ICT a nové trendy v procesu dokazování v přestupkovém řízení

ICT and New Trends in the Process of Proving in Misdemeanor Proceedings

ZDENĚK FIALA¹
MAREK PAČMAG²

Abstrakt

Cílem příspěvku je nastínit korelaci mezi technologickým vývojem v oblasti informačních a komunikačních technologií a dokazováním v přestupkovém řízení. Za tímto účelem autoři nejprve poukazují na v aplikační praxi nejfrekventovaněji řešené přestupky spáchané za využití ICT a v navazující části příspěvku se zabývají využitelností informací z prostředí kyberprostoru, popřípadě podkladů získaných za využití ICT v procesu dokazování v kontextu soudní judikatury.

Klíčová slova

ICT, dokazování, kyberprostor, přestupkové řízení

Abstract

The aim of the article is to outline the correlation between technological development in the field of ICT and evidence in administrative offense proceedings. For this purpose, the authors first point out the most frequently administrative offenses committed using ICT and in the second part of the paper deal with the usability of information from the Internet environment, respectively evidence obtained from the using of ICT in the process of taking evidence in the context of judicial case law.

Key words

ICT, evidence, cyberspace, administrative offence proceedings

DOI

<http://dx.doi.org/10.37355/fvpk-2020/2-06>

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

1 doc. JUDr. PhDr. Zdeněk Fiala, Ph.D., Katedra správního práva a veřejné správy, Vysoká škola finanční a správní, a.s., Estonská 500, 101 00 Praha 10, e-mail: 35342@mail.vsfs.cz

2 npor. Mgr. Marek Pačmag, MBA, Policie České republiky, e-mail: pacmag.marek@seznam.cz

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 páčání trestné činnosti (v širším slova smyslu).

Tyto vývojové tendence se logicky promítají i do procesu odhalování, prověřování a pozdějšího dokazování protiprávního jednání, rozhodovací činnosti soudů (zejména pokud jde o otázky nastavení mantinelů přípustnosti „digitálních“ důkazů) a v neposlední řadě i do příslušné právní úpravy (např. zakotvením specifických zajišťovacích prostředků – např. § 7b trestního řádu, podle kterého může orgán činný v trestním řízení nařídít jakékoli osobě, která disponuje daty uloženými v počítačovém systému nebo na jiném nosiči informací, aby je uchovala v nezměněné podobě či jí uložit, aby tato osoba znemožnila přístup k datům osobám jiným).

Zjednodušeně lze říci, že ICT vnesly procesu dokazování, ať již jde o oblast občanského soudního řízení, daňového řízení, trestního řízení či správního řízení, novou kvalitu. V řadě oblastí podstatně změnily charakter a způsob výkonu činnosti orgánů veřejné moci. Příkladem zde mohou být např. digitální registry, které ve spojení s optickými sledovacími kamerovými systémy umožnily příslušným orgánům zavést zcela nové metody, odstranit vizuální kontroly apod.

Cílem tohoto příspěvku je nastínit, jak se tyto vývojové tendence projevují v oblasti přestupkového práva. Samotný text je přitom rozdělen na dvě části. V první části autoři poukazují na typově nejčastěji řešené přestupky páchané v prostředí Internetu,³ v druhé části se pak zabývají využitím ICT v procesu dokazování v přestupkovém řízení v kontextu soudní judikatury.

I. Nejčastěji oznamované přestupky spáchané v prostředí Internetu

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

- 1) přestupky proti majetku** – za typický příklad lze na tomto úseku označit následující skutkový děj: *„Neznámý pachatel na internetovém portálu <http://www.bazos.cz> 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.“* Jiný relativně rozšířený majetkový přestupek je z prostředí veřejné sociální sítě Facebook a spočívá v tom, že: *„Neznámý pachatel na veřejné sociální síti Facebook*

³ Internet s velkým písmenem je v příspěvku užíván ve smyslu vlastního jména celosvětové informační a komunikační sítě.

vytvořil uživatelský účet s názvem Michaela Vymyslena podle již existujícího účtu, který se od toho skutečného lišil pouze v chybějící diakritice ve slově Vymyšlena, i se shodnou úvodní fotografií. Následně rozeslal soukromé zprávy uživatele A. N., kterou měl originální účet v seznamu, kde se snažil využít jejich přátelství a žádal ji o sdělení jejího telefonního čísla, a poté i zaslaného ověřovacího kódu. A. N. však rozpoznala zvláštnost situace a ověřovací kód na telefonní číslo již nepřeposlala, tedy nebyla způsobena žádná faktická škoda. V případě přeposlání ověřovacího kódu na mobilní platbu by poškozené byla způsobena majetková škoda ve výši 1 380 Kč.“

- 2) přestupky na úseku občanského soužití** – sociální sítě, coby masově využívané prostředky pro vzájemnou komunikaci, nabízejí takřka neomezenou možnost diskuse o různých tématech. Při nich často dochází k vulgaritám a určitému stupni ponižování. Vedle klasické urážky na internetovém blogu je třeba upozornit i na daleko závažnější situace, podřaditelné pod tzv. kyberšikanu: „Neznámý pachatel používá na gayseznamce <http://iboys.cz> 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 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 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:⁴ „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 nespécifikoval, 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.“

U majetkových přestupků je orgán policie ve smyslu ustanovení § 74 zákona o odpovědnosti za přestupky povinen konat tzv. kvalifikované šetření.⁵ U příkladů přestupků proti občanskému soužití, uvedených pod bodem 2, není orgán policie sice povinen kvalifikované šetření provést, nicméně musí vždy primárně vyloučit spáchání trestného činu. Jinými slovy, i u přestupků proti občanskému soužití si musí opatřit podklady a provést nezbytná šetření k potvrzení či vyvrácení spáchání trestného činu. Proto se druhá část příspěvku zaměřuje nejen na samotný proces dokazování před správním orgánem, ale rovněž poukazuje i na specifika (možnosti) předšetřování těchto přestupků ze strany orgánu policie. Nepochybně lze postulovat, že důkladné prošetření přestupkového jednání výrazně usnadňuje správnímu orgánu následné prokázání skutku.

⁴ 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/>

⁵ V podrobnostech se odkazuje na publikaci FIALA Zdeněk a kol. Správní právo trestní. Leges, 2017.

II. ICT a jejich využitelnost v procesu dokazování v přestupkovém řízení

Z obecně známých pravidel je zřejmé, že správní orgán musí získat v řízení určité poznatky či znalosti z oblasti skutkové a oblasti právní. Skutkové poznatky získává správní orgán jako podklady pro vydání rozhodnutí. Mohou to být zejména návrhy účastníků, důkazy, skutečnosti známé správnímu orgánu z úřední činnosti, podklady od jiných správních orgánů nebo orgánů veřejné moci, jakož i skutečnosti obecně známé.

Z uvedeného současně vyplývá, že podklad je širším pojmem než důkaz. V tomto směru platí, že důkazem je vždy toliko informace mající vztah k projednávané věci, která vzešla z důkazního prostředku, resp. z procesu dokazování (výpověď vs. výslech).

Ve vztahu k provádění dokazování v přestupkovém řízení se přitom uplatní především obecná úprava obsažená v § 53 a násl. správního řádu. Podklady od jiných orgánů veřejné moci (např. od Policie České republiky či okresního soudu rozhodujícího v trestní věci, anebo jiného správního orgánu) správní řád sice obecně jako podklad pro rozhodnutí připouští, což potvrzuje i soudní judikatura, často však s dovětkem, že i tak své rozhodnutí musí správní orgán opřít zejména o důkazy původní, které sám provede (např. protokol o výslechu osoby z trestního řízení vs. výslech osoby ve správním řízení). Nejvyšší správní soud k tomu např. ve svém rozhodnutí ze dne 31. 8. 2011, sp. zn. 1 As 16/2011-98 uvedl: „Ať již však správní orgán využije jakýkoli ze zdrojů podkladů pro rozhodování, stále hlavním kritériem pro zjišťování skutkového stavu zůstává zásada materiální pravdy. Ani převzetí podkladů pro rozhodování od jiného správního orgánu tak správní orgán, který dané řízení vede, v tomto případě tedy ministerstvo, nezbavuje zodpovědnosti za zajištění dostatečného důkazního standardu pro dané řízení, jaký požaduje právě § 3 správního řádu.“ Pro poznatky správnímu orgánu známé z úřední činnosti platí, že správní orgán musí uvést, ze které jeho konkrétní činnosti či postupu jsou mu tyto skutečnosti známé. A konečně pokud jde o tzv. notoriety (skutečnosti všeobecně známé), platí, že ty se nedokazují, ledaže by je účastníci zpochybňovali, a správní orgán není povinen uvádět ani zdroj, z něhož se o existenci této skutečnosti dozvěděl.

Z ustanovení § 50 odst. 1 správního řádu přitom vyplývá, že výčet podkladů pro vydání rozhodnutí je demonstrativní a že správní řád jednotlivým podmnožinám výčtu podkladů nepřisuzuje různý význam a hierarchicky je nečlení. Z tohoto pohledu má tudíž při rozhodování správního orgánu stejný význam podmnožina „podkladů od jiného orgánu“ jako „podmnožina důkazů“ (zásada volného hodnocení důkazů).⁶ Obecně však platí, že jako podklad pro vydání rozhodnutí může sloužit vše, co může přispět k objasnění věci. Podkladem pro vydání rozhodnutí tak mohou být nepochybně i důkazní prostředky správním řádem výslovně neupravené, např. internetové mapy, otevřené internetové diskuse, důkaz o tom, že e-mail byl odeslán z určité IP adresy, kamerové záznamy, printscreeny a podobně.

Základní podmínkou pro použití určitého podkladu pro rozhodnutí je jeho opatření zákonným způsobem.

⁶ Srov. rozhodnutí Krajského soudu v Hradci Králové, sp. zn. 22 Ca 293/2009-30.

Byť v daných souvislostech nelze při dokazování přehlédnout právo účastníka řízení navrhnout důkazy, povinnost opatřit si podklady pro vydání rozhodnutí leží v přestupkovém řízení především na správním orgánu, který musí i bez návrhu zjistit všechny rozhodné okolnosti svědčící ve prospěch i v neprospěch účastníka. Je to tedy správní orgán, kdo rozhoduje o tom, jaké důkazní prostředky během řízení provede a které s řádným odůvodněním odmítne.

V tomto kontextu se lze s ohledem na stanovený cíl a zaměření tohoto příspěvku zmínit především o následujících podkladech (důkazech) a postupech, které lze při rozhodování o přestupcích využít a otázkách s nimi souvisejícími.

1) Využitelnost videozáznamů, fotografií, radarových měření, printscreenů a jiných příloh připojených k oznámení o přestupku

Původní judikatura správních soudů vycházela z absolutní nepoužitelnosti úředního záznamu o přestupku a z oznámení o přestupku jako důkazů v přestupkovém řízení. Tyto závěry byly vysloveny především v rozsudcích ze dne 22. 1. 2009, čj. 1 As 96/2008-115, publikovaném pod č. Sb. NSS 1856/2009, a ze dne 9. 9. 2010, čj. 1 As 34/2010-73, publikovaném pod č. Sb. NSS 2208/2011. Obdobně se vyjádřil Nejvyšší správní soud i v rozsudku ze dne 17. 6. 2011, čj. 7 As 83/2010-63.

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. Tyto závěry byly vysloveny např. v rozsudcích Nejvyššího správního soudu např. ze dne 27. 2. 2014, čj. 4 As 118/2013-61, dále ze dne 22. 8. 2013, čj. 1 As 45/2013-37, nebo ze dne 29. 5. 2014, čj. 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 „*l 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) 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.⁷

⁷ Srov. rozhodnutí Nejvyššího správního soudu, sp. zn. 8 As 152/2014-34.

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.“

2) Využitelnost tzv. printscreenů a jiných způsobů zachycujících obsah internetových stránek

Specifickou zvláštností u přestupků (typicky na úseku občanského soužití) spáchaných na Internetu se stále častěji stávají tzv. printscreeny,⁸ které se stávají nedílnou přílohou úředního záznamu o ohledání věci.

V této souvislosti je třeba zdůraznit, že pokud orgán policie či poté správní orgán nezachytí stav internetové stránky, kterou vzal v potaz pro své rozhodnutí, ať již tiskem nebo uložením na elektronický nosič dat, znemožní tak správnímu soudu úkol vycházet při přezkumu rozhodnutí ze skutkového stavu, který tu byl v době rozhodování správního orgánu (§ 75 odst. 1 soudního řádu správního). Je proto nezbytné, aby důkazy z Internetu, které správní orgán nashromáždí, byly přezkoumatelně označeny minimálně datem svého pořízení.⁹ V závažnějších případech se může jevit za účelem prokázání nezaměnitelnosti pořízených informací (dat) od doby jejich zajištění do doby použití pro účely dokazování před správním orgánem opatřit takto zajištěné podklady tzv. kontrolním součtem souboru (hash), jež představuje 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 další součástí výše zmíněného úředního záznamu o ohledání připojeného k oznámení přestupku, příp. protokolu, který byl pořízen správním orgánem při dokazování. V případě 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 disponovat prostředkem, jak se s takovou námitkou bez obtíží vypořádat.

⁸ Printscreenem se rozumí sejmутí aktuálního obsahu obrazovky počítače a následné převedení obsahu do grafického souboru – viz náleží Ústavního soudu České republiky, sp. zn. III. ÚS 3844/13 ze dne 30. října 2014.

⁹ Rozhodnutí Nejvyššího správního soudu České republiky, sp. zn. 1 As 33/2011-58.

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.

3) Využitelnost „skrytě“ pořízených nahrávek

V úvodu k druhé části příspěvku bylo uvedeno, že základní podmínkou pro použití určitého důkazního prostředku je jeho opatření zákonným způsobem. V této souvislosti se v nedávné minulosti soudní judikatura vyjadřovala k přípustnosti kamerových či zvukových záznamů pořízených soukromou osobou bez souhlasu zaznamenávané osoby s tím závěrem, že použitelnost ani takovýchto důkazů v řízení není zcela vyloučena. Podle rozhodnutí Nejvyššího správního soudu, sp. zn. 2 As 45/2010-56 platí, že „*I za situace, kdy kamerový záznam pořízený soukromou osobou, který zasahuje do sféry osobnostních práv zaznamenané osoby, nebyl pořízen s jejím souhlasem či v souladu se zákonnými výjimkami, není jeho použitelnost pro potřeby dokazování ve správním řízení zcela vyloučena. V těchto případech je vždy nutno poměřit legitimitu cíle, kterého mělo být dosaženo, na straně jedné a přiměřenost užitého postupu na straně druhé. Je tak vždy nutno uvážit, zda v konkrétním případě může nad ochranou osobnostních práv dotčeného subjektu převážet zájem společnosti na objasnění a potrestání deliktů jednání a především pak ochrana ústavně zaručených práv pořizovatele takového záznamu. Je-li kamerový systém, z něhož pochází posuzovaný záznam, provozován bez oznámení úřadu pro ochranu osobních údajů, nejde jen z tohoto důvodu o důkaz nezákonný. Porušení této povinnosti má ve vztahu k dokazování pouze ten následek, že, má-li být takto pořízený záznam použit jako důkaz ve správním či soudním řízení, neplatí presumpce provozování tohoto systému v souladu se zákonem, a bude tak nutné provést celkové posouzení, zda docházelo ke zpracování osobních údajů v rozporu se zákonem či nikoliv.*“

K opačným závěrům dospěla judikatura v případech nezákonně pořízených záznamů samotnými orgány veřejné moci: „*V českém právním řádu neexistuje žádný právní základ pro utajené pořizování audiovizuálních nahrávek orgány veřejné moci pro účely správního trestání, pokud tyto zasahují do „soukromého života“ fyzických osob. Takovým základem není ani § 51 odst. 1 správního řádu z roku 2004. Důkaz audiovizuální nahrávkou pořízenou v utajení orgánem veřejné moci nebo v souvislosti s činností orgánu veřejné moci je proto v řízení o správním trestání zásadně nepoužitelný.*“

4) Využitelnost internetových map

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.¹⁰

¹⁰ Rozhodnutí Nejvyššího správního soudu, sp. zn. 9 As 128/2013, rozhodnutí Nejvyššího správního soudu, sp. zn. 7 As 129/2013.

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.

5) Charakter a podmínky provedení důkazů pořízených z Internetu, včetně promítnutí audiovizuálního záznamu

Internetové mapy, diskuse na sociálních sítích, uživatelské účty, fotografie, audiovizuální záznamy, jakož i veškeré jiné objekty existující v prostředí Internetu lze z hlediska provedení důkazů považovat za specifický případ provedení důkazu ohledáním.¹¹

Ohledáním je třeba rozumět každý postup, jímž se správní orgán vlastním empirickým nazíráním přesvědčuje o předmětu řízení.¹² Podpůrně lze argumentovat i ustanovením § 51 správního řádu, který upravuje dokazování, kdy za důkazní prostředky považuje správní řád 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 nejbližší právě k ohledání.¹³

Obecně přitom platí, že důkazy (včetně ohledání) mohou být provedeny jak v rámci ústního jednání, tak i mimo ústní jednání. V obou situacích platí, že o provádění důkazů musí být účastníci řízení vždy včas vyrozuměni a musí jim být umožněna přítomnost (účast) při jejich provedení (zásada součinnosti, zásada poučovací). Pokud toto pravidlo nebude dodrženo, představuje to vždy vadu řízení způsobující nezákonnost postupu, jakož i z něj vzešlého rozhodnutí. Jedná se o vadu nezhojitelnou. Nezbytnost vyhotovit protokol o provádění tohoto důkazního prostředku pak plyne z toho, aby bylo skutečně zřejmé, že správní orgán obsah záznamu či internetovou stránku skutečně zhlédl.

Výjimku z povinné protokolace představuje pouze provedení listinou, a to při splnění dvou podmínek, kterými jsou 1) založení listiny do spisu podle § 17 odst. 1 správního řádu a 2) účastník řízení má možnost se s těmito listinami seznámit při nahlížení do spisu podle § 36 odst. 3 správního řádu. Jedině za těchto podmínek lze provádět dokazování jednoduše tím, že je listina vložena do spisu.¹⁴

11 Rozhodnutí Nejvyššího správního soudu ze dne 26.11.2008, čj. 2 As 59/2008–80.

12 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.

13 Obdobný názor zaujímá např. KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, s. 102.

14 Rozhodnutí Nejvyššího správního soudu, sp. zn. 2 As 33/2016–53.

6) Využitelnost registračních údajů od poskytovatelů internetového připojení a služeb, mobilních operátorů pro účely dokazování

U přestupků páchaných na Internetu jsou zákonné možnosti vyžadování pomoci od fyzických a právnických osob či jiných orgánů nepochybně užší, než je tomu u trestných činů. Při tzv. předšetření přestupků nelze například nařídit uchování nebo znepřístupnění dat jiným osobám (§ 7b TR), odposlouchávat budoucí či probíhající zájmové komunikace (§ 88 TR), vyžadovat údaje o telekomunikačním provozu (§ 88a TR), sledovat obsah e-mailových schránek a cloudových úložišť (§ 158d TR).

Právním základem se z hlediska tzv. předšetřování přestupků ze strany orgánů policie v těchto případech stává zákon o policii. Je třeba na tomto místě zmínit, že využití možnosti vyžadovat registrační údaje od níže uvedených poskytovatelů je ze strany orgánů policie v mnohem nižší míře, než by bylo žádoucí. Jako jeden z faktorů se jeví nedostatečné vzdělávání příslušníků Policie České republiky v této oblasti, z čehož vyvěrá nevědomost o nových možnostech a trendech při předšetření přestupků.

V první řadě je třeba poukázat na ustanovení § 18 ve spojení s ustanovením § 114 citovaného zákona. 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 prostřednictvím Internetu je třeba žádosti směřovat zejména: 1) poskytovatelům internetového připojení (konektivity), a 2) poskytovatelům služeb. Uvedení poskytovatelé bývají relativně často i ze strany odborné veřejnosti nesprávně zaměňováni nebo považováni za totožné.

Informace od poskytovatelů internetového připojení

Poskytovatele internetového připojení lze definovat jako fyzickou či právnickou osobu, která je schopna poskytovat jiným subjektům přístup k Internetu.¹⁵ 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 údaje o držitelích IP adres¹⁶ – 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

15 KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou*. Praha: Policejní akademie České republiky v Praze, 2013, s. 22.

16 KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, s. 137.

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.

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 o elektronických komunikacích, přičemž se provozními údaji rozumí „*jakékoli údaje zpracováváné 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 zpracováváné v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací*“. Jak je 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.¹⁷ 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 by bylo možné získat pouze při splnění taxativně stanovených podmínek v rámci trestního řízení.¹⁸

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

Pod zvýrazněnými body jsou informace, které jsou ze strany uživatele manuálně vloženy. Lze proto přijmout tezi, že pokud je s předchozím rozmyslem využito Internetu k páčání 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 páčání

¹⁷ Tamtéž, s. 442.

¹⁸ ŠÁMAL, Pavel. *Trestní řád: komentář. 7., dopl. a přeprac. vyd. Praha: C. H. Beck, 2013, s. 1232.*

protiprávního jednání nebo o osoby méně technicky zdatné, které svou neznalostí nabývaly klamný pocit anonymity na Internetu.

Někteří poskytovatelé služby 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.

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 registrační 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.

Informace od mobilních operátorů

Ustanovení § 66 odst. 2 zákona o policii 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,¹⁹ datum poslední změny (aktivace, deaktivace nebo suspendace)

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.²⁰ Žádosti i výsledné informace se předávají v elektronické formě jako datové soubory.²¹

19 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 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>

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

21 Ustanovení § 2 odst. 2 vyhlášky Ministerstva vnitra č. 336/2005 Sb.

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.²² 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.²³ 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 potenciální žádost orgánu policie o zajištění uvedených informací bude vždy s negativním výsledkem.

7) Využitelnost počítačové expertizy

Počítačovou expertizu je třeba řadit mezi prostředky využitelné orgánem policie k úspěšnému objasnění přestupku z prostředí Internetu.

Předmětem počítačové expertizy nejsou výhradně objekty výpočetní techniky, včetně některých periférií, ale i mobilní telefony a příslušenství, paměťová média (USB disky, flash paměti) a další obdobné prostředky.

Cílem expertizy je vyhledat, zpřístupnit a zkoumat data důležitá pro objasnění šetřeného přestupku za aplikace poznatků z kybernetiky, informatiky, elektrotechniky a ostatních souvisejících vědních oborů.²⁴

Počítačová expertiza bezprostředně navazuje na stadium zajištění věcí podle ustanovení § 34 zákona o policii. Je notorií, že přístup do objektů zajištěných k počítačové expertize bývá opatřen zpravidla přihlašovacím heslem. U mobilních telefonů v poslední době převládá opatření v podobě tahového gesta. Při zajišťování těchto objektů by neměl orgán policie opomenout provést pokus směřující k získání přihlašovacích hesel od osob, které je vydaly nebo jim byly odňaty. I zde platí zásada *nemo tenetur se ipsum accusare*,

²² Například <http://www.@Bcoo.com> nebo <http://@eellee.org>

²³ 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>

²⁴ NĚMEC, Miroslav. *Kriminalistická taktika pro policisty a studenty Policejní akademie České republiky v Praze*. Praha: Abook, 2017, s. 175.

tedy sdělení hesla se odvíjí zcela na vůli vydávající osoby a nelze jej ze strany orgánu policie v žádném případě vynucovat.

S objekty, které budou podrobeny budoucí expertize, je nezbytné již od doby jejich zajištění zacházet nanejvýš opatrně, zejména, aby nedošlo ke smazání či změně uložených dat.²⁵

Po zajištění musí být provedena fotografická dokumentace, následně jsou objekty vloženy do ochranného obalu a opatřeny pečeti. Pečeť plní funkci záruky, že od doby zajištění až do doby doručení subjektu, který bude provádět expertizu, nebylo s objektem budoucího zkoumání neoprávněně manipulováno či zasahováno do uložených dat.

Oddělení kriminalistické techniky a expertiz po obdržení zkoumaného objektu nejdříve provede vnější prohlídku k zadokumentování stavu v době jejich dodání k expertize. Provádí se zejména fotografická dokumentace: neporušení balení, zkoumaného objektu se zaměřením na štítek s výrobním číslem, poškození či chybějící části, vnitřní komponenty (například SIM karty) a paměťové nosiče taktéž s akcentem na štítek s výrobním číslem a typem, u počítačových sestav navíc typ a stav pevných disků a dalších připojených periférií.

Po vnější prohlídce zkoumaného objektu se přistupuje k vytvoření identické bitové kopie nosiče informací. Obecně existují dva primární důvody pro její vytvoření. Prvním je náchylnost digitálních dat ke změně, kdy v případě práce s daty dochází činností osoby, která tato data zkoumá, k jistým změnám, proto je vhodné provádět vlastní zkoumání na kopiích. Druhým důvodem je pak skutečnost, že orgán policie již nemusí mít originál z různých důvodů k dispozici, přičemž identická kopie zajištěná správným způsobem je nadána nahradit originál ve správném řízení, neboť je jeho přesnou kopií.²⁶ Vytvořenou bitovou kopii je přitom nutné opatřit kontrolním součtem souboru.

V rámci šetření a objasňování přestupků lze ze zajištěných objektů zjistit následující informace (níže uvedený výčet je toliko demonstrativní):

- obsah SMS i MMS zpráv,
- seznam přijatých a odchozích hovorů,
- seznam telefonních kontaktů,
- záznamy hovorů pořízené mobilním diktafonem,
- obsah komunikátorů (Viber, WhatsApp, Signal a podobně),
- GPS souřadnice,
- uživatelské účty včetně přístupových práv,
- strukturu souborů s dokumenty,
- vytvořené fotografie,
- stažené soubory z Internetu,
- uložené záložky (odkazy na internetové stránky),
- historie navštívených internetových stránek a využití internetového připojení.

25 POLČÁK, Radim, František PÚRY a Jakub HARAŠTA. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015, s. 202.

26 KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016, s. 452.

Získání uvedených informací je podmíněno jejich uložením přímo v paměti zkoumaného objektu. Budou-li ve zkoumaném objektu zjištěny i přihlašovací jména a hesla k uživatelským účtům na Internetu, například e-mailová schránka, Google disk, iCloud, Facebook, Instagram a další, nejsou data z těchto účtů pro orgán policie v rámci šetření přestupků dosažitelná. V trestním řízení lze získat taková data pouze na základě písemného a odůvodněného příkazu soudce příslušného soudu nebo se souhlasem dotčené osoby.²⁷

Zjištění obsahu údajů doručených na datový nosič v době po jeho zajištění orgánem policie, například přijatých SMS zpráv nebo hovorů, je pro šetření přestupků vyloučeno. Uvedené lze odvodit z výkladového stanoviska Nejvyššího státního zastupitelství č. 1/2015, spisová značka 1 SL 760/2014 ze dne 26. 1. 2015.

Závěr

Příspěvek si kladl za cíl zachytit korelaci mezi technologickým vývojem v oblasti ICT a dokazováním v přestupkovém řízení. Progres v tomto směru nelze v přestupkovém právu zaznamenat oproti právu občanskému či trestnímu v samotné právní úpravě, tj. vývoji legislativním (např. ve smyslu zakotvení odpovídajících, specifických důkazních a zajišťovacích prostředků), i přesto však lze konstatovat, že současná právní úprava nevykazuje ve vztahu k využitelnosti ICT v procesu dokazování zásadních nedostatků a lze ji považovat za dostačující a charakteru a účelu přestupkového řízení odpovídající. Případné deficity a problematické oblasti kultivuje v dnešní době již relativně bohatá soudní judikatura, která na technologický pokrok dostatečně reflektuje.

Literatura

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

GRÍVNA, 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.

KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou*. Praha: Policejní akademie České republiky, 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, František PÚRY a Jakub HARAŠTA. *Elektronické důkazy v trestním řízení*. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8073-7.

²⁷ Ustanovení § 88a odst. 1, odst. 4 trestního řádu.

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

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

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

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