

3. 12. 2021

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

Poskytování údajů elektronických komunikací oprávněným orgánům

Nejen v souvislosti s celosvětovou pandemií COVID-19, pokračujícími kybernetickými útoky zasahujícími často oblast citlivých údajů, ale také v kontextu navrhovaných legislativních změn v oblasti elektronických komunikací, se v posledních letech otevírá téma samotného rozsahu přístupu k údajům, které jsou generovány v rámci poskytování služeb elektronických komunikací nebo přímo vznikají v souvislosti s provozem těchto služeb.

Jednou z otázek je tedy i přístup k údajům elektronických komunikací (nově dle návrhu Nařízení ePrivacy označovaných také jako metadata) ze strany orgánů státní správy (tzv. law enforcement agencies). Polemiky nad tím, v jakém rozsahu a za jakých podmínek mohou být metadata využívána, vyústily dokonce ve zrušení směrnice Evropského parlamentu a Rady 2006/24/ES o uchovávání údajů, a to rozhodnutími ze strany Evropského soudního dvora ve spojených věcech C-293/12 a C-594/12[1] ze dne 8. 4. 2014. Tato rozhodnutí poukazovala na skutečnost, že podle směrnice je umožněné sledování velkého objemu informací o populaci jako celku, aniž by takové plošné sledování mělo či mohlo mít přímou souvislost s faktickým ohrožením veřejné bezpečnosti. Dále Evropský soudní dvůr kritizoval absenci kontrolních mechanismů a pravidel přístupu pro oprávněné veřejné orgány, včetně přiměřené doby pro uchovávání údajů. Evropský soudní dvůr na druhou stranu dovedl, že zpracování metadat za účelem boje proti terorismu, posilování národní bezpečnosti a prevence závažné trestné činnosti, je účelem legitimním a odpovídá obecnému zájmu. Evropský soudní dvůr však nakonec i přesto rozhodl, že směrnice Evropského parlamentu a Rady 2006/24/ES o uchovávání údajů není plně v souladu s úpravou v Listině základních práv Evropské unie[2]. Tento právní výklad následně potvrzoval i ve svých dalších rozsudcích (viz C-623/17 [3] či C-746/18[4]).

Odlíšný přístup k problematice míry a extenzity při poskytování metadat ze strany povinných osob je navíc zřejmě viditelným i v prostředí České republiky, kde také opakovaně dochází k určitým názorovým střetům a určité dichotomii ve vnímání této problematiky, zejména v odborné rovině. Tyto názorové rozdíly částečně podporují případné snahy dalších orgánů státní moci o rozšiřování pravomocí i v této oblasti.

V České republice jsou v tomto ohledu významné nálezy Ústavního soudu, pod sp. zn. Pl. ÚS 24/10[5], ze dne 22. 3. 2011 a Pl. ÚS 24/11[6], ze dne 20. 12. 2011, které zrušily § 97 odst. 3 a 4 zákona o elektronických komunikacích[7] a § 88 a § 88a trestního řádu[8], a to dnem vyhlášení nálezů ve sbírce zákonů 12. 4. 2011. Zde je nutné konstatovat, že se jedná o nálezy vydané ještě před zrušením směrnice Evropského parlamentu a Rady 2006/24/ES o uchovávání údajů. Zrušení uvedených ustanovení zahájilo práce na novele legislativy, která byla provedena zákonem č. 273/2012 Sb., který nabyl účinnosti 1. 10. 2012. Jelikož novela zákona o elektronických komunikacích, která nově upravila problematiku tzv. data retention, byla přijata s určitým časovým odstupem, došlo k určitému otestování stavu, kdy přístup k těmto typům údajů elektronických komunikací fungoval po určité období bez této speciální právní úpravy, a to pouze na základě obecných oprávnění (např. § 8 trestního řádu), tedy bez dostatečné právní jistoty, jak pro oprávněné orgány, povinné osoby, tak i pro subjekty údajů (koncové uživatele služeb).

Následně byl pak v roce 2017 podán další návrh na zrušení zmíněného § 97 odst. 3 a 4 zákona o

elektronických komunikacích, § 88a trestního řádu a § 68 odst. 2 a § 71 písm. a) zákona o policii^[9], z důvodu jeho ústavní nekonformnosti. V tomto případě však Ústavní soud neshledal dovozovanou protiústavnost. Plénum Ústavního soudu zamítlo návrh skupiny 58 poslanců na zrušení některých ustanovení zákona o elektronických komunikacích, trestního řádu, zákona o Policii České republiky a vyhlášky o uchovávání, předávání a likvidaci provozních a lokalizačních údajů (Pl. ÚS 45/17^[10]).

Jaký je tedy současný rozsah orgánů oprávněných získat přístup k datům vznikajících v rámci poskytování služeb elektronických komunikací? Na základě jakých podmínek je takový přístup umožněn? Jaké jsou nastaveny kontrolní mechanismy zajišťující, že budou dodržena všechna nezbytná pravidla pro zákonné zpracování?

Pro určité zjednodušení platí, že v oblasti poskytování služeb elektronických komunikací, resp. údajů spojených a vzniklých v souvislosti s jejich zákonným poskytováním oprávněným orgánům se pohybujeme zhruba v následujících oblastech:

1. Oblast provozních a lokalizačních údajů, již upravuje zejména zákon o elektronických komunikacích v podobě tzv. data retention a trestní řád nebo zákon o policii;
2. Oblast obsahu komunikace neboli tzv. odposlechy, jež je taktéž se svými podmínkami upravena prostřednictvím zákona o elektronických komunikacích, ale i trestním řádem;
3. Oblast poskytování údajů o účastnících služeb elektronických komunikací, tj. zejména v ohledu, komu patří jaké telefonní číslo a identifikační údaje takové osoby, kdy samotná úprava je opět vtělena do zákona o elektronických komunikacích a další související legislativy, upravující uplatňování tohoto práva pro jednotlivé oprávněné orgány.

Souhrnný přehled možností přístupu oprávněných orgánů k údajům elektronických komunikací, včetně uvedení povinností povinných subjektů, rozsahu údajů a kontrolních mechanismů je [ZDE](#).

Uvedený přehled by tak mohl sloužit jako případné vodítko pro vzájemnou spolupráci poskytovatelů služeb elektronických komunikací s příslušnými oprávněnými orgány.

Na závěr uvádíme příklad z poslední doby, v kontextu ukázky možného přístupu ze strany oprávněných orgánů ke specifickým kategoriím údajů o komunikačním provozu, a to novelu zákona o elektronických komunikacích promítnutou do § 98a (v oblasti bezpečnosti a integrity veřejných komunikačních sítí a služeb elektronických komunikací) a novelu zákona o Vojenském zpravodajství^[11] provedenou zákonem č. [150/2021](#) Sb. Tato novela zavádí pro Vojenské zpravodajství speciální oprávnění pro zřízení rozhraní pro připojení nástroje detekce umožňujícího provádět cílenou detekci jevů nasvědčujících existenci kybernetického útoku nebo hrozby a jejich identifikaci podle zákona o Vojenském zpravodajství. V této souvislosti je nutné uvést, že toto právo vzniká Vojenskému zpravodajství až poté, co nedosáhne dohody o spolupráci s jednotlivými právníky nebo fyzickými osobami zajišťujícími veřejnou komunikační síť nebo poskytujícími veřejně dostupnou službu elektronických komunikací nebo zajišťování detekce na základě dohody o spolupráci není účinné. Tímto legislativním nastavením by tak měla být zajištěna určitá nižší míra extenzity ze strany Vojenského zpravodajství v získávání těchto údajů pro účely kybernetické obrany. Zejména takovým způsobem, aby se co nejvíce minimalizoval negativní dopad na samotné poskytování služeb elektronických komunikací ze strany právnických či fyzických osob.

Mgr. Vojtěch Rusz

Mgr. Vanda Kellerová

Spolek pro ochranu osobních údajů

118 00 Praha 1

Tel: +420 730 677 644

e-mail: spolek@ochranaudaju.cz

[1] [CURIA - Dokumenty \(europa.eu\)](#)

[2] [Listina základních práv Evropské unie \(europa.eu\)](#)

[3] [CURIA - Dokumenty \(europa.eu\)](#)

[4] [CURIA - Dokumenty \(europa.eu\)](#)

[5] [NALUS - databáze rozhodnutí Ústavního soudu \(usoud.cz\)](#)

[6] [NALUS - databáze rozhodnutí Ústavního soudu \(usoud.cz\)](#)

[7] Zákon č. [127/2005](#) Sb.

[8] Zákon č. [141/1961](#) Sb.

[9] Zákon č. [273/2008](#) Sb.

[10] [Pl_US_45_17_vcetne_disentu.pdf \(usoud.cz\)](#)

[11] Zákon č. [289/2005](#) Sb.

© EPRAVO.CZ - Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- [Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026](#)
- [Jak zahájit provoz mezinárodní letecké linky do České republiky \(EU\): právní požadavky pro aerolinky ze třetích zemí](#)
- [Mimořádné vydržení a vývoj judikatury Nejvyššího soudu](#)
- [Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu](#)
- [Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?](#)
- [Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše](#)

- [Zneužití práva na přístup podle GDPR](#)
- [Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona](#)
- [Právní povaha sítě elektronických komunikací - režim náhrady škody](#)
- [Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory](#)
- [Jak fungují plánovací smlouvy v reálných situacích \(2. díl\)](#)