

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

IP adresa osobním údajem?

Povaha IP adresy jako osobního údaje není dosud zcela jednoznačná. Na evropské úrovni se této otázce před již poměrně dlouhou dobou věnoval SDEU v rozsudku *Scarlet Extended*,[1] kde v podstatě učinil závěr, že IP adresy internetových uživatelů jsou chráněnými osobními údaji, neboť umožňují přesně určit totožnost těchto uživatelů. Tento závěr Soudního dvora se však týkal případu, v němž shromažďování a identifikování IP adres internetových uživatelů bylo prováděno poskytovatelem internetového připojení.

Podobně po Internetu koluje (ještě starší) stanovisko ÚOOÚ č. j. CJ08469/05UOOÚ,[2] které shrnuje, že samostatně být IP adresa považována za osobní údaj nemůže. V tomto světle se jeví jako přelomové nedávné rozhodnutí Soudního dvora, dle kterého se IP adresa za určitých okolností osobním údajem stává i pro jiné subjekty, než poskytovatele internetového připojení.

Dne 19. října 2016 vydal Soudní dvůr Evropské unie rozsudek ve věci *Patrick Breyer vs Německo* pod sp. zn. C-582/14,[3] jehož předmětem bylo rozhodnutí o předběžné otázce podané německým Spolkovým soudním dvorem (Bundesgerichtshof).

První předběžná otázka se týkala výkladu čl. 2 písm. a) směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů[4] (kterému odpovídá ustanovení § 4 odst. a) českého zákona o ochraně osobních údajů[5]), tj. definice pojmu osobních údajů. V rámci původního sporu se Patrick Breyer domáhal správním žalobou zákazu uchovávání záznamů jeho IP adresy provozovateli webových stránek německých spolkových orgánů (poskytovateli on-line mediálních služeb), k čemuž docházelo při jeho návštěvách těchto stránek. S cílem zabránit útokům a umožnit trestněprávní stíhání „útočníků“ jsou v případě většiny webových stránek všechny přístupy ukládány do logovacích datových souborů. V těchto souborech se po navštívení stránek zpravidla ukládá název otevíraného souboru nebo internetové stránky, pojmy zadané do vyhledávacího pole, okamžik požadavku, množství přenesených dat, hlášení o úspěšnosti požadavku a IP adresa zařízení, ze kterého je k nim uskutečňován přístup.

V tomto ohledu je důležité zmínit, že se v případě P. Breyera jednalo o tzv. dynamickou IP adresu, tedy takovou, která je poskytovatelem internetového připojení přidělována z rozsahu určité množiny IP adres kterými disponuje, každému účastníkovi (resp. koncovému zařízení) dočasně pokaždé, když se připojí k síti Internet na dobu onoho připojení. Za použití veřejně dostupných nástrojů[6] tedy není možné zjistit identitu účastníka s takovou IP adresou, přičemž touto informací disponuje pouze poskytovatel internetového připojení. V současnosti drtivá většina nekorporátních zákazníků poskytovatelů internetového připojení disponuje právě dynamickou IP adresou.

Podstatou první předběžné otázky bylo to, zda-li definice osobních údajů obsažená v čl. 2 písm. a) směrnice[7] musí být vykládána v tom smyslu, že dynamická IP adresa, kterou poskytovatel online mediálních služeb uchovává v souvislosti s přístupem osoby na internetovou stránku, kterou tento poskytovatel zpřístupnil veřejnosti, pro uvedeného poskytovatele představuje osobní údaj ve smyslu tohoto ustanovení, pokud má k dispozici další informace potřebné k identifikaci této osoby jediné třetí subjekt, v projednávaném případě poskytovatel internetového připojení.

SDEU se tedy zabýval tím, zda-li údaj o přístupu z dynamické IP adresy ve spojení s datem a hodinou

připojení dává provozovateli webových stránek možnost nepřímo identifikovat fyzickou osobu (subjekt údajů), která danou stránku navštívila, při vědomí toho, že účastník kterému aktuální IP adresa náleží nemusí být s touto osobou totožný, čímž by byla definice osobního údaje naplněna. V návaznosti na to soud dovodil, že dynamická IP adresa, kterou poskytovatel online mediálních služeb uchovává v souvislosti s přístupem osoby na internetovou stránku zpřístupněnou veřejnosti, pro uvedeného poskytovatele představuje osobní údaj ve smyslu ustanovení čl. 2 písm. a) směrnice, pokud má tento poskytovatel k dispozici právní prostředky, které mu umožňují nechat identifikovat subjekt údajů díky dalším informacím, kterými disponuje poskytovatel internetového připojení tohoto subjektu.

Dále je tedy nutné položit si otázku, zda-li český právní řád poskytuje provozovatelům webových stránek právní prostředky ke zjištění totožnosti osob, které je navštívili. V první řadě je nutno uvést, že povinnost poskytovatelů internetových služeb uchovávat informace vedoucí ke ztotožnění účastníka s dynamickou IP adresou v konkrétní okamžik byla na evropské úrovni uložena tzv. data retention směrnicí,[8] jelikož se jedná o provozní a lokalizační údaj ve smyslu jejího čl. 5 odst. 2 bodu iii). Ačkoliv byla směrnice následně rozhodnutím SDEU zrušena,[9] dočkala se předtím v tomto ohledu transpozice do českého zákona o elektronických komunikacích,[10] především do jeho § 97 odst. 3, který ukládá poskytovatelům internetového připojení uchovávat provozní a lokalizační údaje po dobu šesti měsíců. Současně zákon ve stejném ustanovení ukládá provozovatelům povinnost poskytnout provozní a lokalizační údaje na vyžádání pěti subjektům: orgánům činným v trestním řízení (tj. všem subjektům, které mohou být za takový orgán považovány), Policii ČR při (vyjmenovaných) činnostech podle zákona o Policii ČR, Bezpečnostní informační službě, Vojenskému zpravodajství a České národní bance.

Trestní řád[11] ve svém ustanovení § 88a umožňuje prostřednictvím soudu nařídít poskytovateli internetového připojení vydání údajů o telekomunikačním provozu, tedy i identifikaci účastníka dynamické IP adresy jakožto provozního údaje, policejnímu orgánu v případech taxativně vymezených trestných činů. Jedním z těchto trestných činů je trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 trestního zákoníku[12]), který dopadá mimo jiného právě na případy kyberútoků proti webovým stránkám (resp. serverům, na nichž jsou umístěny).[13] Důležité je si uvědomit, že ačkoliv účastník nemusí být (a často ani nebude) totožný s osobou, která webovou stránku navštívila, účelem tohoto nástroje je mimo jiné danou osobu identifikovat, což může provozovatel následně využít například pro uplatňování nároků na náhradu škody vůči ní, přičemž to ostatně představuje jeden z důvodů, proč podobné záznamy provozovatel vůbec vytváří a uchovává (ve shromažďování IP adres za tímto účelem mimochodem nemůže být provozovatel národní úpravou omezen, což byl závěr druhé předběžné otázky judikátu).

Lze tedy uzavřít, že český právní řád dává provozovatelům webových stránek právní prostředky k nepřímé identifikaci osob, které je navštívili, a IP adresy které takto uchovávají jsou tudíž osobními údaji. V tomto ohledu je podle mého názoru bezpředmětné, že judikát hovoří výslovně pouze o dynamických IP adresách, jelikož uvedené závěry lze beze zbytku aplikovat i na adresy statické, nehledě na to, že provozovatel webových stránek v rámci automatického logování samotného nemá možnost od sebe tyto dvě kategorie odlišit.

Provozovatelé webových stránek se následkem rozhodnutí SDEU zřejmě dostávají do pozice správců osobních údajů v režimu § 5 odst. 2 písm. e)[14] zákona o ochraně osobních údajů, jelikož tímto postupem systematicky provádějí automatizované zpracování osobních údajů bez souhlasu subjektu údajů, se všemi důsledky z toho plynoucími. Na okraj je možné uvést, že účinnost Obecného nařízení o ochraně osobních údajů[15] nejspíše nepovede k neaplikovatelnosti závěru soudu, jelikož to definici osobních údajů oproti směrnici nejenom nezužuje, ale dokonce uvádí „síťový indetifikátor“ jako jeden z demonstrativních prvků, na jehož základě lze subjekt údajů identifikovat (čl. 4 odst. 1

nařízení).



Jaroslav Kuba,

student 5. ročníku Právnické fakulty Univerzity Karlovy

e-mail: jar.kuba@gmail.com

[1] Rozsudek ze dne 24. listopadu 2011, Scarlet Extended, C-70/10, EU:C:2011:771, bod 51, dostupné na [www](#), k dispozici >>> [zde](#).

[2] Dostupné na [www](#), k dispozici >>> [zde](#).

[3] Dostupné na [www](#), k dispozici >>> [zde](#).

[4] Dostupné na [www](#), k dispozici >>> [zde](#).

[5] Zákon č. [101/2000](#) Sb., o ochraně osobních údajů a o změně některých zákonů.

[6] např. dostupné na [www](#), k dispozici >>> [zde](#).

[7] Pro účely směrnice se rozumí cit: „a) "osobními údaji" veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů); identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity;“.

[8] Směrnice Evropského parlamentu a Rady č. 2006/24/ES, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí (směrnice o uchovávání údajů); dostupné na [www](#), k dispozici >>> [zde](#).

[9] Rozsudek Soudního dvora EU ze dne 8. 4. 2014 ve spojených věcech C-293/12 a C-594/12; dostupné na [www](#), k dispozici >>> [zde](#).

[10] Zákon č. [127/2005](#) Sb., o elektronických komunikacích a o změně některých souvisejících zákonů.

[11] Zákon č. [141/1961](#) Sb., o trestním řízení soudním.

[12] Zákon č. 40/2009 Sb, trestní zákoník.

[13] Blíže viz GRIVNA, Tomáš. § 230 Neoprávněný přístup k počítačovému systému a nosiči informací. In: ŠÁMAL a kol., Trestní zákoník (EVK). 2.vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 2301 - 2315.

[14] Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat, cit.: „e) pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života“.

[15] 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); dostupné na [www](#), k dispozici >>> [zde](#).

Další články:

- [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](#)
- [DEAL MONITOR](#)