Data retention v (nejen) policejní praxi

Iuridicum Remedium; Vobořil, Jan
2012

Dostupný z http://www.nusl.cz/ntk/nusl-188284

Iuridicum Remedium, o.s.
U Průhonu 23/1201, 170 00 Praha 7
tel./fax: 222 515 564
e-mail: iure@iure.cz
www.iure.org

Data retention v (nejen) policejní praxi

Analýza postupů Policie ČR a dalších orgánů při vyžadování a využívání provozních a lokalizačních údajů o elektronických komunikacích v České republice.

Zpracoval: Jan Vobořil, 25. září 2012

Sídlo: Vírská 14/278, 198 00 Praha 9, IČ: 265 34 487

NADACE OPEN SOCIETY FUND PRAHA

esf evropský sociální fond v ČR EVROPSKÁ UNIE

OPERAČNÍ PROGRAM LIDSKÉ ZDROJE A ZAMĚSTNANOST

PODPORUJEME VAŠI BUDOUCNOST www.esfcr.cz

Trust for Civil Society in Central & Eastern Europe

www.iure.org www.slidilove.cz www.bigbrotherawards.cz

Obsah

I. Úvod

Listovní tajemství je jedním z nejstarších příkladů uplatňování práva na soukromí. V průběhu dějin přibývaly další a další způsoby komunikace, na něž se právo na soukromí také postupně vztahovalo, ať už jde o telegraf, telefon nebo různé způsoby komunikace či předávání informací s využitím internetu. Právo na soukromí se přitom podle výkladu judikatury nevztahuje pouze na samotný obsah sdělení, ale i na informace, které jsou s komunikací spojeny, zejména kdo s kým a za jakých okolností komunikoval. Z těchto údajů, které se netýkají přímo obsahu komunikace a jsou souhrnně nazývány provozní a lokalizační údaje o elektronických komunikacích, lze zjistit celou řadu informací o sociálních kontaktech a pohybu zájmové osoby. Zpracováním těchto dat lze pak sestavovat sociální sítě, odhalovat sociální role v těchto sítích nebo předpovídat činnost a pohyb konkrétních osob v budoucnu. Proto jsou provozní a lokalizační údaje považovány za velmi citlivé a jejich citlivost je srovnávána s obsahem samotné komunikace. Plošné uchovávání a masivní využívání těchto údajů státními orgány pak znamená značný zásah do soukromí občanů, s kterým je spojeno i riziko zneužití těchto údajů.

Názory na data retention, jak se obecně říká povinnému uchovávání a následnému využívání provozních a lokalizačních údajů o elektronických komunikacích, se značně liší. Kontroverzní je zejména plošnost a nevýběrovost tohoto nástroje, kdy se podezřelým stává každý z nás. Ne náhodou označil Evropský inspektor osobních údajů Peter Hustinx Směrnici o data retention za nejinvazivnější nástroj zásahu do soukromí, který byl kdy v EU přijat, pokud jde o rozsah zásahu a množství osob, kterých se týká.[1] To, jestli jde o nástroj užitečný je předmětem sporů, na jedné straně stojí zkušenosti policistů, podle nichž jde často o nezbytný důkazní prostředek, na druhé straně pak statistiky trestné činnosti, které napříč Evropou neprokazují žádné významné změny v míře kriminality ani její objasněnosti v souvislosti se zavedením data retention. Cílem této studie není primárně zhodnotit princip data retention jako takový, ačkoli ani tomu se nakonec nevyhneme, ale popsat to, jakým způsobem jsou v České republice provozní a lokalizační údaje využívány, a upozornit na problémy, které se v praxi objevují a mají nebo v budoucnu mohou mít negativní dopady na úroveň ochrany lidských práv.

Tato studie, která vznikla v rámci projektu Digital Rights and Awareness of Citizens (DRAC) podpořeném Trust for Civil Society in Central and Eastern Europe řešeným o.s. Iuridicum Remedium

[1] Dostupné na: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf

(IuRe), navazuje na studii zpracovanou občanským sdružením Iuridicum Remedium v roce 2010 pod názvem „Co dělají provideři a telefonní operátoři s našimi daty? Studie praxe poskytovatelů internetových a telekomunikačních služeb (ISP)“[2], která se věnovala problematice nakládání s osobními údaji ze strany poskytovatelů služeb elektronických komunikací včetně jejich praxe při poskytování provozních a lokalizačních údajů. Na rozdíl od této dřívější studie, která se zaměřila hlavně na praxi u poskytovatelů služeb elektronických komunikací, se zde zaměříme na praxi při využívání provozních a lokalizačních údajů na straně oprávněných orgánů, zejména Policie ČR.

V průběhu sběru podkladů k této studii probíhala jednání a připomínková řízení jak k novému zákonu, tak k nové prováděcí vyhlášce, které nově data retention upravují. De facto se tak v této studii odráží trojí právní úprava uchovávání a využívání provozních a lokalizačních údajů. Situaci na poli uchovávání a využívání těchto údajů můžeme rozdělit podle uplatňované legislativy do třech období. První období končí 12. 4. 2011, kdy nabyl účinnosti nález Ústavního soudu sp. zn. Pl. ÚS 24/10, kterým došlo ke zrušení úpravy povinnosti uchovávat provozní a lokalizační údaje pro potřeby oprávněných orgánů, zejména policie, v zákoně o elektronických komunikacích a v prováděcí vyhlášce. Druhé období pak začíná právě tímto datem a s největší pravděpodobností skončí 1.10.2012, kdy by měla nabýt účinnosti nová právní úprava několika zákonů včetně zákona o elektronických komunikacích a trestního řádu, která reaguje na zmíněný nález Ústavního soudu a vyšla již ve sbírce zákonů jako zákon č. 273/2012 Sb. Pro toto období je typická neexistence zákonné povinnosti poskytovatelů služeb elektronických komunikací uchovávat provozní a lokalizační údaje pro potřeby oprávněných orgánů. Následující třetí období pak přinese znovuzavedení této povinnosti, snad i vyjasnění některých sporných otázek v dřívější právní úpravě, ale možná i negativní dopady problémů, které z různých důvodů nejsou v nové zákonné úpravě řešeny.

Studie vychází zejména z informací, které jsme získali při dvou schůzkách s ředitelem Útvaru zvláštních činností služby kriminální policie a vyšetřování Tomášem Almerem, dále na schůzkách se zástupci Odboru bezpečnostní politiky Ministerstva vnitra a Bezpečnostní informační služby v souvislosti s připomínkovým řízením k nové úpravě data retention, které se uskutečnily v roce 2011. Dále jsme vycházeli z písemných informací, které nám na základě žádostí dle zákona o svobodném přístupu k informacím poskytla Policie ČR, Česká národní banka, Bezpečnostní informační služba, Vojenské zpravodajství nebo Generální inspekce bezpečnostních sborů. Získané informace jsme dále porovnávali

[2] Iuridicum Remedium, Co dělají provideři a telefonní operátoři s našimi daty? Studie praxe poskytovatelů internetových a telekomunikačních služeb (ISP), Praha 20.4.2010, dostupné na: http://slidilove.cz/sites/default/files/Studie%20ISP_final.pdf

se zjištěními naší studie z roku 2010, ale také ověřovali u vybraných poskytovatelů služeb elektronických komunikací, konkrétně při osobní schůzce se zástupcem příslušného útvaru jednoho ze tří velkých telefonních operátorů, či rozhovory a dotazníkovým šetřením u několika menších poskytovatelů internetového připojení. Oproti předchozím letům se nově otázce využívání provozních a lokalizačních údajů věnuje i Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2011 připravená Policejním prezidiem ČR, s kterou studie také pracuje.

Studie je rozdělena do dvou částí. První část obsahuje popis vývoje právní úpravy uchovávání a využívání provozních a lokalizačních údajů v České republice v letech 2009-2012. Druhá část pak popisuje praxi při vyžadování těchto údajů se zaměřením zejména na praxi u Policie ČR, přináší statistiky, jak byly údaje v uplynulých třech letech využívány a k jakým změnám došlo v souvislosti s nálezem Ústavního soudu, který zrušil povinnost poskytovatelů data uchovávat. V závěru pak shrneme poznatky, k nimž ve studii dojdeme.

II. Data retention a právo

Právní úpravu uchovávání a využívání provozních a lokalizačních údajů je třeba rozdělit do dvou skupin. Jednak je to právní úprava oprávnění nebo povinnosti tato data uchovávat. Druhou skupinou je pak právní úprava oprávnění vybraných státních orgánů tato data vyžadovat.

Právo a povinnost data uchovávat

Oprávnění a povinnosti osob zajišťujících veřejnou komunikační síť a poskytovatelů služeb elektronických komunikací (dále také „poskytovatelé“) uchovávat provozní a lokalizační údaje může vyplývat jednak ze smlouvy, jednak přímo z právního předpisu.

Kdo (ne)bude mít povinnost data uchovávat?

Zásadní otázkou, kterou je potřeba si zodpovědět je, na koho se vlastně povinnost údaje uchovávat bude v budoucnu vztahovat. Podle definice se veřejnou komunikační sítí rozumí v souladu s § 2 písm. j) zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (dále jen „ZEK“) síť elektronických komunikací, která slouží zcela nebo převážně k poskytování veřejně dostupných služeb elektronických komunikací, a která podporuje přenos informací mezi koncovými body sítě, nebo síť elektronických komunikací, jejímž prostřednictvím je poskytovaná služba šíření rozhlasového a televizního vysílání. Službou elektronických komunikací se pak rozumí služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací. Tento pojem přitom nezahrnuje služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací.[3]

Jak už ukázala naše studie z roku 2010, tak pokud jde o internetové služby, tak poskytovatelem a tedy i povinnou osobou jsou zpravidla pouze poskytovatelé připojení. Naopak provozovatelé webových služeb

[3] Celá definice služby elektronických komunikací dle § 2 písm. n) ZEK zní: Služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize, s výjimkou služeb, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaným službami elektronických komunikací; nezahrnuje služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací

se sami považují zpravidla za poskytovatele služeb informační společnosti, kteří se řídí ustanoveními zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „ZIS“).[4] Při určení toho, kdo bude muset data uchovávat, je tak rozdíl jestli stejnou službu poskytuje subjekt, který zároveň poskytuje i služby připojení, nebo subjekt, který tyto služby neposkytuje. Příkladem mohou být údaje o přenosech zpráv elektronické pošty, které by měli poskytovatelé uchovávat v souladu s § 2 odst. 3 písm. d) návrhu nové vyhlášky. Ty samé údaje ale nemusí uchovávat subjekty, které poskytují pouze webové služby. Těch druhých je naprostá většina. Je tedy otázkou, jaký smysl vůbec uložení takové povinnosti má, pokud je zároveň většina poskytovatelů daných služeb z této povinnosti vyjmuta. Z této povinnosti jsou vyjmuti také provozovatelé neveřejných wi-fi sítí, může jít například o univerzity, o knihovny apod.

Dalším problémem v určení na koho se vlastně povinnost vztahuje je otázka malých poskytovatelů služeb připojení. Zejména s rozmáhající se praxí řady kaváren, restaurací a dalších zařízení, které jako jeden z benefitů pro své zákazníky nabízí veřejně přístupné wi-fi připojení k internetu. Ačkoli poskytování wi-fi tedy naplní definici služby elektronických komunikací, tak představa, že by všichni ti, kteří tyto služby poskytují, měli uchovávat údaje, které se v jejich síti vytváří a stát by jim měl proplácet v souladu s § 97 odst. 7 ZEK vynaložené náklady je poněkud bizarní.

Zdá se tedy, že zejména u internetového provozu je povinnost uchovávat uložena subjektům, které nebudou schopny tuto povinnost plnit a zřejmě to po nich ani nebude vyžadováno (malí poskytovatelé internetového připojení, provozovatelé veřejných wi-fi sítí) a naopak není uložena subjektům, bez jejichž zapojení do uchovávání údajů ztrácí data retention v internetovém prostředí do jisté míry smysl (poskytovatelé webových služeb).

Jak je uchovávání údajů upraveno?

Obecným právním předpisem, který reguluje práva a povinnosti při zpracování osobních údajů je zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen „ZOOÚ“). Oblast poskytování služeb elektronických komunikací včetně úpravy nakládání s provozními a lokalizačními údaji a důvěrnosti komunikací pak reguluje ZEK.

[4] Iuridicum Remedium, Co dělají provideři a telefonní operátoři s našimi daty? Studie praxe poskytovatelů internetových a telekomunikačních služeb (ISP), Praha 20.4.2010, s.5n, dostupné na: http://slidilove.cz/sites/default/files/Studie%20ISP_final.pdf

Právním předpisem, který upravuje povinnost poskytovatelů služeb elektronických komunikací uchovávat provozní údaje je například § 90 odst. 3 ZEK, podle něhož je podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinen uchovávat provozní údaje služby poskytnuté účastníkovi nebo uživateli do doby rozhodnutí sporu podle § 129 odst. 3 ZEK nebo do konce doby, během níž může být vyúčtování ceny nebo poskytnutí služby elektronických komunikací právně napadeno nebo úhrada vymáhána.

Ve vztahu k oprávnění Policie a dalších orgánů provozní a lokalizační údaje vyžadovat je nicméně klíčový zejména § 97 odst. 3 a 4 ZEK, který dlouho upravoval povinnost uchovávat provozní a lokalizační údaje pro potřeby oprávněných orgánů, čímž byla v podstatě s předstihem v roce 2005 implementována Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES (dále jen „Směrnice 2006/24/ES“). Uvedená ustanovení pak prováděla vyhlášky Ministerstva průmyslu a obchodu č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání (dále jen „vyhláška č. 485/2005 Sb.) Úpravu v § 97 odst. 3 a 4 ZEK, jakož i prováděcí vyhlášku č. 485 /2005 Sb. zrušil na návrh skupiny poslanců připravený občanským sdružením Iuridicum Remedium Ústavní soud nálezem ze dne 22.3.2011, sp. zn. Pl. ÚS 24/10[5] pro neproporcionální zásah do soukromí. Ústavní soud v nálezu kritizoval nejen úpravu v samotném ZEK, ale i nedostatečnou úpravu přístupu policie a dalších orgánů činných v trestním řízení k provozním a lokalizačním údajům v § 88a trestního řádu (dále jen „TŘ“). Vzhledem k tomu, že Ústavní soud nemohl zrušit i kritizovaný § 88a TŘ, protože návrh na jeho zrušení nebyl v podaném návrhu požadován, podal návrh na jeho zrušení Obvodní soud pro Prahu 6. Tomuto návrhu bylo Ústavním soudem vyhověno v nálezu ze dne 20.12.2011 sp. zn. Pl. ÚS 24/11.[6]

V reakci na březnový a později i prosincový nález Ústavního soudu začalo Ministerstvo vnitra ve spolupráci s Ministerstvem průmyslu a obchodu připravovat novou právní úpravu data retention. Důvodem byl zejména fakt, že zrušením povinnosti operátorů data uchovávat, došlo k situaci, kdy nebyla řádně implementována směrnice 2006/24/ES. Zejména policie se navíc nespokojila s údaji, které jí poskytovatelé předávali po rozhodnutí Ústavního soudu. Nová úprava po vnějším připomínkovém řízení (srpen – září 2011) byla po schválení vládou (22.2.2012) schválena i Poslaneckou sněmovnou

5 http://www.concourt.cz/clanek/GetFile?id=5075

6 Dostupné na: http://www.concourt.cz/soubor/6113

(20.6.2012), Senátem (18.7.2012) a nakonec podepsána prezidentem republiky (1.8.2012).[7] Účinnosti schválená právní úprava nabude jako zákon č. 273/2012 Sb. dne 1.10.2012.

Nový zákon přináší vedle úpravy povinnosti poskytovatelů uchovávat pro potřeby oprávněných orgánů provozní a lokalizační údaje podle nového znění § 97 odst. 3 a 4 ZEK také novelizaci § 88a TŘ a některých dalších ustanovení TŘ, dále novelizace zákona o dohledu v oblasti kapitálového trhu, novelizace zákona o Bezpečnostní informační službě a zákona o Vojenském zpravodajství. Ministerstvo průmyslu a obchodu zároveň rozeslalo dne 28.7.2012 do vnějšího připomínkového řízení prováděcí vyhlášku o uchovávání, předávání a likvidaci provozních a lokalizačních údajů, která provádí § 97 odst. 4 zákona o elektronických komunikacích. Vyhláška by stejně jako zákon měla nabýt účinnosti dne 1.10.2012. V době poslední revize této studie (25.9.2012) byla vyhláška v připomínkovém řízení na Legislativní radě Vlády.

Podle nově schválené právní úpravy v § 97 odst. 3 a 4 ZEK jsou právnické a fyzické osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinny 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. Dále mají povinnost v případě, že je vytváří a zároveň zaznamenávají, uchovávat provozní a lokalizační údaje týkající se neúspěšných pokusů o volání. Současně je tato právnická nebo fyzická osoba povinna zajistit, aby při tomto uchovávání údajů nebyl zároveň uchováván i obsah zpráv.

Důležitý je zde pojem vytváření údajů. Panuje obecné přesvědčení, že povinnost údaje uchovávat se vztahuje na určité osoby, které mají povinnost technicky zajistit, aby požadované údaje měly k dispozici pro potřeby oprávněných orgánů. Klíčové ovšem je, jestli se tyto údaje při poskytování služby technicky vytváří. Pokud tomu tak není, tak povinnost dané údaje uchovávat poskytovatelé nemají.

Pokud jsou údaje uchovávány, tak mají být v souladu s § 97 odst. 3 ZEK na vyžádání bezodkladně předány:

a) orgánům činným v trestním řízení pro účely a při splnění podmínek stanovených trestním řádem

[7] Dostupné na: http://eklep.vlada.cz/eklep/page.jsf?pid=RACK8KS9P9FK; http://www.senat.cz/xqw/xervlet/pssenat/historie?cid=pssenat_historie.pHistorieTisku.list&forEach.action=detail&forEach.value=s3170

b) Policii České republiky pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované 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 zákonem č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů (dále jen „PolZ“) a zákonem 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 (dále jen „ZZOS“).

c) Bezpečnostní informační službě pro účely a při splnění podmínek stanovených zákonem č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů.

d) Vojenskému zpravodajství pro účely a při splnění podmínek stanovených zákonem č. 289/2005 Sb., o Vojenském zpravodajství

e) České národní bance pro účely a při splnění podmínek stanovených zákonem č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu a o změně a doplnění

V § 97 odst. 4 ZEK je pak řečeno, že 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.

Návrh vyhlášky, která by měla provést § 97 odst. 4 ZEK, definuje pojmy, stanovuje jak okruh provozních a lokalizačních údajů, které mají být uchovávány u jednotlivých typů služeb, tak rovněž způsob jejich předávání oprávněným orgánům, či povinnost uchovávat data po jejich předání.

Za neuchovávání požadovaných údajů, ale i za porušení pravidel pro jejich zabezpečení se může poskytovatel dopustit správního deliktu dle § 118 odst. 14 písm. c), respektive § 118 odst. 15 ZEK. Za neuchovávání provozních a lokalizačních údajů hrozí v souladu s § 118 odst. 21 písm. b) a c) ZEK poskytovatelům pokuta až do výše 20 milionů Kč, za porušení pravidel pro jejich zabezpečení 10 milionů Kč.

Na závěr této kapitoly je nezbytné znovu připomenout, že výše popsaná povinnost poskytovatelů nabude účinnosti až 1. 10. 2012. Do té doby tedy stále platí, že uchovávání provozních a lokalizačních údajů pouze z důvodu jejich možného vyžádání ze strany oprávněných orgánů není povinností

poskytovatele a v případě, že by tak chtěl poskytovatel činit sám ze své vůle, musel by k této činnosti disponovat souhlasem svých klientů nebo jiným právním titulem. Tím samozřejmě není dotčeno uchovávání provozních a lokalizačních údajů k jiným účelům (vyúčtování, marketing) a jejich předávání policii.

Oprávnění data vyžadovat

V souladu s čl. 2 odst. 3 Ústavy ČR (dále jen „Ústava“) a čl. 2 odst. 2 Listiny základních práv a svobod (dále jen „Listina“) lze státní moc uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon. Zároveň v souladu s § 2 odst. 4 Ústavy ČR a čl. 2 odst. 3 Listiny může každý občan činit, co není zákonem zakázáno, a nikdo nesmí být nucen činit, co zákon neukládá.

Státní orgán, který by rád získal přístup k provozním a lokalizačním údajům tedy musí mít k vyžadování těchto údajů zákonné zmocnění. Tomuto zmocnění pak odpovídá povinnost poskytovatele data předat. Provozní a lokalizační údaje jsou podobně jako obsah komunikace chráněna čl. 13 Listiny, který upravuje listovní tajemství, či v dnešním slova smyslu spíše již tajemství komunikační. Povinnost zachovávat diskrétnost komunikace je poskytovatelům uložena v § 89 odst. 1 ZEK. 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 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.

Úprava oprávnění data vyžadovat by vzhledem ke zvýšené a ústavně zaručené ochraně těchto údajů měla výslovně uvádět, že se jedná o oprávnění vyžadovat provozní a lokalizační údaje o elektronických komunikacích, případně data o telekomunikačním provozu, což jsou označení, která se dle výkladového ustanovení v § 136 odst. 20 písm. b) ZEK významově kryjí. Zároveň by měly být stanoveny limity pro získání a využití těchto údajů. K dovození povinnosti poskytnout provozní a lokalizační údaje nepostačí například obecná ustanovení o povinnosti součinnosti v § 8 odst. 1 TŘ nebo v § 18 PolZ, či definice toho, co může v trestním řízení posloužit jako důkaz dle § 89 odst. 2 a § 112 TŘ.[8] Tato specifická

[8] K tomu např. Stanovisko Nejvyššího státního zastupitelství č. 4/2005, ke sjednocení výkladu zákonů a jiných právních předpisů k postupu v případech, kdy je třeba pro účely trestního řízení zjistit obsah údajů uložených v nalezeném, vydaném či odňatém mobilním telefonu, včetně údajů uložených na SIM kartě, dostupné na: http://portal.justice.cz/nsz/PrintPage.aspx?o=29&j=39&k=4128&d=129636

oprávnění a okruh oprávněných orgánů lze nalézt v zákonech, na něž odkazuje nové znění § 97 odst. 3 ZEK.

Orgány činné v trestním řízení

Orgány činnými v trestním řízení se v souladu s § 12 odst. 1 TŘ rozumí soud, státní zástupce a policejní orgán. To, kdo je policejním orgánem stanoví § 12 odst. 2 TŘ. Vedle Policie ČR se jedná v určitých případech například o Generální inspekci bezpečnostních sborů, pověřené celní orgány, pověřené orgány Vojenské policie nebo pověřené orgány zpravodajských služeb.

Oprávnění orgánů činných v trestním řízení využívat v rámci trestního řízení provozní a lokalizační údaje je upraveno v § 88a TŘ. Právě toto ustanovení doznalo v nové právní úpravě zřejmě nejpodstatnějších změn. Podle zrušené právní úpravy[9] se oprávnění v § 88a TŘ značně odchylovalo od relativně přísné úpravy využívání odposlechů v § 88 TŘ. Provozní a lokalizační údaje bylo možno podle tohoto ustanovení žádat v případě vyšetřování jakéhokoli trestného činu. Omezení oprávnění policie tak spočívalo pouze ve skutečnosti, že vydání těchto údajů musel nařídit soud, pokud s poskytnutím údajů nesouhlasil sám sledovaný dle § 88a odst. 2 TŘ. Žádosti často postrádaly identifikaci zájmových osob a omezovaly se na seznam i několika desítek telefonních čísel a odůvodnění, proč je nezbytné zjistit provozní údaje týkající se těchto čísel. Možnost soudu tyto žádosti přezkoumat pak byla značně limitována. Ve zrušené právní úpravě chyběl důraz na zdůvodnění této žádosti nebo na identifikaci osoby, jejíž údaje měly být zjišťovány. Zároveň chyběla povinnost informovat po ukončení trestního řízení osobu, jejíž údaje byly zjišťovány, jakož i možnost této osoby domáhat se soudní cestou přezkoumání oprávněnosti tohoto zásahu do soukromí. To nahrávalo možnostem zneužití pravomocí ze strany konkrétních policistů. Nejznámějším případem zneužití pravomocí v této věci byl případ varnsdorfského policisty, který si zjišťoval provozní údaje o komunikace desítek osob ze státní správy i soukromé sféry, včetně předsedy Ústavního soudu.[10]

Nová právní úprava § 88a TŘ s účinnosti od 1.10.2012 přibližuje úpravu využívání provozních a lokalizačních údajů v trestním řízení úpravě odposlechů. Kromě omezení okruhu trestných činů[11], u

---

9 § 88a TŘ byl zrušen nálezem Ústavního soudu ze dne 20.12.2012, sp. zn. Pl. ÚS 24/11

10 K tomu viz http://zpravy.idnes.cz/policista-nelegalne-shanel-vypisy-mobilu-spehoval-i-rychetskeho-phy-/krimi.aspx?c=A110617_225431_krimi_abr

11 Napříště by mělo být možné využívat provozní a lokalizační údaje v případě trestního řízení pro úmyslný trestný čin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky, pro trestný čin porušení tajemství dopravovaných zpráv (§ 182 trestního zákoníku), pro trestný čin podvodu (§ 209 trestního zákoníku), pro trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§

nichž lze tyto údaje vyžadovat, zavádí i přísnější pravidla pro podání žádosti, ať už jde o formální náležitosti nebo nutnost podat v přípravném řízení žádost o nařízení poskytnutí údajů k soudu přes státního zástupce. Zdůrazněna je i subsidiarita užití tohoto nástroje. Nová právní úprava dále zavádí v § 88a odst. 2 a 3 TŘ informační povinnost vůči prověřované osobě, jakož i možnost soudního přezkumu žádosti. I nadále je zachována možnost využívat provozní a lokalizační údaje bez povolení soudu se souhlasem sledované osoby dle nového § 88a odst. 4 TŘ.

Policie ČR mimo trestní řízení

Vedle oprávnění Policie ČR vyžadovat údaje v rámci trestního řízení existuje i možnost vyžadovat provozní a lokalizační údaje v dalších případech upravených v PolZ a v ZZOS. V PolZ upravují oprávnění policie tři ustanovení. Podle § 66 odst. 3 PolZ může Policie 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. Jiným právním předpisem se zde myslí ZEK.

Konkrétní oprávnění v PolZ požadovat po poskytovatelích předání provozních a lokalizačních údajů o uživatelích jejich služeb lze najít na dvou místech PolZ. Podle § 68 odst. 2 PolZ Policie může žádat provozní a lokalizační údaje pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě a za účelem zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly. V souladu s § 71 PolZ pak může útvar policie, jehož úkolem je boj s terorismem za účelem předcházení a odhalování konkrétních hrozeb v oblasti terorismu v nezbytném rozsahu žádat poskytnutí provozních a lokalizačních údajů.

Na rozdíl od úpravy § 88a TŘ nedošlo v nové právní úpravě k žádným změnám, ačkoli příliš široká oprávnění policie, nedostatečné záruky proti zneužití tohoto oprávnění byla v průběhu připomínkového

230 trestního zákoníku), pro trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 trestního zákoníku), pro trestný čin nebezpečného vyhrožování (§ 353 trestního zákoníku), pro trestný čin nebezpečného pronásledování (§ 354 trestního zákoníku), pro trestný čin šíření poplašné zprávy (§ 357 trestního zákoníku), pro trestný čin podněcování k trestnému činu (§ 364 trestního zákoníku), pro trestný čin schvalování trestného činu (§ 365 trestního zákoníku), nebo pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána.

řízení předmětem kritiky nejen ze strany Úřadu pro ochranu osobních údajů, Úřadu vlády nebo IuRe, ale i samotné Policie.[12]

Problematické je zejména oprávnění dle § 68 odst. 2 PolZ, kdy policista může bez povolení soudu požadovat poskytnutí údajů pro účely pátrání po hledané nebo pohřešované osobě, případně při pátrání po identitě osoby neznámé totožnosti. Předně je nutné zdůraznit, že podle znění tohoto oprávnění nemusí jít o provozní a lokalizační údaje této osoby, ale teoreticky kohokoli. Poskytnutí údajů nemusí nařizovat soud, jako je tomu v trestním řízení. Nejsou zde ani další limity použití, které přinesl do trestního řádu zákon č. 273/2012 Sb., jako je povinnost informovat prověřovanou osobu, podrobně odůvodnit žádost nebo zdůraznění subsidiarity použití tohoto nástroje přímo v § 68 PolZ. Obecně formulovaná subsidiarita zásahu do práv a svobod osob při policejním postupu zakotvená v § 11 PolZ nevede k dostatečné zdrženlivosti policejních orgánů nejen v otázce, zda podat či nepodat žádost o výpisy, ale i při omezení věcného a časového rozsahu vyžadovaných údajů.

Jak v případě hledaných, tak pohřešovaných osob, přitom půjde o případy, kdy je především žádoucí zjistit aktuální pobyt dané osoby. Využitelnost historických dat o elektronické komunikaci je tedy podstatně nižší, než je tomu například v trestním řízení. Je sice pravda, že v některých případech, kdy má daná osoba například vypnutý či vybitý mobilní telefon, může jako vodítko k jejímu nalezení sloužit i záznam o jejím pohybu v minulosti, ale bude se zpravidla jednat o údaje staré několik hodin, maximálně dní. Využitelnost údajů starých několik týdnů či dokonce měsíců bude zpravidla nulová. Přesto je pravidlem, že provozní a lokalizační údaje o konkrétní osobě jsou vyžadovány kompletně, tedy vše co je daným poskytovatelem, v tomto případě telefonním operátorem, uchováváno. Policisté tak od počátku října tohoto roku, poté, co vstoupí v účinnost nový § 97 odst. 3 ZEK, získají výpisy o komunikaci včetně poznačení BTS stanic, k nimž se mobilní telefon připojoval za uplynulých 6 měsíců. O účelnosti tohoto zásahu do soukromí lze pochybovat.

Jestliže u pohřešovaných osob[13] je do jisté míry odůvodnitelný důraz na rychlost a tedy by bylo za stanovení podrobnějších pravidel pro vyžadování těchto údajů (např. časové omezení pro vyžadované údaje, zpětné informování prověřovaných osob, nutnost aby byly vyžadovány údaje výlučně konkrétní

[12] To nezávisle na sobě potvrdil jak ředitel Útvaru zvláštních činností Tomáš Almer během schůzky se zástupci IuRe dne 11.52012, tak Karel Bačkovský, zástupce ředitele Odboru bezpečnostní politiky Ministerstva vnitra během vypořádání připomínek IuRe dne 14.9.2011. Novelizace PolZ nicméně narazila právě na odpor Ministerstva vnitra.

[13] Pohřešovanou osobou je v souladu s § 111 písm. d) PolZ 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.

pohřešované osoby) přijatelné jejich využití. Tak v případě hledaných osob[14], kde není policejní orgán pod takovým časovým tlakem a možné dopady pozdějšího vypátrání dané osoby, nebudou tak fatální, jako tomu může být u pohřešované osoby, je využití provozních a lokalizačních údajů odůvodnitelné jen těžko. I dle vyjádření Tomáše Almera z ÚZČ by bylo možné odstranit v těchto případech oprávnění z PolZ bez náhrady a ponechat pouze možnost vyžadovat údaje v případě pátrání po pohřešovaných osobách.[15]

Vedle případů využití provozních a lokalizačních údajů při pátrání po osobách je nutné zmínit i další možnosti policie tato data využívat, která jsou nicméně využívána spíše sporadicky. V § 68 PolZ je zakotvena možnost vyžadovat provozní a lokalizační údaje, pokud je to nezbytné k identifikaci osoby neznámé totožnosti.

Ani u oprávnění v § 71 PolZ nedošlo k žádným změnám a omezením. Jistou zárukou oproti § 68 PolZ je skutečnost, že údaje může vyžadovat pouze specializovaný útvar policie. Je nicméně nelogické, aby možnost využití těchto údajů nebyla vázána na povolení soudu. Zvláštní útvar policie v těchto případech de facto vykonává totéž, co zpravodajské služby. Ty ovšem podle nově schválené úpravy budou muset k vyžadování provozních a lokalizačních údajů, stejně jako k provádění odposlechů, disponovat souhlasem vrchního soudu. U takto zásadního zásahu do práva na soukromí občanů by měla být absence soudního povolení dostatečně odůvodněna. Těžko lze za dostatečný důvod považovat argument, že zavedení soudního povolení k určitým úkonům Policie dle PolZ by bylo nesystematické.

Skutečnost, že i v činnosti Policie mimo trestní řízení je v určitých případech již dnes vyžadováno soudní povolení ostatně dokládá i poslední případ oprávnění Policie vyžadovat provozní a lokalizační údaje. Jde o oprávnění dle § 10a ZZOS, který dává Policii možnost v případě podezření, že chráněná osoba nedodržuje povinnosti ochranného režimu, vyžadovat mimo jiné i údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství nebo na něž se vztahuje ochrana osobních a zprostředkovacích dat. Tato možnost je podmíněna tím, že podezření nelze prověřit jiným způsobem. K vyžadování těchto údajů musí dát v souladu s § 10a odst. 2 ZZOS souhlas předseda senátu vrchního soudu.

---

[14] Hledanou osobou je v souladu s § 111 písm. c) PolZ fyzická osoba, u které je dán některý ze zákonných důvodů omezení její osobní svobody, místo jejího pobytu není známo a policií bylo po ní vyhlášeno pátrání

[15] Toto stanovisko k využívání provozních a lokalizačních údajů v pátrání po hledaných osobách nám potvrdil při osobní schůzce dne 11.5.2012 Tomáš Almer z Útvaru zvláštních činností Policie ČR.

Zpravodajské služby

Stávající oprávnění zpravodajských služeb využívat provozní a lokalizační údaje bylo sporné. Ministerstvo vnitra v důvodové zprávě k zákonu č. 273/2012 Sb. dochází k závěru, že BIS i VZ mají oprávnění vyžadovat provozní a lokalizační údaje již v současné době dle § 8 zákona č.154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů (dále jen „ZoBIS“) a v § 8 zákona č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů (dále jen „ZoVZ“). S tímto závěrem ovšem nelze bezvýhradně souhlasit. BIS i Vojenské zpravodajství mají oprávnění ve stanovených případech využívat zpravodajskou techniku. Za zpravodajskou techniku je třeba v souladu s § 8 odst. 1 ZoBIS a § 8 odst. 1 ZoVZ považovat technické prostředky a zařízení, zejména elektronické, fototechnické, chemické, fyzikálně-chemické, radiotechnické, optické, mechanické anebo jejich soubory, používané utajovaným způsobem. V obou zákonech stojí, že využitím zpravodajské techniky se rozumí mimo jiné i zjišťování údajů o telekomunikačním provozu. Zároveň ovšem v obou zákonech chybělo zakotvení povinnosti poskytovatelů tyto údaje BIS a Vojenskému zpravodajství předávat. Zákon tak bylo možno vykládat tak, že sice zpravodajské služby mají právo zjišťovat údaje o telekomunikačním provozu, ale zároveň zákon neukládá poskytovatelům, aby tyto údaje sami od sebe na vyžádání zpravodajským službám předávali. Tomuto výkladu nahrávala i právní úprava odposlechů zpravodajskými službami, kde v § 8a ZoBIS a ZoVZ je přímo zakotvena povinnost poskytovatelů umožnit připojení odposlouchávacích zařízení.

V průběhu připomínkového řízení byl tedy návrh zákona doplněn i o novelizaci ZoBIS a ZoVZ, která zavedla výslovné zmocnění k vyžadování těchto údajů v pozměněném § 8a ZoBIS a §8a ZoVZ, které v současné době do nabytí účinnosti zákona č. 273/2012 Sb. upravovaly pouze povinnost poskytovatelů umožnit zpravodajským službám odposlechy. Tyto paragrafy v podobě účinné od října 2012 shodně říkají, že BIS, respektive Vojenské zpravodajství, jsou oprávněny v rozsahu potřebném pro plnění konkrétního úkolu požadovat od právnické nebo fyzické osoby zajišťující veřejnou komunikační síť anebo poskytující veřejně dostupnou službu elektronických komunikací zřízení, popřípadě zabezpečení rozhraní pro připojení koncového telekomunikačního zařízení pro odposlech nebo záznam zpráv v určených bodech jejich sítě, a poskytnutí provozních nebo lokalizačních údajů způsobem, ve formě a v rozsahu stanoveném ZEK. V souladu s § 9 odst. 1 ZoBIS a § 9 odst. 1 ZoVZ je k tomuto vyžádání údajů potřeba svolení soudce vrchního soudu příslušného dle místa sídla zpravodajské služby.

Česká národní banka

Sporným je oprávnění České národní banky vyžadovat povozní a lokalizační údaje zakotvené v § 8 odst. 1 písm. d) zákona č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu o změně a doplnění

dalších zákonů (dále jen „ZDKT“). Podle tohoto ustanovení může ČNB vyžadovat poskytnutí provozních a lokalizačních údajů od osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací. Toto oprávnění bylo původně implementací čl. 12 odst. 2 písm. d) směrnice 2003/6/ES, o obchodování zasvěcených osob a manipulaci s trhem. Nedošlo však již k transpozici odst. 3 tohoto článku, který říká, že má být šetřeno profesní tajemství, což lze vztáhnout i na povinnost zachovávat důvěrnost komunikací zakotvenou v § 89 odst. 1 ZEK. Zavedením povinnosti uchovávat provozní a lokalizační údaje získalo toto ustanovení zcela nový rozměr. V původní úpravě zcela chyběly jakékoli limity užití tohoto oprávnění.

V průběhu připomínkového řízení k zákonu č. 273/2012 Sb. se podařilo prosadit do nového znění tohoto oprávnění v § 8 odst. 1 písm. d) ZDKT zavedení povinnosti disponovat písemným povolením předsedy senátu vrchního soudu příslušného podle sídla České národní banky. Vyžadování údajů by také napříště mělo být přípustné, pouze pokud lze důvodně předpokládat, že poskytnuté údaje mohou přispět k objasnění skutečností důležitých pro odhalení správního deliktu 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.

I přes tato jistá zlepšení právní úpravy zůstává samo oprávnění České národní banky využívat provozní a lokalizační údaje sporné. Jak vyplývá z Hodnotící zprávy o směrnici o uchovávání údajů (směrnice 2006/24/ES) (dále také „Hodnotící zpráva“), kterou zpracovala Evropská komise, je přístup České národní banky k údajům v rámci sledovaných evropských států ojedinělý.[16]

[16] Evropská komise, ZPRÁVA KOMISE RADĚ A EVROPSKÉMU PARLAMENTU, Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES), KOM (2O11) 225, 18.4.2011, s. 9n, dostupné na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF

III. Data retention v praxi

Tato analýza si vedle zmapování právní úpravy povinností a oprávnění spojených s uchováváním a vyžadováním provozních a lokalizačních údajů o elektronických komunikacích vzala za cíl zejména zmapování praxe při využívání těchto údajů. Těžiště této kapitoly tvoří zejména popis praxe využívání těchto údajů ze strany Policie ČR, a to ať už v rámci trestního řízení, či mimo něj.

Praxe při vyžadování provozních a lokalizačních údajů u Policie ČR

Policie žádá o výpisy provozních a lokalizačních údajů ve dvou typově odlišných případech. Buď má policista k dispozici údaje ke konkrétnímu uživateli (číslo jeho mobilní linky, pevné linky, IP adresu, IMEI, apod.) a v takovém případě se zajímá o kontakty, činnost, případně pohyb tohoto konkrétního uživatele (jeho telefonu, počítače apod.) nebo tyto údaje nezná, disponuje ale informacemi, kde se zájmový uživatel pohyboval, případně kde došlo k trestnému činu. V těchto případech se Policie zajímá zejména o údaje z jednotlivých stanic BTS, které určí, jaké mobilní telefony se v danou chvíli k dané buňce připojovaly.[17]

Ačkoli Policie opakovaně tvrdí, že údaje jsou využívány zejména při odhalování závažné násilné kriminality, jako jsou vraždy, loupeže, sériové krádeže apod., tak je faktem, že žádné statistiky toho, u vyšetřování jakých trestných činů jsou údaje vyžadovány, neexistují, protože tyto údaje nejsou u žádostí o poskytnutí údajů evidovány. To nám potvrdilo ve své odpovědi na žádost o informace Policejní prezidium Policie ČR.[18] Využívání těchto údajů se v minulosti ani dnes zpravidla neřídí závažností trestného činu, ale důkazní situací. Vyjádření policistů je tak třeba brát s rezervou a s vědomím, že odráží pouze zkušenosti vyjadřující se osoby, nikoli ale nutně i celkovou situaci.

---

17 Právě výpisy ze stanic BTS, které telefonní operátoři nemají většinou důvod sami od sebe uchovávat, pociťovala Policie jako jednu z největších ztrát v souvislosti se zrušením povinnosti údaje uchovávat. Operátoři odmítají Policii tyto údaje předávat s tím, že je nemají k dispozici. Podle Tomáše Almera je jedinou výjimkou mezi třemi operátory společnost Telefónica O2, která tyto údaje uchovává po dobu 48 hodin a na vyžádání policii předává.

18 Odpověď Policejního prezidia Policie ČR na žádost IuRe o informace, 7.5.2012 .

Jak policista získává provozní a lokalizační údaje?

V rámci trestního řízení je oprávněným k vyžádání provozních a lokalizačních údajů orgán činný v trestním řízení. Vzhledem k tomu, že využitelnost těchto údajů je vzhledem k jejich charakteru nejvyšší na počátku trestního řízení, žádá v drtivé většině případů o tyto údaje policejní orgán, konkrétně pak Policie ČR.

Možnosti postupu jsou dvě, buď získává policie údaje se souhlasem sledované osoby (§ 88a odst. 2 TŘ), nebo bez jejího souhlasu (§88a odst. 1 TŘ). Případy, kdy se tak děje se souhlasem sledovaného, jsou výjimečné. V roce 2011 se jednalo podle Analýzy zpracované Policejním prezidiem o 2,7% případů.[19]

Podrobné postupy toho, jakým způsobem má Policie ČR, respektive její jednotlivé útvary či příslušníci, o tyto údaje žádat, není v současné době upravena v žádném právním předpise. Podrobnější úprava je tak obsažena v interním předpise a totiž v Závazném pokynu policejního prezidenta č. 186/2011, o vyžadování odposlechu a záznamu telekomunikačního provozu a údajů o uskutečněném telekomunikačním provozu, který ovšem není veřejnosti přístupný a Policejní prezidium nám ho pro potřeby této analýzy odmítlo poskytnout. O jeho obsahu se tak můžeme jenom dohadovat. Popis praxe při vyžadování provozních a lokalizačních údajů vychází tedy zejména z informací získaných od ředitele Útvaru zvláštních činností služby kriminální policie a vyšetřování Policie ČR (dále také „ÚZČ“) Tomáše Almera a z informací od samotných poskytovatelů služeb elektronických komunikací, kteří nám popsali své zkušenosti s kontakty s Policií v této věci.

V současné době, tzn. po zrušení starší právní úpravy Ústavním soudem a před nabytím účinnosti zákona č. 273/2012 Sb., probíhá podle informací z ÚZČ obvyklý postup Policie při vyžadování provozních a lokalizačních údajů následujícím způsobem. V trestním řízení se policista, který žádá o poskytnutí provozních a lokalizačních údajů obrací prostřednictvím státního zástupce s žádostí o přikázání poskytnutí provozních a lokalizačních údajů na soud. Ingerence státního zastupitelství zde v současnosti nevyplývá ze zákona, ale po kritice a následném zrušení § 88a TŘ se stalo praxí podávat žádost prostřednictvím státního zástupce.[20] S příkazem soudu se policista obrací na Útvar zvláštních

[19] Policejní prezidium ČR, Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2011, 25.7.2012, s. 173, dostupné na: https://racek.vlada.cz/e-vlada/eklep.nsf/0/A33D6700F2C74F97C1257A7500320166?Opendocument (přístup pouze s heslem do aplikace eKlep)

[20] Zákon č. 273/2012 Sb. zakotvil toto pravidlo přímo do § 88a trestního řádu.

činností Policie ČR (dále také „ÚZČ“), který zprostředkuje kontakt s daným poskytovatelem. V případě žádostí dle § 68 a 71 PolZ tato první fáze odpadá, neboť policista nepotřebuje příkaz soudu s poskytnutím provozních a lokalizačních údajů. V těchto případech se tedy policista přímo obrací na jednu z expozitur ÚZČ. ÚZČ přitom už nijak neprověřuje oprávnění daného policisty data vyžadovat a v podstatě pouze zprostředkovává předání údajů od poskytovatele danému policistovi.

Na jedné ze 7 expozitur ÚZČ se nejprve vyplní požadavek do terminálu „Výpisy“ (číslo požadavku, výpis od-do, kdo se ptá – právní titul, č.j. policejního spisu, č.j. povolení soudu - to chybí u §§ 68 a 71 PolZ kde není třeba příkazu soudu). Požadující policista určí heslo, kterým bude možné odpověď následně rozbalit. Centrum informačních systémů (CIS) na centrále ÚZČ se obrátí na poskytovatele služeb elektronických komunikací a zažádá o příslušný výpis. V podstatě to znamená přeposlání žádosti, která dorazila z expozitury ÚZČ. Poskytovatel v současné době zpravidla odpoví zasláním údajů v nejednotné formě. Tento výpis je pak centrálou ÚZČ v Praze zaslán na příslušnou expozituru ÚZČ, kde je vygenerován dopis a přehledová tabulka, která je prostřednictvím intranetu zaslána příslušnému policistovi, který si údaje vyžádal. K rozbalení tabulky potřebuje policista heslo, které si při podání žádosti stanovil. Celý proces vyžádání těchto údajů touto cestou trvá zpravidla 1 den, maximálně 3 dny. Přenos informací mezi providerem a policií je uskutečněn prostřednictvím sdílených adresářů na dedikovaných trasách zejména u velkých telefonních operátorů, respektive prostřednictvím rarovaných emailů u menších poskytovatelů.

V případě, že policista chce s údaji dále pracovat například v trestním řízení, potřebuje zpravidla od poskytovatele autorizovaný výpis s podpisem a razítkem, který je v případě potřeby následně vyžádán ze strany ÚZČ písemně po poskytovateli.

Po odeslání konkrétnímu policistovi jsou údaje na ÚZČ ve zpracované podobě uchovávány po dobu 5 dnů, v nezpracované podobě jsou pak údaje ukládány do archivu, kde je ÚZČ uchovává po dobu 3 let. V případě, že policista po pěti dnech chce získat daný výpis znovu (např. ho ztratil, smazal apod.), musí proběhnout celý proces vyžádání znovu. To znamená, že znovu proběhne na expozituře na žádost příslušného policisty zadání údajů do terminálu „Výpisy“ a následné zaslání dotazu na centrálu ÚZČ, které vyhledá v archivu příslušný výpis a odešle ho zpět. Rozdíl je v tom, že nejsou znovu dotazováni poskytovatelé, ale výpis se získá z archivu ÚZČ.

V této souvislosti je nutné upozornit na povinnost uchovávat poskytnuté údaje ze strany poskytovatelů, kterou zavádí nově navržená prováděcí vyhláška v § 4. Dle tohoto ustanovení by měli poskytovatelé

uchovávat výpisy, které předali oprávněným orgánům po dobu 12 měsíců.[21] Je otázkou z jakého titulu je povinnost dále archivovat tyto výpisy obsahující osobní údaje poskytovatelům uložena, neboť výklad, že se jedná o provedení § 97 odst. 4 ZEK, který odkazuje prováděcímu právnímu předpisu toliko úpravu rozsahu provozních a lokalizačních údajů, které mají být uchovávány, formu a způsob jejich předávání a způsob jejich likvidace, nikoli tedy jejich další uchovávání nad rámec doby 6 měsíců stanovené v § 97 odst. 3 ZEK, je velmi extenzivní. V každém případě bude paralelní uchovávání vyžádaných výpisů ve spisu vedeného daným policistou, v archivu ÚZČ a v databázích poskytovatele zbytečné a bezdůvodně zvýší riziko zneužití těchto údajů.

Výše popsaný postup by měl být standardním postupem u Policie ČR. Jak nám nicméně sdělili někteří menší poskytovatelé a jak nám potvrdil i Tomáš Almer z ÚZČ, tak v praxi policisté někdy považují oficiální postup s vyžadováním provozních a lokalizačních údajů za příliš komplikovaný a v řadě případů se na poskytovatele obrací přímo buď zcela neformálně, nebo s odkazem na povinnost součinnosti například podle § 8 TŘ. Až v případě, kdy touto cestou údaje nezískají, zkouší cestu podání žádosti přes ÚZČ. Této praxi, k níž dochází zejména při vyžadování údajů od menších poskytovatelů, nahrává i skutečnost, že postup přes ÚZČ v současné době není upraven v žádném obecně závazném právním předpisu a poskytovatelé se tak mohou stěží odvolávat na skutečnost, že budou komunikovat pouze s ÚZČ. Zejména menší internetoví provideři nemají dostatečné vědomosti o oprávněních policie, o podmínkách, které musí policie splnit, aby mohla o údaje žádat, ani o své povinnosti zachovávat důvěrnost komunikací i vůči orgánům státní správy. V případě, kdy se na ně obrátí policista a oni mají dané údaje k dispozici, je tak policistovi často bez dalšího vydají. V případech, kdy policie argumentuje postupem dle § 8 TŘ nebo žádá o údaje zcela neformálně, pak zpravidla chybí i soudní příkaz ke zjišťování těchto údajů. Využitelnost takto získaných důkazů v trestním řízení může být samozřejmě pochybná, to ovšem za podmínky, že by byly tyto důkazy v trestním řízení napadeny obhajobou. Navíc i neformální informace od poskytovatelů bez dalšího využití v trestním řízení mohou vést k získání dalších důkazů, případně lze vždy zažádat o stejný výpis oficiální cestou.

V každém případě ale platí, že tento postup není v souladu s TŘ ani PolZ. Poskytovatelé pak předáním těchto údajů policistovi porušují povinnost zachovávat důvěrnost komunikace dle § 89 odst. 1 ZEK a vystavují se nebezpečí uložení pokuty za přestupek nebo správní delikt dle § 118 odst. 21 písm. d) ZEK až ve výši 10 milionů Kč.

[21] V podobě otisků pak mají být výpisy neobsahující již osobní údaje uchovávány po dobu 3 let.

V této souvislosti lze přivítat návrh § 3 odst. 1 nové vyhlášky, který říká, že jak oprávněné orgány, tak poskytovatelé, si při prvním kontaktu sdělí, kdo je podle interních předpisů oprávněn provozní a lokalizační údaje vyžadovat. Údaje by měly být pak předávány pouze tomuto pracovišti. Lze předpokládat, že v případě Policie ČR se bude jednat o ÚZČ. To, jestli toto ustanovení přispěje k omezení případů, kdy jsou policistům předávány údaje v rozporu se zákonem, ukáže budoucnost a bude to záležet zejména na právním povědomí samotných poskytovatelů a důsledném postihu policistů, kteří budou vyžadovat údaje způsobem, který je v rozporu se zákonem.

V této souvislosti je inspirativním řešením pro předávání údajů mezi poskytovateli a oprávněnými subjekty rakouský koncept tzv. Durchlaufstelle, tedy „průtokového" místa, kde dochází k předání výpisů v šifrované podobě, upravený v §§ 8 a následujících Verordnung der Bundesministerin für Verkehr, Innovation und Technologie betreffend die Datensicherheit (Datensicherheitsverordnung TKG-DSVO). Jedná se o systém zřízený pro předávání provozních a lokalizačních údajů, na nějž jsou napojeny jak oprávněné orgány, respektive jejich kontaktní pracoviště, tak poskytovatelé služeb elektronických komunikací.[22] Zabezpečeným způsobem pak dochází k výměně informací v tomto systému, každý dotaz je veden pod jedinečným identifikačním číslem a data jsou předávána v jednotném formátu. Vedle větší transparentnosti by přitom předávání dat bylo šifrováno a zejména v případě menších poskytovatelů by bylo předání údajů bezpečnější, než je tomu v současnosti. Šifrování je nastaveno jako hybridní a spojuje v sobě výhody symetrického a asymetrického šifrování. Tento hybridní systém spočívá v tom, že přenášená data jsou šifrována symetricky a současně s nimi je distribuován asymetricky zašifrovaný klíč k rozšifrování těchto dat. Systém tak v sobě spojuje bezpečnost asymetrických šifer s rychlostí symetrických. Vedle dat jsou šifrovány i transportní kanály pro přenos zpráv. Klíče k rozšifrování zpráv nemá správce Durchlaufstelle, kterým je v Rakousku společnost Bundesrechenzentrum vlastněná plně rakouským státem, ale pouze vyžadující orgán a poskytovatel, který data předává. Nehrozí tak, že by správce Durchlaufstelle prováděl centrální monitoring předávaných dat. Systém rovněž vede jednotnou statistiku žádostí a odpovědí. Ačkoli ze strany Iuridica Remedia byl tento koncept představen při vypořádání připomínek k prováděcí vyhlášce, tak zejména z časových důvodů nebyl do návrhu začleněn. Ze strany zástupců poskytovatelů i oprávněných orgánů ovšem byla tato myšlenka přijata spíše pozitivně, což by mohlo být příslibem pro její realizaci v budoucnu.

[22] Technická specifikace Durchlaufstelle viz Technische Universität Wien, Spezifikation zur Durchlaufstelle (DLS), 3.2.2012, dostupná zde: portal.wko.at/wk/dok_detail_file.wk?angid=1&docid=1599700&conid=625986.

Jak často policie o údaje žádá?

Určit v kolika případech policie o provozní a lokalizační údaje žádala, není nijak jednoduché. Sice existují statistiky vedené ÚZČ, ty ale logicky zachytí pouze žádosti, které ÚZČ zprostředkoval. Z policejní evidence lze zjistit jednak počty žádostí a jednak počty odpovědí. Tato čísla se často zásadně liší, přičemž počet odpovědí je vyšší než počet žádostí. Bohužel Policejní prezidium na naše opakované žádosti o informace poskytovalo počty žádostí a odpovědí dosti chaoticky, takže to, jestli se jedná o žádosti či odpovědi nebylo často z odpovědí Policie zřejmé. Rozdíly v množství žádostí a odpovědí jsou dány metodikou počítání, kdy jako jednu žádost Policie eviduje například žádosti k jednomu číslu IMEI, zaslané všem třem operátorům. Počet odpovědí zvyšují i výpisy z BTS stanic. Pokud například Policie chce získat výpisy z BTS stanice všech tří operátorů v určitém místě, tak odpovědi získává v souborech za období 3 hodin. Pokud tedy například policie chce výpisy z třech BTS stanic různých operátorů za uplynulých 24 hodin, může dostat až 24 odpovědí, kterým ovšem odpovídá pouze jedna žádost.

Tab. 1: Vyžadování provozních a lokalizačních údajů ze strany policie ČR v letech 2009-2011[23]

Rok	2009	2010	2011[24]
Počet žádostí dle § 88a TŘ	70 407	83 304	44 328
Počet trestních spisů	10 222	11 121	6 072
Počet žádostí dle § 68 PolZ	2 196	2 687	1 457
Počet žádostí dle § 71 PolZ	23	80	140
Počet odpovědí poskytovatelů Policii ČR (dle § 88a TŘ, § 68 a § 71 PolZ)	145 368	163 726	93 157
Dotazy na konkrétní BTS	46 045	48 207	31 451
Dotazy na IP u internetu	966	1 565	1 132

Jak ukazuje následující tabulka (Tab 2.), tak v trestním řízení měl zcela zásadní vliv na vyžadování provozních a lokalizačních údajů nález Ústavního soudu Pl. ÚS 24/2010, který nabyl účinnosti právě

[23] Čísla vycházejí z informací poskytnutých IuRe na schůzce se zástupci ÚZČ dne 1.6.2012

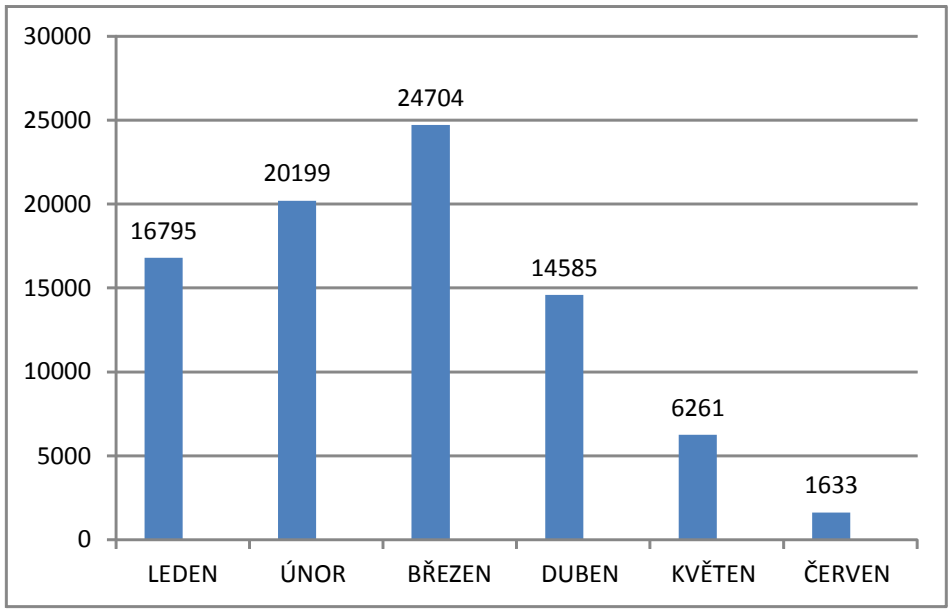
[24] Policejní prezidium uvádí ve své Analýze poněkud nižší čísla u všech položek (Policejní prezidium ČR, Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2011, 25.7.2012, dostupné na: https://racek.vlada.cz/e-vlada/eklep.nsf/0/A33D6700F2C74F97C1257A7500320166?Opendocument)

dne 12.4.2012. Z následujícího grafu (Tab.3) je zřetelný nárůst počtu odpovědí v prvních třech měsících roku 2011 a následný prudký pokles, přičemž v červnu 2011 byly poskytovateli předány údaje ve více než 15x méně případech než v březnu 2011.

Tab. 2: Vliv rozhodnutí Ústavního soudu sp. zn. Pl ÚS 24/2010 na pokles žádostí o provozní a lokalizační údaje podaných dle § 88a trestního řádu.[25]

Období	1.1.2011 - 12.4.2011	13.4.2011 - 31.8.2011	1.9.2011 - 31.3.2012
Počet žádostí podle § 88a TŘ	33 526	8 250	5 117
Průměrný počet žádostí za 1 den	328,69	58,93	24,02

Tab.3: Počet odpovědí poskytovatelů na žádosti policie dle § 88a TŘ o poskytnutí provozních a lokalizačních údajů v lednu-srpnu 2011[26]



[25] Odpověď Policejního prezidia Policie ČR na žádost IuRe o informace, 7.5.2012.

[26] Odpověď Policejního prezidia Policie ČR na žádost IuRe o informace, 27.9.2011.

Tab.4: Počty druhů žádostí o provozní a lokalizační údaje dle § 88a odst. 1 a 2 TŘ v roce 2011[27]

Počet spisů	Výpisy na pevnou linku dle §88a odst. 1 TŘ	Výpisy na pevnou linku dle §88a odst. 2 TŘ	Výpisy na mobilní linku dle § 88a odst. 1 TŘ	Výpisy na mobilní linku dle §88a odst. 2 TŘ	Výpisy na buňku	Ostatní údaje dle §88a odst. 1 TŘ	Ostatní údaje dle §88a odst. 2 TŘ	Výpisy datové komu-nikace	Celkem
5 974	133	278	9 816	898	31 370	351	11	1 119	43 976

Paralelně s Policií vedou statistiky i samotní poskytovatelé. § 97 odst. 10 ZEK ukládá poskytovatelům povinnost vést evidenci počtu případů, ve kterých na základě žádosti poskytla provozní a lokalizační údaje orgánům oprávněným k jejich vyžádání, doby, která v jednotlivých případech uplynula ode dne, kdy zahájila uchovávání provozních a lokalizačních údajů do dne, kdy o tyto údaje oprávněný orgán požádal, a počtu případů, kdy nemohla žádosti o poskytnutí provozních a lokalizačních údajů vyhovět. Tyto souhrnné údaje za kalendářní rok pak v souladu s § 97 odst. 11 ZEK předá poskytovatel do 31.1. následujícího roku Českému telekomunikačnímu úřadu, který je souhrnně poskytne Evropské komisi.[28] Tyto statistiky za roky 2008 a 2009 uveřejnila Evropská komise v rámci Hodnotící zprávy.[29]

Pokud srovnáme statistiky poskytnuté souhrnně poskytovateli a statistiky policejní, tak zjistíme, že například v roce 2009 evidovali poskytovatelé celkem 280 271 žádostí o poskytnutí údajů, z nichž nebylo vyhověno 10 446 žádostem.[30] Vzhledem k tomu, že čísla operátorů vycházejí z plnění povinnosti dle § 97 odst. 10 ZEK, jedná se o počet případů, kdy byly údaje oprávněným orgánům poskytnuty. Policie ČR v téže době evidovala pouze 72 626 žádostí a 145 368 odpovědí. Přitom právě počet

[27] Policejní prezidium, Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2011, 25.7.2012, s. 173, dostupné na: https://racek.vlada.cz/e-vlada/eklep.nsf/0/A33D6700F2C74F97C1257A7500320166?Opendocument

[28] Vzor formuláře ČTÚ pro rok 2011 dostupný zde: www.ctu.cz/cs/download/esd/formulare-vzory/xls/2011/pl11.xls

[29] Evropská komise, ZPRÁVA KOMISE RADĚ A EVROPSKÉMU PARLAMENTU, Hodnotící zpráva o směrnici o uchovávání údajů (směrnice 2006/24/ES), KOM (2O11) 225, 18.4.2011, dostupné na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:CS:PDF

[30] Tamtéž, str. 40

odpovědí přijatých od poskytovatelů by měl odpovídat počtu případů, kdy byly údaje poskytnuty dle § 97 odst. 10 ZEK. Mezi těmito čísly je nicméně rozdíl téměř dvojnásobný.

Samozřejmě je nutné přihlédnout k tomu, že Policie ČR neeviduje žádosti a odpovědi jiných oprávněných orgánů. Ty se nicméně na počtu žádostí podílejí marginálně. Jediným možným vysvětlením tak zřejmě je, že poměrně významná část případů poskytnutí provozních a lokalizačních údajů ze strany poskytovatelů není v policejních statistikách zachycena. Důvodem pak může být právě skutečnost, že nezjištěné množství dotazů je vznášeno přímo policisty bez ingerence ÚZČ a tedy i bez jakéhokoli začlenění do oficiálních statistik. I v této souvislosti je vhodné připomenout možné řešení s využitím rakouské inspirace. Nejednotná pravidla pro předávání a rozdílná metodika počítání žádostí a odpovědí vede v současné době ke stavu, kdy se v závislosti na použité metodice nabízí hned několik diametrálně odlišných čísel dokumentujících případy, v nichž Policie o údaje žádala. Z hlediska transparentnosti využívání provozních a lokalizačních údajů je tento stávající stav chaotický a zavedení systému obdobného rakouskému Durchlaufstelle by nepochybně přispělo k zpřehlednění počtu případů využívání těchto dat. Tento systém by sám prováděl počítání dotazů a odpovědí u všech oprávněných orgánů a všech poskytovatelů podle stejné metodiky. Systém by zároveň snížil administrativní náklady poskytovatelů, kteří by nemuseli v budoucnu Českému telekomunikačnímu úřadu oznamovat počty žádostí dle § 97 odst. 10 a 11 ZEK.

Jak vyplývá z Policií poskytnutých údajů (viz Tab.1 a Tab.4), tak pouze minimum případů směřuje ke zjišťování IP adres uživatelů internetu. V roce 2011 se podle policejní Analýzy se mělo jednat o pouhé 2,5 %.[31] To ostatně potvrzuje i Hodnotící zpráva Evropské komise, podle níž například v roce 2009 se drtivá většina případů poskytnutí provozních a lokalizačních údajů v České republice týkala mobilní telefonie. V porovnání s internetovým provozem byla tato data poskytnuta zhruba 25x častěji.[32] Ve všech sledovaných letech zcela dominoval zájem o výpisy na BTS buňky, a to i v roce 2011, kdy policie podle svých slov měla po rozhodnutí Ústavního soudu značný problém tyto výpisy od poskytovatelů získat.

S vědomím tohoto nepoměru je třeba pohlížet i na tvrzení, že uchovávání provozních a lokalizačních údajů je nezbytné zejména z důvodu prudkého nárůstu využívání nových prostředků komunikace a z

[31] Policejní prezidium ČR, Analýza odposlechů a záznamů telekomunikačního provozu a sledování osob a věcí dle trestního řádu a rušení provozu elektronických komunikací Policií ČR za rok 2011, 25.7.2012, s. 173, dostupné na: https://racek.vlada.cz/e-vlada/eklep.nsf/0/A33D6700F2C74F97C1257A7500320166?Opendocument

[32] Tamtéž, str. 40

důvodu přesunu trestné činnosti do internetového prostředí. Z počtu v minulosti zjišťovaných údajů o internetovém provozu je zřejmé, že provozní a lokalizační údaje jsou využívány v drtivé většině případů při vyšetřování klasické kriminality, k níž dochází mimo internet a to jako další z řady potenciálních důkazních prostředků, jejichž absenci lze ve většině případů nahradit důkazy jinými.

Nahraditelnost provozních a lokalizačních údajů jinými důkazními prostředky do značné míry potvrzují i statistiky Policie ČR. Zrušení povinnosti poskytovatelů uchovávat pro potřeby policie provozní a lokalizační údaje se nijak neodrazila na celkovém počtu trestných činů ani na objasněnosti kriminality. Jak vyplývá z oficiálních statistik Policie ČR, tak nejhorším rokem z let 2009-2011 pokud jde o počet trestných činů, byl rok 2009, tedy rok, kdy Policie ČR hojně využívala možnost požadovat provozní a lokalizační údaje. Nejvyšší míra objasněnosti trestných činů pak byla v roce 2011, kdy tuto možnost policie po většinu roku neměla.

Tab.5: Počty trestných činů a jejich objasněnost v letech 2009-2011[33]

Rok	2009	2010	2011
Počet trestných činů	332 839	313 387	317 177
Počet objasněných TČ	127 604	117 685	122 238
Objasněné TČ v %	38,34%	37,55%	38,54%

Přestože uvedené statistiky je třeba hodnotit s vědomím, že jak na počet evidovaných trestných činů, tak na jejich objasněnost má vliv celá řada faktorů, tak je zřejmé, že zrušení povinnosti operátorů uchovávat pro potřeby policie provozní a lokalizační údaje neměla fakticky žádný negativní vliv na růst kriminality nebo pokles objasněnosti trestných činů, případně, že tento negativní vliv byl eliminován efektivnějším využíváním jiných důkazních prostředků. Vzhledem k tomu, že Policie ČR neeviduje, při vyšetřování jakých trestných činů, byly provozní a lokalizační údaje využívány, není možné hodnotit, jaký byl dopad zrušení této povinnosti u jednotlivých druhů trestné činnosti.

[33] Statistické přehledy kriminality Policie ČR za léta 2009-2011, dostupné na: http://www.policie.cz/statistiky-kriminalita.aspx

Praxe při využívání údajů zpravodajskými službami a ČNB

Vedle Policie ČR využívají provozní a lokalizační údaje i další orgány, ať už v rámci trestního řízení, nebo v rámci jiných činností. Při zjišťování jejich praxe jsme se zaměřili na postupy mimo trestní řízení, tedy na praxi zpravodajských služeb a České národní banky při využívání těchto údajů. S žádostí o informace o praxi při využívání provozních a lokalizačních údajů jsme oslovili BIS i Vojenské zpravodajství. V žádosti jsme požadovali informace o tom, zda a případně v kolika případech zpravodajské služby žádaly v letech 2009-2012 o poskytnutí provozních a lokalizačních údajů. Dále jsme požadovali informaci o tom, o jaká zákonná ustanovení se žádosti případně opírají. Se zástupci BIS jsme se navíc celkem dvakrát sešli, abychom si vzájemně vysvětlili naše názory na existenci povinného uchovávání provozních a lokalizačních údajů a na možnost zpravodajských služeb tyto údaje využívat.

Jak BIS, tak Vojenské zpravodajství nám na písemně podané žádosti o informace odmítly odpovědět. BIS odůvodnila své odmítnutí odkazem na § 7 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále také „ZSPI“).[34] Vojenské zpravodajství odmítlo informace poskytnout s odkazem na § 11 odst. 4 písm. c) ZSPI. [35]

BIS nám nicméně v písemné odpovědi sdělila, že oprávnění ke zjišťování údajů o telekomunikačním provozu vyplývá z § 8 odst. 1 písm. b) ZoBIS. Toto přesvědčení nám potvrdili i zástupci BIS na společném jednání. V podobném duchu se vyjádřilo i Vojenské zpravodajství, které nám sdělilo, že oprávnění vyplývá z §§ 7- 11 ZoVZ. Tento výklad přijalo i Ministerstvo vnitra v důvodové zprávě k návrhu nového zákona.[36]

Jak potvrdili zástupci BIS v odpovědi na naši žádost o informace, tak při osobním setkání, tak toto oprávnění je při praxi zpravodajských služeb těžko uplatnitelné, protože zejména velcí telefonní operátoři přijali výklad, že jim není zákonem uložena povinnost data předávat, a tak oprávnění zpravodajských služeb zůstalo pouze v teoretické rovině, protože provozní a lokalizační údaje jednoduše zpravodajským službám nebyly a nejsou na základě příslušných ustanovení ZoBIS a ZoVZ poskytovány. To dokládá i opakovaná snaha BIS prosadit zákonnou úpravu nejen oprávnění získávat provozní a lokalizační údaje, ale i jejich poskytnutí vyžadovat.

---

34 Odpověď BIS na žádost o informace podanou IuRe, 21.5.2012.

35 Odpověď Vojenského zpravodajství na žádost o informace podanou IuRe, 10.5.2012.

36 Důvodová zpráva k zákonu č. 273/2012 Sb., s. 14

S novou právní úpravou v zákoně č. 273/2012 Sb., která definuje zpravodajské služby jako oprávněné orgány k vyžadování provozních a lokalizačních údajů a zároveň upravuje podmínky, za nichž mohou zpravodajské služby o tyto údaje žádat (zejména nutnost disponovat souhlasem soudce vrchního soudu) lze tedy očekávat, že poskytovatelé začnou zpravodajským službám údaje předávat.

V případě České národní banky jsme se celkem dvakrát obrátili s žádostí o informace na ČNB. V první odpovědi z 10.6.2011 nám ČNB sdělila, že údaje vyžaduje, ale zákon jí neukládá vést evidenci dotazů, takže tuto evidenci nevede.[37] O rok později nám už v reakci na druhou žádost dne 4.6.2012 byly požadované údaje sděleny.[38] V letech 2009-2012 (k červnu 2012) bylo podle vyjádření ČNB vyžádáno poskytnutí provozních a lokalizačních údajů od poskytovatelů v celkem 4 případech. Vzhledem k tomu, že v některých případech byly údaje vyžádány od více poskytovatelů, případně byly požadovány doplňující údaje, bylo zasláno celkem 10 žádostí.

Typově se podle vyjádření ČNB jednalo o případy vyšetřování podezření na nezákonné jednání v oblasti kapitálového trhu, založené na podezření na zneužití vnitřní informace o osobě emitenta akcií obchodovaných na regulovaném trhu nebo podezření na spáchání trestného činu. Pokud jde o vyšetřování trestných činů, tak je otázka, z jakého ustanovení ČNB odvozuje svoje právo či povinnost trestnou činnost vyšetřovat, když není policejním orgánem ve smyslu § 12 odst. 2 TŘ.

Podle vyjádření ČNB probíhá proces vyžadování informací následujícím způsobem. Podání žádosti navrhuje příslušný inspektor, který je pověřen prošetřením případu. Jeho nadřízený vedoucí referátu vyhodnotí, zda vyžádané údaje mohou přispět k objasnění skutečností důležitých pro odhalení správního deliktu a jeho pachatele a nelze-li sledovaného účelu dosáhnout jinak. Konečné rozhodnutí, zda bude žádost o poskytnutí informací odeslána a jaké údaje budou vyžádány, učiní ředitel příslušného odboru, který podepisuje spolu s vedoucím referátu dopis, jímž jsou údaje od povinné osoby vyžádány. Povinná osoba odpovídá rovněž dopisem, v němž uvede požadované informace nebo důvod, proč tyto informace nemohou být ČNB poskytnuty.

Kolik nás to všechno stojí?

Proplácení nákladů na povinné uchovávání a poskytování provozních a lokalizačních údajů je zakotveno v § 97 odst. 7 ZEK, podle něhož náleží právnické nebo fyzické osobě od oprávněného subjektu, který si úkon (odposlechy, poskytnutí uchovávaných provozních či lokalizačních údajů nebo

[37] Odpověď ČNB na žádost o informace podanou IuRe,10.6.2011.

[38] Odpověď ČNB na žádost o informace podanou IuRe, 4.6.2012.

údaje z databáze účastníků veřejné telefonní služby) vyžádal nebo jej nařídil, úhrada efektivně vynaložených nákladů. Prováděcí vyhláška č. 486/2005 Sb. stanoví pravidla pro proplácení mimo jiné i uchovávání a poskytování provozních a lokalizačních údajů.

V období po nálezu Ústavního soudu sp. zn. Pl. ÚS 24/10 chybí právní titul pro proplácení uchovávání a poskytování provozních a lokalizačních údajů, protože povinnost proplácet byla úzce vázána na povinnost uchovávat a poskytovat zakotvenou ve zrušeném § 97 odst. 3 ZEK. Proto po dubnu 2011 by nemělo k úhradám docházet. Od října 2012 po nabytí účinnosti nové právní úpravy by měl platit stejný systém náhrad, jaký platil před nálezem Ústavního soudu.[39]

Propláceny podle vyhlášky č. 486/2005 Sb. mají být jednak fixní náklady zejména na hardwarové vybavení a jeho zabezpečení (CAPEX) a dále náklady na poskytnutí výpisu (OPEX). Výše nákladů na uchovávání provozních a lokalizačních údajů se určuje jako součet účetních odpisů zařízení sloužícího pro jejich uchovávání a nákladů vynaložených na zabezpečení tohoto zařízení. To, co konkrétně se bude proplácet, pokud jde o fixní náklady, obvykle záleží na dvoustranném jednání mezi poskytovatelem a zástupci Policie ČR. Naopak výše úhrady za jednotlivé výpisy je stanovena v příloze vyhlášky a má být proplácena orgány, které si údaje vyžádají.

Tab. 6 Náklady proplacené Policií ČR poskytovatelům podle § 97 odst. 7 ZEK[40]

Rok	2009	2010	2011
OPEX	37 954 990,00 Kč	39 736 536,00 Kč	20 431 464,00 Kč
CAPEX	146 693 103,00 Kč	124 789 242,00 Kč	91 220 706,00 Kč
Celkem	184 648 093,00 Kč	164 525 778,00 Kč	111 652 170,00 Kč

Nárok na proplácení nákladů se vztahuje na všechny poskytovatele. V letech 2010 a 2011 před zrušením příslušné právní úpravy ale o proplacení nákladů žádal pouze zlomek povinných poskytovatelů. Proplacení fixních nákladů (CAPEX) na uchovávání provozních a lokalizačních údajů požadovalo podle údajů Ministerstva vnitra v roce 2010 15 poskytovatelů, kterým bylo proplaceno celkem 25,5 milionu Kč, v témže roce pak bylo proplaceno celkem 25,1 milionu Kč 19 subjektům za poskytnutí údajů. V prvním čtvrtletí roku 2011 se o proplacení fixních nákladů přihlásilo už 40 subjektů,

[39] Důvodová zpráva k zákonu č. 273/2012 Sb., s. 31n

[40] Jsou zahrnuty náklady na vyžadování provozních a lokalizačních údajů a na realizaci odposlechů a poskytnutí informací z databáze účastníků. Čísla vycházejí z informací poskytnutých IuRe na schůzce se zástupci ÚZČ dne 1.6.2012.

kterým bylo proplaceno 7,8 milionu Kč. Za jednotlivé výpisy se pak 15 poskytovatelům vyplatilo 9,6 milionu Kč.[41]

V současné době eviduje Český telekomunikační úřad celkem 3187 záznamů o nahlášení podnikání v oboru elektronických komunikací.[42] Jedná se o právnické či fyzické osoby, na něž se bude zpravidla vztahovat povinnost uchovávat a případně poskytovat provozní a lokalizační údaje. K tomuto číslu je možné přičíst i další subjekty, které v daném oboru přímo nepodnikají, ale poskytují veřejně přístupnou službu jako vedlejší produkt jiné své služby, například již zmínění poskytovatelé bezplatného wi-fi připojení v kavárnách, restauracích, hotelech apod., ačkoli jejich povinnost uchovávat provozní a lokalizační údaje je sporná.

Bylo by nepochybně zajímavé, pokud by všechny tyto povinné subjekty požadovaly proplacení svých faktur za příslušné technické vybavení a zabezpečení dat. Jde nicméně spíše o teorii, k jejíž realizaci v praxi zřejmě nedojde. Přesto do jisté míry dokumentuje tento stav jistou absurdnost data retention, kdy povinnost údaje uchovávat má velmi široký okruh povinných subjektů, přičemž pravděpodobnost, že tyto subjekty budou policií někdy osloveny s žádostí o informace, je mizivá. Je ostatně otázkou nakolik skutečně tyto subjekty svoji povinnost uchovávat údaje po stanovenou dobu před nálezem Ústavního soudu plnily nebo v budoucnu plnit budou a zda případné neplnění této povinnosti bude vůbec někomu vadit.

41 Důvodová zpráva k zákonu č. 273/2012 Sb., s. 31

42 http://www.ctu.cz/ctu-online/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni.html

IV. Závěr

Povinné uchovávání provozních a lokalizačních údajů se se zákonem č. 273/2012 sb. vrací do našeho právního řádu. Přestože novou právní úpravu lze považovat za zlepšení oproti právní úpravě, kterou zrušil Ústavní soud, zejména pokud jde o jasné vyjmenování oprávněných orgánů, vyjasnění oprávnění zpravodajských služeb nebo o řadu pozitivních změn v § 88a TŘ, tak řada věci zůstala nedořešena. Za velký problém nové právní úpravy lze považovat nezměněnou úpravu oprávnění údaje vyžadovat podle příslušných ustanovení PolZ, které paradoxně kritizovali i sami policisté. Zejména široké oprávnění žádat údaje v souvislosti s pátráním po hledané nebo pohřešované osobě bude se zpřísněním úpravy vyžadování údajů v trestním řízení nejsnazší cestou ke zneužití pravomocí. V současné době je Generální inspekci bezpečnostních sborů jeden takový případ zneužití tohoto oprávnění již vyšetřován.[43] Vhodným řešením by bylo zrušení tohoto oprávnění u hledaných osob a osob neznámé totožnosti, vázat možnost zjišťovat tyto údaje pouze na pohřešovanou osobu, omezit časový rozsah údajů, o něž lze žádat, případně zavést soudní příkaz k poskytnutí údajů.

Otázkou rovněž je nakolik nová právní úprava odstraní praxi, kdy provozní a lokalizační údaje jsou vyžadovány přímo od poskytovatelů bez zprostředkování ÚZČ, případně bez splnění zákonných podmínek, jako je například povolení soudu. Odstranění této praxe bude vyžadovat jednak zvýšení právního povědomí poskytovatelů, kteří se nebudou bát tyto žádosti odmítat s odkazem na povinnost mlčenlivosti, ale i důsledné odmítnutí těchto praktik ze strany Policie ČR. Krokem správným směrem může být vydefinování kontaktních pracovišť, které požaduje návrh nové vyhlášky. Komplexnějším řešením by byla inspirace rakouským modelem *Durchlaufstelle*, který by umožnil nejen bezpečné a zákonné předávání údajů, ale i transparentní statistiky využívání těchto údajů.

Jako zbytečné riziko vnímáme centralizované uchovávání již vyžádaných výpisů ze strany poskytovatelů i ÚZČ po předání údajů vyžadujícímu policistovi. I v tomto se lze inspirovat modelem *Durchlaufstelle,* kde je sice předávání údajů mezi poskytovatelem a konečným příjemcem realizováno prostřednictvím centralizovaného místa, tímto uzlem nicméně data „protékají“ v zašifrované podobě, přičemž jejich rozšifrování je schopen provést pouze poskytovatel a vyžadující policista, nikoli správce „průtokového“ místa.

Zdůvodňování existence data retention skutečností, že se kriminalita přesunuje do virtuálního prostoru, kde Policie nemá k dispozici klasické důkazní prostředky, je rovněž pochybné. Ne, že by se snad

[43] Odpověď GIBS na žádost o informace podanou IuRe,18.7.2012.

kriminalita do jisté míry skutečně do virtuálního prostoru nepřesouvala, využívání provozních a lokalizačních údajů při vyšetřování internetové kriminality ale tvoří zcela nepatrný zlomek celkového počtu žádostí o výpisy. Pravým důvodem je tedy spíše snaha získat další potenciální důkazní prostředek pro potírání klasické kriminality v reálném prostoru. Tato snaha není sama o sobě ničím špatným, pokud bychom netrvali na pojmenování pravých důvodů pro existenci data retention, naše analýza ale potvrdila i další postřeh, který již popsala například stínová zpráva European Digital Rights[44] k Hodnotící zprávě Evropské komise. Jedná se o absenci statistických údajů, které by dokazovaly nezbytnost data retention. Z údajů poskytnutých Policií vyplývá, že ačkoli došlo v reakci na nález Ústavního soudu od poloviny dubna 2011 k rapidnímu poklesu počtu žádostí o provozní a lokalizační údaje, tak toto se nijak neodrazilo na míře kriminality nebo na úrovni její objasněnosti v roce 2011.

Tradičním problémem, který je ovšem zakódován v samotném genomu data retention, či přesněji řečeno ve Směrnici 2006/24/ES, je nejasné vymezení osob, na něž se vztahuje povinnost údaje uchovávat. I nadále přetrvává situace, kdy existují široké možnosti obcházení data retention s využitím služeb subjektů, které nemají povinnost data uchovávat, například proto, že jsou poskytovateli služeb informační společnosti a nikoli elektronických komunikací. Policie se situaci snaží řešit například návrhy na rozšiřování okruhu povinných osob i na poskytovatele serverových služeb[45] v marné naději, že jednou možná na žádosti o informace začnou reagovat i společnosti jako Facebook. I pokud by se toto rozšíření v budoucnu podařilo realizovat, což by mimochodem s sebou neslo obrovské finanční náklady, existují a v budoucnu se budou objevovat stále nové způsoby, jak se data retention vyhnout, ať už jde o využívání různých druhů šifrování, proxy serverů nebo využívání služeb poskytovaných ze zemí, kam ruka Policie nedosáhne. Tyto způsoby pak logicky využívají v první řadě ti, k jejichž odhalování měla data retention původně sloužit, a v sítích data retention uvíznou spíše ti, na které by ruka zákona dosáhla s využitím jiných důkazů stejně. Je pak otázka, kam až budeme v budoucnu ochotni zajít, jaké náklady, ať už v penězích nebo v našich svobodách, budeme ochotni za děravou plošnost data retention platit.

---

44 EDRi, Shadow evaluation report on the Data Retention Directive (2006/24/ES), Brusel, 17.4.2011, dostupné na: http://www.edri.org/files/shadow_drd_report_110417.pdf

45 Jedna z připomínek Ministerstva vnitra při připomínkovém řízení k návrhu nové vyhlášky.