doc. JUDr. PhDr. Zdeněk Fiala, Ph.D.
Policejní akademie České republiky v Praze
Fakulta bezpečnostního managementu
Katedra veřejnoprávních disciplín
Mgr. Marek Pačmag, MBA
Policie České republiky

Specifické aspekty předšetřování přestupků spáchaných v prostředí Internetu

Úvod

Moderní informační a komunikační technologie (SMS a MMS zprávy, e-mail, Facebook, Twitter, Skype, ICQ, WhatsApp a mnoho dalších – dále jen „ICT“) se staly substrátem ekonomického, společenského a politického života. Většina populace si běžný den již nedokáže bez těchto technologií představit, neboť výraznou měrou ovlivňují mezilidské vztahy a vzájemné sociální interakce. Je však notoricky známo, že každý „vynález“ sloužící prvotně ke správnému účelu, může být následně zneužit k páchání trestné činnosti (v širším slova smyslu).

S ohledem na širokou paletu možných protiprávních jednání v prostředí Internetu[1] není patrně možné podat úplný výčet všech v úvahu přicházejících přestupků. Vycházeje však ze zkušeností autorů[2] lze v aplikační praxi za nejčastěji oznamované a následně správními orgány také projednávané přestupky označit:

1) přestupky proti majetku - za typický příklad lze označit následující skutkový děj: *„Neznámý pachatel na internetovém portálu umožňující prodej věcí, nabízel k prodeji mobilní telefon značky IPhone 6 za částku 4 900 Kč. Poškozená po vzájemné domluvě poslala finanční zálohu ve výši 2 500 Kč na bankovní účet prodávajícího. Po obdržení finanční hotovosti přestal prodávající jakkoliv komunikovat a mobilní telefon ani finanční zálohu poškozené zpět nezaslal“*.

2) přestupky proti občanskému soužití - sociální sítě, coby masově využívané prostředky pro vzájemnou komunikaci, nabízejí takřka neomezenou možnost diskuse o různých tématech. Tyto se však mnohdy neobejdou bez různých vulgarit a vzájemného ponižování. Vedle klasické urážky na cti na internetovém blogu je třeba upozornit i na daleko závažnější situace, podřaditelné pod tzv. kyberšikanu: „*Neznámý pachatel použil na veřejně přístupné gay seznamce u svého uživatelského účtu fotografie poškozeného, který však homosexuál není, čímž se cítí být poškozen mezi vrstevníky, kteří se mu kvůli uvedenému účtu posmívají“*. Obdobně: „*Dívka ve věku 13-ti let fascinovaná youtuberingem vytvořila video zobrazující výcvik na běžkách doplněné o vlastní názory dívky. Toto video umístila na sociální síť http://youtube.com, kde se však dočkala pouze negativních komentářů ze strany jejích spolužáků, kteří ji ponižovali a značně ubližovali. V souvislosti s danou situací dívka*

[1] Internet s velkým písmenem je v příspěvku užíván ve smyslu vlastního jména celosvětové informační a komunikační sítě.
[2] Pozn. autorů: Níže uváděné skutkové děje vycházejí z reálných případů, které autoři řešili ať už v rámci jejich konzultační či služební činnosti.

nechtěla chodit do školy. Rodiče se proto rozhodli pro pomoc ze strany Policie České republiky“. Jakož i na skutky spojené v současné době s rozšířeným jevem v podobě sextingu:[1] „*Chlapec na veřejné sociální síti Facebook při vzájemné komunikaci s dívkou ve věku 14 let nejprve pokládal sexuálně zaměřené otázky ve smyslu kolik už měla kluků, jestli jí to už někdo udělal a podobně, kdy následně začal po dívce požadovat fotografie, které ovšem blíže nespecifikoval, pouze uvedl, že mají být pořízeny v koupelně. Při kontrole Facebooku v rámci rodičovské odpovědnosti byla předmětná komunikace objevena, následkem čehož matka zakázala dceři s uživatelským účtem pachatele dále komunikovat. Nadto se matka rozhodla celou věc oznámit na Policii České republiky“.*[2]

Při objasňování výše popsaných přestupků se efektivním nástrojem jeví vyžadování tzv. registračních údajů od poskytovatelů internetových služeb nebo určitých informací k IP adresám od poskytovatelů připojení (podrobněji viz dále). Tyto možnosti jsou však ze strany příslušných orgánů využívány v mnohem nižší míře, než by bylo mnohdy potřebné. Lze vyjmenovat celou řadou příčin, nicméně za jednu z významných je možné považovat nedostatek relevantních informací a znalostí z této oblasti.

Vycházeje z tohoto předpokladu cílem předkládaného přehledového článku je přiblížit v kontextu aktuální právní úpravy povinnosti a možnosti při předšetřování přestupků spáchaných (nejen) v prostředí Internetu.

Obecně k předšetřování přestupků ze strany orgánů policie

Podle ustanovení § 73 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, ve znění pozdějších předpisů (dále jen „zákon o odpovědnosti za přestupky“ či „ZOPŘ“) platí, že má-li orgán Policie České republiky nebo Vojenské policie (dále jen „orgán policie“) nebo jiný správní orgán důvodné podezření, že byl spáchán přestupek, a není-li sám příslušný k jeho projednání, oznámí tuto skutečnost bez zbytečného odkla věcně a místně příslušnému správnímu orgánu.

V závislosti na povaze (typu) přestupku lze přitom v rámci oznamování přestupků příslušným správním orgánům ze strany orgánů police v kontextu právní úpravy rozlišovat mezi A) tzv. jednoduchým oznamováním přestupku, tzn. oznamováním bez povinnosti provést nezbytná šetření jimi oznamovaného přestupku, a B) tzv. kvalifikovaným oznamováním přestupku, tzn. oznamováním s povinností provést předchozí nezbytná šetření za účelem zjištění osoby podezřelé a k zajištění důkazních prostředků.

Ad A) Jednoduché oznamování přestupky ze strany orgánů policie

Při oznamování přestupků, jež nejsou zahrnuty v taxativním výčtu přestupků uvedených v ustanovení § 74 odst. 1 ZOPŘ (tzn. u většiny přestupků), není postup orgánů policie při oznamování přestupků nijak formálně upraven. To jim umožňuje

[1] Pojem sexting je složeninou slov „sex“ a „texting“ a lze jej definovat jako elektronické rozesílání textových zpráv, fotografií či videí se sexuálním obsahem viz *Sexting.cz: Co je vlastně sexting?* [online]. [cit. 2020-03-09]. Dostupné z: http://www.sexting.cz/

[2] Popisovaný případ 14 leté dívky by mohl být rovněž kvalifikován podle § 193b trestního zákoníku. Podrobněji k hranici mezi trestným činem a přestupkem srov. např. FIALA, Zdeněk; FRUMAROVÁ, Kateřina; HORZINKOVÁ, Eva a Martin ŠKUREK. *Správní právo trestní*. Praha: Leges, 2017, s. 67 a násl.

postupovat při oznamování přestupků relativně rychle a efektivně. Nicméně i v těchto případech se určité (základní) předšetření přestupku předpokládá, což vyplývá z ustanovení § 73 ZOPŘ, které stanoví výčet podstatných náležitostí, které by oznámení o přestupku ze strany orgánů policie mělo obsahovat. Jedná se zejména o vymezení toho, kdo je podezřelým z přestupku, pokud je znám, popis skutku, ve kterém je přestupek spatřován, místo a čas, kdy měl být přestupek spáchán, zákonné ustanovení obsahující skutkovou podstatu předmětného přestupku a důkazní prostředky, které jsou orgánům policie známy. S odkazem na použití slova zejména lze říci, že by měl orgán policie v oznámení uvést všechny relevantní skutečnosti, které zjistil. Jinak vyjádřeno, jeho oznámení by mělo být co možná nejúplnější, aby věcně a místně příslušný správní orgán mohl věc následně posoudit a případně v rámci postupu před zahájením řízení doplnit. Nepochybně lze v této souvislosti postulovat, že předšetřování přestupkového jednání výrazně usnadňuje správnímu orgánu následné prokázání skutku. Orgány policie by se proto neměly pasovat do role pouhých „přeposílačů“ oznámení.

Ad B) Kvalifikované oznamování přestupků ze strany orgánů policie

Zvláštní postup v podobě povinného nezbytného šetření je stanoven před oznámením přestupků uvedených v ustanovení § 74 ZOPŘ, tzn. přestupků proti veřejnému pořádku, proti občanskému soužití, v jehož důsledku došlo k ublížení na zdraví, proti majetku, proti pořádku ve státní správě, proti pořádku v územní samosprávě, podle zákona o silničním provozu, proti pořádku ve státní správě v působnosti Policie České republiky nebo Vojenské policie, na úseku požární ochrany, nebo na oznámení přestupků, o nichž to stanoví zvláštní právní předpis.

Zákon o odpovědnosti za přestupky společně s tím v ustanovení § 74 odst. 3 stanoví pravomoc orgánu policie samostatně věc v těchto případech předat nebo odložit a v ustanovení § 74 odst. 4 povinnost orgánu policie vyrozumět oznamovatele přestupku o provedených opatřeních.

O provedení nezbytného šetření orgán policie podle ustanovení § 74 odst. 2 ZOPŘ sepíše záznam, který se stává součástí oznámení o spáchání přestupku, které musí orgán policie předložit věcně a místně příslušnému správnímu orgánu ve lhůtě do 30 dnů ode dne, kdy se o přestupku dozvěděl.

Aby orgány policie mohly jim uloženou povinnost řádně plnit, tak jim zákon č. 273/2008 Sb., o Policii ČR (dále jen „zákon o Policii“ nebo „PolZ“), příp. zákon č. 300/2013 Sb., o Vojenské policii, svěřuje řadu pravomocí (dále jen „zákon o Vojenské policii“).

Obecně platí, že v rámci předšetřování přestupků orgány policie mohou:

- provádět ohledání místa přestupku, ohledání věci mající vztah ke spáchanému přestupku a v souvislosti s tím zjišťovat stopy;
- provést orientační vyšetření při podezření na ovlivnění alkoholem nebo jinou návykovou látkou pomocí dechové zkoušky nebo odběrem slin anebo potu, či toto zjistit prostřednictvím odborného lékařského vyšetření;
- vyzvat určitou osobu, aby se dostavila na určité místo k sepsání úředního záznamu o podání vysvětlení, pokud tato osoba výzvě nevyhoví, může být i předvedena;
- požadovat prokázání totožnosti od osoby, která je podezřelá ze spáchání přestupku, dále od osoby, od níž je požadováno vysvětlení, od osoby zdržující se

v blízkosti místa, kde došlo ke spáchání přestupku, od osoby, která má být předvedena na žádost příslušného orgánu a která je oznamovatelem podezření ze spáchání přestupku;

- vyzvat určitou osobu k vydání věci, u které lze mít za to, že v přestupkovém řízení může být věcně a místně příslušným správním orgánem uloženo její propadnutí anebo může být zabrána nebo jde-li o věc pro přestupkové řízení důležitou.[1]

Pokud výsledky šetření nasvědčují tomu, že prověřované jednání naplňuje znaky jednání, které má znaky přestupku (např. ve věci vyjde najevo, že se přestupku dopustil příslušník bezpečnostního sboru), orgán policie věc předá věcně a místně příslušnému správnímu orgánu. Nasvědčují-li však zjištěné skutečnosti, že jde o trestný čin, věc předá příslušnému orgánu činnému v trestním řízení k přijetí dalších opatření.

Naopak pokud orgán policie dojde k závěru, že není dáno ani podezření z přestupku nebo že nelze přestupek projednat, anebo nezjistí do 30 dnů ode dne, kdy se o přestupku dozvěděl, skutečnosti odůvodňující podezření, že jej spáchala určitá osoba, věc odloží.

Specifika tzv. předšetřování přestupků spáchaných v prostředí internetu

U přestupků spáchaných na Internetu jsou zákonné možnosti vyžadování součinnosti od fyzických a právnických osob či jiných orgánů nepochybně užší, než je tomu v případě prověřování trestných činů. Při tzv. předšetřování přestupků nelze například nařídit uchování nebo znepřístupnění dat jiným osobám (§ 7b zákona č. 141/1961, trestní řád, ve znění pozdějších předpisů, dále jen „trestní řád“), odposlouchávat budoucí či probíhající zájmové komunikace (§ 88 trestního řádu), vyžadovat údaje o telekomunikačním provozu (§ 88a trestního řádu), sledovat obsah e-mailových schránek a cloudových úložišť (§ 158d trestního řádu).

Právním základem se v tomto případě stává, jak již bylo uvedeno výše, zákon o Policii, příp. zákon o Vojenské polici.

V prvé řadě je třeba poukázat na ustanovení § 18 PolZ ve spojení s jeho dalším ustanovením, a to konkrétně § 114. Tím je zajištěna explicitní povinnost dotčených subjektů, aby na oprávněné žádosti orgánů policie o poskytnutí potřebných informací řádně a včas reagovaly.

V souvislosti s přestupky spáchanými v prostředí Internetu je třeba žádosti směřovat zejména: A) poskytovatelům služeb a následně B) poskytovatelům internetového připojení (konektivity), tzn., že orgán policie si nejprve od poskytovatele služby vyžádá tzv. registrační údaje, včetně IP adresy, ke které bude následně vyžadovat informace od poskytovatele internetového připojení (registrační údaje → informace k IP adrese - poskytovatel konektivity → informace k tel. číslu (telefonní operátor).

[1] Srov. FIALA, Zdeněk; FRUMAROVÁ, Kateřina; HORZINKOVÁ, Eva a Martin ŠKUREK. *Správní právo trestní*. Praha: Leges, 2017.

A) Informace od poskytovatelů služeb

Poskytovatelem služeb se rozumí každá fyzická či právnická osoba, která umožňuje využívat služby, které uspokojují potřeby jednotlivě určených uživatelů. Pro názornost si lze pod tuzemským poskytovatelem služeb představit například Seznam.cz, Centrum.cz, Lide.cz, Bazos.cz, Hyperinzerce.cz, Libimseti.cz a mnoho dalších. Významnými informacemi budou údaje, které jsou uživatelem vědomě vloženy za účelem vytvoření profilu (uživatelského účtu) k využívání nabízených služeb. Takové údaje se odborně nazývají registrační. Je třeba upozornit na v praxi se frekventovaně vyskytující záměnu registračních údajů za údaje provozní a lokalizační a naopak.

Definici provozních a lokalizačních údajů poskytuje ustanovení § 90 odst. 1 zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů, přičemž se provozními údaji rozumí „*jakékoli údaje zpracovávané pro potřeby přenosu zprávy sítí elektronických komunikací nebo pro její účtování*“, a podle ustanovení § 91 odst. 1 citovaného zákona se lokalizačními údaji 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*“. Jak vidno, registrační údaje mají principiálně zcela odlišnou povahu, vznik a obsah, než tomu je u provozních a lokalizačních údajů, které vznikají v souvislosti s telekomunikačním provozem a jsou předmětem telekomunikačního tajemství.[1] Vyžadování údajů o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, je při šetření přestupků vyloučeno. Tyto údaje je možné získat pouze při splnění taxativně stanovených podmínek v rámci trestního řízení.[2]

Od poskytovatele služeb lze pro účely předšetřování přestupků vyžádat následující registrační údaje k uživatelskému účtu: jméno, příjmení, datum narození, adresa, telefonní kontakt, e-mail, IP adresu, ze které došlo k vytvoření účtu, logy IP adres připojení uživatele do účtu.

Pod potrženými body jsou informace, které jsou ze strany uživatele manuálně vloženy. Lze proto přijmout tezi, že pokud je s předchozím rozmyslem využito Internetu k páchání protiprávního jednání, úsilí pachatelů k sofistikovanému zakrytí své skutečné totožnosti bude vysoké. Na uživatelské účty budou zpravidla vloženy smyšlené údaje. Avšak existují i případy z aplikační praxe, kdy získané informace vedou přímo ke konkrétní osobě pachatele. Zpravidla se jedná o osoby, které primárně nevytvářely daný účet pro páchání protiprávního jednání nebo o osoby méně technicky zdatné, které svou neznalostí nabývaly klamný pocit anonymity na Internetu.

Někteří poskytovatelé služeb vyžadují k úspěšnému vytvoření uživatelského účtu vložení účastnického telefonního čísla, na které je následně odeslán zpravidla formou SMS zprávy potvrzovací kód, jenž musí být pro vytvoření účtu vložen do potvrzovacího pole. Tím dochází k provázání uživatelského účtu s konkrétním telefonním číslem, které nejméně po dobu vytváření účtu musí být aktivní.

[1] KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC, s. 442.
[2] ŠÁMAL, Pavel, a kol. *Trestní řád: komentář. 7. dopl. a přeprac. vyd*. Praha: C. H. Beck, 2013. Velké komentáře, s. 1232.

Pochopitelně v prostředí Internetu nepůsobí pouze domácí poskytovatelé služeb, ale ve značné míře i zahraniční subjekty. Představitelé zahraničních poskytovatelů služeb jsou například Facebook.com (Instagram.com), Google.com (Gmail.com), LinkedIn.com, SnapChat.com, Twitter.com a další. Nicméně od uvedených poskytovatelů je možné získat potřebné údaje pouze v rámci probíhajícího trestního řízení na základě příkazu vnitrostátního soudu. Pro účely šetření přestupků za současné právní úpravy není umožněno orgánu policie či správnímu orgánu legitimní získání takových údajů.

B) Informace od poskytovatelů internetového připojení

Poskytovatele internetového připojení lze definovat jako fyzickou či právnickou osobu, která je schopna poskytovat jiným subjektům přístup k Internetu.[1] Tito poskytovatelé jsou povinni držet a uchovávat značnou paletu informací o počítačových systémech, mimo jiné včetně informací o IP adrese, času a délce používání dané služby. Nutně pro orgán policie vyvstává otázka, jakému poskytovateli svou žádost směřovat. Identifikaci poskytovatele připojení na základě zájmové IP adresy lze provést prostřednictvím regionálních registrátorů, kteří na svých stránkách provozují volně dostupné databáze, v nichž jsou evidovány určité údaje (nikoli však všechny) o držitelích IP adres[2] - jako příklad lze uvést http://www.whois.net. Od takto zjištěného poskytovatele lze získat informaci o povaze zájmové IP adresy (zdali je přidělena přímo koncovému uživateli tzv. statická nebo více uživatelům tzv. dynamická adresa). Pokud se jedná o IP adresu přidělenou přímo koncovému uživateli a tento údaj vyplývá ze smluvního ujednání mezi poskytovatelem internetového připojení a klientem, je možné získat kopii této smlouvy nebo jejího dodatku. V případě zjištění dynamické IP adresy nemůže orgán policie v zákonných mantinelech získat žádné jiné informace o koncovém uživateli, tím tedy šetření přestupku v této oblasti končí.

C) Informace od mobilních operátorů

Ustanovení § 66 odst. 2 PolZ opravňuje orgán policie žádat od správce evidence nebo zpracovatele poskytnutí informací mimo jiné z databáze účastníků veřejně dostupné telefonní služby, zdali vložené účastnické telefonní číslo je SIM karta s předplacenou anonymní službou nebo paušální. O SIM kartách s předplacenou anonymní službou nejsou vedeny žádné evidence kupujících subjektů a jejich dohledání je takřka nemožné. U paušálních SIM karet je situace zcela odlišná, neboť poskytované služby v rámci paušálního tarifu musejí být ze strany fyzické či právnické osoby v pravidelných intervalech mobilnímu operátorovi hrazeny. Od mobilního operátora budou k paušální SIM kartě zjištěny následující informace: jméno a příjmení uvedené na faktuře, fakturační a doručovací adresu, rodné číslo nebo identifikační číslo uvedené na faktuře, stav ke dni uplatnění žádosti (aktivní, deaktivován, suspendován), IMSI a ICCID,[3] datum poslední změny (aktivace, deaktivace nebo suspendace).

[1] KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013, s. 22.
[2] KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC, s. 137.
[3] IMSI (International Mobile Subscriber Identity) je celosvětově jednoznačné číslo, které identifikuje SIM kartu ve veřejné telefonní síti. Z pohledu uživatele jde jednoduše o telefonní číslo. ICCID (Integrated Circuit Card Identifier) je pak výrobní číslo předmětné SIM karty viz

Uvedené informace získává orgán policie na základě žádosti podané na kontaktní pracoviště policie, kterým je Útvar zvláštních činností služby kriminální policie a vyšetřování, přičemž komunikace s mobilním operátorem probíhá prostřednictvím dálkového přístupu.[1] Žádosti i výsledné informace se předávají v elektronické formě jako datové soubory.[2]

D) Informace k e-mailové schránce

K e-mailové schránce, vložené při vytváření uživatelského účtu, lze shodně vyžadovat veškeré registrační údaje jako k uživatelskému účtu. V této souvislosti je však třeba zmínit i skutečnost, že v poslední době se rozšiřuje mezi pachateli využívání služby dočasných, jednorázových e-mailových adres. Tyto e-mailové schránky se v angličtině označují jako **tempmail, 10minutmail, fake či trash mail** a poskytují je zpravidla zahraniční internetové domény.[3] Služba spočívá v tom, že je uživateli automaticky vygenerována e-mailová adresa se životností deset minut, bez nutnosti jakékoli registrace. Služba je zcela anonymní. Některé domény umožňují uživateli na základě jeho uvážení prodloužit životnost na hodinu, den, týden nebo dokonce i měsíc. Po uplynutí uvedené doby je e-mailová schránka systémem nenávratně odstraněna, a tedy do ní již není možné vstoupit.[4] Z pohledu šetření přestupků se jedná o interval doslova smrtící. Ve své podstatě nestačí oznamovatel ani podezření ze spáchání přestupku orgánu policie oznámit, aniž by informace byly již v době oznámení nenávratně smazány. V neposlední řadě je třeba konstatovat, že provozovatelé těchto domén prakticky ani neuchovávají žádné logy IP adres či data o e-mailových adresách. Jakákoli potencionální žádost orgánu policie o zajištění uvedených informací bude vždy s negativním výsledkem.

Obecně k významu oznámení o přestupku a jeho použitelnosti ve správním řízení

Původní judikatura správních soudů vycházela z absolutní nepoužitelnosti úředního záznamu o přestupku a z oznámení o přestupku jako důkazů v přestupkovém řízení.[5] Nicméně aktuální judikatura Nejvyššího správního soudu závěry uvedené v citovaných rozsudcích modifikovala tak, že listiny předložené Policií ČR postačují k postihu pachatele přestupku, pokud nejsou v řízení před správním orgánem zpochybněny.[6]

GoMobil.cz: Co je ICCID u SIM karty? [online]. 2020 [cit. 2020-03-08]. Dostupné z: https://napoveda.gomobil.cz/tema/nastaveni-a-parametry-sluzby-sim-karta/co-je-iccid-u-sim-karty

[1] VANGELI, Benedikt. *Zákon o Policii České republiky: komentář*. 2. vyd. Praha: C. H. Beck, 2014, s. 280.

[2] Ustanovení § 2 odst. 2 Vyhlášky Ministerstva vnitra č. 336/2005 Sb.

[3] Například http://www.@Bcoo.com nebo http://@eellee.org.

[4] *Pocket-lint: Temp-Mail.org temporary disposable email address lets you keep your email anonymous* [online]. 2017 [cit. 2020-02-29]. Dostupné z: https://www.pocket-lint.com/apps/news/141363-temp-mail-org-temporary-disposable-email-address-lets-you-keep-your-email-anonymous

[5] Srov. např. rozsudky NSS 1 As 96/2008-115; NSS 1 As 34/2010-73, NSS 7 As 83/2010-63.

[6] Srov. např. NSS 4 As 118/2013-61, NSS 1 As 45/2013-37, NSS 10 As 25/2014-48.

K obdobným závěrům dospěl i Ústavní soud ČR, který v usnesení ze dne 13. 11. 2014 ve věci sp. zn. III. ÚS 1838/14 uvedl, že „*I v tomto směru může Ústavní soud odkázat na napadená rozhodnutí a ústavně konformní závěr judikatury Nejvyššího správního soudu, dle níž dokumenty obvykle obsažené v příslušném spisu (tj. oznámení o přestupku spolu s úředním záznamem o podezření z přestupku, záznam o přestupku, ověřovací list k radarovému zařízení, výpis z evidenční karty řidiče) zpravidla postačují k vydání rozhodnutí o spáchání či nespáchání přestupku spočívajícího v překročení nejvyšší povolené rychlosti (obdobně např. rozsudek Nejvyššího správního soudu ze dne 22. 5. 2014 čj. 2 As 39/2014-30 nebo ze dne 22. 8. 2013 čj. 1 As 45/2013-37). Další dokazování je pak potřeba provádět pouze v případech, kdy z účastníkem řízení uplatněných námitek vyplývají důvodné pochybnosti o správnosti výroku o vině či trestu.*“

Z citovaných rozhodnutí vyplývá, že pokud budou správní orgány vycházet z listin (oznámení o přestupku a k nim připojeným úřední záznamům, videozáznamům na CD, ověřovacím listům k radarovému zařízení, atp.) za předpokladu, že nevzniknou důvodné pochybnosti o spáchání přestupku, bude jejich postup v souladu se zákonem a se závěry aktuálních rozhodnutí Nejvyššího správního soudu a Ústavního soudu.[1]

V případě potřeby (zpochybnění), lze uvedené podklady poté v řízení doplnit (podpořit) provedením výslechu - viz např. rozhodnutí Krajského soudu v Plzni, sp. zn. 17 Ca 47/2009-50, podle kterého: „*Ke zjištění, zda žalobce překročil nejvyšší povolenou rychlost, stačí, když kontrolující strážníci vyslechnutí správním orgánem jako svědci, odkázali na obsah svého úředního záznamu zpracovaného několik hodin po kontrole vozidla žalobce, a pokud existuje výsledek radarového měření, které překročení rychlosti dokládá*“. Obdobně lze v tomto směru odkázat i na rozhodnutí Krajského soudu v Ostravě, sp. zn. 58 A 65/2010-34: „*Pokud ve správním řízení nebyly zpochybněny úřední záznamy o oznámení přestupku a policisté potvrdili jejich správnost, byť si na detaily přestupku již nepamatovali, není možno přisvědčit žalobní námitce, že jejich svědecké výpovědi jsou nevěrohodné.“*

Specifické součásti oznámení o přestupku spáchané v prostředí internetu a jejich použitelnost ve správním řízení

Specifickou přílohou oznámení přestupku spáchaného na Internetu se stále častěji stávají tzv. **printscreeny.**[2] V této souvislosti je třeba zdůraznit, že pokud orgán policie či poté správní orgán nezachytí stav internetové stránky, ať již tiskem nebo uložením na elektronický nosič dat, znemožní tak správnímu soudu úkol v podobě vyjít při přezkumu rozhodnutí ze skutkového stavu, který tu byl v době rozhodování správního orgánu (§ 75 odst. 1 zákona č. 150/2002 Sb., soudní řád správní). Je proto nezbytné, aby důkazy z Internetu, které výše jmenované subjekty v předmětné věci nashromáždí, byly přezkoumatelně označeny minimálně datem svého pořízení.[3] V závažnějších případech se může jevit za účelem prokázání nezaměnitelnosti pořízených informací (dat) od doby jejich zajištění, opatřit takto zajištěné podklady

[1] Srov. NSS 8 As 152/2014-34.

[2] Printscreenem se rozumí sejmutí aktuálního obsahu obrazovky počítače a následné převedení obsahu do grafického souboru - viz nález Ústavního soudu České republiky, sp. zn. III. ÚS 3844/13 ze dne 30. října 2014.

[3] Rozhodnutí NSS1 As 33/2011-58.

tzv. **kontrolním součtem souboru (hash)**. Kontrolní součet lze charakterizovat jako digitální podpis souboru. Jde o specifickou hodnotu, která je vypočtena z datové sady pomocí specifického algoritmu, jež pomáhá kontrolovat integritu informací (dat) při jejich ukládání a přenosu. Pokud mají dva soubory shodný kontrolní součet, znamená to, že tyto soubory jsou autentické, tj. velikostně i obsahově totožné, čímž je zaručeno, že nedošlo ke smazání či změně například úseků zajištěných komunikací, části uživatelských účtů a podobně. Tento kontrolní součet se pak stává obsahovou náležitostí například úředního záznamu o ohledání věci (kyberprostoru) připojeného k oznámení přestupku, příp. protokolu, který byl pořízen správním orgánem v rámci dokazování. Případné námitky některého z účastníků řízení spočívající v neoprávněné manipulaci se zajištěnými informacemi (daty), ať již ze strany orgánu policie či správního orgánu, bude správní orgán provádějící dokazování, popřípadě správní soud při přezkumu, disponovat prostředkem, jak se s takovou námitkou bez obtíží vypořádat.

Obdobně by mohli postupovat i případní „občanští“ oznamovatelé přestupků; důvěryhodnost jimi předkládaných printscreenů, kopií e-mailové či SMS komunikace mohou podpořit např. i tím, že si tyto kopie nechají notářsky ověřit.

Rovněž i **užití internetových map** (např. www.mapy.cz či www.maps.google.com) správním orgánem pro účely dokazování shledala soudní judikatura se zákonem souladné, zřetelné a účelné a příhodné z hlediska naplňování cílů spravedlivého přestupkového procesu.[1] Je sice obecně známo, že provozovatelé mapových služeb negarantují správnost dat a nelze tak vyloučit výskyt chyb, ale občasný výskyt chyb nečiní tento důkazní prostředek nezpůsobilým pro dokazování, zvláště nejedná-li se o mapu zastaralou nebo pořízenou z omezeného či pochybného zdroje. Opět tedy platí, že tyto podklady jsou v řízení obecně použitelné za předpokladu, že nejsou zpochybněny.

Internetové mapy, diskuse na sociálních sítích, uživatelské účty, fotografie, audiovizuální záznamy, jakož i veškeré jiné objekty existující v prostředí Internetu lze z hlediska provedení nezbytného šetření považovat za **specifický případ ohledání věci**.[2] Ohledáním je totiž třeba rozumět každý postup, jímž se příslušný orgán vlastním empirickým nazíráním přesvědčuje o předmětu řízení.[3] Podpůrně lze argumentovat např. i ustanovením § 51 zákona č. 500/2004 Sb., správní řád, který upravuje dokazování, kdy za důkazní prostředky považuje listiny, ohledání, svědeckou výpověď a znalecký posudek. Jedná se o výčet demonstrativní (s ohledem na slovo „zejména“ použité zákonodárcem v § 51 odst. 1 správního řádu). Vzhledem ke skutečnosti, že se správní řád o výše uvedených prostředcích nezmiňuje, je poté zřejmé, že promítnutí záznamu či seznámení se s obsahem internetové stránky má svou povahou z vyjmenovaných prostředků zdaleka nejblíže právě k ohledání.

Literatura

FIALA, Zdeněk; FRUMAROVÁ, Kateřina; HORZINKOVÁ, Eva a Martin ŠKUREK. *Správní právo trestní*. Praha: Leges, 2017. Student (Leges). ISBN 978-80-7502-219-6.

[1] Rozhodnutí NSS 9 As 128/2013, NSS 7 As 129/2013.
[2] Srov. Rozhodnutí NSS 2 As 59/2008 – 80.
[3] Srov. např. STRAUS, Jiří. *Kriminalistická technika*. 3., rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012; NĚMEC, Miroslav. *Kriminalistická taktika pro policisty a studenty Policejní akademie České republiky v Praze*. Praha: Abook, 2017.

GŘIVNA, Tomáš a Radim POLČÁK, ed. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

JEMELKA, Luboš a Pavel VETEŠNÍK. *Zákon o odpovědnosti za přestupky a řízení o nich. Zákon o některých přestupcích. Komentář. 2. vydání.* Praha: C. H. Beck, 2020. ISBN 978-80-7400-772-9.

KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC

KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013.

NĚMEC, Miroslav. *Kriminalistická taktika pro policisty a studenty Policejní akademie České republiky v Praze*. Praha: Abook, 2017. ISBN 978-80-906974-0-9.

POLČÁK, Radim; PÚRY, František a Jakub HARAŠTA. *Elektronické důkazy v trestním řízení.* Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8073-7.

STRAUS, Jiří. *Kriminalistická technika.* 3. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2012. ISBN 978-80-7380-409-1.

ŠÁMAL, Pavel, a kol. *Trestní řád: komentář. 7., dopl. a přeprac. vyd.* V Praze: C. H. Beck, 2013. Velké komentáře. ISBN 978-80-7400-465-0.

ŠTEINBACH, Miroslav. *Zákon o Policii České republiky: komentář*. Praha: Wolters Kluwer, 2019. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7598-193-6.

VANGELI, Benedikt. *Zákon o Policii České republiky: komentář. 2. vyd*. Praha, C. H. Beck, 2014. Beckovy komentáře. ISBN 978-80-7400-543-5.

R E S U M É

Příspěvek seznamuje čtenáře s možnostmi předšetřování přestupků spáchaných v prostředí Internetu. Za tímto účelem podávají autoři návod jaké informace (vedoucí ke zjištění osoby přestupce) a jakým způsobem lze získat od poskytovatelů internetového připojení a internetových služeb, mobilních operátů, správců. V druhé části příspěvku autoři poukazují na význam a použitelnost podkladů shromážděných z prostředí Internetu v navazujícím přestupkovém řízení a na opatření, které mohou vést k posílení jejich důkazní hodnoty.

Klíčová slova: přestupek, Internet, orgán policie, předšetřování přestupků, poskytovatel internetového připojení, poskytovatel služeb, registrační údaje.

S U M M A R Y

FIALA, Zdeněk; PAČMAG, Marek: SPECIFICS OF INVESTIGATION OF ADMINISTRATIVE OFFENCES COMMITTED IN THE INTERNET ENVIRONMENT

The article informs the readers of the possibilities of investigating administrative offences committed in the Internet environment. For this purpose the authors give instructions on what information leading to the perpetrator´s detection can be obtained and how the information can be obtained from the Internet service providers, Internet operators, mobile operators and registration data administrators. In the second part the authors point out the importance and applicability of documents obtained from the Internet environment in the follow-up administrative offences proceedings and they describe the steps that may lead to the strengthening of their evidence value.

Key words: administrative offence, Internet, police authority, investigation, internet service provider, service provider, registration data.