16. 1. 2017

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Přípustnost a podmínky použití lokalizačních údajů v trestním řízení

Se stále větším využitím internetových aplikací používaných ke komunikaci, sjednávání obchodů, platbám bankovním i nebankovním se nabízí řada nových důkazů, které mohou být využity v soudním řízení, a to jak civilním, tak zejména trestním. V tomto rozboru se pokusíme popsat současnou situaci, kdy opatřování a používání důkazů orgány činnými v trestním řízení, souvisejících s používáním internetových aplikací, probíhá zcela živelně a podle našeho názoru i v rozporu s existující právní úpravou. Jedná se tak o důkazy neúčinné, z kterých by nemělo být čerpáno, přesto se tak, i přes námitky, zcela běžně děje.

Často jsou pro potřeby trestního řízení získávány údaje o tom, z jaké IP adresy byly prováděny platby, objednávky, či jiná komunikace. IP adresa, tj. adresa internetového protokolu, je řada binárních čísel, která je přidělena konkrétnímu zařízení (počítač, tablet, chytrý telefon), slouží k identifikaci tohoto zařízení a umožňuje mu přístup k síti elektronických komunikací. IP adresa se zasílá na server, na kterém je uložena právě otevíraná internetová schránka (obdobně například stanovisko generálního advokáta Manuela Campose Sánchez-Bordony ve věci C-582/14).

IP adresu je třeba považovat za lokalizační údaj ve smyslu ust. § 91 zákona č. 127/2005 Sb., o elektronických komunikacích (dále jen „zákon o elektronických komunikacích), neboť *jde o údaj, který určuje zeměpisnou polohu telekomunikačního zařízení uživatele veřejně dostupné služby elektronických komunikací. Dle daného ustanovení, pokud podnikatel zajišťující veřejnou telekomunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací zpracovává lokalizační údaje vztahující se k uživateli nebo účastníku,* ***musí tyto údaje učinit anonymními nebo získat souhlas uživatele nebo účastníka*** *se zpracováním v rozsahu nezbytném pro poskytování služeb s přidanou hodnotou*.

Poskytování takových údajů orgánům činným v trestním řízení je pak umožněno ust. § 88a tr. řádu, když tento byl ke dni 30.9.2012 zrušen nálezem Ústavního soudu ČR a bylo přijato znění nové. Dle ust. § 88a tr.ř., ve znění do 30.9.2012, *je-li k objasnění skutečností důležitých pro trestní řízení třeba zjistit údaje o uskutečněném telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, nařídí předseda senátu a v přípravném řízení soudce, aby je právnické nebo fyzické osoby, které vykonávají telekomunikační činnost, sdělily jemu a v přípravném řízení buď státnímu zástupci nebo policejnímu orgánu. Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn*.

Na úpravu § 88a tr. řádu, která byla později shledána za protiústavní a zrušena nálezem Ústavního soudu ČR sp. zn. Pl. ÚS 24/11, navazovalo v oblasti uchovávání IP adres ust. § 96 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích, a vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům

oprávněným k jejich využívání. Tato úprava byla zrušena již předchozím nálezem sp. zn. Pl. ÚS 24/10 ze dne 22.3.2011.

Dle ust. § 88a tr.ř., v současném znění, *je-li třeba pro účely trestního řízení vedeného pro úmyslný trestný čin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky, pro trestný čin porušení tajemství dopravovaných zpráv (§ 182 trestního zákoníku), pro trestný čin podvodu (§ 209 trestního zákoníku), pro trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 trestního zákoníku), pro trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 trestního zákoníku), pro trestný čin nebezpečného vyhrožování (§ 353 trestního zákoníku), pro trestný čin nebezpečného pronásledování (§ 354 trestního zákoníku), pro trestný čin šíření poplašné zprávy (§ 357 trestního zákoníku), pro trestný čin podněcování k trestnému činu (§ 364 trestního zákoníku), pro trestný čin schvalování trestného činu (§ 365 trestního zákoníku), nebo pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána,* ***zjistit údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat****, a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené, nařídí v řízení před soudem jejich vydání soudu předseda senátu a v přípravném řízení nařídí jejich vydání státnímu zástupci nebo policejnímu orgánu soudce na návrh státního zástupce. Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn, včetně konkrétního odkazu na vyhlášenou mezinárodní smlouvu v případě, že se vede trestní řízení pro trestný čin, k jehož stíhání tato mezinárodní smlouva zavazuje. Vztahuje-li se žádost ke konkrétnímu uživateli, musí být v příkazu uvedena jeho totožnost, je-li známa.*

Dle ust. § 97 odst. 3 zákona o elektronických komunikacích, ve znění od 1.10.2012, *právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací. Provozní a lokalizační údaje týkající se neúspěšných pokusů o volání je právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna uchovávat pouze tehdy, jsou-li tyto údaje vytvářeny nebo zpracovávány a zároveň uchovávány nebo zaznamenávány. Současně je tato právnická nebo fyzická osoba povinna zajistit, aby při plnění povinnosti podle věty první a druhé nebyl uchováván obsah zpráv a takto uchovávaný dále předáván. Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout*

- *a) orgánům činným v trestním řízení pro účely a při splnění podmínek stanovených zvláštním právním předpisem,*
- *b) Policii České republiky pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby a při splnění podmínek stanovených zvláštním právním předpisem,*
- *c) Bezpečnostní informační službě pro účely a při splnění podmínek stanovených zvláštním právním předpisem,*
- *d) Vojenskému zpravodajství pro účely a při splnění podmínek stanovených zvláštním právním předpisem,*
- *e) České národní bance pro účely a při splnění podmínek stanovených zvláštním právním předpisem.*

Po uplynutí doby podle věty první je právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, povinna je zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich využívání podle zvláštního právního předpisu nebo pokud tento zákon nestanoví jinak (§ 90).

Ústavní soud v nálezu Pl. ÚS 24/10 uvedl, že ***sběr a uchovávání lokalizačních a provozních údajů tak rovněž představuje významný zásah do práva na soukromí, a z toho důvodu je nezbytné pod rozsah ochrany základního práva na respekt k soukromému životu v podobě práva na informační sebeurčení*** *(ve smyslu čl. 10 odst. 3 a čl. 13 Listiny) zahrnout nejen ochranu vlastního obsahu zpráv podávaných prostřednictvím telefonní komunikace či komunikace prostřednictvím tzv. veřejných sítí, ale i provozní a lokalizační údaje o nich.*

Z daného vyplývá, že se **jedná o osobní údaje, jejichž shromažďování je možné výhradně se souhlasem uživatele nebo účastníka, popř. pouze na základě zvláštního zákona, kde jiný zájem aprobovaný Listinou či Ústavou převáží nad zájmem na ochraně soukromého života**. Skutečnost, že IP adresa je osobním údajem, vyplývá mimo jiné z judikatury Evropského soudního dvora ve věci Scarlet Extended SA v. Sociétébelge des auteurs, compositeurs et éditeurs SCRL (SABAM), C – 70/10 (bod 51), daný názor ostatně dlouhodobě zastává i Úřad pro ochranu osobních údajů.

Právě výše citované ustanovení § 97 odst. 3 zákona o elektronických komunikacích zakotvuje výjimku, kdy bylo možné bez souhlasu uživatele nebo účastníka uchovávat provozní a lokalizační údaje, a to za účelem jejich poskytnutí orgánům oprávněným k jejich vyžádání podle zvláštního předpisu. Uchovávání provozních a lokalizačních údajů je zákonem o elektronických komunikacích časově omezeno na dobu 6 měsíců a po uplynutí této doby, která byla pro jednotlivé údaje zpřesněna prováděcími předpisy, byla povinnost údaje zlikvidovat, pokud tedy již nebyly na základě oprávněné žádosti poskytnuty.

Vzhledem ke stanovení takto krátkých lhůt pro uchování lokalizačních a provozních údajů, je zřejmý záměr zákonodárce, aby do práva na ochranu soukromého života bylo zasahováno po co nejkratší dobu. **Přitom je zřejmé, že provozní a lokalizační údaje mohou uchovávat pouze zákonem vymezené osoby – právnická nebo fyzická osoba zajišťující veřejnou telekomunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, a pokud by takto činily jiné osoby, nebyl by jejich zásah do práva na ochranu soukromého života zákonem aprobován.**

Orgány činné v trestním řízení však právní úpravu a závěry Ústavního soudu obchází tím, že IP adresy jsou od bank vyžadovány dle ust. § 8 odst. 2 tr. řádu, tedy žádostí o poskytnutí údajů, které jsou předmětem bankovního tajemství. Bankovní tajemství je upraveno zákonem č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů (dále jen „BankZ“). Konkrétně ustanovení § 38 BankZ vymezuje bankovní tajemství. Zde je v prvním odstavci stanoveno, že bankovní tajemství se vztahuje na všechny **bankovní obchody, peněžní služby bank, včetně stavů na účtech a depozit**. IP adresa, ze které klient banky přistupuje k internetovému bankovnictví, není předmětem bankovního tajemství, ale banka je povinna k daným údajům, tj. lokalizačním údajům, přistupovat v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů, a tedy bez souhlasu osoby, které se takové údaje týkají, je nemůže zpracovávat. Údaje o používání IP adres od jiných, „nebankovních“ subjektů jsou již požadovány zcela neformálně, tedy v některých případech i bez žádosti státního zástupce, neboť orgány činné v trestním řízení nepovažují tyto informace za údaje chráněné zvláštním zákonem, konkrétně tedy zákonem č. 101/2000 Sb.

Zcela bez povšimnutí zůstává fakt, že různé subjekty od bank, přes některé státní podniky a další subjekty zjevně shromažďují chráněné lokalizační údaje o přístupu uživatelů k jejich serverům z IP

adres, aniž by respektovaly platnou právní úpravu a aniž by společnosti, či konkrétní osoby, jimž byl zřízen přístup k elektronickému bankovnictví, vyslovily souhlas se zpracováním jejich osobních údajů ve formě IP adresy, ze které se do internetového bankovnictví přihlašují. Pokud tedy banky a jiné subjekty uchovávají a zpracovávají tyto údaje (a nejedná se přitom ani o údaje o proběhlých transakcích, nýbrž pouze o přihlášeních), činí tak v rozporu se zákonem.

Je tedy třeba upozornit, že již samotná existence seznamů přihlášení s IP adresami je v rozporu se zákonem a je zásadním porušením práva na ochranu soukromého života. Jsme přesvědčeni, že **je-li samotná existence důkazu v rozporu se zákonem, je tím způsobena nezákonnost důkazu samotného**.

Pokud jde o možnost získávání lokalizačních údajů ze strany orgánů činných v trestním řízení, to bylo umožněno již zmiňovaným ust. § 88a tr. řádu. V první řadě by se však muselo jednat o lokalizační údaje shromažďované v souladu se zmiňovanou právní úpravou a rovněž by **orgány činné v trestním řízení měly získávat údaje postupem dle ust. § 88a tr. řádu, tedy na základě příkazu soudu k zajištění údajů o telekomunikačním provozu**, což se ovšem v praxi neděje. K tomu je třeba doplnit, že Ústavní soud ČR zásadně při výkladu práva na soukromý život a práva na informační sebeurčení nerozlišuje, zda údaje o telekomunikačním provozu získává a jsou vyžadovány od „operátorů“, tj. osob, které zajišťují veřejnou telekomunikační síť nebo poskytují veřejně dostupnou službu elektronických komunikací, nebo od třetích osob, například provozovatelů nejrůznějších internetových stránek, vyhledávačů či aplikací, či internetového bankovnictví. Jsou-li tedy požadovány údaje vymezené v ust. § 88a tr. řádu, pod které lze podřadit i údaje lokalizační, lze je žádat pouze postupem dle tohoto ustanovení.

Ze současného znění ust. § 88a tr. řádu, přijatého po zrušení tehdejšího ustanovení nálezem Ústavního soudu ČR, kdy **není subjekt povinný k poskytnutí údajů výslovně vymezen**, lze vyložit, že ust. § 88a tr. řádu lze užít i pro případy, kdy jsou lokalizační údaje uchovávány subjekty, které nezajišťují veřejnou komunikační síť nebo neposkytují veřejně dostupnou službu elektronických komunikací. Jak však bylo výše uvedeno, tyto osoby **nemají zákonné zmocnění k uchovávání lokalizačních údajů a jejich schraňování by muselo být odsouhlaseno konkrétními uživateli**. Nadto je třeba poukázat na to, že právo shromažďovat lokalizační a provozní údaje neměly v době od 11.4.2011 do 30.9.2012 ani subjekty zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, když ust. § 96 odst. 3 zákona o elektronických komunikacích v té době neplatilo. **Pokud tedy nemohli lokalizační údaje v té době shromažďovat „operátoři“, tím spíše ne běžné třetí osoby, jako jsou provozovatelé různých internetových serverů, či banka.**

Ostatně, Ústavní soud ČR ve svém nálezu sp. zn. I. ÚS 191/05 judikoval, že **záznam telefonického hovoru fyzických osob může být jako důkaz použit zásadně jen se svolením osoby, která byla účastníkem nahrávaného hovoru**. Obdobně by pak mělo být pohlíženo na situace, kdy jsou údaje umožňující lokalizaci volajícího, či jako v tomto případě lokalizaci osoby používající internetové bankovnictví, shromažďovány osobou třetí, odlišnou od té, které to zákon umožňuje v ust. § 97 zákona o elektronických komunikacích. V této souvislosti lze odkázat i na závěry Ústavního soudu ČR ve věci II. ÚS 502/2000. Soud rozhodoval v situaci, kdy nebyla v trestním řádu specifická úprava pro získávání lokalizačních a provozních údajů (nyní ust. § 88a tr. řádu). Uvedl, že dle jeho názoru, *který se tímto ztotožňuje s rozsudkem Evropského soudu pro lidská práva ze dne 2. 8. 1984 ve věci Malone proti Spojenému království, je třeba považovat výše uvedené údaje, a zvláště pak volaná čísla, za nedílnou součást komunikace uskutečněné prostřednictvím telefonu. Soukromí každého člověka je hodno zásadní (ústavní) ochrany nejen ve vztahu k vlastnímu obsahu podávaných zpráv, ale i ve vztahu k výše uvedeným údajům. Lze tedy konstatovat, že čl. 13 Listiny zakládá i ochranu tajemství volaných čísel a dalších souvisejících údajů, jako je datum a čas hovoru, doba jeho*

trvání, v případě volání mobilním telefonem i označení základových stanic zajišťujících hovor.

Ústavní soud ČR dále v dané věci uvedl: *Jestliže ústavní pořádek České republiky připouští průlom této ochrany, děje se tak pouze a výlučně v zájmu ochrany demokratické společnosti, případně v zájmu ústavně zaručených základních práv a svobod jiných; sem spadá především nezbytnost daná obecným zájmem na ochraně společnosti před trestnými činy a dále tím, aby takové činy byly zjištěny a potrestány. Přípustný je tedy pouze zásah do základního práva nebo svobody člověka ze strany státní moci, jestliže jde o zásah nezbytný ve výše uvedeném smyslu. K tomu, aby nebyly překročeny meze nezbytnosti, musí existovat systém adekvátních a dostatečných záruk, skládající se z odpovídajících právních předpisů a účinné kontroly jejich dodržování. Tyto právní předpisy musí být přesné ve svých formulacích, aby daly občanům dostatečnou informaci o okolnostech a podmínkách, za kterých jsou státní orgány oprávněny k zásahu do soukromí; přesně musí být definovány i pravomoci udělené příslušným orgánům a způsob jejich provádění tak, aby jednotlivcům byla poskytnuta ochrana proti svévolnému zasahování (viz také shora citovaný rozsudek Evropského soudu pro lidská práva). V případě, že tyto zásady nebudou ze strany státní moci respektovány, jsou zásahy do uvedeného základního práva vyloučeny a dojde-li k nim, stávají se protiústavními.*

V návaznosti na danou úpravu Ústavní soud ČR uzavřel, že policejní orgán byl povinen při vyžadování provozních a lokalizačních údajů postupovat subsidiárně dle ust. § 88 tr. řádu, a pokud tak neučinil, byl předmětný důkaz pro účely trestního řízení pořízen protiprávně. Ústavní soud ČR uvedl, že *obecné soudy tedy zásadním způsobem pochybily, když připustily, že evidence telekomunikačního provozu byla do spisu nejen zařazena, ale také jimi jako důkaz provedena a následně v jejich rozhodnutích hodnocena*. **Orgány činné v trestním řízení totiž tím, že si opatřují údaje o IP adresách, které jsou získávány a uchovávány bez souhlasu uživatelů a navíc bez toho, aby byl dodržen postup předvídaný ust. § 88a tr. řádu, porušují nejen právo na soukromý život, jak je zakotveno v čl. 13 Listiny, ale současně také právo na spravedlivý proces dle čl. 36 Úmluvy.**

I vzhledem k výše uvedenému zastáváme názor, že důvodem pro vložení institutu zjišťování údajů z telekomunikačního provozu do ust. § 88a tr. řádu byla nezbytnost ochrany osobních údajů jednotlivce. Je pak zcela irelevantní, zda jsou dané údaje uchovávány osobami, které vykonávají telekomunikační činnost, či osobami jinými, které dané telekomunikační údaje osobní povahy shromažďují v rámci své jiné činnosti.

Dle obou výše zmiňovaných znění ust. § 88a tr. řádu pak příkazu není třeba, pokud k poskytnutí údajů dá souhlas uživatel telekomunikačního zařízení, ke kterému se mají údaje o telekomunikačním provozu vztahovat. V autory zmiňovaných konkrétních případech však nebyl výslovný souhlas osobám, které údaje orgánům činným v trestním řízení lokalizační údaje poskytly, udělen. Nadto nejsme přesvědčeni, že se dané ustanovení aplikovalo v případech, kdy jsou dané údaje uchovávány a poskytovány institucemi jako jsou banky, jejichž postavení nelze srovnávat s běžným koncovým uživatelem, naopak, jejich postavení je bližší poskytovateli telekomunikačních služeb.

Právní teorie i praxe rozlišují absolutní neúčinnost důkazu, která je důsledkem existence podstatné (závažné) procesní vady, která je neodstranitelná, a dále relativní neúčinnost důkazu, jež je důsledkem existence podstatné (závažné) procesní vady, která je odstranitelná. Rovněž je všeobecně akceptováno, že vadně provedený nebo nezákonným způsobem opatřený důkaz je dle povahy a závažnosti porušení zákona buď absolutně neúčinný, respektive nepřípustný (tj. nelze k němu přihlížet a musí být vyloučen z hodnocení při zjišťování skutkového stavu) nebo relativně neúčinný (tj. nelze k němu přihlížet, jen pokud se neodstraní vada, která se při jeho opatřování nebo provádění sběhla) anebo posléze jde o důkaz plně účinný, protože vada, ke které došlo, není podstatná.

Proto považujeme za zřejmé, že v případě, kdy jsou pro potřeby trestního řízení získávány lokalizační údaje o IP adresách od subjektů, které nemají právo takové údaje uchovávat, a navíc bez souhlasu soudce, jedná se o absolutně neúčinné důkazy, k nimž by nemělo být v řízení přihlíženo.

Mgr. Hana Líňová,
advokát

JUDr. Tomáš Vymazal,
advokát

Advokátní kancelář JUDr. Tomáše Vymazala

Wellnerova 1322/3C
779 00 Olomouc

Tel.: +420 581 200 576
e-mail: info@ak-vymazal.cz

Další články:

- Podmíněné propuštění ve světle zásady ústnosti a přímosti
- Poučení z krizového vývoje v kauze bitcoiny
- Podmíněné upuštění od trestního stíhání: racionální odklon u právnických osob
- Zkreslené vzpomínky v trestním řízení vedeném pro pohlavní zneužívání
- Přenositelnost důkazů z daňového do trestního řízení
- Praktický návod na úspěch žádosti o podmíněné propuštění od roku 2026
- Přijetí prohlášení viny a povinnost soudu vypořádat námitky poškozeného
- Podmínky pro uložení trestu vyhoštění cizince
- Zamyšlení nad systémem alternativních trestů: poznámky na pozadí mezinárodní vědecké konference „Rethinking Sentencing: Are We Getting Justice Right?“
- Správné určení počátku běhu lhůty pro podání stížnosti proti usnesení soudu, kterým se

nařizuje výkon trestu odnětí svobody
- Rozšiřování státní moci při implementaci acquis EU: český fenomén gold-platingu na příkladu konfiskační směrnice