetové tak té telefonické zaznamenávat i neproběhlá telefonická spojení nebo nedoručenou elektronickou poštu.

Snad jako všechny právní úpravy, tak ta o uchovávání provozních a lokalizačních údajů se stala terčem kritiky, a to vlastně za celou dobu své existence jak v Evropské unii, tak v České republice. U nás bylo nejhlasitějším kritikem sdružení Iuridicum Remedium[13]. Toto sdružení vypracovalo stížnost, která byla následně podpořena skupinou 51 poslanců. Této stížnosti následně vyhověl Ústavní soud, dne 22.března 2011, který nařídil úplné zrušení příslušných pasáží zákona č. 127/2005 Sb., o elektronických komunikacích. Konkrétně bylo zrušeno ust. §97 odst. 3) a odst. 4) prováděcí vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů. Velmi volně určené postupy, které dané subjekty musely splnit, aby se k výpisům Data retention dostaly, byly hlavním důvodem tohoto úplného zrušení.

Zákon i evropská směrnice měly být využity jako prostředek k odhalování závažných zločinů. Před tím, než byl výše zmíněný paragraf zrušen, Česká republika obsadila slušné, třetí místo ve využívání výpisů Data retention za Belgií a Litvou. Tato statistika byla z roku 2008, tedy tři roky před zrušením příslušného paragrafu z provozní vyhlášky. Dle tiskové zprávy Českého telekomunikačního úřadu pak operátoři například v roce 2016 předali provozní a lokalizační údaje ve 214 522 případech, přičemž ve zmíněném roce 2008 bylo žádostí 131 560. V roce

[13] Iuridicum Remedium, o.s. je nevládní nezisková organizace na ochranu lidských práv v oblasti data retention. Každoročně pořádá Ceny Velkého bratra, v níž jsou zařazeny subjekty, které nejvíce narušili soukromí lidí.

2017 to bylo již 253 380 případů poskytnutí Data Retention. Z tohoto je jasně vidět, že počet žádostí stále přibývá.

Dalším důvodem ke zrušení vyhlášky pak byly nedostatečně určené kroky k likvidaci těchto dat. Nebyl zde zadán přesný postup, jak s daty naložit po uplynutí šesti měsíců. Také zde nebyl dán přesný účel, pro které je možné údaje vyžadovat ani odpovědnost a sankce za nesplnění povinností při archivaci. Ústavní soud doporučil obměnu zákona, vzhledem k tomu, že se jedná o důležitý prostředek při odhalování trestné činnosti.

1.4.2 Současná situace

V důsledku výše zmíněného nálezu Ústavního soudu sp. Zn. Pl. ÚS 24/10, kde Ústavní soud uzavřel, že plošný, preventivní sběr a uchovávání údajů je zásah do práva na soukromí a na sebeurčení natolik intenzivní, že je třeba na splnění požadavků přípustnost zásahu klást co nejpřísnější měřítka, bylo reagováno přijatým zákonem č. 273/2012 Sb. s účinností od 1.10. 2012. A to tak, že byla zkrácena doba uchovávání provozních a lokalizačních údajů na dobu šesti měsíců, explicitně vyjmenovány subjekty oprávněné k vyžádání údajů, včetně účelů, k jakým mohou oprávněné subjekty údaje žádat. Také byla doplněna zákonná definice provozních a lokalizačních údajů a v podrobnostech odkázáno na prováděcí předpis.

V roce 2019 byl pak podán návrh skupinou 58 poslanců na zrušení některých ustanovení zákona o elektronických komunikacích[14], trestního řádu, zákona o Policii České republiky[15] a vyhlášky o uchovávání předávání a likvidaci provozních a lokalizačních údajů[16]. Dle navrhovatelů je napadená právní úprava neproporcionální ve vztahu k ústavně zaručenému právu na soukromí.

Tento návrh byl však plénem Ústavního soudu zamítnut.

[14] z.č. 127/2005 Sb., Zákon o elektronických komunikacích a o změně některých souvisejících zákonů
[15] z.č. 273/2008 Sb., Zákon o Policii České republiky
[16] Vyhláška č. 257/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů

V současné době však dochází ke zcela nové situaci, kdy celosvětově vypukla pandemie nemoci Covid-19. Jako jeden z prostředků, kterým vlády na celém světě chtějí předejít co největšímu počtu nakažených osob je trasování osob. Systém obecného omezení pohybu osob je tak nahrazen systémem zpětného trasování pohybu nakažené osoby. Využití lokalizačních údajů uchovávaných na principu data retention bude možné na základě usnesení vlády ze dne 18.3.2020 č.250. Toto usnesení předpokládá, že po vyslovení informovaného souhlasu bude možné zpětně využít plošně uchované lokalizační údaje pro sestavení orientačního přehledu o pohybu osoby, která k tomu poskytne souhlas. Téma data retention a Covid-19 bude rozvedeno dále v této bakalářské práci.

1.4.3 Zneužití Data retention

Nejznámější kauzou v souvislosti se zneužitím Data retention je kauza bývalého policejního důstojníka Mariana Hudce. Tento varnsdorfský policista si od října roku 2009 nechal posílat výpisy telefonních hovorů významných lidí, například šéfa Ústavního soudu Pavla Rychetského nebo manažera společnosti ČEZ Daniela Rouse. Hudec získal výpisy na základě lživého tvrzení, že telefonní čísla souvisí s vyšetřováním obchodu s bílým masem na severu Čech. Díky získaným informacím bylo možné zjistit s kým si tito lidé telefonovali, komu posílali nebo od koho přijímali SMS. Bylo také možné zjistit kudy chodili, kde se zastavili nebo na jak dlouho. Toto bylo s přesností na metry. K obsahu hovorů se Hudec dostat nemohl.

1.5 Data retention v Evropské unii

1.5.1 Historie

15. března 2006 bylo přijato nařízení Evropského parlamentu a Rady s názvem „The Data retention Directive“. Toto nařízení uděluje všem členům Evropské unie povinnost uchovávat údaje vytvářené nebo zpracovávané v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí. Proti přijetí této směrnice vznikla petice, která byla adresována Evropskému parlamentu, kterou podepsalo přes 50 000 občanů Evropské unie. Ani tato petice, ani evropský komisař na ochranu osobních údajů

Peter Hustinx[17] však nezabránili nezvykle rychlému přijetí této směrnice. Ta byla přijata v období asi tří měsíců, přičemž normálně takovýto legislativní proces trvá roky.

Evropské státy měly tuto směrnici implementovat do 15.září 2007. Implementace do tohoto data se nevztahovala na povinnosti týkající se uchovávání údajů o připojení k internetu, elektronické poště a internetové telefonii. Zde byla možnost odložení o 18 měsíců.

8. dubna 2014 byla následně tato směrnice zrušena. Důvodem zrušení byla skutečnost, že tato směrnice byla v rozporu s Chartou základních práv EU. Členské státy odmítaly od plošného sběru dat ustoupit a právní základ našly v čl. 15 odst. 1) Směrnice Evropského parlamentu a Rady 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.

1.5.2 Současná situace v EU

K souladu principu plošného uchovávání provozních a lokalizačních údajů se vyjádřil Soudní dvůr Evropské unie v dalším rozhodnutí dne 21.prosince.2016. Zde Soudní dvůr konstatuje, že uvedený čl. 15 odst. 1) Směrnice o soukromí a elektronických komunikací musí být vykládán tak, že brání vnitrostátní právní úpravě zavést plošné a nerozlišující uchovávání provozní a lokalizačních údajů všech účastníků.

Dne 6. října 2020 Soudní dvůr vydal další dva rozsudky rozvíjející výše uvedená starší rozhodnutí. Soudní dvůr konstatoval, že předávání osobních údajů bezpečnostním složkám ze strany provozovatelů služeb elektronických komunikací spadá pod čl. 15 odst. 1) Směrnice o soukromí a elektronických komunikacích.

Ve druhém rozsudku pak Soudní dvůr konstatuje, že čl. 15 odst. 1) Směrnice o soukromí a elektronických komunikacích výslovně zapovídá plošné a nevýběrová data retention. Toto připouští pouze v případech závažného

[17] Peter Johan Hustinx (nar. 1945) je právník z Nizozemska. Pozici evropského komisaře na ochranu osobních údajů zastával v období let 2004-2014. Vystudoval Universitu v Nijmegenu, následně pracoval na Univerzitě v Michiganu v oblasti práva. V letech 1971-1991 pracoval v Nizozemí na Ministerstvu spravedlnosti. V oblasti ochraně dat začal pracovat v roce 1972.

ohrožení bezpečnosti, a to na základě rozhodnutí příslušného orgánu do budoucna a pouze po omezenou dobu trvání hrozby.

Zde dochází k rozporu mezi čl. 15 odst. 1 o soukromí a elektronických komunikacích a ust. §97 odst. 3) a 4) zákona o elektronických komunikacích. Právo Evropské unie by mělo mít přednost před českou úpravou, ovšem jak se k tomu Česká republika bude nadále stavět není známo. Směr, jakým se Česká republika pak bude ubírat je možné vysledovat na příkladu z 27.listopadu 2020 kdy ministerstvo zdravotnictví poslalo do připomínkového řízení úpravu zákona, upravujícího činnost hygieny i novelu zákona o elektronických komunikacích, která má hygieně umožnit přistupovat k lokalizačním údajům osob, u nichž byla prokázána nákaza infekční nemocí.

2 PRÁVO A DATA RETENTION

Provozní a lokalizační údaje lze dle právní úpravy rozdělit do dvou skupin. Jedná se o právní úpravu ve smyslu povinnosti nebo oprávnění tato data uchovávat a následně pak oprávnění určitých státních orgánů k tomu, aby mohly tato data využívat.

2.1 Uchovávání provozních a lokalizačních údajů

Osoby zajišťující veřejné komunikační sítě[18] nebo poskytovatelé služeb elektronických komunikací mají oprávnění a povinnosti uchovávat provozní a lokalizační údaje dle právních předpisů ale také ze smluv.

Tyto povinnosti jsou obsaženy v zákoně č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů. Tento zákon vešel v platnost dne 22.února 2005. Dle ust. §1 odst. 2 zákona č. 127/2005 Sb. se tento zákon nevztahuje na obsah služeb poskytovaných prostřednictvím sítí elektronických komunikací, jako je obsah rozhlasového a televizního vysílání, finančních služeb a některých služeb informační společnosti, není-li dále stanoveno jinak. Službou elektronických komunikací se pak rozumí služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací. Samotné uchovávání provozních a lokalizačních údajů poté upravuje ust. §90 odst. 3) z.č. 127/2005 Sb. Zde je uvedeno, že *„Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, je povinen uchovávat provozní údaje služby poskytnuté účastníkovi nebo uživateli do doby rozhodnutí sporu podle § 129 odst. 3 nebo do konce doby, během níž může být vyúčtování ceny nebo poskytnutí služby elektronických komunikací právně napadeno nebo úhrada vymáhána“3.*

Policie České republiky a další orgány jsou pak oprávněny vymáhat provozní a lokalizační údaje zejména dle ust. §97 odst. 3) a 4) z.č. 127/2005 Sb. Povinnost,

[18] Veřejná komunikační síť je síť elektronických komunikací, která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací.

vyplývající z toho paragrafu tak vešla v platnost dříve, než vyšla směrnice Evropského parlamentu a Rady 2006/24/ES. Ta byla implementována 15.března 2006. O tom, co se následně dělo s výše uvedenými paragrafy již byla řeč v historii Data Retention v České republice. Dle nově schválené právní úpravy jsou pak v §97 odst. 3) a 4) zákona č. 127/2005 Sb. „Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací. Provozní a lokalizační údaje týkající se neúspěšných pokusů o volání je právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna uchovávat pouze tehdy, jsou-li tyto údaje vytvářeny nebo zpracovávány a zároveň uchovávány nebo zaznamenávány. Současně je tato právnická nebo fyzická osoba povinna zajistit, aby při plnění povinnosti podle věty první a druhé nebyl uchováván obsah zpráv a takto uchovávaný dále předáván. Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout

a) Orgánům činným v trestním řízení pro účely a při splnění podmínek stanovených zvláštním právním předpisem
b) Policii České republiky pro účely zahájení pátrání po konkrétní hledané[19] nebo pohřešované[20] osobě, zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby a při splnění podmínek stanovených zvláštním právním předpisem
c) Bezpečnostní informační službě[21] pro účely a při splnění podmínek stanovených zvláštním právním předpisem

[19] Hledaná osoba je fyzická osoba, u které je dán některý ze zákonných důvodů omezení její osobní svobody, místo jejího pobytu není známo a policií po ní bylo vyhlášeno pátrání.
[20] Pohřešovanou osobou se rozumí fyzická osoba, o níž se lze důvodně domnívat, že je ohrožen její život nebo zdraví, místo jejího pobytu není známo a policií po ní bylo vyhlášeno pátrání.
[21] Bezpečnostní informační služba (BIS) je česká ozbrojená zpravodajská služba s vnitřním polem působnosti. Tento bezpečnostní sbor získává, shromažďuje a vyhodnocuje informace důležité pro

d) Vojenskému zpravodajství[22] pro účely a při splnění podmínek stanovených zvláštním právním předpisem
e) České národní bance pro účely a při splněný podmínek stanovených zvláštním právním předpisem

Dle §97 odst. 4) z.č. 127/2005 Sb. se provozními a lokalizačními údaji podle odstavce 3 jsou zejména údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace a dále údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace. Rozsah provozních a lokalizačních údajů uchovávaných podle odstavce 3, formu a způsob jejich předávání orgánům oprávněným k využívání podle zvláštního právního předpisu a způsob jejich likvidace stanoví prováděcí právní předpis.

2.2 Vyžadování dat

Které orgány jsou oprávněny vyžadovat provozní a lokalizační údaje jsou tedy výše uvedené orgány. K tomu, aby získaly přístup k těmto údajům mít zákonné zmocnění. Následně, díky tomuto zmocnění pak musí poskytoval služeb tato data vydat. V tomto případě se jedná o uplatňování státní moci. Ta lze však uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon. Toto je zakotveno v Ústavě ČR, konkrétně v čl. 2, odst. 3) a také čl. 2 odst. 2) Listiny základních práv a svobod. Provozní a lokalizační údaje jsou stejně jako obsah komunikace chráněny listovním tajemstvím dle čl. 13 Listiny základních práv a svobod. Poskytovatelé služeb pak mají povinnost zachovávat diskrétnost komunikace dle ust. §89 odst. 1) zákona č. 127/2005 Sb. Podle tohoto ustanovení platí, že *„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 a veřejně*

bezpečnost, ochranu ústavního zřízení, demokratických principů a významných ekonomických zájmů České republiky. Vznikla 30.července 1994.

[22] Vojenské zpravodajství (VZ) je ozbrojená zpravodajská služba, součást Ministerstva obrany a Armády České republiky. Zabezpečuje informace o možném vojenském ohrožení České republiky, o činnostech namířených proti obraně ČR a o činnostech ohrožujících utajované skutečnosti v oblasti obrany ČR.

dostupných služeb elektronických komunikací. Zejména nesmí připustit 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“3.

2.3 Kdo může vyžadovat data

2.3.1 Orgány činné v trestním řízení

Nejdříve je potřeba určit, kdo je orgánem činným v trestním řízení. Toto je uvedeno v ust. §12 odst. 1) Trestního řádu. Orgánem činným v trestním řízení se tedy rozumí soud, státní zástupce a policejní orgán. To, kdo je policejním orgánem je dále stanoveno v ust. §12 odst. 2) Trestního řádu. Jedná se o Policii České republiky a v určitých případech pak také např. o Generální inspekci bezpečnostních sborů, pověřené celní orgány, pověřené orgány Vojenské policie nebo pověřené orgány zpravodajských služeb.

V rámci trestního řízení mají orgány činné v trestním řízení oprávnění využívat provozní a lokalizační údaje zakotveno v ust. §88a Trestního řádu.

Tento paragraf byl v roce 2012 zrušen nálezem Ústavního soudu ze den 20.12.2012. Před úpravou tohoto paragrafu byl v podstatě možné žádat o provozní a lokalizační údaje pro jakýkoliv trestný čin. Žádosti byly nadužívány a také šlo velmi složitě přezkoumávat žádosti. Osoby, dotčené touto žádostí pak nebyly ani vyrozuměny po ukončení trestního řízení o tom, že bylo zasahováno do jejich soukromí. Proto možnost zneužití byla velká, jak již bylo pospáno v kauze Hudec. V nové úpravě ust. §88 Trestního řádu je pak vymezen okruh trestných činů, kterých se vyžadování provozních a lokalizačních údajů týká. Také jsou zpřísněna pravidla pro podávání žádostí. Byla také zavedena informační povinnost směrem k prověřované osobě.

2.3.2 Policie České republiky mimo trestní řízení

Vyžadování provozních a lokalizačních údajů mimo rámec trestního řízení upravuje zákon č. 273/2008 Sb. o Policii České republiky a 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. Dle ust. §66 odst. 3) zákona č. 273/2008 Sb. může *„Policie může v případech stanovených zákonem a v rozsahu potřebném pro plnění konkrétního úkolu žádat od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací poskytnutí provozních a lokalizačních údajů způsobem umožňujícím dálkový a nepřetržitý přístup, nestanoví-li jiný právní předpis jinak. Tyto osoby jsou povinny žádosti vyhovět bez zbytečného odkladu, ve formě a v rozsahu stanoveném jiným právním předpisem“15.*

Jak bylo již v této práci zmíněno, Policie České republiky má také oprávnění provozní a lokalizační údaje žádat, pokud je to nutné při pátrání po pohřešované nebo hledané osobě. Toto oprávnění pak upravuje ust. § 68 odst. 2) zákona č. 273/2008 Sb. kdy *„Policie může žádat pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě a za účelem zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly poskytnutí provozních a lokalizačních údajů od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací způsobem umožňujícím dálkový a nepřetržitý přístup, nestanoví-li jiný právní předpis) jinak. Informace se poskytne ve formě a v rozsahu stanoveném jiným právním předpisem)“15.*

Posledním ustanovením paragrafu v zákoně o Policii České republiky, zabývajícím se provozními a lokalizačnímu údaji je pak ust. § 71 zákona č. 273/2008 Sb. Ten říká že *„Útvar policie, jehož úkolem je boj s terorismem, může za účelem předcházení a odhalování konkrétních hrozeb v oblasti terorismu v nezbytném rozsahu žádat od*

a) právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací poskytnutí provozních a lokalizačních údajů způsobem umožňujícím dálkový a nepřetržitý přístup, nestanoví-li jiný právní předpis jinak; informace se poskytne ve formě a v rozsahu stanoveném jiným právním předpisem,

b) banky předávání dat o době a místě použití elektronického platebního prostředku,
c) zdravotní pojišťovny nebo poskytovatele zdravotních služeb poskytnutí informací o době a místě poskytnutí zdravotních služeb.“[15]

Tato ustanovení se od samotného vzniku zákona o Policii České republiky nezměnily, i když byly terčem kritiky během připomínkových řízení. A to ze strany Úřadu pro ochranu osobních údajů ale také samotné Policie České republiky. Největším problémem tak zůstává to, že poskytování provozních a lokalizačních údajů nemusí nařizovat soud, dokonce ani nemusí jít údaje o hledané nebo pohřešované osobě. V tomto smyslu je největší problém u ust. § 68 odst. 2 zákona č. 273/2008 Sb. Nastavené nejsou ani žádné další mantinely jako například podrobné odůvodnění žádosti nebo povinnost informovat dotčenou osobu. V těchto ohledech je úprava popsaná v trestním řádu dokonalejší a méně zneužitelná.

V situacích, kdy je vyhlášeno pátrání po hledané nebo pohřešované osobě jde hlavně o čas. Nicméně žádostí o provozní a lokalizační údaje je méně. Hledaná nebo pohřešovaná osoba má často vypnutý telefon, a tak nelze s jistotou říct, na jakém místě se nachází v reálném čase. Přitom, když je telefon zapnutý, lze osobu dohledat s přesností na metry, a to díky tomu, že se telefon signálem připojí na nejbližší základovou stanici. Tyto stanice jsou označovány jako Base Transceiver Station (BTS). Jsou to v podstatě vysílače a přijímače rádiových signálů. Síť těchto stanic v dnešní době hustě pokrývá plochu celé České republiky. Mobilní telefony se následně připojují k jednotlivým stanicím. Právě díky tomu je možné určit polohu osob, vlastnících zapnutý mobilní telefon. Údaje o poloze různých telefonů jde samozřejmě sledovat i do minulosti. Je tak možné podívat se na často navštěvovaná místa hledanou nebo pohřešovanou osobou. Vzhledem k tomu, že operátoři mají nyní povinnost uchovávat data až 6 měsíců, pak je vzorek dat dost velký na to, aby mohla být hledaná nebo pohřešovaná osoba nalezena. Toto lze ovšem aplikovat v případech, kdy nalezení hledané nebo pohřešované osoby není akutní. Pokud by se jednalo například o ztracené dítě v lese, nebo ve městě, pak je prioritou jeho co nejrychlejší nalezení a data o poloze 6 měsíců zpět nijak nepomohou.

Dalším oprávněním mimo trestní řízení je pak oprávnění dle ust. §10a zákona č. 137/2001 Sb. kdy je Policie České republiky oprávněna požadovat data *„Je-li dáno podezření, že chráněná osoba nedodržuje povinnosti uvedené v § 6, a nelze-li toto podezření prověřit jiným způsobem, je policie oprávněna v nezbytně nutném rozsahu získávat poznatky utajovaným způsobem pomocí technických nebo jiných prostředků; při tom je oprávněna pořizovat zvukové, obrazové nebo jiné záznamy, provádět odposlech a záznam telekomunikačního provozu a požadovat po osobě vykonávající telekomunikační činnost údaje o uskutečněném telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství nebo na něž se vztahuje ochrana osobních a zprostředkovacích dat“*[23].

2.3.3 Zpravodajské služby

Bezpečnostní informační služba a Vojenské zpravodajství mají oprávnění požadovat provozní a lokalizační údaje dle ust. § 8 zákona č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů a dle ust. § 8 zákona č. 289/2005 Sb., o Vojenském zpravodajství. K tomuto pak obě zpravodajské služby využívají zpravodajskou techniku. Tímto způsobem utajeně získávají informace. Tyto informace jsou následně zpracovávány a interpretovány. Výsledná analýza bývá často utajená. Zpravodajskou technikou je pak například technika pro získávání zvuku, obrazu, dat či přístroje registrující vyzařování. Oba zákony pak uvádí, že účelem může být i získávání údajů o telekomunikačním provozu. Obě zpravodajské služby si vlastně informace získávají sami, na rozdíl od Policie ČR, která poskytovatele služeb o informace žádá. V dřívějších úpravách chyběla povinnost poskytovatele služeb poskytnout informace, což se změnilo během připomínkového řízení, kdy jsou teď poskytovatelé povinni zajistit podmínky pro připojení zpravodajské techniky pro odposlech nebo záznam zpráv. K tomuto vyžádání je potřeba souhlas soudce vrchního soudu dle místa, kde sídlí konkrétní zpravodajská služba.

[23] z.č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízení a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů

2.3.4 Česká národní banka

Oprávnění vyžadovat provozní a lokalizační údaje má Česká národní banka[24] dle ust. § 8 odst. 1) písm. d) zákona č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu o změně a doplnění dalších zákonů.

Dle tohoto ustanovení je *„Česká národní banka je oprávněna pro účely výkonu dohledu nad kapitálovým trhem vyžadovat od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací poskytnutí provozních a lokalizačních údajů podle zvláštního právního předpisu, a to po předchozím písemném povolení předsedy senátu vrchního soudu příslušného podle sídla České národní banky, pokud lze důvodně předpokládat, že poskytnuté údaje mohou přispět k objasnění skutečností důležitých pro odhalení přestupku na úseku podnikání nebo obchodování na kapitálovém trhu podle zákona upravujícího podnikání na kapitálovém trhu, včetně jeho pachatele, a nelze-li sledovaného účelu dosáhnout jinak, nebo jen s vynaložením neúměrného úsilí“27.*

V souvislosti s tímto ustanovením musí mát ČNB písemné povolení od předsedy senátu vrchního soudu, a to dle sídla České národní banky. Toto oprávnění, kterým Česká národní banka disponuje, je, co se týče států Evropské unie ne-li jedinečný.

[24] Česká národní banka je centrální banka České republiky a orgán, který vykonává dohled nad finančním trhem v zemi.

3 PRAXE ZÍSKÁVÁNÍ PROVOZNÍCH A LOKALIZAČNÍCH ÚDAJŮ

Policie České republiky žádá o výpisy provozních a lokalizačních údajů, a to zejména takto. První možnost je taková, že je známa zájmová osoba, jejíž údaje je potřeba znát a policista má například telefonní číslo mobilního telefonu nebo pevné linky případně IMEI mobilního telefonu. Z tohoto lze pak zjistit kde se osoba pohybovala, její kontakty a podobně. Druhým příkladem je pak situace, kdy je známo pouze místo činu a pachatel je neznámý. V tomto případě se pak policista zajímá o všechny telefony, které se v době spáchání činu pohybovaly kolem místa činu. Toto lze zjistit dle jednotlivých stanic BTS, ke kterým se připojí telefonní zařízení v dosahu. Zde policista spoléhá na to, že měl u sebe pachatel telefonní přístroj, který byl zapnutý.

3.1 Jak získat provozní a lokalizační údaje

Jak již bylo napsáno, provozní a lokalizační údaje může vyžadovat orgán činný v trestním řízení. Tyto údaje jsou důležité zejména v počátku šetření trestného činu, a proto ve velké většině o tyto údaje žádá Policie České republiky. Police údaje získává buď se souhlasem sledované osoby dle ust. §88a odst. 2) Trestního řádu nebo bez jejího souhlasu, a to dle ust. §88a odst. 1) Trestního řádu.

Co se týče statistik tak se dá předpokládat, že souhlas poskytne jen malé procento osob a také tomu tak je.

Samotný postup policisty při vyžadování provozních a lokalizačních údaje probíhá tak, že policista žádá soud prostřednictvím státního zástupce. Pokud policista od soudu dostane povolení, žádost následně předá na Útvar zvláštních činností SKPV[25]. Útvar zvláštních činností následně kontaktuje konkrétního zprostředkovatele elektronických služeb. Policista se může také přímo obrátit na Útvar zvláštních činností, a to v případě, pokud jsou provozní a lokalizační údaje

[25] Útvar zvláštních činnost, zkráceně ÚZČ je jeden ze servisních útvarů Policie České republiky s celostátní působností. Provádí ve prospěch oprávněných především odposlech a záznam telekomunikačního provozu, sledování osob a věcí a další specializované úkony.

důležité při nalezení hledané nebo pohřešované osoby. V tomto případě pak odpadá krok žádosti soudu prostřednictvím státního zástupce. Co se týče samotného zákona, není v něm uvedeno státní zastupitelství jako prostředník mezi policií a soudem. Zřejmě kvůli kritice předchozích verzí zákonů se toto však stalo běžnou praxí.

Policista pak dále může s údaji pracovat, k tomu však potřebuje výpis od poskytovatele, který je autorizovaný a opatřený razítkem. Veškeré došlé údaje jsou pak na Útvaru zvláštních činností uchovány po dobu 5 dnů. Útvar zvláštních činností následně údaje uchovává v nezpracované podobě po dobu 3 let. Policista má možnost poslat žádost na jedno ze 7 pracovišť Útvaru zvláštních činností. Ty jsou rozmístěny v Praze, Ústí nad Labem, Plzni, Českých Budějovicích, Hradci Králově, Brně a Ostravě. Žádost je vypsána ve speciálním formuláři, je zapsáno číslo požadavku, doba od-do, kdo o výpis žádá, následně číslo jednací policejního spisu, ke kterému má být požadavek přiřazen, číslo jednací povolení soudu. Číslo jednací povolení soudu není potřeba, pokud je žádáno dle ust. § 68 zákona č. 273/2008 Sb. nebo ust. § 71 zákona č. 273/2008 Sb. Aby se zamezilo zneužití informací, policista určí heslo, kterým bude poté možné otevřít následnou odpověď. Útvar zvláštních činností se následně s touto žádostí obrátí přímo na poskytovatele služeb elektronických komunikací. Odpověď následně přichází na centrálu Útvaru zvláštních činností v Praze. Ta je poté přeposlána na konkrétní expozituru a ta je odeslána konkrétnímu policistovi. Ten celý soubor otevře heslem, které zvolil na začátku celého procesu.

Také se však stává, že tento zavedený postup policisté obcházejí a na poskytovatele služeb se obrací přímou cestou. Při tomto se pak odvolávají na ust. § 8 Trestního řádu, který říká, že „*státní orgány, právnické a fyzické osoby jsou povinny bez zbytečného odkladu, a nestanoví-li zvláštní předpis jinak, i bez úplaty vyhovovat dožádáním orgánů činných v trestním řízení při plnění jejich úkolů. Státní orgány jsou dále povinny neprodleně oznamovat státnímu zástupci nebo policejním orgánům skutečnosti nasvědčující tomu, že byl spáchán trestný čin*“[26].

[26] z.č. 141/1961 Sb. o trestním řízení soudním

Tento postup je policisty v některých případech považován za oficiální postup. Až poté, když není této žádosti vyhověno se policista uchýlí k oficiálnímu postupu. Vzhledem k tomu, že postup, který vede přes Útvar zvláštních činností není zakotven v žádném obecně závazném právním předpisu se poskytovatelé můžou jen stěží odvolávat právě na takovýto postup. Proto je takovéto žádosti často vyhověno. Co se pak týká využitelnosti takto nabytých důkazů u soudu, tak ta je pak velmi pochybná. Takto nabyté důkazy může samozřejmě napadnout obhajoba. Nehledě na skutečnost, že i tyto informace, poskytnuté neformální cestou mohou vést i k dalším důkazům.

Tento postup není v souladu ani s Trestním řádem ani se zákonem o Policii České republiky. Poskytovatel služeb elektronických komunikací tímto porušuje ust. §89 odst. 1 zákona č. 127/2005 o elektronických komunikacích čím se dopouští přestupku dle ust. § 118 odst. 21 písm. d) zákona č. 127/2005 Sb. o elektronických komunikacích. Může mu pak být uložena sankce až do výše 10 milionů Kč.

3.2 Praxe při využívání data retention ZS a ČNB

Česká národní banka má oprávnění vyžadovat provozní a lokalizační údaje dle ust. § 8 odst. 1 písm. d) zákona č. 15/1998 Sb.[27] Provozní a lokalizační údaje jsou vyžadovány od osob, zajišťujících veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací. Předlohou pro toto oprávnění byl čl. 12 odst. 2 písm. d) směrnice 2003/6/ES[28]. Toto oprávnění bylo však sporné a bylo upraveno během připomínkového řízení k zákonu č. 273/2012 Sb. Mimo jiné byla zavedena povinnost disponovat souhlasem předsedy senátu vrchního soudu příslušného podle sídla České národní banky. Přípustnost vyžadování údajů je přípustné, pokud lze důvodně předpokládat, že tyto údaje budou důležité při objasnění skutečností důležitých pro odhalení správního deliktu na úseku podnikání nebo obchodování na kapitálovém trhu, včetně jeho pachatele, a nelze-li sledovaného účelu dosáhnout jinak, nebo jen s vynaložením neúměrného úsilí.

[27] z.č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu o změně a doplnění dalších zákonů
[28] Směrnice 2003/6/ES o obchodování zasvěcených osob a manipulaci s trhem

Stejně jako u oprávnění ČNB, tak i oprávnění zpravodajských služeb, byla během připomínkového řízení upravena. Dle ust. § 8 zákona č. 154/1994 Sb.[29] a

ust. § 8 zákona č. 289/2005 Sb.[30], měla sice Bezpečnostní informační služba a Vojenské zpravodajství nárok na provozní a lokalizační údaje. Chybělo však zakotvení povinnosti poskytovatelů tyto údaje BIS a Vojenskému zpravodajství předávat. Od října roku 2012 jsou již právnické nebo fyzické osoby zajišťující veřejnou komunikační síť anebo poskytující veřejně dostupnou službu elektronických komunikací povinny provozní a lokalizační údaje poskytnout.

3.3 Závazný pokyn policejního prezidenta č. 139/2012

Pro potřeby této bakalářské práce byl Útvarem zvláštních činností služby kriminální police a vyšetřování poskytnut Závazný pokyn policejního prezidenta č. 139/2012 o vyžadování odposlechu a záznamu telekomunikačního provozu a údajů o uskutečněném telekomunikačním provozu (dále jen „ZPPP“) ve zredukované formě. Tímto ZPPP se policisté řídí při získávání provozních a lokalizačních údajů. V následující části bude podrobně tento dokument prozkoumán.

V **článku 1** se uvádí, že odposlech a záznam telekomunikačního provozu (dále jen „odposlech“) a zjišťování údajů o uskutečněném telekomunikačním provozu pro potřeby celé Policie České republiky (dále jen „policie“) provádí Útvar zvláštních činností služby kriminální policie a vyšetřování (dále jen „útvar zvláštních činností“). V praxi to tedy znamená, že všechny žádosti o výpis provozních a lokalizačních údajů by měly být směrovány přes útvar zvláštních činností.

Článek 2 se zabývá výkladem pojmů. Pro účely tohoto závazného pokynu se rozumí

a) úkonem odposlech nebo výpis,

[29] z.č. 154/1994 Sb., Zákon o Bezpečnostní informační službě, ve znění pozdějších předpisů
[30] z.č. 289/2005 Sb., Zákon o Vojenském zpravodajství, ve znění pozdějších předpisů

b) objektem úkonu objekt, ke kterému se úkon vztahuje (telekomunikační zařízení identifikované účastnickým telefonním číslem, e-mailovou adresou, IP adresou apod.),
c) oprávněným subjektem je policejní orgán nebo Útvar speciálních činností služby kriminální policie a vyšetřování,
d) oprávněným žadatelem je příslušní policie (dále jen „policista“), zařazený v oprávněném subjektu a pověřený prováděním úkonů v trestním řízení, v jehož rámci je úkon vyžadován, nebo policista, který poskytuje zvláštní ochranu a pomoc svědkům a dalším osobám, zařazený v Útvaru speciálních činností služby kriminální policie a vyšetřování,
e) specializovaným pracovištěm je organizační článek útvaru zvláštních činností, který provádí nebo technicky zabezpečuje odposlech a výpis,
f) určeným policistou je vedoucí policista specializovaného pracoviště nebo jím pověřený policista, který projednává a přijímá žádost o odposlech nebo výpis (dále jen „žádost“)
g) uživatelem je osoba, která využívá objekt úkonu,
h) účastník je osoba, která o využívání objektu úkonu uzavřela smlouvu s poskytovatelem služeb elektronických komunikací,
i) záznamem je informace získaná odposlechem a předávaná oprávněnému subjektu v průběhu odposlechu za účelem průběžného vyhodnocování; záznam není určen k použití jako důkaz v trestním řízení,
j) archivním záznamem je informace získaná odposlechem, u které je možné garantovat úplnost a autentičnost a která se předává oprávněnému subjektu zpravidla po ukončení úkonu v otevřené podobě na nepřepisovatelném paměťovém médiu,
k) doprovodnými daty je pak záznam údajů o uskutečněné komunikaci obsahující provozní a lokalizační údaje, avšak nikoliv obsah komunikace,
l) záznamem obsahu komunikace je obsah přenášených zpráv; záznamem obsahu komunikace může být
    1. Zvukový záznam – soubor obsahující nahrávku hovoru při odposlechu hlasové služby,
    2. SMS – zpráva v textovém formátu předávaná zpravidla zároveň s doprovodnými daty hlasové služby,

3. Záznam datové komunikace – soubor obsahující přenášenou zprávu u datových služeb (e-mail, chat, http, ftp, MMS, fax atd.)

m) výpisem je záznam údajů o uskutečněném telekomunikačním provozu obsahující provozní a lokalizační údaje, avšak nikoliv obsah komunikace; na rozdíl od doprovodných dat se nezískává v reálném čase, nýbrž dodatečným vyžádáním od poskytovatele služeb elektronických komunikací zpravidla v elektronické podobě; pokud není opatřen elektronickým podpisem, není určen k použití jako důkaz v trestním řízení,

n) výpisem hlasové komunikace je výpis údajů z hlasových služeb; specializované pracoviště jej konvertuje do formátu potřebného pro zpracování v informačním systému „Poznatkový analytický fond“,

o) výpisem datové komunikace je výpis údajů z datových služeb; specializované pracoviště k němu zpravidla doplňuje přílohu s interpretací těchto údajů,

p) autorizací výpisu je ověření výpisu poskytovatelem služeb elektronických komunikací; vyžádá se k výpisu již poskytnutému v elektronické podobě bez elektronického podpisu, pokud vznikne potřeba využití výpisu jako důkazu v trestním řízení,

q) koncovým bodem je počítač určený pro příjem dat z odposlechu

r) databázovým koncovým bodem je počítač s nainstalovaným databázovým prostředím určený přednostně pro příjem doprovodných dat v databázovém formátu, případně i pro příjem záznamu obsahu komunikace.

V **článku 3** je následně popsán postup při vyžadování úkonu. Provedení úkonu může oprávněný subjekt vyžadovat výhradně u specializovaného pracoviště. Úkon může vyžadovat pouze oprávněný žadatel a při vyžadování úkonu je třeba předložit:

a) schválenou žádost a příkaz k úkonu (dále jen „příkaz“) vydaný soudcem příslušného soudu (dále jen „soudce“); žádost obsahuje náležitosti stanovené pro příkaz právním předpisem, nebo

b) v případě odposlechu, pokud není vydán příkaz podle písmene a)
   1. Schválenou žádost o odposlech

2. Příkaz oprávněného subjektu
3. Souhlas uživatele

c) V případě výpisu, pokud není vydán příkaz podle písmene a)
   1. Schválenou žádost o výpis
   2. Souhlas uživatele

Všechny vzory žádostí, příkazů či souhlasů uživatele jsou pak uvedeny v příloze samotného ZPPP.

Článek 4 se zabývá žádostmi a všemi náležitostmi, které samotná žádost musí mít.

1) Žádost o odposlech podle čl. 3 odst. 3 písm. a) se označí stupněm utajení VYHRAZENÉ způsobem stanoveným právním předpisem[31], případně vyšším stupněm utajení, pokud to z jejího obsahu vyplývá[32]. Na žádost o výpis podle čl. 3 odst. 3 písm. a) se uveden označení „Pro vnitřní potřebu“[33], popřípadě se označí stupněm utajené VYHRAZENÉ způsobem stanoveným právním předpisem[31], pokud to z jejího obsahu vyplývá[32].
2) Na žádost o odposlech a příkaz podle čl. 3 odst. 3 písm. b) bodů 1 a 2 se uvede označení „Pro vnitřní potřebu“[33], popřípadě se označí stupněm utajení VYHRAZENÉ způsobem stanoveným právním předpisem[31], pokud to z jejich obsahu vyplývá[32]. Na souhlas uživatele podle čl. 3 odst. 3 písm. b) bodu 3 se uvede označení „Pro vnitřní potřebu“[33].
3) Na dokumenty podle čl. 3 odst. 3 písm. c) se uvede označení „Pro vnitřní potřebu“[33]
4) V žádosti musí být přesně formulován požadavek, zejména jednoznačně identifikován účel úkonu, jeho uživatel a účastník, pokud je možné jejich totožnosti zjistit.

[31] Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací.
[32] Bod 9 přílohy č. 1 k nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací.
[33] Čl. 18 odst. 4 ZPPP č. 222/2011, kterým vydává spisový řád Policie České republiky.

5) Oprávněný žadatel je povinen v případě úkonu týkajícího se hlasové komunikace učinit elektronickou cestou u útvaru zvláštních činností dotaz za účelem zjištění účastníka[34]; v případě úkonu týkajícího se datové komunikace se toto zjištění provádí v rámci předběžného projednání podle čl. 5. Nebude-li znám výsledek dotazu, bude k žádosti připojena kopie dotazu učiněného cestou specializovaného pracoviště poskytovateli služeb.
6) Žádost se vyhotovuje v příslušném počtu výtisků pro potřebu
a) Specializovaného pracoviště
b) Oprávněného žadatele
7) Oprávněný žadatel musí být přítomen podepsání souhlasu a potvrdit v něm pravost podpisu uživatele. Nemůže-li uživatel vyjádřit svůj souhlas podpisem, je nutné zajistit podpis další osoby, která byla udělení souhlasu přítomna.
8) Žádost o odposlech a žádost o výpis podle čl. 3 odst. 3 písm. a) předkládá oprávněný žadatel soudci cestou příslušného státního zástupce.
9) Přílohou žádosti o výpis hlasové komunikace je protokol o předávání dat elektronickou poštou. Oprávněný žadatel zde uvede elektronickou adresu a heslo k zašifrování odpovědi.
10) Přílohou žádosti o výpis datové komunikace je protokol o předávání dat.

Vzory žádostí jsou opět uvedeny v příloze ZPPP.

Předběžným projednáním žádosti se pak zabývá **článek 5**.

1) Žádost je oprávněný žadatel před jejím schválením povinen projednat s určeným policistou.
2) Určený policista žádost posoudí a rozhodne, zda je úkon v požadovaném rozsahu a termínu proveditelný. Při rozhodování přihlédne zejména k technickým, operativním a kapacitním možnostem specializovaného pracoviště. Po dohodě s oprávněným subjektem

[34] ZPPP č. 138/2008 o informačním systému TELEFONY

stanoví nutný podíl oprávněného subjektu na přípravě a provádění úkonu.

3) Dojde-li specializované pracoviště k závěru, že úkon nelze provést, oznámí tuto skutečnost oprávněnému subjektu a dohodne s ním další postup.
4) Své rozhodnutí podle předchozího odstavce vyznačí určený policista na všech výtiscích žádosti.
5) Při souběhu více žádostí, které nelze z kapacitních důvodů zajistit, konzultuje určený policista s oprávněnými subjekty možnost jiného termínu provedení. Nedojde-li k dohodě, rozhodne o prioritě nebližší společný nadřízený souběžně žádajících oprávněných žadatelů po projednání se všemi dotčenými orgány činnými v trestním řízení.

Článek 6 je zaměřen na schvalování žádosti.

1) Žádost o odposlech, kterou předkládá oprávněný žadatel zařazený
a) ve službě kriminální policie a vyšetřování
   1. doporučuje jeho přímý nadřízený,
   2. schvaluje vedoucí policista ustanovený na služebním místě v řídící úrovni[35]

není-li dále stanoveno jinak,

b) v Úřadu dokumentace a vyšetřování zločinů komunismu služby kriminální policie a vyšetřování,
   1. doporučuje jeho přímý nadřízený,
   2. schvaluje ředitel tohoto útvaru.
2) Žádost o výpis, kterou předkládá oprávněný žadatel,
   a) doporučuje jeho přímý nadřízený,
   b) schvaluje vedoucí policista ustanovený na služebním místě v řídící úrovni[35] vedoucího odboru.

[35] Část šestá ZPPP č. 40/2009

3) Vedoucí policista, který žádost doporučuje, je povinen podle jemu dostupných dokumentů[36] ověřit způsob (zdroj) získání údajů o objektu úkonu.
4) Žádost je oprávněn schválit i příslušný přímý nadřízený vedoucího policisty uvedeného v odstavci 1 písm. a) bodu 2, písm. b) bodu 2 a v odstavci 2 písm. b). Je-li vedoucí policista ustanovený na služebním místě v řídící úrovni vedoucího odboru přímým nadřízeným oprávněného žadatele, žádost doporučuje tento vedoucí policista a schvaluje ji jeho přímý nadřízený.
5) Vedoucí policista, který žádost schvaluje, odpovídá za její řádné vyplnění, odůvodnění a soulad s právními předpisy.

V **článku 7** je pak uvedeno, že v případě, že projednanou žádost vedoucí policista neschválí, státní zástupce nenavrhne nebo soudce odmítne vydat příkaz nebo pokud ještě před zahájením pominou důvody úkonu, je oprávněný žadatel povinen o těchto skutečnostech neprodleně písemně informovat specializované pracoviště.

Článek 8 byl celý zredukovaný a pro potřeby této bakalářské práce nemůže být použit. **Články 9-14** se pak zabývají pouze odposlechy. Ty byly v této práci zmíněny pouze okrajově, a proto není potřeba jednotlivé články z tohoto ZPPP zmiňovat.

Článek 15 se následně zabývá tím, jak správně nakládat s výpisy. První dva odstavce je zredukované, ve třetím je pak uvedeno, že pokud bylo dohodnuto osobní převzetí výpisů, je oprávněný žadatel povinen tyto výpisy vyzvednout do 7 dnů od zaslání výzvy specializovaným pracovištěm k jejich převzetí.

Pokud nebyly při nakládání s výpisem zjištěni skutečnosti významné pro trestní řízení se přiměřeně použije postup pro nakládání se záznamy, stanovený právním předpisem[37].

[36] Čl. 2 odst. 1 písm. f) ZPPP č. 222/2011
[37] ust. § 88 odst. 7 zákona č. 141/1961 Sb.

Článek 16 říká, že archivní záznam může být použit v trestním řízení jako důkaz. V takovém případě zpracuje specializované pracoviště na požádání protokol k archivnímu záznamu.

Policisté a zaměstnanci policie zařazení v oprávněném subjektu a ve specializovaném pracovišti odpovídají za ochranu informací získaných prováděným úkonem a dalších souvisejících informací před vyzrazením a zneužitím. Toto říká **článek 17**.

Z výše uvedeného je jasně vidět, že ZPPP plní funkci podrobného popisu toho, jak postupovat při získávání nejen provozních a lokalizačních údajů, ale také například odposlechů. Co se týče odposlechů, tak těm je v tomto dokumentu věnováno více času než samotným provozním a lokalizačním údajům.

Co však v závazném pokynu zmíněno není, je pak postup při zajišťování dat pohřešované nebo hledané osoby. V tomto případě je důležité, aby tato data byla zajištěna v co nejrychlejší možné době. Nedokážu si proto představit, že policista sepisuje formulář, který následně odesílá na místně příslušné pracoviště Útvaru zvláštních činností, a to následně žádost posuzuje, zkoumá a odesílá dále. Pokud je postup pro tyto situace popsán jinde, myslím si, že by měl být spíše zakomponován do tohoto ZPPP.

3.4 Žádosti oprávněných orgánů

Žádostmi oprávněných orgánů se zabývá Český telekomunikační úřad[38](dále jen „ČTÚ“). Ten na svých webových stránkách každoročně uvádí tiskové zprávy, ve kterých jsou uvedeny statistiky o výkazu o poskytnutých provozních a lokalizačních údajích. Poslední tisková zpráva tohoto typu byla však vydána v roce 2018 a to z důvodu, že povinnost sběru a zpracování provozních a lokalizačních údajů byla zrušena v předchozím znění zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů.

[38] Český telekomunikační úřad je ústřední správní úřad České republiky pro výkon státní správy ve věcech stanovených zákonem, včetně regulace trhu a stanovování podmínek pro podnikání v oblasti elektronických komunikací a poštovních služeb.

ČTÚ ve svých statistikách zmiňuje jak počty případů poskytnutých údajů, tak i počty případů, kdy údaje nebyly poskytnuty. Dále pak jsou statistiky rozděleny na veřejné pevné sítě, veřejné mobilní sítě, služby přístupu ke schránkám pošty a sítím el. komunikací s přepojováním paketů, IP telefonie[39] a služby přenosu zpráv elektronické pošty prostřednictvím sítí elektronických komunikací s přepojováním paketů.

V následujících tabulkách bude popsán trend při žádostech o provozní a lokalizační údaje.

Tabulka 1: Počty uznaných žádostí

	2012	2013	2014	2015	2016	2017	2018
VEŘEJNÉ PEVNÉ SÍTĚ	22477	19730	11861	6616	6299	6379	6818
VEŘEJNÉ MOBILNÍ SÍTĚ	30842	173087	214705	219070	214522	253380	332892
SLUŽBY PŘÍSTUPU KE SCHRÁNKÁM	706	583	695	525	5661	7089	8747
IP TELEFONIE	2283	2035	3019	3668	2381	2068	1892
SLUŽBY PŘENOSU ZPRÁV EL. POŠTY	27	69	63	245	426	263	228

Zdroj: vlastní zpracování

Z tabulky vyplývá, že co se týče žádostí provozních a lokalizačních údajů ve veřejné mobilní síti, jejich počet každoročně roste. Zatímco v roce 2012 bylo těchto žádostí jen 30 842, v roce 2018 jich bylo již 332 892. Asi nejvýraznější skok je zaznamenán mezi roky 2012 a 2013 a to proto, že v roce 2011 byla nálezem Ústavního soudu dočasně zrušena povinnost podnikatelských subjektů uchovávat provozní a lokalizační údaje. Zatímco u veřejné pevné sítě je trend zhruba opačný,

[39] IP telefonie je přenos hlasu po datových sítích a hlasová informace je přenášena prostřednictvím komunikačních sítí založených na přenosu dat na základě protokolu IP (Internet Protocol). Tento univerzální přenosový protokol je určen primárně pro datové sítě a na jeho principu funguje celosvětová síť Internet. Hlas je přenášen v jedné síti společně s dalšími datovými informacemi (např. emaily). IP protokol zajišťuje přenášení datových paketů od odesílatele k příjemci.

kdy v roce 2012 bylo vyhověno 22 477 žádostem a v roce 2018 jen 6818 žádostem.

Nabízí se zde srovnání s počtem trestných činů a počtem žádostí, kterým bylo vyhověno, bohužel toto srovnání by bylo z několika důvodů nepřesné a nevypovídající. První důvod je ten, že žádosti se neomezují pouze na žádosti od Policie České republiky, ale jsou zde zahrnuty všechny oprávněné orgány. Není tak možné z těchto statistik zjistit přesný počet žádostí PČR. Druhý důvod je ten, že k jednomu trestnému činu je možno žádat o provozní a lokalizační údaje k více telefonním přístrojům. Ani tato statistika zde není zahrnuta.

Následující tabulka ukazuje počty případů, kdy údaje nebyly poskytnuty.

Tabulka 2: Počet zamítnutých žádostí

	2012	2013	2014	2015	2016	2017	2018
VEŘEJNÉ PEVNÉ SÍTĚ	1104	597	679	548	349	540	524
VEŘEJNÉ MOBILNÍ SÍTĚ	9161	2437	3040	2826	4461	5822	6259
SLUŽBY PŘÍSTUPU KE SCHRÁNKÁM	1028	22	437	74	137	52	208
IP TELEFONIE	19	259	105	44	19	10	13
SLUŽBY PŘÍSTUPU ZPRÁV EL. POŠTY	4	3	2	11	27	26	8

Zdroj: vlastní zpracování

Když se opět zaměříme na počet žádostí ve veřejných mobilních sítích, uvidíme zde stejný trend jako u počtu případů, kdy bylo žádostem vyhověno, tedy počet zamítnutých žádostí od roku 2013 každoročně roste. ČTÚ neuvádí důvody zamítnutí jednotlivých žádostí. Nevíme tak, jaké procento bylo zamítnuto například kvůli špatně vyplněné žádosti nebo kvůli právním aspektům dané žádosti.

O počtu žádostí po roce 2018 můžeme pouze spekulovat, pokud by však měl růst pokračovat v nastoleném trendu z posledních let, umím si představit, že jen u veřejných mobilních sítích by se mohlo číslo žádostí pohybovat kolem půl milionu. Otázkou také je, jaký vliv měla na statistiku pandemie koronaviru Covid-19.

4 DATA RETENTION A COVID-19

Šíření nového koronaviru COVID-19 a jeho rychlá eskalace v pandemii v prvních měsících roku 2020 představuje první skutečně velkou, rozšířenou globální zdravotní krizi informačního věku. Ostatní ohniska onemocnění v předchozích desetiletích byla buď malá a relativně lokalizovaná (jako například SARS[40] v roce 2003, MERS[41] v roce 2012 a propuknutí Eboly v západní Africe od roku 2013 a viru Zika v Brazílii v roce 2015), nebo v případě H1N1[42] z roku 2009 epidemie prasečí chřipky, která měla nižší míru infekce a úmrtnosti, než se původně predikovalo.

Včasná analýza nemoci COVID-19 pomocí rámce pro hodnocení pandemické závažnosti CDC[43] naznačuje, že probíhající pandemie byla co do závažnosti více srovnatelná se španělskou chřipkou z roku 1918 než s jakýmkoli novějším propuknutím choroby a je to zdaleka nejzávažnější taková událost, k níž došlo za desetiletí od zavedení a širokého přijetí informačních technologií a síťových spotřebitelských zařízení. V důsledku toho se politická reakce na COVID-19 v mnoha zemích účinně stala testovacím místem pro životaschopnost a účinnost přístupů, které využívají informační a komunikační technologie[44] (dále jen „ICT“) k umožnění nebo zlepšení různých aspektů poskytování a zacílení veřejného zdraví.

Role, kterou hrají ICT, digitální zařízení a platformy v pandemii COVID-19, bude důležitým tématem pro studium po mnoho nadcházejících let, protože existuje jen málo aspektů této pandemie a reakcí veřejného a soukromého sektoru na ni, které nebyly hluboce ovlivněny digitální technologií. Technologie práce na dálku umožnila některým částem ekonomiky, včetně velké části akademického výzkumu, pokračovat ve fungování i přes jinak rozsáhlé odstávky na národní

[40] SARS (z angl. Severe Acute Respiratory Syndrome, česky těžký akutní respirační syndrom) je virové onemocnění dýchacích cest způsobené koronavirem SARS-CoV.
[41] MERS (Middle East Respiratory Syndrome) je příbuzný viru SARS.
[42] H1N1 (prasečí chřipka) je respirační onemocnění způsobené chřipkovým virem kmene A/H1N1.
[43] Centers for Disease Control and Prevention (zkratka CDC, česky Střediska pro kontrolu a prevenci nemocí) je národní institut Spojených států amerických pro veřejné zdraví.
[44] Informační a komunikační technologie, zkráceně ICT, zahrnují veškeré informační technologie používané pro komunikaci a informatiku.

a regionální úrovni. Platformy digitální komunikace a sociálních médií hrály roli při podpoře duševního zdraví občanů a udržování jejich sociálních a rodinných vztahů prostřednictvím dlouhých období sociálního odstupu a izolace, ale také se staly bojištěm pro konkurenční úhly pohledu na pandemii, kdy zdravotnické úřady a odborníci často bojují o výsluní s konspiračními teoriemi a nepravdivými nebo zastaralými informacemi.

Jak se občané snažili porozumět postupu pandemie, datoví vědci pracující v různých organizacích vedli úsilí shromáždit a ověřit údaje o infekci, testování a úmrtnosti a zpřístupnit je veřejnosti online pomocí efektivní vizualizace dat. Každá z výzev, příležitostí, silných a slabých stránek spojených s těmito rolemi ICT v reakci na COVID-19 bezpochyby urychlí vznik významné vědecké literatury v nadcházejících měsících a letech. Snad nejvýznamnější rolí ICT v pandemii a rozhodně jednou z nejkontroverznějších a nejspornějších i v této rané fázi bylo experimentální přijetí digitálního sledování kontaktů a upozornění na kontakt s infikovanou osobou pomocí osobních digitálních zařízení občanů, jako jsou chytré telefony. Sledování jejich fyzického pohybu a interakce s ostatními občany, což umožňuje samotným občanům nebo lékařským orgánům být informováni o tom, jestli přišli do kontaktu s infikovanými osobami.

4.1 Sledování kontaktů a digitální technologie

Sledování kontaktů samo o sobě není nic nového. Je to dobře zavedená součást reakce na jakékoliv propuknutí nakažlivé nemoci. V rozhovoru pro média z dubna 2020 popsal ředitel CDC Robert Redfield[45] „velmi agresivní“ sledování kontaktů infikovaných jedinců jako zásadní krok v tom, jak dostat COVID-19 pod kontrolu, ale i když poznamenal, že technologická řešení za účelem zlepšení sledování kontaktů byla teprve hodnocena, jeho pozornost byla zaměřena na tradičnější a nesmírně pracně náročnou formu sledování kontaktů. Ta vyžaduje, aby velký počet terénních pracovníků v oblasti veřejného zdraví kontaktoval rodinu, přátele,

[45] Robert Ray Redfield Jr. (nar. 10.6.1951), virolog, ředitel CDC v letech 2018-2021.

spolupracovníky a další kontakty infikovaných jedinců, zajistil jejich otestování nebo umístění do karantény.

Pro pandemii rozsahu COVID-19 by i středně velká země mohla vyžadovat desítky tisíc terénních pracovníků na plný úvazek, aby tímto způsobem provozovali komplexní program pro vyhledávání kontaktů. Proto bylo zapotřebí aby se velké množství pozornosti a zdrojů zaměřilo na hledání způsobů, jak využít digitální technologie k automatizaci významných částí tohoto procesu. A to s využitím skutečnosti, že většina občanů ve vyspělých zemích (a velký počet v rozvojových zemích) nosí u sebe chytré telefony, které mají integrované GPS čipy schopné přesného sledování polohy, rádia Bluetooth, která dokáží snímat blízkost mezi zařízeními a neustálé připojení k internetu. Digitální sledování kontaktů se snaží využít tuto funkci k přeměně vlastních chytrých telefonů občanů na zařízení pro sledování kontaktů. Hypotetické výhody tohoto přístupu jsou značné. V ideální světové situaci by to umožnilo rozšířit sledování kontaktů na celou populaci země, nikoli pouze na podskupinu infikovaných jedinců, sledovalo by jejich pohyb a sociální kontakty s velmi vysokou mírou přesnosti a bylo by rychlejší, efektivnější a méně pracné a náchylné k lidským chybám než stávající přístupy.

Zatímco základní cíl aplikací pro sledování digitálních kontaktů je relativně přímočarý, různé země zaujaly zcela odlišné přístupy k vývoji, zavádění a fungování takových aplikací. Zpočátku byla tato divergence z velké části pouze aspektem obecnějšího dílčího přístupu k reakci na COVID-19 mezi národy. Do poloviny března 2020 byly vyvinuty a nezávisle spuštěny aplikace pro sledování kontaktů úřady v Izraeli, Singapuru, Jižní Koreji, Tchaj-wanu, Thajsku a Vietnamu, což předcházelo oznámení prodejců chytrých telefonů Google (Android) a Apple (iOS) z 10. dubna 2020, že společně pracují na jednotné softwarové struktuře pro sledování kontaktů, která bude zabudována přímo do operačních systémů telefonů poháněných jejich softwarem. I poté, co Google a Apple zpřístupnily svá řešení, však mnoho zemí pokračovalo ve vývoji vlastních aplikací pro sledování kontaktů, které by zcela obešly softwarovou strukturu Google / Apple. To odhalilo, že rané snahy o vývoj aplikací pro sledování kontaktů trpěly nedostatkem jakéhokoli koherentního, centralizovaného řešení a existoval také zásadní rozdíl

v postojích různých zemí a korporací k tomu, jak by tyto aplikace měly fungovat, a co je nejdůležitější, kdo by měl mít přístup k datům, která vytvářejí.

To vyvolalo to, co zdánlivě vypadá jako přímočarý a pozitivní technologický pokrok, který má pomoci omezit šíření smrtelné nemoci v souvislosti s bouřlivým a těžce bojovaným sporem o práva občanů na jejich vlastní digitální data, online soukromí a sledování v informačním věku.

Zatímco ještě před několika lety mohla být tato debata poněkud abstraktní debatou, která se z velké části odehrávala v řídkém ovzduší akademické půdy nebo na půdě veřejné politiky, bylo to množství velkých skandálů ohledně nezákonného používání digitálních dat občanů společnostmi, jako je Cambridge Analytica[46], které eskalovaly obavy z digitálního sledování a špionáže, zejména ze strany autoritářských vlád. Také docházelo k vysoce sledovaným střetům mezi politiky a veřejnými činiteli a provozovateli sociálních sítí, jako jsou Facebook a Twitter. Toto posunulo debaty do veřejné sféry. Hluboká propast mezi různými filozofiemi ohledně sledování digitálních kontaktů, sdílení dat a soukromí uživatelů jsou proto všechno, jen ne abstraktní, jsou odrazem problémů reálného světa, které mají potenciál hluboce ovlivnit účinnost a úspěch technologie. Účinnost a úspěch, které budou v tomto případě nakonec měřeny zachráněnými nebo ztracenými životy.

4.2 Data nebo soukromí?

Mezi národy a korporacemi existuje mnoho odlišných přístupů ke sledování kontaktů. Možná nejvýraznější z nich je předěl mezi přístupy „data na prvním místě“, které upřednostňují uchovávání údajů ze sledování a jejich dostupnost zdravotnickým úřadům a přístupy „na prvním místě na ochrana soukromí“, které zdůrazňují kontrolu občanů nad jejich vlastními údaji a snaží se poskytnout účinný

[46] Cambridge Analytica LLC byla britskou poradenskou společnostní, která při své práci kombinovala data mining, datové makléřství a datovou analýzu se strategickou komunikací ve volebním procesu. Společnost vznikla v roce 2013 a od počátku svého vzniku byla zaměřena na volby v USA. Svou činnost ukončila v roce 2018 po skandálu kolem nakládání s údaji uživatelů Facebooku.

stupeň sledování kontaktů, aniž by úřady odhalovaly pohyby a interakce identifikovatelných jedinců.

Z pohledu správy dat, první přístup (data-first) obecně zahrnuje přiřazení stabilního identifikátoru každému jednotlivci (nebo zařízení chytrého telefonu) a přenos některých nebo všech podrobností o jejich pohybu a kontaktech na centrální server, kde k nim lze přistupovat a analyzovat je. Druhý přístup (privacy-first) naproti tomu používá dynamické identifikátory pro jednotlivce, které se pravidelně mění, a ukládá jejich kontaktní interakce kryptograficky bezpečným způsobem na jejich místní zařízení, přičemž na centralizovaném serveru uchovává jen málo nebo žádná data.

Nejzákladnější úroveň funkčnosti, kterou tyto dva přístupy umožňují, je stejná – výstraha může být vydána napříč sítí, když je jedinec pozitivně testován na COVID-19, a to buď zdravotnickými úřady, které výstrahu přímo vydávají, nebo tím, že jednotlivec zadá specifický kód. na jejich zařízení. Toto upozornění informuje každého, kdo byl v kontaktu s infikovanou osobou, že mohl být vystaven viru. Kromě této základní úrovně funkčnosti však mezi těmito dvěma přístupy existuje obrovský rozdíl. Přístup „data-first“ potenciálně umožňuje zdravotnickým úřadům přímo identifikovat a kontaktovat osoby, které se dostaly do kontaktu s virem, zatímco přístup založený na ochraně soukromí jednotlivce neidentifikuje a umožňuje jim pouze být informováni na jejich chytrých telefonech, přičemž odpovědnost za kontaktování zdravotnického úřadu nebo podrobení se testu ponechává samotné osobě.

Přístup „data first“ také obvykle zahrnuje údaje o poloze GPS spolu s protokolem interakce kontaktů, což umožňuje zdravotnickým orgánům lokalizovat konkrétní místa, kde se vyskytly shluky infekcí, což není možné s přístupem „privacy first“. Ačkoliv teoreticky tento přístup bude stále informovat lidi potenciálně vystavené shluku infekcí, i když jim neřekne, kde se shluk objevil nebo od koho mohla být infekce přenesena. A konečně, přístup data-first generuje velké množství dat o pohybu a kontaktech mezi jednotlivci a o tom, jak souvisí s šířením viru v populaci, což z něj dělá potenciálně neocenitelný zdroj pro epidemiology a datové vědce zkoumající jak konkrétně virus COVID-19, tak obecně mechanismy epidemií.

Je důležité poznamenat, že zde popsané přístupy ke sledování digitálních kontaktů nejsou binárními protiklady, ale představují spíše extrémy spektra různých přístupů k problému. Různé přístupy vyvinuté různými vládami a korporacemi pokrývají širokou škálu možného spektra. Zejména Jižní Korea zaujala dramaticky „otevřený“ přístup založený na datech, kombinující úsilí o sledování lidského kontaktu a digitálních dat, včetně polohy GPS, se používá k vytvoření „cestovního deníku pacientů s virem“, který je v částečně redukované podobě k dispozici veřejnosti.

Singapurský systém sledování kontaktů sdílí méně osobních informací o infikovaných jednotlivcích, ale vláda udržuje veřejně přístupnou mapu s podrobnostmi o každém případu, což zvyšuje riziko, že jednotlivci budou správně nebo nesprávně identifikováni jako přenašeči viru. Spojené království, Francie a Austrálie, mezi mnoha dalšími národy, preferují přístup založený na datech, který se vyhýbá sdílení shromážděných údajů s veřejností, ale přesto je zpřístupňuje zdravotnickým orgánům. I když i zde existují rozdíly, přičemž některé země chtějí sdílet data s výzkumníky a dalšími zainteresovanými stranami, zatímco jiní ustanovují právní rámce zakazující přístup k datům i v případě soudních příkazů.

Softwarové struktury vyvinuté společnostmi Google a Apple, které z velké části staví na myšlence vytvořené protokolem Decentralized Privacy-Preserving Proximity Tracing (DP-3T) a jsou implementovány v zemích včetně Německa, Itálie, Japonska a mnoha států USA, mezitím spadají silně do oblasti ochrany soukromí, nevytvářejí žádný přístupný archiv kontaktních nebo lokalizačních údajů a zcela skrývají identity uživatelů.

Rozdělení těchto přístupů napříč zeměmi závisí na řadě složitých faktorů. I když je lákavé hledat jedinou vysvětlující proměnnou, jako je míra politické svobody země, je pozoruhodné, že „data first“ přístupy přijaly liberální demokracie, jako je Jižní Korea a Tchaj-wan, stejně jako autoritářské státy, jako je Čína, Írán a Katar, zatímco Francie a Spojené království se tomuto přístupu bránily. Zejména Asie nabízí nejrozmanitější soubor „data first“ a „privacy first“ zemí. Kromě jiných faktorů musíme myslet na předchozí zkušenosti těchto zemí se SARS a MERS a stupněm jejich demokratizace.

Složitost vytvořená těmito velmi odlišnými vnitrostátními přístupy ke sledování digitálních kontaktů byla dále prohloubena velmi krátkým časovým obdobím, ve kterém se pandemie COVID-19 objevila, což znamenalo, že fakta na místě byla velmi proměnlivá a osvědčené postupy se rychle změnily, pokud vůbec existovaly. Některé velké národy byly nuceny zcela změnit svůj přístup. Německo zpočátku upřednostňovalo „data first“, ale později se zcela posunulo k přístupu „privacy first“.

Spousta zemí se následně potýkalo s technickými obtížemi se svými aplikacemi, kdy například ve Spojeném království začali vyvíjet úplně novou aplikaci. Velkým problémem pak bylo to, že tyto aplikace spotřebovávaly velké množství energie telefon, a proto je uživatelé ve velkém začali buď vypínat, nebo ze svých telefonů mazat.

4.3 Rizika nadměrného shromažďování dat

Vzhledem k tlaku, který vyvíjely společnosti Google a Apple, když přijaly přístup silně zaměřený na ochranu soukromí, a ke změnám, které byly provedeny v přístupech zemí jako Německo, Spojené království a Austrálie poté, co se setkaly s řadou potíží s jejich původním přístupem založeným na sběru dat se zdá jasné, že směr pohybu pro sledování digitálních kontaktů směřuje k modelu na prvním místě soukromí. Ačkoli to obhájci soukromí a bezpečnosti uvítali, vyvolalo to znepokojení u některých výzkumníků a zdravotnických úřadů, kteří se obávají, že jejich neschopnost získat přístup k lokalizačním datům a určit původ shluků infekcí výrazně sníží užitečnost sledování kontaktů.

Tento pohled se blíží konvenční moudrosti, která byla v posledních desetiletích rozšířena v mnoha oblastech vědy, zejména však v sociálních vědách a informační vědě. S rychlým pokrokem dosaženým od 90. let v oblasti datové vědy a nyní rozšířenou dostupností nástrojů pro ukládání, manipulaci a analýzu dříve nepředstavitelných objemů dat se mantrou mnoha výzkumníků a veřejných činitelů stalo, že nikdy nemůžete mít příliš mnoho dat. Toto je mantra sdílená se soukromým sektorem, kde velká část hodnoty společností jako Facebook, Google a Amazon ve skutečnosti spočívá v mimořádném množství dat, která mají o svých

uživatelích a zákaznících, oceánu jednotlivých datových bodů, které mohou být jednotlivě bezcenné, ale vyhodnocené algoritmy strojového učení a prozkoumávané z hlediska základních vzorců a korespondencí, může odhalit obrovské množství o chování jak jednotlivých uživatelů, tak komunit a společností jako celku.

Při tomto chápání se přístup k digitálnímu sledování kontaktů zaměřený na ochranu soukromí může jevit jako nesmírně plýtvání, protože se zbavuje (nebo jednoduše nikdy neshromažďuje) obrovského množství dat, která by mohla mít obrovskou hodnotu pro zlepšení protiopatření v oblasti veřejného zdraví proti COVID-19. stejně jako prohlubování našich znalostí epidemiologie a jejích příbuzných oborů.

Jakkoli to může být frustrující pro výzkumníky a zdravotnické úřady, když sledují zamykání a ničení této potenciální pokladnice dat, je důležité si uvědomit, že tato data jsou osobními údaji občanů a při zaznamenávání všech jejich kontaktních interakcí (a v některých případech všechny jejich pohyby) představuje pravděpodobně nejosobnější a nejintimnější údaje, které se kdy vláda snažila shromáždit o svých vlastních občanech. Je zcela nepřekvapivé, že by se to okamžitě dostalo do rozporu s obavami o soukromí, které ujišťování o důvěryhodnosti vládních agentur, omezení distribuce a používání údajů a technická opatření, jako je anonymizace identifikačních údajů, jen málo zmírnily.

Skandál Cambridge Analytica a rostoucí porozumění tomu, jak byly osobní údaje využívány v marketingových a volebních kampaních, byly milníky ve veřejném povědomí o digitálním soukromí, ale základní obavy nejsou nové.

Již na konci 90. let byly vyjádřeny obavy, kdy shromažďování velkého množství zdánlivě neškodných datových bodů mohlo vytvořit kombinovanou datovou sadu s překvapivým množstvím osobních informací, které lze snadno deanonymizovat a připojit ke konkrétnímu občanu. Od té doby se vyvinula rozsáhlá literatura o různých typech digitálního soukromí a metodách jeho ochrany, ale téma zůstává živým a stále více politicky zatíženým problémem. Mainstreamové veřejné diskurzy o digitálním soukromí ukázaly v posledních letech rostoucí míru podezíravosti, od relativně rozšířeného přesvědčení, že zařízení s digitálními

asistenty, jako je Amazon Alexa, mohou „špehovat“ konverzace svých uživatelů, až po široce rozšířenou negativitu ohledně sociálního a politického dopadu společnosti jako Facebook, které otevřeně shromažďují velké množství uživatelských dat.

Hlavním důsledkem toho pro sledování kontaktů COVID-19 je to, že přesvědčit občany, aby si tyto aplikace skutečně nainstalovali a používali, představuje významnou výzvu vzhledem k tomu, že úroveň povědomí o ochraně soukromí a osobních údajů je vyšší než kdy dříve. I když některé země jako Čína, Indie a Katar legálně nařídily používání aplikací.

Známé případy, kdy bylo sledování kontaktů zapojeno nebo zapleteno do porušení soukromí občanů, se již staly dobře známými, jako je potenciální „výjezd“ řady členů LGBT v Jižní Koreji (země s téměř žádnými zákonnými právy nebo ochranou pro LGBT lidí) poté, co došlo ke shluku případů COVID-19 v oblasti Soulu, která je známá svými LGBT bary a kluby, nebo tvrzení úředníka činného v trestním řízení v Minnesotě, že stát používá „sledování kontaktů“ k identifikaci spojení demonstrantů zatčených během květnové demonstrace Black Lives Matter. Tyto incidenty a jim podobné poslouží pouze k prohloubení obav mnoha občanů, že sledování shluků riskuje odhalování jejich soukromých informací způsoby, které by pro ně mohly být v konečném důsledku škodlivé.

Prvním cílem těchto aplikací, daleko před jakýmikoli obavami o uchovávání dat pro výzkumné účely nebo sekundárními cíli zdravotnických úřadů, musí být široké přijetí. Aplikace jsou z hlediska veřejného zdraví víceméně k ničemu, pokud je nenainstaluje a nepoužívá kritická masa občanů. První výzkum těchto systémů zjistil, že každá aplikace vyvolává velké množství otázek, například jak přesně fungují, jaká data ukládají a kde je ukládají, komu předávají informace a jaké mají uživatelé práva týkající se jejich vlastních informací v aplikaci. Ty jsou často špatně nebo nejasně zodpovězeny jak popisy v samotném softwaru, tak úřady odpovědnými za provoz systému. Tento nedostatek jasnosti a transparentnosti také nevyhnutelně povede k tomu, že občané nebudou v úsilí o sledování digitálních kontaktů dodržovat zásady.

COVID-19 tak slouží jako obtížná zkouška důvěry ve veřejné instituce na národní i mezinárodní úrovni. Jiskřička naděje v tom všem, možná ironicky, spočívá v tom, že mnoho občanů, přinejmenším v USA, má podle všeho relativně vysoký stupeň důvěry ve společnosti Google a Apple, což naznačuje, že důraz na jejich roli při vývoji sledování kontaktů a priorita, kterou kladli na soukromí uživatelů, by mohly pomoci zmírnit některé obavy, které byly vytvořeny nadměrným shromažďováním dat, zvýšit účast občanů v těchto systémech a v konečném důsledku zachránit životy.

ZÁVĚR

V této práci jsem prozkoumal problematiku Data retention. Cílem bylo, abych z dostupné literatury a zákonů vytvořil ucelený pohled na současnou problematiku daného tématu.

První kapitola má za úkol ustanovit co jsou provozní a lokalizační údaje a důvod jejich vzniku. Dále je v této kapitole věnován čas předchůdci provozních a lokalizačních údajů, kterým je listovní tajemství. V něm se čtenář dozví, co to je listovní tajemství, jaký je předmět a subjekt listovního tajemství a také v jakých zákonech je listovní tajemství ukotveno. Následně je práce zaměřena na historii a současnou situaci provozních a lokalizačních údajů v České republice a Evropské unii.

Druhá kapitola je pak zaměřena na samotné právní aspekty provozních a lokalizačních údajů. Je zde uvedeno, jaké subjekty mají povinnost data uchovávat a po jakou dobu. Také jsou zde uvedeny oprávněné orgány, které smějí provozní a lokalizační údaje vyžadovat a za jakých podmínek.

Ve třetí kapitole se pak práce zaměřuje na samotnou praxi při získávání provozních a lokalizačních údajů. Hlavním bodem této kapitoly je pak Závazný pokyn policejního prezidenta č. 139/2012, který byl pro účely této bakalářské práce zredukován a poskytnut Útvarem zvláštních činností. V samotném závazném pokynu se čtenář dozví přesný postup policisty a policejního orgánu při získávání provozních a lokalizačních údajů. Pro představu o tom, kolik žádostí ročně oprávněné orgány podají jsou zde také uvedeny tabulky s těmito statistikami. Tyto statistiky jsou uvedeny v podkapitole 3.4.

V poslední, čtvrté kapitole, je pak prozkoumáno asi nejaktuálnější téma v oblasti data retention a to je shromažďování dat v době epidemie Covidu-19. Je zde prozkoumána celosvětová situace s příklady konkrétních států. Asi nejdůležitějším aspektem této kapitoly je pak otázka toho, jestli jsou důležitější data, nebo soukromí občanů a také se následně zabývá riziky nadměrného shromažďování dat.

Tato práce je kombinací právních aspektů provozních a lokalizačních údajů a také praxe při jejich získávání a následná využitelnost pro Policii České republiky.

LITERATURA

MONOGRAFIE

MYŠKA, Matěj, ed. *Data Retention Reloaded: zkušenosti, problémy a aplikační praxe: sborník z workshopu konaného dne 23.4.2013 v Brně.* Brno: Masarykova univerzita, 2013. ISBN isbn978-80-210-6722-6.

PRÁVNÍ NORMY

Zákon č. 273/2008 Sb., o Policii ČR, znění účinné ke dni 1.1.2022

Zákon č. 127/2005 Sb., o elektronických komunikacích v posledním znění

Zákon č. 262/2006 Sb., zákoník práce v posledním znění

Zákon č. 169/1999 Sb., o výkonu trestu odnětí svobody v posledním znění

Zákon č. 293/1993 Sb., o výkonu vazby v posledním znění

Zákon č. 150/2001 Sb., o Vojenském zpravodajství v posledním znění

Zákon č. 29/2000 Sb., o poštovních službách v posledním znění

Zákon č. 89/2012 Sb., Občanský zákoník v posledním znění

Zákon č. 137/2001 Sb., o zvláštní ochraně svědka

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád) v posledním znění

Zákon č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu v posledním znění

Zákon č. 154/1994 Sb., o Bezpečnostní informační službě v posledním znění

Zákon č. 289/2005 Sb., o Vojenském zpravodajství

Zákon č. 142/1867 Ústava Rakouska-Uherska

Zákon č. 40/2009 Sb., Trestní zákoník v posledním znění

Směrnice Evropského parlamentu a Rady 2006/24/ES

INTERNÍ AKTY ŘÍZENÍ

Závazný pokyn policejního prezidenta č. 139/2012

INTERNETOVÉ ZDROJE

Současná právní úprava data retention je dle Ústavního soudu ústavně konformní a tedy přípustná. *Epravo.cz* [online]. Praha: EPRAVO.cz, 2019 [cit. 2022-08-19]. Dostupné z: https://www.epravo.cz/top/clanky/soucasna-pravni-uprava-data-retention-je-dle-ustavniho-soudu-ustavne-konformni-a-tedy-pripustna-110069.html

Současná právní úprava data retention je ústavně konformní. *Usoud.cz* [online]. Brno: Dactyl Group, 2015 [cit. 2022-08-19]. Dostupné z: https://www.usoud.cz/aktualne/soucasna-pravni-uprava-data-retention-je-ustavne-konformni

DATA RETENTION A POSLEDNÍ ROZHODNUTÍ SOUDNÍHO DVORA EU. *Digitální svobody* [online]. Praha, 2021 [cit. 2022-08-19]. Dostupné z: https://digitalnisvobody.cz/blog/2021/04/28/data-retention-a-posledni-rozhodnuti-soudniho-dvora-eu/

Policie viní ředitele hygieny z dalšího trestného činu. K vydírání přibylo porušení listovního tajemství. *Seznam zprávy* [online]. Praha: Seznam zprávy, 2019 [cit. 2022-08-19]. Dostupné z: https://www.seznamzpravy.cz/clanek/policie-vini-reditele-hygieny-z-dalsiho-trestneho-cinu-k-vydirani-pribylo-poruseni-listovniho-tajemstvi-73152

Listovní tajemství. *Wikipedie* [online]. 2021 [cit. 2022-08-19]. Dostupné z: https://cs.wikipedia.org/wiki/Listovn%C3%AD_tajemstv%C3%AD#D%C5%AFvody_omezen%C3%AD_listovn%C3%ADho_tajemstv%C3%AD_v_trestn%C3%ADm_pr%C3%A1vu

Provozní a lokalizační údaje z veřejné komunikační sítě a datová analýza s prvky umělé inteligence – základy nové (komplexní) vyšetřovací strategie ÚOHS?. *Epravo.cz* [online]. Praha: EPRAVO.CZ, 2021 [cit. 2022-08-19]. Dostupné z: https://www.epravo.cz/top/clanky/provozni-a-lokalizacni-udaje-z-

verejne-komunikacni-site-a-datova-analyza-s-prvky-umele-inteligence-zaklady-nove-komplexni-vysetrovaci-strategie-uohs-112786.html?mail

SEZNAM TABULEK