14. 1. 2016

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

Právo ve světě internetu věcí: co nás čeká ve věku 4.0

Rozvoj internetu věcí se dotkne všech sektorů průmyslu a služeb, které budou postupně konvergovat do digitálního světa. V souvislosti s tímto technologickým trendem budou vyvstávat mimo jiné i právní otázky ochrany soukromí, odpovědnosti a regulace elektronických komunikací.

PIERSTONE

Co je internet věcí?

Internet věcí (*internet of things* nebo *machine-to-machine*) je často spojován s přelomovým technologickým řešením, které změní svět, jak jej dnes známe. Ve skutečnosti má však internet věcí mnoho podob, z nichž některé jsou v praxi používané již několik desetiletí (např. čárové, RFID nebo QR kódy), zatímco jiné teprve postupně pronikají do každodenního života (autopilot v automobilech, chytrá domácnost, náramky upozorňující pacienty na to, kdy si mají vzít léky).

Zjednodušeně řečeno označuje internet věcí propojení neomezeného množství nejrůznějších objektů – věcí – prostřednictvím sítě (typicky internetu). Jedná se tedy o síť neomezeného počtu věcí sestávajících z čidel, sensorů, přenosových a jiných zařízení, které sbírají údaje, komunikují mezi sebou, vyhodnocují shromážděné údaje a na základě jejich vyhodnocení mohou samostatně jednat bez aktivního zásahu člověka. Věci, které jsou součástí internetu věcí, tak projevují v důsledku sběru a vyhodnocení shromážděných údajů samostatnost, jakousi „inteligenci," jelikož v některých případech již nebudou ke svému fungování a interakci potřebovat průběžné zásahy a instrukce od lidí, ale budou se „chovat" na základě dat, která si samy shromáždily nebo jim byly zaslány jinými věcmi v rámci společné sítě.

Ne všechny produkty a služby, které lze považovat za součást internetu věcí, mají schopnost analyzovat shromážděné údaje nebo na jejich základě samostatně jednat; některé věci spočívají v pouhém pasivním sběru informací, které následně posílají k analýze a vyhodnocení.

Jak je z uvedeného letmého výčtu patrné, internet věcí zahrnuje mnoho různých technologických možností s nejrůznějšími funkcemi, účely i riziky. Dle některých odhadů bude v roce 2020 v rámci internetu věcí propojených až 50 miliard[1] zařízení a ekonomický přínos internetu věcí dosáhne v roce 2025 až 6.2 bilionu USD.[2]

Tak jako prošlo právo vývojem v souvislosti s rozvojem „klasického" internetu a byly přijaty nové koncepty jako je omezená odpovědnost poskytovatelů služeb informační společnosti (ISPs) za obsah či došlo ke změně náhledu na některé klasické právní instituty, lze očekávat, že i internet věcí bude mít vliv na právní prostředí.

Tento článek se zabývá některými právními otázkami, které se dle našeho názoru budou v souvislosti s rozmachem internetu věcí nabývat na významu.

Otázka soukromí a ochrany osobních údajů

Je možné, že v nedaleké budoucnosti budeme žít v chytrých domácnostech, které zjistí, zda jsme či nejsme doma, zapamatují si naši obvyklou trasu od otevření dveří až do postele, budou znát naši obvyklou dobu vstávání, a na základě těchto informací dokáží automaticky optimalizovat chod domácnosti a dalších předmětů v našem vlastnictví - půl hodiny před typickým časem vstávání zapnou vše, co ráno potřebujeme, od boileru až po kávovar, připraví (vyhřáté nebo klimatizované) auto před dům, při vzdálení se od domova vypnou omylem nevypnutou žehličku apod. Zároveň nám energetické společnosti budou dodávat energii na základě údajů z tzv. smart meteringu, které umožní efektivnější distribuci a spotřebu energie, a místo ručičkových hodinek budeme nosit chytré hodinky, které budou měřit počet kroků, který denně ujdeme, jak dlouho a jak hluboce spíme, zda jsme vzali předepsané léky a další důležité údaje o našem zdraví. Výše uvedené technologie jistě přinesou do našich životů mnoho pohodlí, efektivity a úspor, avšak za cenu sdílení řady údajů o našem životě s velkým množstvím poskytovatelů různých služeb a produktů.

Čím více propojených zařízení bude, tím více osobních údajů budou tato zařízení shromažďovat. Tyto údaje bude následně možné analyzovat, sdílet či jinak spravovat nepředvídatelným a nekontrolovatelným počtem osob, společností a organizací jako jsou výrobci chytrých zařízení, poskytovatelé a správci aplikací (softwarových řešení), poskytovatelé doprovodných služeb či produktů (např. energetická společnost), poskytovatelé připojení a další články finálního řešení internetu věcí. Dnešní právní rámec ochrany osobních údajů není na podobné hromadné zacházení s osobními údaji připravený, a rozhodně není rámcem ideálním.

V prostředí, ve kterém budou naše osobní údaje shromažďovány víceméně neustále a na všech místech, je prakticky nemožné zachovat některé současné principy, na kterých stojí ochrana osobních údajů. V současné době je např. zpravidla nutné od subjektu údajů získat informovaný souhlas se zpracováním jeho osobních údajů nebo jej o zpracování ve většině případů alespoň informovat. Implementace povinného souhlasu nebo povinnosti jasně a určitě informovat v prostředí neustálého a všudypřítomného shromažďování osobních údajů je ovšem velmi složitě aplikovatelná, a i v takovém případě prakticky nekontrolovatelná a nevymahatelná. Jakýkoliv pohyb v rámci tzv. smart cities či smart buildings bude automaticky spouštět některá zařízení internetu věci, která budou moci sledovat pohyb osob a sbírat osobní údaje. Je jen otázkou času a obchodního rozhodnutí, kdy tato zařízení bez obtíží identifikují libovolnou osobu podle jejího profilu na sociálních sítích nebo jiného veřejného zdroje.

Je tedy na místě uvažovat o nových zásadách ochrany osobních údajů, které nebudou spoléhat na současný model stojící převážně na udělení předchozího souhlasu subjektem údajů, a které zároveň zajistí každému uživateli internetu věcí rozumnou míru kontroly nad svou soukromou sférou.

Mezi rizika, která jsou s internetem věcí a obecně s využíváním tzv. big data spojena, patří nedostatek informací a transparence o způsobu zpracování ze strany správců a zpracovatelů osobních údajů, což může vést nejen k narušení soukromí jednotlivců, ale také k nesprávným závěrům o jejich chování či preferencích. Potenciální chyby v algoritmech a způsobem zpracování, analýze či vyhodnocení údajů nemusí být v případě nedostatečné informovanosti subjektů údajů nikdy odhaleny a mohou vést k dlouhodobě nepřesným či nesprávným výsledkům. Evropský inspektor ochrany údajů nedávno ve své zprávě[3] upozornil, že takové chyby mohou mít zásadní diskriminační dopady na jednotlivce. Ve světě datové analytiky již jednotlivci nemusí být posuzováni podle svého skutečného jednání, ale podle toho, jaké jednání u nich bude na základě datové analýzy předpokládáno. Datová analýza tak může předpokládat pravděpodobnost kariérního úspěchu, pravděpodobnost závažné nemoci či předčasné smrti nebo pravděpodobnost nesplácení úvěru. Výsledkům datové analýzy a rozhodnutím činěným na jejím základě nemusí mít jednotlivec žádnou

možnost se bránit. Za účelem eliminace některých rizik, kterou jsou spojena s rozšířením tzv. big data, navrhl Evropský inspektor ochrany údajů zavést pravidla, která zajistí, aby organizace byly transparentnější ohledně způsobu, kterým zpracovávají osobní údaje, aby byla subjektům údajů poskytnuta větší kontrola nad vlastními osobními údaji (např. ve formě opt-out mechanismů), aby bylo zpracování údajů po technické či organizační stránce více zaměřené na ochranu osobních údajů (tzv. *privacy by design*) a aby byly organizace činěny odpovědné za porušování ochrany osobních údajů.

Dalším z nových principů, o kterém se v souvislosti se zaváděním RFID čidel a internetu věcí diskutuje, je tzv. právo na mlčení nebo odpojení čidel (neboli *right to silence the chips*). Jedná se o obdobu práva být zapomenut (*right to be forgotten*), na základě kterého má každý právo na vynětí (tzv. opt-out) z režimu shromažďování informací o jeho osobě. Objevují se i názory, že toto právo by mělo být považováno za jedno ze zásadních lidských práv, zaručovaných mezinárodními dohodami a ústavou. Mezi další návrhy, jak se všudypřítomnému zpracování osobních údajů vyhnout nebo zmírnit jeho dopad, je zvýšení sankcí za porušení právních předpisů po vzoru soutěžního práva, tj. zavedení vysokých pokut odvíjejících se od velikosti obratu provinivší se společnosti.

Další geopoliticky významnou otázkou je problematika předávání osobních údajů do zahraničí. V souvislosti s nedávným rozhodnutím SDEU o zrušení tzv. režimu Safe Harbor pro předávání údajů mezi Evropskou unií a Spojenými státy je tato otázka nanejvýš aktuální.

Otázka odpovědnosti za aktivní jednání propojeného zařízení

V souvislosti s propojením zařízení v rámci internetu věcí nebudou tato zařízení pouze pasivně sbírat údaje, ale budou je umět také poslat dál a tím pomáhat v rozhodovacím procesu, některá budou dokonce umět shromážděné údaje zanalyzovat a na jejich základě také samostatně rozhodovat a aktivně jednat. V současné době se tato zvýšená samostatnost projevuje například v rámci popularity samo-řídících prvků automobilů, stavebních nebo zemědělských strojů a jiných „autopilotů“, kdy zařízení (např. traktor) dokáže automaticky vyhodnocovat a reagovat na vnější prostředí (zatáčet, brzdit, měnit polohu) na základě analýzy sesbíraných údajů.

Za situace, kdy věc, která není dle právního řádu subjektem, nýbrž předmětem, bude sama aktivně „jednat“, vznikne otázka odpovědnosti za takové jednání. Právní odpovědnost za jednání nese dle současného právního řádu vždy osoba (právnická nebo fyzická), a ačkoliv bude míra samostatnosti chytrých zařízení čím dál tím větší, nelze dle našeho názoru opustit premisu, že věc není subjektem právního vztahu a nemůže nést odpovědnost. Nebude však vždy jednoduché určit, která osoba odpovědnost ponese. Bude jí řidič, výrobce automobilu, výrobce jednotlivého chytrého zařízení, poskytovatel konektivity, či ještě někdo jiný? Bude třeba zvážit, zda současná úprava odpovědnosti vlastníka věci v kombinaci s úpravou zvláštních případů odpovědnosti bude dostatečná k zajištění právní jistoty ve světě s potenciálně miliardami propojených a autonomně jednajících zařízení.

Právní otázky související s poskytováním služeb elektronických komunikací

Nezbytným předpokladem internetu věcí je propojenost jednotlivých zařízení. Některá zařízení mohou být propojena pouze v rámci soukromé sítě, avšak lze předpokládat, že většina zařízení bude propojena prostřednictvím sítě, která je předmětem regulace elektronických komunikací, jako jsou sítě typu GSM, CDMA, WiFi či zařízení krátkého dosahu typu Bluetooth.[4] Čím větší bude mít síť dosah, tím větší počet dat bude moci být sdílen a tím větší přínos internet věcí přinese. V rámci práva elektronických komunikací vyvstávají pro poskytovatele služeb internetu sítí některé povinnosti týkající se např. oznamovací povinnosti o zahájení poskytování služeb elektronických komunikací Českému telekomunikačnímu úřadu, povinnosti vztahující se na bezpečnosti a zajištění

sítí, roamingu či možnosti zákazníka přejít ke konkurenci.

V souvislosti s rozvojem internetu věcí, kdy by do veřejné sítě mohly být během několika málo let zapojeny desítky miliard zařízení, je potřeba zmínit také zajištění dostatečného počtu volných čísel či IP adres, případně jiných identifikátorů, aby bylo možné každé zařízení bezpečně identifikovat.

Závěr

Internet věcí nebude jen doménou technologického světa, jak jej dnes chápeme. Vize Evropské komise je, že tradiční průmysl a služby budou postupně konvergovat do digitální sféry. Na rozdíl od Spojených států, kde se digitální svět rozšiřuje do fyzického světa, jak to vidíme např. v automobilovém průmyslu, předpokládá Evropská komise v Evropě opačný vývoj, tedy rozšiřování fyzického světa do světa digitálního. Lze tedy očekávat, že za pár let nebudou existovat klienti, kteří by nebyli v nějaké míře digitálnímu světu a světu internetu věcí vystaveni.

Ačkoliv rozhodně nelze říci, že by stávající právní principy a současná regulace nedopadala na internet věcí, nedisponují dle našeho názoru efektivními nástroji. Tradičním principům ochrany osobních údajů hrozí, že se v blízké budoucnosti stanou obsoletní, jelikož praxe a technologický vývoj již jednoduše nebudou s některými principy kompatibilní. Domníváme se proto, že je potřeba se zamyslet nad novými mechanismy, které umožní regulaci ochrany osobních údajů, jež nebude brzdit technologický vývoj, ale zároveň poskytne dostatečnou ochranu soukromí jednotlivců. Nalezení takových řešení bude vyžadovat úzkou spolupráci nejen právních expertů a regulátorů, ale také inženýrů, vědců, zástupců organizací zpracovávajících osobní údaje a dalších zainteresovaných stran. Pouze interdisciplinární diskurs zahrnující i etické aspekty zaručí, že výsledné řešení bude funkční a spravedlivé.

Mgr. Jana Pattynová, LL.M.

Štefan Kráľ

PIERSTONE s.r.o., advokátní kancelář

Na Příkopě 9
110 00 Praha 1

Tel.: +420 224 234 958

---
[1] Dostupné na www, k dispozici >>> zde.
[2] Dostupné na www, k dispozici >>> zde.

[3] Opinion 7/2015 Meeting the challenges of big data ze dne 19. 11. 2015.
[4] Existují ovšem i jiné typy řešení, které jsou v rámci internetu věcí využívána. Příkladem mohou být sítě s širokým pokrytím, ale s nízkou spotřebou pro koncové zařízení (tzv. LPWAN, low power wide area network).

Další články:

- DEAL MONITOR
- Tři dekády v advokacii a otevřený pohled na to, co profesi i justici nejvíc škodí
- DEAL MONITOR
- Vybrané otázky poskytování zdravotních služeb na dálku
- DEAL MONITOR
- „Za každou kauzou je živý příběh“
- Ombudsman na Maltě – základní parametry a role. A v čem bychom se mohli poučit i my v Česku?
- DEAL MONITOR
- DEAL MONITOR
- Rozhovor s JUDr. Veronikou Janoušek Rudolfovou, samostatnou advokátkou specializující se na sportovní právo
- DEAL MONITOR