Z PRAXE

Jan Strakoš

K využití údajů z telekomunikačního provozu pro potřeby přestupkového řízení

I. Úvodem

Během mé dosavadní správní praxe jsem již několikrát zaznamenal snahu některých správních orgánů získat pro účely dokazování v řízení o přestupku tzv. provozní a lokalizační údaje ve smyslu zákona o elektronických komunikacích[1)]. Důvod byl vždy prostý – důkazní nouze. Nejčastěji se přitom jednalo o případy elektronických podvodů anebo urážek na internetu, přičemž podezřelý subjekt v následném řízení o přestupku rezolutně odmítal spáchání takového činu a na svou obhajobu tvrdil, že elektronické zařízení, jež se stalo nástrojem deliktu, buď v inkriminovanou dobu na inkriminovaném místě nepoužíval anebo přímo připouštěl, že ho mohly užívat jiné osoby, které s ním zařízení sdílejí (nejčastěji osoby blízké). Vzhledem k tomu, že přestupkový zákon[2)] ani správní řád[3)] neposkytuje účinné nástroje, jak tyto pochybnosti lépe prověřit, povětšinou musel správní orgán řízení o přestupku zastavit z důvodu *in dubio pro reo*, protože policejní orgán, na který se správní orgán s žádostí o zajištění a poskytnutí provozních a lokalizačních údajů obrátil, zcela po právu správnímu orgánu sdělil, že k tomu nemá oprávnění. Ve světle stávající platné právní úpravy i judikatury českého Ústavního soudu, zvláště kladoucí důraz na ochranu těchto údajů (z důvodu ústavně zaručeného práva každého na soukromí) a jejich poskytování jen do určitých procesů (v podstatě jen ve výjimečných případech), se však v tomto ohledu mohou jevit jako irelevantní určité situace, k nimž v rámci řízení může dojít, a během nichž se správní orgán k těmto údajům (navzdory veškeré opatrnosti) dostane.

---

1) Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, (dále jen „zákon o elektronických komunikacích“).
2) Zákon č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů, (dále jen „přestupkový zákon“).
3) Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, (dále jen „správní řád“).

Tedy pro upřesnění, cílem tohoto příspěvku není proklamovat posilování pravomocí správních orgánů v řízení o přestupku, byť by se tím měl zákonodárce dle mého soudu minimálně zabývat vzhledem k četnosti přestupků páchaných v digitálním prostředí (nehledě na hrozby *deep fakes* apod.). Smyslem tu není ani popsat celou, poměrně složitou problematiku poskytování provozních a lokalizačních údajů, nýbrž jen upozornit na některé zajímavé otázky, které se naskýtají při jejich využívání orgány činnými v trestním řízení, (dále též „OČTŘ"), při vyšetřování některých trestných činů, z nichž se nakonec mohou stát jen přestupky. Právě zde lze totiž pokládat za pozoruhodný moment, pokud se tyto údaje ocitnou v rukou správních orgánů, které však na ně nárok ze zákona nemají. S tím totiž může souviset i další logická otázka, a to otázka jejich případné použitelnosti jako důkazu v řízení o přestupku, dochází-li v tomto ohledu k zásahu do soukromí (otázka proporcionality).

II. Soukromí jako pojem i subjektivní právo a jeho ochrana

Nejprve dovolte několik obecnějších úvah pro uvedení do problému, k němuž se v návaznosti na využitelnost provozních a lokalizačních údajů vyjádřil i český Ústavní soud, byť ne zrovna v souvislosti s přestupky a byť ne jednotně.[4)]

Žijeme v době rozmachu moderních technologií. V době, kterou bychom bez nadsázky mohli přirovnat nové vlně průmyslové revoluce plné inteligentních věcí. Stroje řídí naši výrobu, dokážou komunikovat mezi sebou,[5)] jejich prostřednictvím můžeme komunikovat s dalšími lidmi i na druhé straně zeměkoule; jednoduše, lacině, ne-li úplně zadarmo. Nic ale není zadarmo a tento digitální luxus už vůbec ne. Digitální svět, který nás obklopuje, je dravý a nebezpečný, zejména pokud jde o naše soukromí. Stroje kódují naše obličeje, analyzují náš hlas nebo tepovou frekvenci a údaje o našich životech, rodině, přátelích, náladách, mnohdy i intimních záležitostech ukládají kdesi v nekonečném moři kvantového prostoru. Nejde přitom jen o kamerové systémy či o stále populárnější drony, které nás mohou sledovat jako zlověstné Sauronovo oko, ale také třeba o chytré hračky dětí či dokonce sexuální hračky dospělých. I ty mohou získávat různá data a dále je analyzovat.[6)] Zohledníme-li navíc problém spojený s uchováváním citlivých údajů operátory v rámci naší každodenní komunikace prostřednictvím

---

4) Jednak v nálezu ze dne 14. 5. 2019, sp. zn. Pl. ÚS 45/17, jímž byla právní úprava uchovávání provozních a lokalizačních údajů v našem právním řádu shledána za ústavně konformní, a jednak v nálezu z roku 2011 (sp. zn. Pl. ÚS 24/10), v němž byl shledán pravý opak.

5) V této souvislosti se někdy hovoří o tzv. komunikaci *machine-to-machine*, neboli zkráceně M2M.

6) K tomu viz např. POVŠE, D. F.: "Screwdriving" and the age of free (data on) love. *Katholieke Universiteit Leuven - Center for IT & IP Law (CiTiP)* [online]. 28. 11. 2017 [cit. 24. 7. 2019]. Dostupné z: https://www.law.kuleuven.be/citip/blog/screwdriving-and-the-age-of-free-data-on-love/

elektronických komunikačních kanálů[7] a naši celkovou neschopnost autarkie, tj. snahy se vymanit ze závislosti na těchto technologiích, logicky se postupně zmenšuje i míra naší důvěry v okolní svět, protože to, co bychom dříve pokládali za diskrétní, tedy skryté před druhými, již tak nenápadné být nemusí. Svým způsobem lze proto souhlasit s názorem, že se sami dobrovolně svlékáme a vstupujeme tak do éry, v níž publicita začíná být normou a soukromí každého z nás jen jakousi ozdobou.[8] Slovy Margrethe Vestagerové, bývalé evropské komisařky pro hospodářskou soutěž je přitom *„soukromí základním aspektem bytí“*[9] a právo na soukromí je v kontinentální Evropě[10] vnímáno jako základní hodnota, lidské právo vtělené v právu na soukromý život, jehož součástí je i právo na informační sebeurčení (viz čl. 10 odst. 3 Listiny základních práv a svobod, dále jen „Listina“);[11] tedy právo jednotlivce rozhodovat se podle

---

7) Za nebezpečnou pro naše soukromí lze však označit v zásadě jakoukoliv elektronickou službu založenou na nevýběrovém a plošném monitoringu a uchovávání dat. V této souvislosti lze např. negativně zhodnotit produkt Společnosti pro informační databáze, a. s., v podobě její služby TelcoScore, zaměřující se na predikce chování zákazníků. Pokud totiž mobilní operátoři O2 Czech Republic a. s., T-Mobile Czech Republic a. s. a Vodafone Czech Republic a. s. hodnotí („skórují“) své zákazníky podle toho, na kolik využívají jejich služby, zda jsou bohatí či chudí, a toto skóre pak dále poskytují např. bankám, které se na jeho základě rozhodují, zda konkrétnímu uživateli elektronické služby, žádajícímu o úvěr v bance, úvěr poskytnou nebo ne, v tomto nelze než spatřovat cosi z obrysů čínského bodování důvěryhodnosti občanů. Přitom v Číně, jak je obecně známo, soukromí jednotlivce téměř neexistuje. Podrobněji viz TelcoScore. *SID* [online]. © 2019 Společnost pro informační databáze a.s. [vid. 24. 7. 2019]. Dostupné z: https://www.sid.cz/telco-score/.

8) Příhodně dnešní stav vystihují slova: *„Maybe privacy is the kink now, and publicity the norm./ Možná že soukromí je teď zločin a publicita normou.“* In POVŠE, op. cit.

9) In KEEN, A.: *Jak opravit budoucnost.* Praha: Argo, 2019, s. 122.

10) Stranou ponechávám poněkud odlišné americké chápání tohoto práva jako práva akcesorického k některému ze základních práv zakotvených v americké ústavě. Obdobně viz např. FIALOVÁ, E.: *Bezkontaktní čipy a ochrana soukromí.* Praha: Leges, 2016, s. 28. K prolínání evropského a amerického pojetí ochrany soukromí dále viz POLČÁK, R. a kol.: *Právo informačních technologií.* Praha: Wolters Kluwer ČR, 2018, s. 404 až 406.

11) Dle čl. 10 odst. 3 Listiny: *Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.* V českém právním prostoru je však východiskem ochrany soukromí především čl. 7 odst. 1 Listiny, v němž se uvádí *Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem*. Dále je významný čl. 10 odst. 2: *Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života*, popř. čl. 13, zakotvující listovní tajemství *(stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením)*. Na nižší, tj. zákonné úrovni nelze nezmínit třeba § 86 zákona č. 89/2012 Sb., občanský zákoník: *Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.* Každý má tedy právo na soukromý život a ochranu svého soukromí. Nejinak se k tomu staví i čl. 8 Úmluvy o ochraně lidských práv a základních svobod: *(1) Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence. (2) Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky*

vlastního uvážení, jaké údaje a v jakém rozsahu ze své intimní zóny uvolní a zpřístupní jiným subjektům.[12)]

III. Provozní a lokalizační údaje

Provozní a lokalizační údaje nepředstavují vlastní obsah komunikace uskutečňované prostřednictvím telefonu, tzn., kdo, co řekl (ať už formou telefonního hovoru) nebo napsal (např. cestou SMS nebo MMS zprávy), ale jak už napovídá označení těchto údajů, ve shodě s § 90 a 91 zákona o elektronických komunikacích[13)] jde vlastně o jakékoli údaje, které mají schopnost identifikovat volajícího i volaného, což zahrnuje nejen údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace, ale v širším slova smyslu jsou jimi třeba i teplotní mapy, tj. grafické znázornění údajů za použití barev k naznačení přítomnosti osob v určité lokalitě.[14)] Podle § 97 odst. 4 zákona o elektronických komunikacích ve spojení s § 2 prováděcí vyhlášky Ministerstva průmyslu a obchodu č. 357/2012 Sb., kde jsou tyto údaje dále podrobněji specifikovány, se tak např. u sítí elektronických komunikací s přepojováním paketů u služby přístupu k internetu z mobilního připojení jedná o: *1. typ připojení, 2. telefonní číslo uživatele, 3. identifikátor mobilního zařízení, 4. datum a čas zahájení a ukončení připojení k internetu, 5. označení základnové stanice Start a základnové stanice Stop, 6. adresa IP[15)] a číslo portu, ze kterých bylo připojení uskutečněno.*

Okolnost, že se jedná pouze o metadata, nicméně neznamená, že by tyto údaje nebyly součástí elektronické komunikace, a že by si jejich plošným sledováním (zejména po delší dobu) nebylo možné učinit úsudek, např. s kým se konkrétní jedinec stýká či k jakým sklonům nebo slabostem inklinuje. Za zvláště problematické lze pak označit sledování osob s povinností mlčenlivosti. Proto i tyto údaje jsou hodny ochrany. K tomu se ostatně podrobně vyslovil i český Ústavní soud již v roce 2001,[16)] když se přiklonil k rozsudku Evropského soudu pro lidská práva (dále jen „ESLP“) ze dne

---

nebo ochrany práv a svobod jiných nebo čl. 7 Listiny základních práv EU (dostupná z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A12012P%2FTXT).

12) Srov. např. s nálezem Ústavního soudu ČR ze dne 22. 1. 2001, sp. zn. II. ÚS 502/2000: *„Soukromí každého člověka je hodno ochrany podle čl. 13 Listiny základních práv a svobod…“*. Dále viz nález Ústavního soudu ČR ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10.

13) Zatímco *provozními údaji se rozumí jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování* (§ 90 odst. 1), *lokalizačními údaji se rozumí jakékoli údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací* (§ 91 odst. 1).

14) Viz str. 15 důvodové zprávy k návrhu nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích). Dostupné z: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

15) Jen připomeňme, že i dynamická IP adresa je osobním údajem (viz rozsudek Soudního dvora EU, dále jen „ESD“ ze dne 19. 10. 2016, C-582/14, ***Patrick Breyer v. Německo***).

16) Viz nález Ústavního soudu ČR ze dne 22. 1. 2001, sp. zn. II. ÚS 502/2000.

2. 8. 1984 ve věci *Malone proti Spojenému království,*[17] a názoru, že ochrana soukromí se vztahuje též k těmto údajům. Snad právě proto je užívání těchto údajů zejména v trestních procesech zvláště ožehavým tématem, neboť s tím souvisí ona otázka proporcionality zásahu do soukromí. A snad právě pro tuto konstruktivní nejednoznačnost není v Evropě na tento problém jednotného názoru.[18]

V této souvislosti český zákon o elektronických komunikacích stanoví povinnost tyto údaje uchovávat podnikatelům (tj. právnickým nebo fyzickým osobám) zajišťujícím veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací.[19] Tato povinnost se však nevztahuje na poskytovatele tzv. *over-the-top* služeb nebo-li OTT služeb (např. *Skype, Viber, WhatsApp*).

Samotný podklad pro povinnost podnikatele uchovávat tyto údaje pak lze najít v § 97 odst. 3 téhož zákona, kde je stanovena maximální šestiměsíční lhůta jejich uchování včetně taxativního výčtu subjektů, kterým musí být bezodkladně (optikou judikatury tzn. zpravidla do 3 dnů) poskytnuty, v případě že o ně požádají, a to pro účely a při splnění podmínek stanovenými konkrétními zvláštními předpisy, postupem podle zákona o elektronických komunikacích. Pokud některý z níže uvedených subjektů o jejich vydání nepožádá anebo není vydán příkaz podle zvláštního právního předpisu, aby byly uchovány, po uplynutí této doby je podnikatel povinen je zlikvidovat. "Oprávněným subjektem" zmíněné ustanovení přitom rozumí:

a) **orgán činný v trestním řízení (OČTŘ)**, který o ně požádá pro účely a při splnění podmínek stanovených trestním řádem,[20]

---

17) Rozhodnutí ESLP ze dne 2. 8. 1984, č. 8691/79, ***Malone proti Spojenému království.*** [online]. [vid. 24. 7. 2019]. Dostupné z: https://hudoc.echr.coe.int/eng#{"itemid":["001-57533"]}

18) Právní úprava uchovávání provozních a lokalizačních údajů byla po přijetí směrnice 2006/24/ES promítnuta do řady právních řádů členských států EU, avšak na základě později přijatého rozsudku ESD ze dne 8. 4. 2014 ve spojených věcech C-293/12 a C-594/12 *(Digital Rights Ireland Ltd)*, jenž uvedenou směrnici prohlásil za neplatnou, se k tomuto tématu v Evropě v zásadě vyprofilovaly dva antipodní přístupy. První přístup reprezentují země, jejichž ústavní soudy vlivem zmíněného judikátu ESD začaly právní úpravy, vycházející ze zneplatněné směrnice, rušit (např. Rakousko či Bulharsko - v případě těchto zemí v podstatě zafungoval jakýsi „domino efekt"), příp. přistoupily k úplnému zákazu plošného uchovávání těchto údajů (příkladem tu budiž Slovensko - viz nález Ústavního soudu Slovenské republiky sp. zn. PL. ÚS 10/2014 z 29. dubna 2015) - kde se uplatňuje pouze tzv. *quick freeze* systém, tzn. že údaje o veškeré komunikaci se neuchovávají plošně, ale jen ve vztahu k podezřelým subjektům. K uchovávání přitom dochází až poté, co o to požádá kompetentní orgán veřejné moci.). Druhý přístup pak reprezentuje ČR a další země (např. Dánsko), které považují svou národní právní úpravu za přísnou a proporcionální ve vztahu k přípustnosti zásahu do práva na informační sebeurčení.

19) Shodně KOLOUCH, J.: *CyberCrime.* Praha: nakladatelství Milan Hodek, 2016, s. 117.

20) Viz § 88a zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád) v aktuálně platném a účinném znění.

b) **Policii ČR**, která o ně může požádat 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 a při splnění podmínek stanovených zákonem o Policii ČR[21] nebo prověřování chráněné osoby a při splnění podmínek stanovených zákonem o zvláštní ochraně svědka,

c) **BIS**, která o ně může požádat pro účely a při splnění podmínek stanovených zákonem o BIS,

d) **Vojenské zpravodajství**, které o ně může požádat pro účely a při splnění podmínek stanovených zákonem o Vojenském zpravodajství,

e) **ČNB**, která o ně může požádat pro účely a při splnění podmínek stanovených zákonem o dohledu v oblasti kapitálového trhu.

IV. Obecně k § 88a trestního řádu

Možnost zjistit údaje o telekomunikačním provozu pro účely trestního řízení je upravena v § 88a trestního řádu a představuje jeden z důkazních prostředků, který trestní řád přímo nabízí. Obecně lze přitom souhlasit s názorem, že v boji proti trestné činnosti dokonce představuje nenahraditelnou pomůcku, protože provozní a lokalizační údaje, které se dají jeho cestou získat, mohou být zásadní digitální stopou při vyšetřování. Nelze se proto divit, že tento důkazní prostředek OČTŘ využívají rády a že jsou samozřejmě pro zachování této možnosti v zákoně. Na tom ale nelze obecně spatřovat nic špatného ani zvláštního. Posláním OČTŘ je stíhat trestnou činnost; to je smysl jejich existence. Ostatně i ESD v již zmiňovaném rozsudku *Digital Rights Ireland Ltd*, uvádí, že tyto údaje pomáhají při objasňování závažné trestné činnosti. Zde je však třeba zdůraznit, že by mělo jít o „závažnou trestnou činnosť" a zde již můžeme narazit na odlišné vnímání toho, co je pro koho vlastně závažné, neboť někdo může uvedené interpretovat extenzivně[22] (z pohledu toho kterého státu ostatně není výjimkou, že v některých zemích se určité trestné činy považují za extrémně závažné, zatímco v jiných jsou stejné činy subsumovány pod méně závažné trestné činy či dokonce pod přestupky), jiný zase restriktivně.

A protože nesporně jde o výraz vágní, možná tu je záhodno připomenout, proč se úprava elektronických komunikací, včetně zpracování provozních a lokalizačních údajů (která do té doby byla v Evropě značně rozmanitá) vlastně začala harmonizovat a řešit. Byla to právě snaha EU i jednotlivých členských států lépe čelit hrozbám teroristických útoků. Proto nelze než souhlasit s ESD, resp. s jeho názorem v rozsudku *Tele2 Sverige AB a Watson*

---

[21] Viz § 68 odst. 2 a § 71 písm. a) zákona č. 273/2008 Sb., o Policii ČR.

[22] Což svým způsobem může podporat rozsudek ESD ze dne 2. 9. 2018, C-207/16, ***Ministerio Fiscal***.

(byť částečně zmírněným v rozsudku ***Ministerio Fiscal***),[23] že i v tomto směru, tedy restriktivně by měl být interpretován čl. 15 odst. 1 směrnice 2002/58/ES, na nějž se někdy někteří odvolávají s přesvědčením, že se neomezuje jen na boj proti závažným trestným činům. Podle názoru zastávaného v tomto příspěvku by však závažnost (a to i navzdory rozsudku *Ministerio Fiscal*, v němž byl ovšem řešen jen minimální zásah do práv dotčených osob) měla být určujícím kritériem, aby mohl být aprobován veřejný zájem na zásahu do práva na soukromí a informačního sebeurčení. Ostatně i Ústavní soud ČR se již několikráte vyjádřil v tom smyslu, že zásah musí být proporcionální[24] a za tím účelem si příliš nelze představit, že by aproboval zásahy do soukromí při každé trestné činnosti, potažmo u projednávání přestupků, vezme-li se v úvahu, že sám poměrně přísně podrobuje jednotlivá ustanovení právních předpisů, u kterých hrozí zásah do základních práv a svobod, testu proporcionality. Tento test zahrnuje celkem tři kritéria: 1) korektiv účelnosti (vhodnosti) zásahu, 2) korektiv potřebnosti zásahu a 3) korektiv přiměřenosti zásahu (ten je zvláště důležitý, vezmou-li se v potaz všechny aspekty monitoringu elektronické komunikace).

---

[23] V tomto případě španělský vyšetřující soudce odmítl na návrh kriminální policie uložit několika poskytovatelům služeb elektronických komunikací povinnost poskytnout telefonní čísla aktivovaná od 16. 2. do 27. 2. 2015 v návaznosti na loupež ze dne 16. 2. 2015, při níž byla oběti, která byla zraněna, odcizena peněženka a mobilní telefon. Odmítnutí bylo učiněno z důvodu, že nešlo o závažnou trestnou činnost [podle soudce totiž španělský zákon č. 25/2007 o uchovávání údajů o elektronické komunikaci a veřejných komunikačních sítí ze dne 18. 10. 2007 (BOE č. 251 ze dne 19. 10. 2007, s. 42517) omezuje předávání údajů uchovávaných poskytovateli služeb elektronických komunikací na případy závažné trestné činnosti; podle španělského trestního zákoníku ze dne 23. 11. 1995 (BOE č. 281 ze dne 24. 11. 1995, s. 33987), jsou závažné trestné činy trestány trestem odnětí svobody na dobu delší pěti let, kdežto ve věci v původním řízení podle všeho o takovou trestnou činnost nejde]. To se však nelíbilo státnímu zástupci, který proti usnesení o odmítnutí poskytnutí údajů vyšetřujícího soudce podal odvolání s tím, že údaje měly být poskytnuty s ohledem na povahu činů a rozsudek Tribunal Supremo (Nejvyššího soudu Španělska) ze dne 26. 7. 2010 týkající se obdobného případu. Následně španělský soud položil ESD předběžnou otázku, týkající se výkladu čl. 15 odst. 1 směrnice 2002/58/ES. Konkrétně otázka č. 1 zněla takto: *„Lze dostatečnou závažnost trestných činů jako kritérium, které odůvodňuje zásah do základních práv zakotvených v článcích 7 a 8 Listiny, určit výlučně s ohledem na trest, který lze za vyšetřovaný trestný čin uložit, nebo je navíc nezbytné v trestném jednání identifikovat zvláštní míru poškození individuálních nebo kolektivních právních zájmů?“* **V tomto směru je však třeba zdůraznit, že ač ESD zkonstatoval, že** *„...zásah daný zpřístupněním takových údajů lze tedy odůvodnit cílem spočívajícím v prevenci, vyšetřování, odhalování a stíhání „trestných činů“ obecně, který zmiňuje čl. 15 odst. 1 první věta směrnice 2002/58, a není nutné, aby tyto trestné činy byly kvalifikovány jako „závažné““,* **v tomto případě šlo o snahu vysledovat používání ukradeného mobilního telefonu prostřednictvím SIM karet vložených do tohoto telefonu, kdy tedy k zásahu do práv dotčených osob došlo pouze minimálně**. Rozsudek dostupný z: http://curia.europa.eu/juris/document/document.jsf;jsessionid=552850AEC422F98EAD280C3A629222A0?text=&docid=206332&pageIndex=0&doclang=CS&mode=lst&dir=&occ=first&part=1&cid=5774427.

[24] *„Podle ustálené judikatury Ústavního soudu je prostředkem pro řešení vzájemné kolize základních práv, případně ústavním pořádkem chráněných veřejných statků, princip proporcionality, a to jak v řízení o ústavních stížnostech, tak při abstraktní kontrole norem.“* Viz nález Ústavního soudu ze dne 1. 3. 2007, sp. zn. Pl. ÚS 8/06.

V. Podmínky, které musí být splněny

Ustanovení § 88a trestního řádu pochopitelně nepředstavuje jedinou cestu, jak se k údajům tohoto typu dostat. Ustanovení se totiž vztahuje jen na subjekty, které jsou vázány zvláštní povinností mlčenlivosti ve smyslu zákona o elektronických komunikacích. Tato povinnost se ovšem nevztahuje například na nevýdělečné spolky, budující a spravující metropolitní sítě (ukázkovým příkladem tu budiž nekomerční neveřejná síť PilsFree[25]), zde je proto nabíledni postup podle § 8 odst. 1 trestního řádu.[26] Paradoxem ovšem je, že ač jde o postup OČTŘ podle trestního řádu ve vztahu k citlivým údajům, uvedené ustanovení nevyžaduje příkazu ze strany soudu a není svázáno jen s úmyslnými trestnými činy, jako je tomu u § 88a trestního řádu. Podle zmíněného ustanovení lze totiž data získat jen za těchto podmínek:

1) v případě trestního řízení vedeného pro úmyslný trestný čin, k jehož stíhání zavazuje mezinárodní smlouva, nebo v případě trestního řízení vedeného pro úmyslný trestný čin s horní hranicí trestní sazby tři roky,
2) současně však musí být splněna podmínka, že nebude možné sledovaného účelu dosáhnout jinak nebo pokud hrozí, že jeho dosažení by bylo podstatně ztížené.
3) V řízení před soudem jejich vydání soudu nařídí předseda senátu.
4) V přípravném řízení nařídí jejich vydání státnímu zástupci nebo policejnímu orgánu soudce na návrh státního zástupce.
5) Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn.
6) Důležitá je zde také povinnost zpětného informování v případě, je-li věc pravomocně skončena.

Výčet trestných činů, u kterých lze žádat o poskytnutí údajů o telekomunikačním provozu je v § 88a trestního řádu taxativní a zahrnuje následující trestné činy: *trestný čin porušení tajemství dopravovaných zpráv (§ 182 trestního zákoníku), trestný čin podvodu (§ 209 trestního zákoníku), trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 trestního zákoníku), trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 trestního zákoníku), trestný čin nebezpečného vyhrožování (§ 353 trestního zákoníku), trestný čin nebezpečného pronásledování (§ 354 trestního zákoníku), trestný čin šíření poplašné zprávy (§ 357 trestního zákoníku), trestný čin podněcování k trestnému činu (§ 364 trestního zákoníku) a trestný čin schvalování trestného činu (§ 365 trestního zákoníku).*

---

[25] Chci být členem PilsFree. PilsFree [online]. © 2003 - 2019 PilsFree, z. s. [vid. 24. 7. 2019]. Dostupné z: http://www.pilsfree.net/.

[26] Podle § 8 odst. 1 trestního řádu: *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.*

VI. Zvláštní procesní situace – trestní řízení versus přestupkové řízení

Z výše vyjmenovaných trestných činů lze pro účely mého příspěvku zvláště upozornit na trestný čin podvodu a trestný čin nebezpečného pronásledování (tzv. *stalking*). V případě těchto trestných činů je totiž s přihlédnutím k tomu, že oba mají v zákoně č. 251/2016 Sb., o některých přestupcích, v platném znění, svůj korespondující přestupek[27)] poměrně velmi častý následující scénář:

Varianta A):

1) Policie ČR obdrží trestní oznámení na některý z těchto trestných činů.

- U podvodu se obvykle jedná o vylákání peněžní částky na základě fiktivního inzerátu na online serveru. Pachatel v protiprávní činnosti navíc pokračuje a předběžně zjištěná škoda dosahuje částky více než 8.000,- Kč. O přestupek podvodu se proto jednat nemůže.[28)] Pro policii je v tomto případě jedním z nejdůležitějších úkolů zjistit nejen totožnost pachatele, ale také totožnost případných dalších poškozených.
- U nebezpečného pronásledování jde obvykle o dlouhodobé obtěžování partnerky ze strany jejího bývalého partnera prostřednictvím opakovaných telefonátů, zasílání SMS zpráv nebo e-mailů, v nichž se též objevují stupňující se výhrůžky včetně všelijakých difamací. Ty mohou být přitom různě realizovány z osobního nebo služebního mobilu, domácího PC nebo hotspotů – například z kavárny, nákupního centra, knihovny apod.

2) Policie na základě trestního oznámení sepíše záznam o zahájení úkonů trestního řízení ve smyslu § 158 odst. 3 trestního řádu, kdy v tu chvíli se zároveň stane OČTŘ, který podle § 97 odst. 3 zákona o elektronických komunikacích může při splnění dalších podmínek žádat například T-Mobile Czech Republic a.s. o poskytnutí provozních a lokalizačních údajů. Než se k tomu ovšem policie odhodlá, pokusí se potřebné údaje zjistit v jednodušším režimu § 8 odst. 1 trestního řádu. Tedy policie se nejprve obrátí na providera (provozovatele online serveru) s žádostí o poskytnutí součinnosti podle § 8

---

27) Přestupek je druhem veřejnoprávního deliktu správní povahy, který projednávají správní orgány. Podvod lze najít v § 8 zákona o některých přestupcích; nebezpečné pronásledování je podřaditelné pod tzv. hrubé jednání ve smyslu § 7 téhož zákona. Důležitá je subsidiarita přestupků k trestným činům. Ta je vyjádřena § 5 přestupkového zákona: *Přestupkem je společensky škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje znaky stanovené zákonem, nejde-li o trestný čin.* Dále je třeba zohlednit princip ultima ratio trestního práva, zdůrazněný např. v nálezu Ústavního soudu ČR ze dne 5. 8. 2010, sp. zn. III. ÚS 2278/07: *„Ústavní soud chápe trestní právo jako právo ultima ratio, tedy právo, jehož prostředky mají a musejí být užívány tehdy a jen tehdy, pokud užití jiných prostředků právního řádu nepřichází v úvahu nebo je zjevně neúčelné...“*

28) Byť je v této souvislosti záhodno upozornit na existující sněmovní tisk č. 466, který si mj. klade za cíl změnit § 138 odst. 1 trestního zákoníku, tj. zákona č. 40/2009 Sb., a „limit“ 5.000 Kč pro rozlišení přestupku a trestného činu zvýšit na 10.000 Kč. Viz Sněmovní tisk 466. Poslanecká sněmovna Parlamentu České republiky [online]. [vid. 24. 7. 2019]. Dostupné z: http://www.psp.cz/sqw/text/tiskt.sqw?O=8&CT=466&CT1=0.

odst. 1 trestního řádu a ten policii v zásadě vyhoví a poskytne jí údaje, které mu jsou známy z jeho činnosti; obvykle v rozsahu: jméno, příjmení, e-mail, telefon, IP adresu, které uživatel služby uvedl při uzavření smlouvy na dálku či její změně. Zde však nemusí být záruka o pravdivosti těchto údajů (byť dnes již existují algoritmy, které jsou schopny podvodné údaje odhalit) ani záruka, že těmito údaji bude poskytovatel služby vždy disponovat. Z toho důvodu se policie obrátí na státního zástupce, který se souhlasem soudu umožní využít § 88a trestního řádu. Je třeba zdůraznit, že nejde o nijak závažnou trestnou činnost.

3) Po podání obžaloby státním zástupcem soud v rámci trestního stíhání a po provedeném dokazování dospěje k názoru, že u projednávaného skutku není přítomna taková společenská škodlivost, aby bylo možno dovozovat, že jde o trestný čin (což je samo o sobě v tuto chvíli trochu na hraně, ne-li dokonce za ní, se závěrem Ústavního soudu, vyjádřeným např. v jeho nálezu ze dne 27. 9. 2007, sp. zn. II. ÚS 789/06[29]). Z toho důvodu soud odevzdá věc k projednání přestupku správnímu orgánu, tj. věcně a místně příslušnému obecnímu úřadu, kterému zašle i celý spisový materiál, včetně všech podkladů, které byly zajištěny.

4) Ač je přestupkové řízení neveřejné a oprávněná úřední osoba je povinna zachovávat mlčenlivost, provozní a lokalizační údaje (na které jinak mají právo jen orgány veřejné moci vymezené v § 97 odst. 3 zákona o elektronických komunikacích) se najednou dostávají do rukou správního orgánu, který na ně nárok ze zákona nemá. Navíc je třeba dodat, že skutečnost, že je řízení neveřejné ještě nevylučuje připuštění veřejnosti, anebo nebrání subjektům ve smyslu § 38 správního řádu (a to nemusí být jen účastníci řízení, ale třeba i svědci) nahlížet do spisu (z nahlížení do spisu jsou přitom vyloučeny pouze utajované informace nebo skutečnosti, na něž se vztahuje zákonem uložená nebo uznaná povinnost mlčenlivosti); nehledě na další možnost, jak se do spisu dostat, kterou zde představuje zákon č. 106/1999 Sb., o svobodném přístupu k informacím[30] (byť v jeho případě se osobní údaje při zveřejnění „samozřejmě" anonymizují).

5) Nyní má o věci rozhodovat správní orgán, který zpravidla, aniž by se nad legitimitou přístupností k provozním a lokalizačním údajům nějak

---

[29] *„Z hlediska ústavně chráněných základních práv je nepřípustné, aby zahájení úkonů k objasňování a prověřování skutečností důvodně nasvědčujících tomu, že byl spáchán trestný čin podle § 158 odst. 3 trestního řádu, např. ve formě odposlechů, bylo zneužíváno jako prostředku k teprve dodatečnému opatřování podkladů pro tento postup, tj. samotné důvodnosti podezření."*

[30] Zákon o svobodném řístupu k informacím je totiž aplikovatelný vždy, pokud neexistuje komplexní úprava, která by postup podle tohoto zákona vylučovala. Judikatura správních soudů označila jako komplexní úpravu § 38 správního řádu avšak jen pro žádosti o informace, které směřují k poskytnutí informací formou nahlížení do spisu nebo formou poskytnutí kopií (v listinné či elektronické podobě) celého spisu (analogie nahlížení do spisu). Viz např. rozsudek NSS ze dne 13. 8. 2008, č. j. 2 As 38/2007-78, rozsudek NSS ze dne 11. 8. 2009, č. j. 1 As 51/2009-106, a rozsudek NSS ze dne 13. 12. 2012, č. j. 7 Ans 18/2012-23.

zabýval, podklady a případně již důkazy provedené OČTŘ bez dalšího převezme a na jejich základě také rozhodne. Lze však takový důkaz použít? Nedošlo zde k nepřiměřenému zásahu do práva na soukromí?

Varianta B):

Za povšimnutí v této souvislosti stojí ještě jeden scénář i když méně častý:

1) Správní orgán obdrží oznámení o přestupku podvodu a přestupek projedná tak, že obviněného pravomocně shledá vinným, uloží mu správní trest pokuty a povinnost uhradit státu náklady řízení spojené s projednáním přestupku. Přestupek rovněž zapíše do celostátní evidence přestupků.

2) Nezávisle na tomto postupu orgán policie, který předtím správnímu orgánu přestupek oznámil, provede další pátrání a zjistí, že pachatel v protiprávním jednání ještě pokračoval a způsobil mnohem větší škodu, což ve výsledku zakládá odpovědnost pro trestný čin pokračujícího podvodu. Policejní orgán sepíše záznam o zahájení úkonů trestního řízení - v tuto chvíli je trestní řízení zahájeno. OČTŘ získá prostřednictvím § 88a trestního řádu provozní a lokalizační údaje a bude chtít zahájit trestní stíhání. V jeho zahájení nebo pokračování (pokud již trestní stíhání dokonce zahájil) však brání pravomocné rozhodnutí o přestupku, neboť to představuje překážku *rei iudicatae*.

3) Pokud trestní stíhání ještě zahájeno nebylo, policejní orgán postupuje podle § 159b odst. 4 trestního řádu, tedy jeho zahájení dočasně odloží, pokud dosud neuplynuly lhůty pro odstranění rozhodnutí o přestupku v přezkumném řízení podle § 100 přestupkového zákona. Následně po právní moci rozhodnutí o dočasném odložení podá správnímu orgánu podnět k postupu podle přestupkového zákona.

4) Pokud již trestní stíhání zahájeno bylo, ale dosud neuplynuly lhůty pro odstranění tohoto rozhodnutí v přezkumném řízení podle § 100 přestupkového zákona a není tedy důvodu trestní stíhání zastavit podle § 11 odst. 1 písm. k) trestního řádu, státní zástupce podle § 173 odst. 1 písm. e) trestního řádu přeruší trestní stíhání a po právní moci rozhodnutí o přerušení podá podnět příslušnému správnímu orgánu ke zrušení rozhodnutí o přestupku v přezkumném řízení.

5) Správní orgán následně nebude rozhodovat o tom, zda skutek, z něhož pachatele uznal vinným z přestupku, je skutečně trestným činem, ale o tom, zda jsou splněny podmínky podle § 100 přestupkového zákona,[31)] a za tím

---

[31)] Podle § 100 přestupkového zákona: *(1) Vyjdou-li najevo skutečnosti, které odůvodňují posouzení skutku, o kterém již bylo pravomocně rozhodnuto jako o přestupku, jako trestného činu, zruší příslušný správní orgán rozhodnutí o přestupku v přezkumném řízení. Rozhodnutí o přestupku správní orgán zruší v přezkumném řízení též tehdy, pokud bylo vydáno přesto, že o totožném skutku již pravomocně rozhodl orgán činný v trestním řízení tak, že se nestal, nespáchal jej obviněný, spáchání skutku se nepodařilo obviněnému prokázat nebo že skutek je trestným činem, trestní stíhání bylo podmíněně zastaveno, trestní stíhání bylo zastaveno na základě schválení*

účelem bude obvykle potřebovat více než jen jeden „dopis“ OČTŘ. I zde se tedy může stát, že správní orgán obdrží jako podklad pro své rozhodnutí provozní a lokalizační údaje, na které podle § 97 odst. 3 zákona o elektronických komunikacích nárok nemá.

VII. Shrnutí poznatků pro účely výkonu přestupkového práva

Z provedeného rozboru lze dovodit následující závěry:

Informační efekt provozních a lokalizačních údajů z telekomunikačního provozu je značný, a proto jakákoliv jejich kumulace na jednom místě představuje pro soukromí hrozbu. Je proto žádoucí, aby se údaje tohoto typu předně nesoustředily v rukou jednoho subjektu (např. státu). K tomu sice v našich podmínkách „nedochází“, nicméně přesto je v tomto směru za zásadní označit zabezpečení a důslednou ochranu těchto údajů nejen před operátorem, ale i státem. Jak totiž potvrzují incidenty z minulosti, ne vždy tomu tak bohužel je.[32)]

V samotném procesním uchovávání a poskytování provozních a lokalizačních údajů operátory orgánům činným v trestním řízení pro účely trestního řízení nelze spatřovat nic špatného, pokud se tak děje cestou zákona. Předmětné údaje totiž mohou být při odhalování trestné činnosti nadmíru užitečné. Mělo by se však více zohlednit, že tyto údaje mohou být poskytovány do dalších procesů a již z toho důvodu by měla být reflektována především závažnost trestného činu, pro který jsou tyto údaje poskytovány, včetně toho jaké údaje se přesně poskytují a zda je nezbytné je vzhledem ke sledovanému účelu poskytnout všechny (někdy se v této souvislosti hovoří o zásadě minimalizace údajů). V tomto směru by proto nebylo od věci, jak ostatně uvádí i doc. Polčák,[33)]

---

narovnání, bylo podmíněně odloženo podání návrhu na potrestání nebo bylo odstoupeno od trestního stíhání mladistvého. (2) Přezkumné řízení podle odstavce 1 se zahájí a) do 3 měsíců ode dne, kdy se správní orgán dozvěděl o důvodu pro zahájení přezkumného řízení, a b) nejpozději do 3 let od zahájení trestního stíhání nebo ode dne nabytí právní moci rozhodnutí orgánu činného v trestním řízení o tom, že se skutek nestal, skutek nespáchal obviněný, že spáchání skutku se nepodařilo obviněnému prokázat nebo že skutek je trestným činem, trestní stíhání bylo podmíněně zastaveno, trestní stíhání bylo zastaveno na základě schválení narovnání, bylo podmíněně odloženo podání návrhu na potrestání nebo bylo odstoupeno od trestního stíhání mladistvého. (3) Přezkumné řízení podle odstavce 1 nelze zahájit po uplynutí 3 let od právní moci rozhodnutí o přestupku.

32) V České republice došlo k neoprávněnému vyžádání osobních údajů desítek osob, zejména politiků nebo podnikatelů, včetně předsedy Ústavního soudu nebo osob z okolí prezidenta republiky, příslušníkem cizinecké policie. Viz Policista nelegálně sháněl výpisy mobilů, špehoval i Rychetského, iDnes 18. 6. 2011, dostupné z: http://zpravy.idnes.cz/policista-nelegalne-shanel-vypisy-mobilu-spehoval-i-rychetskeho-phy-/krimi.aspx?c=A110617_225431_krimi_abr in VOBOŘIL, J.: Přínos a ztráty data retention - kritická reflexe společného soužití. *Revue pro právo a technologie. [Online]. 2011, č. 4*, s. 19-22. [cit. 24. 7. 2019]. Dostupné z: https://journals.muni.cz/revue/article/viewFile/4085/pdf.

33) POLČÁK, R.: *Ochrana soukromí a osobních údajů*. [přednáška]. Brno, Masarykova univerzita, Právnická fakulta, 22. 2. 2019.

zákonem odstupňovat úložní dobu vzhledem k závažnosti činu. Ustanovení § 88a trestního řádu by tedy nemělo být nadužíváno; jeho použití by mělo být omezeno jen na nezbytné případy a pokud by sledovaného účelu skutečně nešlo dosáhnout jinak. Jelikož praktická zkušenost je jiná, v tomto ohledu je udržitelnější závěr Ústavního soudu ČR ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10.

Předně byl ovšem diskutován problém přístupnosti k těmto údajům prostřednictvím přestupkových řízení. A k tomu je třeba uvést následující.

Jak již bylo uvedeno, údaje se mohou dostat do rukou orgánů, které na ně nárok ze zákona nemají. Pomineme-li ČNB, jejíž zakotvení ve výčtu subjektů v § 97 odst. 3 zákona o elektronických komunikacích je trochu zvláštní, může jít též o subjekty nastupující po OČTŘ, tedy správní orgány. S tím souvisí i následná otázka použitelnosti provozních a lokalizačních údajů jako důkazu v přestupkovém řízení.

K této otázce lze nicméně uvést, že pokud byly tyto údaje získány v trestním řízení zákonnou cestou a byly v něm i jako důkaz také provedeny, nelze než zkonstatovat, že jde o důkaz získaný v souladu se zákonem. Jak bylo přitom dále zjištěno, ustálená judikatura NSS nemá problém s tím, takové důkazy přijmout, neboť jako důkaz lze v zásadě použít cokoliv, co poslouží k objasnění stavu věci. Např. v rozsudku ze dne 27. 8. 2014, č. j. 1 As 97/2014–29, NSS přímo uvádí: *„…NSS zároveň souhlasí se závěrem krajského soudu, podle nějž obecně nic nebrání tomu, aby správní orgán, kterému je postoupena věc, v níž bylo původně vedeno trestní řízení, v navazujícím přestupkovém řízení rozhodl na základě důkazů provedených v trestním řízení. Lze předpokládat, že zpravidla bude skutkový stav zjištěný orgány činnými v trestním řízení možno považovat za dostatečný a bylo by nehospodárné a nadbytečné provádět dokazování ve správním řízení opětovně. Samozřejmě nelze vyloučit, že v konkrétních případech bude nutné dokazování doplnit…“* (obdobně viz rozsudky NSS ze dne 30. 1. 2008, č. j. 2 Afs 24/2007-119, ze dne 22. 7. 2009, č. j. 1 Afs 19/2009–57, ze dne 17. 6. 2015, č. j. 1 As 168/2014–27).

I přesto zastávám názor, že to nemusí být až tak jednoduché, zohledním-li:

1) k čemu mají provozní a lokalizační údaje primárně sloužit, poskytují-li se [k odhalování a stíhání závažných trestných činů], 2) dále kdo je může získat [subjekty podle § 97 odst. 3 zákona o elektronických komunikacích] a konečně 3) vezmu-li v úvahu podstatné rozdíly mezi správním právem a jeho nástroji a trestním právem a jeho nástroji, které se mají navíc analogicky aplikovat jen v omezeném rozsahu [navíc jen instituty hmotného práva[34)]], a pouze tam, kdy to, co má být aplikováno, určitou otázku vůbec neřeší, nevede-li takový výklad k újmě účastníka řízení a ani k újmě na ochranu hodnot, na jejichž

[34)] Podle usnesení Ústavního soudu ze dne 7. 10. 2010, sp. zn. III. ÚS 1845/08, totiž *„Úprava, týkající se trestního řízení dle § 9 až 12 citovaného zákona, resp. příslušných ustanovení trestního řádu, je úpravou speciální, podle níž ve věci přestupků nelze postupovat.“*

vytváření a ochraně je veřejný zájem.[35)] Zejména je třeba evidovat, že trestní řízení má mnohem přísnější režim a důkazní prostředky, jež mohou OČTŘ využívat, by proto měly být v zásadě restriktivně omezeny jen na trestní řízení. To by ovšem při této logice zase vedlo k závěru, že by pak přestupkový orgán nemohl v řízení o přestupku použít ani třeba poznatky, které v předchozím trestním řízení obstarala policie při domovní nebo osobní prohlídce. Z toho důvodu se domnívám, že provozní a lokalizační údaje lze v řízení o přestupku použít jako listinného důkazu, ale nabádám k opatrnosti, neboť jak již bylo uvedeno, jejich použití a uchovávání ve správním spise, do něhož se lze dostat mnohem snadněji než do trestního spisu, je zde poněkud v rozporu s cíli evropské legislativy.

[35)] Dle rozsudku NSS ze dne 16. 4. 2008, č. j. 1 As 27/2008-67.