

25. 7. 2018

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

## Dopady ePrivacy na Internet of Things

„Lepší regulace komunikačních služeb typu WhatsApp, Skype či Viber a větší bezpečí pro soukromí jejich 3,3 miliardy aktivních uživatelů“[1] - tak by mohl ve zkratce vypadat podtitul nového návrhu nařízení o soukromí a elektronických komunikacích ePrivacy[2].



**Návrh nařízení totiž míří v první řadě na tzv. „over-the-top“ (OTT) služby, které distribuují audio a video obsah prostřednictvím internetu bez možnosti poskytovatele internetového připojení kontrolovat přenášený obsah. Předchůdce nařízení ePrivacy - Směrnice o soukromí a elektronických komunikacích (č. 2002/58/ES, resp. její novelizace č. 2009/136/ES, známé i pod populárním označením „cookie směrnice“) totiž na tyto služby nepamatovalo, což s ohledem na jejich rapidní nárůst popularity nemohla Evropská komise ponechat bez povšimnutí.**

Vedle OTT služeb si nové nařízení klade za cíl nastavit zároveň i regulační rámec pro využívání tzv. cookies, resp. „informací uchovávaných v koncových zařízeních koncových uživatelů“. Evropská komise tak činí ve snaze dosáhnout cíle formulovaného ve Strategii pro jednotný digitální trh: vedle mediálně známého obecného nařízení na ochranu osobních údajů[3] (GDPR) má být ePrivacy klíčem pro zvýšení důvěry uživatelů v internetové služby. Sám návrh ePrivacy pak explicitně uvádí, že se jedná o úpravu lex specialis vůči GDPR: na všechny záležitosti týkající se zpracování osobních údajů, které nejsou konkrétně upraveny v tomto návrhu, se tedy bude vztahovat GDPR.

Klíčovým ustanovením návrhu je čl. 5, dle kterého musí každý, kromě koncového uživatele, dodržovat generální zákaz jakéhokoliv zásahu do elektronické komunikace včetně zpracování dat. Výjimky, kdy je zpracování těchto dat povoleno, jsou uvedeny v čl. 6. Stejně jako v případě GDPR, i zde je třeba najít pro zpracování dat odpovídající právní základ, přičemž oproti GDPR jsou zde poskytovatelé a správci komunikačních sítí zbaveni možnosti využít titulu oprávněného zájmu či především plnění smlouvy: dle e-Privacy mohou využívat pouze souhlas koncového uživatele nebo nezbytnosti pro poskytnutí služby/splnění zákonných požadavků na kvalitu služby. V tomto případě je třeba uvést, že návrh nařízení pracuje s rozdělením na metadata a obsah, přičemž souhrnně tyto kategorie nazývá data: pokud je naplněn právní základ (a tím výjimka pro zpracování dat), je možno zpracovávat obsah a/nebo metadata. V opačném případě je třeba hledat odpovídající právní základ pro zpracování pouze dané kategorie: zpracování obsahu elektronické komunikace, kterým je z definice například „hlas, video, obrazy a zvuk“, **je přitom vždy vázané na souhlas koncového uživatele**. Pokud tedy správce nesplní výjimku nezbytnosti zpracování pro přenos komunikace, případně pro zachování/obnovení bezpečnosti služeb, musí pro zpracování obsahu vždy získat

souhlas koncového uživatele.

Jak už to ovšem bývá, při snaze regulovat rozvíjející se technologie, i v tomto případě má současný návrh nevyhnutelně dopady mimo zamýšlený segment komunikačních služeb. Jedním z těchto odvětví, pro které návrh ePrivacy přináší podstatně více dotazů, nežli odpovědí, je Internet of Things (Internet věcí, IoT). Jeho běžným příkladem, který se stává každodenní součástí našich životů, je vzájemná komunikace čidel na měření dopravy nebo inteligentních zařízení v rámci domácí sítě (TV, ledničky nebo chytrých domácích pomocníků typu Amazon Echo). Internet věcí si lze představit jako „Twitter pro stroje“: zařízení se přihlašují a odhlašují k odebírání dat a vzájemnou komunikaci skrze nespécifikované komunikační sítě a nepotřebují vědět, jakým způsobem jsou připojeny další zařízení. Internet věcí je zároveň klíčovým prvkem pro iniciativu Průmyslu 4.0, tzn. pro fungování kyberfyzikálních systémů a spolupráci samostatných řídicích jednotek schopných se autonomně rozhodovat. Na podobném principu je založen též koncept Smart Cities, spočívající v komunikaci zařízení a čidel v rámci městské komunikační či dopravní infrastruktury.

Uplatňování ePrivacy na IoT vyplývá z klíčového recitálu č. 12 návrhu e-Privacy ve spojení se základní premisou důvěrnosti dat elektronických komunikací. V tomto bodě návrh explicitně vyjasňuje, že nařízení by se mělo vztahovat na komunikaci mezi stroji, když tato komunikace zahrnuje přenos signálů po síti. Působnost na IoT návrh odůvodňuje nutností zajistit plnou ochranu práv na soukromí a důvěrný charakter sdělení a současně podporou důvěryhodného a bezpečného Internetu věcí v rámci dalšího rozvoje Jednotného digitálního trhu. Problematické je, že nařízení ePrivacy ovšem tento recitál a především autonomní komunikaci mezi zařízeními nereflektuje v žádném ze samotných článků nařízení! Tuto skutečnost přímo uvádí ve svém stanovisku[4] k návrhu ePrivacy skupina WP29, resp. Evropský sbor pro ochranu osobních údajů. Skupina dále uvádí, že konečné znění nařízení by sice mělo dopadat na většinu komunikací, které obsahují informace chráněné právem na soukromí, ovšem současně by úzká kategorie komunikací, která nemá žádný dopad na soukromí nebo na důvěrný charakter sdělení, měla být vyjmuta z působnosti. Existuje tedy možnost, že současný návrh bude doplněn o další výjimky, které by se mohly uplatnit zejména v průmyslovém sektoru.

Problematické je už samotné zařazení využívaných informací (dat) do konkrétních kategorií. Obvyklá povaha přenášených informací mezi zařízeními bude mít dle definic v základní podobě obvykle formu metadat, přenášených specifickým komunikačním protokolem. Přitom však prostřednictvím této komunikace bude přenášen právě zásadní obsah, dle kterého je třeba konkrétně jednat (např. odeslání informace řídicí jednotce, že čidlo zatížení u lavičky v parku registruje obsazení fyzickou osobou, což má vyvolat reakci kamerového systému ostrahy parku). Z takového důvodu se jeví jako nezbytné přistupovat ke každému zpracování individuálně a vedle zajištění ochrany před kybernetickými riziky posuzovat povahu elektronické komunikace.

Sledovat další legislativní postup nařízení ePrivacy se tak jeví jako velice zajímavé a je otázkou, jak bude k soukromí fyzické osoby v rámci IoT dále přistupováno. Najít rozumný kompromis pro právní rámec, který zajistí neexistenci „Velkého bratra“ a současně nezbrzdí malé start-upy i velké průmyslové hráče v možnostech inovace neúměrnými legislativními povinnostmi, bude dalším oříškem pro zákonodárce. Konečně využívání veškerých výtěžků moderních technologií, aniž by uživatel musel neustále udělovat souhlasy a současně měl jistotu, že veškerým zasílaným informacím včetně jeho polohy nebo zdravotního stavu je zajištěno dostatečné soukromí, za jeho rozlousknutí určitě stojí. Vzhledem k dynamice vývoje textu návrhu nařízení ePrivacy nelze předpokládat, že by nařízení bylo ve finálním znění v nejbližších týdnech, ale nelze pochybovat o nezbytnosti nahradit původní zastaralou směrnici o soukromí a elektronických komunikacích novou právní úpravou, která bude reflektovat tak dynamický vývoj v oblasti informačních a komunikačních technologií.

**JUDr. Josef Donát, LL.M.,**  
partner

**Tomáš Kasalický**

[ROWAN LEGAL, advokátní kancelář s.r.o.](#)

GEMINI Center  
Na Pankráci 1683/127,  
140 00 Praha 4

Tel.: +420 224 216 212  
Fax: +420 224 215 823  
e-mail: [paha@rowanlegal.com](mailto:paha@rowanlegal.com)



[1] Most popular mobile messaging apps worldwide as of April 2018, based on number of monthly active users (in millions). The Statistic Portal [online]. [cit. 2018-06-25]. K dispozici >>> [zde](#).

[2] Návrh Nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích), („e-Privacy“). K dispozici >>> [zde](#).

[3] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). K dispozici >>> [zde](#).

[4] Stanovisko č. 1/2017 k návrhu nařízení o soukromí a elektronických komunikacích (2002/58/ES). Pracovní skupina pro ochranu osobních údajů podle článku 29 [online]. [cit. 2018-06-25]. K dispozici >>> [zde](#).

© EPRAVO.CZ - Sběrka zákonů, judikatura, právo | [www.epravo.cz](http://www.epravo.cz)

## Další články:

- [Posouzení shody dle AI Act - zkušenosti z praxe](#)
- [Začínají soudy zohledňovat náklady podnikatelů při plnění právních povinností v oblasti e-commerce?](#)
- [Byznys a paragrafy, díl 35: Ručení za dluhy z podnikání u OSVČ a s.r.o.](#)
- [Bezpilotní systémy vlastní konstrukce v kategorii Specific: regulatorní požadavky a praktické aspekty](#)
- [Nefungující rozsah péče o dítě. Cesta přes využití terapie a dalších opatření podle ustanovení § 503 zákona o zvláštních řízeních soudních](#)
- [De iure traktor, de facto nákladní vozidlo, už ne tolik výhodná dualita](#)
- [Digitální důkazy z webu v soudním řízení: jak doložit, co bylo online zveřejněno?](#)
- [Pokuta 32 mil. EUR pro Dacia/Renault - evropské soutěžní úřady tvrdě došlapují na no-](#)

[poaching. Měla by Vaše společnost být na pozoru?](#)

- [Rozdělení společného jmění manželů v případech výdělečné činnosti pouze jednoho z manželů](#)
- [Oběť znásilnění má nárok na peněžitou satisfakci](#)
- [Digitalizace AML povinností: jak technologie mění plnění povinností pro tisíce povinných osob](#)