

3. 5. 2018

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

## „Velký Facebookový únik“ aneb jak si chránit soukromí na internetu

Zatímco Spojené státy americké v posledních týdnech žijí svůj sdílený sociální život na Facebooku v pobouření a ve strachu z úniku osobních údajů ve prospěch politicky profanovaných společností, většina Čechů i nadále přemýšlí, která fotografie jejich dítěte půjde nejlépe „na zed“ vedle fotografií nového auta, babičky nebo líbajícího se páru. Většina uživatelů zřejmě nejznámější sociální sítě zaznamenala v uplynulém měsíci aféru, která byla médií obecně označována právě jako „velký facebookový únik dat“, neřku-li přímo velká facebooková krádež. Ale nic není tak černobílé. Zatímco všemožné novinové články po světě se hemží nařčeními z nelegálního prodeje dat a zpravodajské portály se plní videi omlouvajících se vývojářů, jen málokdo vlastně tuší, že z větší části si za tzv. „únik dat“ mohl víceméně sám uživatel.



Téměř každý uživatel Facebooku už někdy zjišťoval v rámci nabízených externích aplikací, např. které holywoodské hvězdy se nejvíce podobá, nebo které zvíře ho nejvíce charakterizuje. Takže i když se po světě prohání spousta Bradů Pittů se srdcem lva nebo Angelin Jolie s ladností labutě, už méně lidí ví, že se za zjištění takto spolehlivých informací téměř upsali ďáblu. Obdobně to také bylo s výše zmíněným případem, ve kterém figurovala společnost Cambridge Analytica. Ta je nařčena, že skrze externí aplikaci dostupnou skrze facebookové stránky, zneužila osobní údaje až 50 milionů uživatelů. Tato data měla být následně využita, či možná zneužita, v rámci volební kampaně Donalda Trumpa, kdy s využitím tzv. neuronových map a celkového mapování sociálního profilu uživatelů, mohlo dojít k cíleně mířené politické marketingové kampani. A jak že vlastně došlo k samotnému zneužití dat? V rámci externí aplikace na Facebooku je potřeba před jejím spuštěním poskytnout vývojářům či provozovatelům aplikace souhlas s tím, k jakým datům či osobním údajům se daná aplikace skrze sociální sítě dostane. V tomto konkrétním případě pak aplikace požadovala přístup k veškerým datům uživatele a všech jeho přátel – ano, přesně, ke kompletní databázi veškerých údajů, které o svých uživatelích Facebook shromažďuje. Takže ačkoli souhlas poskytl např. pouze několik stovek tisíc uživatelů, aplikace získala přístup k datům 50 milionů uživatelů. A zde se začínají rojit ty nejčastější dotazy. Nakolik je Facebook zodpovědný za únik dat? Lze ještě hovořit o zneužití údajů, když s tím uživatel souhlasil? Je poskytnutý souhlas legitimní a byl poskytnut dostatek informací uživatelům, aby byly schopni zvážit rizika a veškeré konsekvence poskytnutí souhlasu? Je správné, že Facebook umožnil externí aplikaci přístup k tak rozsáhlému množství dat, které mohlo zahrnovat nejen dobrovolně zveřejněný obsah uživatelů na stránkách, ale také záznamy aktivity uživatelů či obsahy jejich konverzací? Facebook tuto skulinu v zabezpečení, resp. možnost údaje v takovém rozsahu získat, označil za nešťastnou událost.

Není divu, že s ohledem na výše uvedené se v srdci nejednoho angloamerického právníka zrodila

myšlenka na hromadnou žalobu a možnost získání přiměřeného zadostiučinění pro poškozené uživatele ze strany Facebooku. Jaké možnosti by měl ale český uživatel v rámci práva kontinentálního?

V prvé řadě je nutno si uvědomit, k jakému poškození práv uživatelů vůbec dochází. Pomineme-li sféru veřejnoprávní, resp. rovinu správního práva a s tím spojené kontroly vykonávané různými dozorovými úřady pro ochranu osobních údajů fyzických osob, v rámci které je možno postupovat proti společnosti Facebook alespoň formou podnětů na správní orgány, zůstává stále rovina soukromoprávní.

Mezi běžným uživatelem a společností Facebook Ireland Ltd., což je evropská pobočka společnosti, dochází k uzavření smlouvy o poskytování služeb. V rámci této smlouvy se společnost Facebook mimo jiné zavazuje k ochraně osobních údajů a veškerých shromažďovaných dat svých uživatelů v rozsahu, jak popisuje ve svých obchodních a smluvních podmínkách a zásadách ochrany osobních údajů a dat. Nad rámec této povinnosti je Facebook také povinen zachovávat soukromí veškerých osob, stejně jako ostatní přirozená osobnostní práva uživatelů. S ohledem na výše uvedené tak běžným uživatelům, kteří se cítí být poškozeni ze strany Facebooku, zůstává dvojí možnost získat náhradu škody a nemajetkové újmy způsobené:

- porušením smlouvy, resp. porušením povinnosti ochrany dat uživatelů,
- zásahem do osobnostních práv člověka, zejména porušením pramenícím ze zásahu do práva na soukromí člověka.

A podle jakých právních předpisů určit příslušné soudiště a hmotněprávní úpravu, podle které se bude případný spor posuzovat? Nezbyvá, než zabrousit do norem mezinárodního práva soukromého a pokusit se nalézt odpovědi tam.

Poněkud snadnější je to u prvé zmíněné možnosti, tedy v případě porušení povinností ze smlouvy, které mají za následek vznik škody. V takovém případě je možno použít Nařízení Evropského Parlamentu a Rady (ES) č. 593/2008, o právu rozhodném pro smluvní závazkové vztahy (dále též „Řím I“). Řím I obsahuje ve svém článku 6 specifickou úpravu pro spory z tzv. spotřebitelských smluv. V takovém případě platí, že hmotněprávní rovina vztahů se bude posuzovat dle práva, ve kterém má spotřebitel své obvyklé bydliště. Soudiště pak bude v takovém případě posuzováno dle Nařízení Evropského Parlamentu a Rady (EU) č. 1215/2012, o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech (dále též „Brusel I bis“). Ten obdobně jako u hmotněprávní stránky obsahuje úpravu příslušnosti soudů pro spotřebitelské spory. V článku 17 Nařízení Brusel I bis je uvedeno, že spotřebitel může podat žalobu u soudu místa, kde má bydliště. Povahu Facebooku jako osoby podnikající a profesionální a uživatele jakožto spotřebitele může hovořit také obdobný případ, který v současné chvíli projednávají místní soudy v Rakousku. V tomto případě rakouský aktivista Max Schrems podal žalobu právě na společnost Facebook u rakouských soudů, kdy příslušnost místních soudů byla řešena i před Evropským soudním dvorem. Tento se na podzim roku 2017 vyjádřil v tom smyslu, že pan Schrems je skutečně vůči Facebooku spotřebitelem a tedy mu přísluší možnost žalovat společnost z důvodu narušení ochrany dat u rakouských soudů. Spor tak nadále pokračuje.

Poněkud horší, resp. nejasnější situace nastává ve druhém případě, tedy v případě, kdy dochází k zásahu do osobnostních práv člověka. V takovém případě totiž Řím I nemůže být použit, když mimosmluvní závazkové vztahy, které vznikají z narušení soukromí a osobnostních práv jsou zcela vyňaty z jeho působnosti. Brusel I bis pak ve věci určení příslušnosti soudu určuje tzv. obecnou příslušnost a následně zvláštní příslušnost soudů. Obecně vždy platí, že osoby mohou být žalovány tam, kde mají bydliště, resp. sídlo. Zvláštní příslušnost soudu pak není výlučná, ale přináší další

možnost žalobce, kde případné spory řešit. V článku 7 odst. 2 Brusel I bis říká, že v případech souvisejících s delikt ní odpovědností, je příslušný soud místa, kde došlo ke škodné události. Avšak určení, kde ke škodní události došlo, je poněkud problematické v případě, kdy škoda vznikla v souvislosti s internetem. Obecně totiž nelze říci, že informace poskytnuté, získané nebo zveřejněné na internetu jsou takto zneužity pouze na území státu, kde má uživatel bydliště, ale naopak, je taková informace zveřejněna v podstatě kdekoli, kde je dostupná. Takový výklad by však mohl být v zásadním nesouladu s účelem nařízení a celkově mezinárodní úpravou, protože by umožňoval žalobci zvolit k podání žaloby téměř jakýkoli stát, jehož právní úprava by pro něj byl nejvýhodnější a naopak, žalovaný by pak nebyl schopen předvídat, k jakému soudu bude žaloba podána. V rozhodovací praxi se soudy ve větší míře dosud zabývaly víceméně pouze ochranou soukromí na internetu ve vztahu k tzv. pomluvě (angl. difamation), resp. střetem práva na soukromí osoby a právem na svobodu projevu. Toto ale není úplně vhodný případ pro právě výše zmíněné úniky a zneužití dat a předávání osobních údajů třetím osobám mimo interní síť a uložiště. Pro tyto případy by muselo být zkoumáno zejména to, kde k takové škodě došlo, kdo data předal, kdo data získal a kde jsou data zpracována. Konkrétně by pak ve výše uvedeném případě Facebooku a společnosti Cambridge Analytica pravděpodobně záleželo na tom, ve které zemi a k jaké příležitosti byla data zneužita a která pobočka společnosti data zpracovala. Vždy však bude možnost využít sudiště určené generální klauzulí, tedy bude možno žalovat v místě sídla žalovaného. Rozhodné právo pak bude určeno dle jednotlivých právních pravidel a principů daného státu, neboť jak již uvedeno výše, Řím I v těchto případech nepomůže.

Právo na ochranu soukromí v moderní době získává a do budoucna ještě i bude získávat stále větší a větší důležitost, kdy problematika celkové ochrany dat v rámci internetu, sociálních sítí a celkově sdílení informací bude i nadále zásadním tématem, ve kterém až budoucí případy přinesou jasná specifika případných sporů. Nakolik je však rozumné pouštět se do žalob, kde obrana klienta bude spočívat v tom, že byl příliš hloupý, naivní nebo neprozíravý na to, aby pochopil, komu a k jakému účelu vlastně poskytuje a předává své údaje, to ukáže teprve čas.

**Mgr. Lucie Šimková**

[Advokátní kancelář JELÍNEK & Partneři s.r.o.](#)

Pardubice - Dražkovice 181  
533 33 Pardubice - Dražkovice

Velké náměstí 1  
500 03 Hradec Králové

Truhlářská 1108/3  
110 00 Praha 1

Tel.: +420 466 310 691  
Fax: +420 466 310 691  
gsm: +420 724 794 986  
e-mail: [advokati@advokatijelinek.cz](mailto:advokati@advokatijelinek.cz)

## Další články:

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