Vliv definičních autorit na compliance developerů: souhlas, nebo život!

Anna Stárková

Některé podnikatelské subjekty disponují jedinečnými technickými kompetencemi a faktickými možnostmi, které jim bezprostředně umožňují stanovit pravidla chování ve virtuálním prostředí a rovněž ukládat citelné sankce v případech jejich porušení. Tyto podnikatelské subjekty nazýváme definičními autoritami. V technologickém odvětví se jedná především o poskytovatele digitálních služeb, jako např. internetové vyhledávače, online tržiště a cloud computing. Na pomyslné druhé stran vůči nim stojí subjekty ve slabším postavení. Ty je nutné hledat nejen na úrovni spotřebitelské, ale také mezi podnikateli.

Slabšími podnikatelskými subjekty na trhu s technologiemi jsou typicky developeři, kteří vyvíjí softwarové programy v podobě doplňků pro internetové vyhledávače či v podobě samostatných aplikací, jež jsou následně nabízeny na on-line tržištích umožňujících jejich digitální distribuci. K tomu, aby software mohl být uveden do prodeje, musí developer splnit požadavky konkrétního obchodu, které vyplývají nejen z právní regulace, ale rovněž ze sledování prosazování vlastních zájmů subjektů odlišných od státu. Na základě této dispozice bezprostředně stanovit pravidla chování a tím ovlivnit compliance developerů, nazýváme provozovatele těchto obchodů, jimiž jsou např. Google, Mozilla, Opera, Microsoft, Apple či Amazon, definičními autoritami.

Ač se na první pohled může zdát, že zájmy definičních autorit a státu jsou rozdílné, vzájemná spolupráce zvyšuje účinnost práva a jestliže zároveň přispívá ke kvalitě virtuálního prostředí, a tím i komerčního potenciálu, je pro obě strany výhodná – proto stále posiluje. V kontextu výše nadepsaného tématu je však třeba především pamatovat na existenci řady zájmů, jejichž ochranu stát prosazuje, byť z podnikatelského hlediska definičních autorit přínosné nejsou. Kvůli tomuto konfliktu zájmů poté definiční autority některé právní normy nerealizují a efektivní nástroje ochrany subjektů z nich oprávněných chybí.[1]

Co se týče konkrétního příkladu výše představeného konfliktu zájmů a nerealizace právních norem, pomineme-li institut ochrany slabší strany a další nástroje ochrany soukromého práva, které jsou ve virtuálním prostředí pro rozdílnost právních kultur těžko uchopitelné, nabízí se z oblasti veřejného práva, zejm. práva Evropské unie, skupina norem na ochranu osobních údajů. Tyto normy totiž historicky nebyly definičními autoritami realizovány, a to až do zavedení adekvátní motivace v podobě vyšších sankcí za jejich porušení. Obecným nařízením o ochraně osobních údajů. Pokuty lze nyní udělit buď do výše 20 000 000 eur nebo až do 4 % celkového ročního celosvětového obratu, jde-li o podnik ve smyslu soutěžního práva.[2]

Právě na tomto příkladu nikoli dobrovolné ale sankcemi motivované realizace práva lze pozorovat, jaké zájmy jsou definičními autoritami prosazovány a jakým způsobem. Na rozdíl od státních autorit, které mohou svoji moc uplatňovat jen na základě a v mezích zákona, mohou definiční autority vzhledem ke své soukromoprávní povaze činit vše, co není zákonem zakázáno.[3] Aby byla tato svoboda maximálně zachována, definiční normy jsou nejčastěji

[1] POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012, str. 107 – 111.

[2] Viz čl. 83 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), OJ L 119, 4.5.2016.

[3] Viz čl. 2 odst. 3 a 4 zákona č. 1/1993 Sb., Ústava České republiky, čl. 2 odst. 2 a 3 zákona č. 2/1993 Sb., Listiny základních práv a svobod.

obsaženy v zásadách developerů zveřejněných na internetových stránkách autorit. Tato forma jednak zaručuje velkou míru flexibility (zejm. možnost činit jednostranné změny na rozdíl od smluvních ujednání) a díky povaze veřejně dostupných dokumentů i informovanost adresátů, vč. využití principu „neznalost zásad neomlouvá“.

Výsledkem jsou obecně platná pravidla pro konkrétní prostředí, která specifika jednotlivých jurisdikcí překonávají přiznáním vyššího standardu ochrany subjektu údajů. Díky definičním autoritám tak za standard na trhu s technologiemi platí mimo jiné širší vymezení pojmu osobní údaj, rekategorizace „citlivých“ údajů, specifické zásady zpracování pro každý jednotlivý softwarový program nad rámec obecných informací o zpracování osobních údajů, omezení zpracování na operace zajišťující funkčnost, úzké vymezení pojmu funkčnost nebo určení právních základů pro typy účelů zpracování či kategorií údajů.

Na první pohled pozitivní důraz na ochranu jedné slabší strany může ovšem paradoxně vést ke zhoršení postavení jiné. Zaměříme-li se na compliance developerů v oblasti ochrany osobních údajů, jedná se zejména o případy, kdy definiční autority ve snaze chránit se proti vysokým sankcím definují normy rigidněji, než stanoví zákon, či zákonné normy formalističtěji interpretují, čímž nastavují meze svobodě podnikání a na developery přenášejí veškeré náklady spojené se změnou softwaru, compliance programů k doložení souladu či jeho případného prokázání státní autoritě.

Definiční autority tak na sebe přebírají některá práva a zároveň přenášejí veškeré povinnosti spojené s postavením správců osobních údajů. Tato práva a povinnosti by přitom měla výlučně náležet developerům, které definiční autority výslovně označují za samostatné správce a jako takoví se musí řídit principem založeným na riziku a odpovědnosti.

Jak bylo nastíněno výše, jednou z povinností správců osobních údajů je určení právního základu pro zpracování a doložení jeho zákonnosti. Je však právem správce, aby dle povahy zpracování za konkrétním účelem a všech okolností zvolil vhodný právní základ, jelikož k tomu má nejlepší předpoklady. Zatímco státní autority se kauzálnímu určování správných právních základů pro ten či onen typ účelu zpracování zdržují, definiční autority do suverenity developerů aktivně zasahují, když stanovují typy účelů či kategorií údajů, pro které je nutný souhlas.

Po právu tak činí zejména v případech, kdy je nezbytnost souhlasu dovozena rozhodovací praxí státních autorit pro konkrétní případ, ke kterému v rámci poskytování digitální služby dochází, či vyžaduje-li souhlas právní řád některé jurisdikce, jejíž trh je pro developera relevantní (např. Children’s Online Privacy Protection Rule). Jsou zde ovšem také případy, kdy je výklad zákona nejasný a rozhodovací praxe chybí, pro které preventivní vyžadování souhlasu jde nad rámec zákona. V extrémním případě mohou být definiční normy i v rozporu se zákonem. Jejich vynucování následně staví podnikatelské subjekty před obtížnou volbu mezi souladem se zákonem a souladem s definiční normou, jemuž bývá podnikání developerů podmíněno.

Konkrétní příklady takovýchto definičních norem není nutné hledat daleko. Společnost Mozilla provozující internetový prohlížeč Mozilla Firefox požaduje ve svých zásadách Add-on Policies – User Interactions & Technical Data po developerech doplňků (z angl. add-ons), jejichž technologie zpracovává URL adresy či vyhledávané výrazy, opatření výslovného souhlasu uživatele bez rozlišování účelu takového zpracování a zakazuje sběr jakýchkoli údajů, které

nejsou nezbytně nutné pro základní funkcionalitu.[4] Tento zákaz se vztahuje rovněž na použití analytických nástrojů třetích stran, jako např. Google Analytics, které jsou pro mnohé podnikatelské subjekty nenahraditelným zdrojem informací k porozumění chování uživatelů a zlepšování svých produktů či služeb.

Další internetový prohlížeč Opera ve svých Acceptance Criteria pro schválení doplňků výslovně vyžaduje nezpracování žádných osobních údajů bez předchozího souhlasu uživatele.[5]

Rovněž Google provozující internetový prohlížeč Chrome podmiňuje ve svých zásadách Updated Privacy Policy & Secure Handling Requirements zpracování údajů, ke kterému dochází prostřednictvím doplňků, jejich nezbytností pro zajištění funkcí nabízeným přímo uživatelům.[6] Na rozdíl od Mozilly ovšem nespatřuje porušení tohoto požadavku v analýze dat za použití Google Analytics.

Microsoft Edge ve svých Microsoft Edge Addons Catalog Developer Policies požaduje souhlas uživatelů pro předávání osobních údajů a souvisejících metadat externí službě či jakékoli třetí straně.[7]

Chce-li developer nabízet aplikaci na Apple Store, musí dle pokynů App Store Review Guidelines získat souhlas uživatele i v případě, že se jedná o anonymní údaje již v době zpracování. Běžným požadavkem definičních autorit se v této oblasti navíc stalo poskytnutí informací specifických pro daný produkt, a to nad rámec obecných informací o zpracování osobních údajů, které jsou obvykle zveřejněny na internetových stránkách podnikatelských subjektů.[8]

Amazon vyžaduje po developerech na základě Privacy and Security Policy obecný souhlas uživatelů, jestliže aplikace zpracovává jakékoli osobní údaje za jakýmkoli účelem.[9]

Jak je z výše uvedených příkladů patrné, tyto a další obdobné požadavky definičních autorit jdoucí nad rámec zákona vedou k četným, komplikovaným, nestálým, málo předvídatelným a často ekonomicky iracionálním pravidlům,[10] která omezují svobodu podnikání subjektů nedisponujících vlastnostmi definičních autorit. Svým jednáním zasahují do principu založeném na riziku a odpovědnosti developerů tím, že namísto nich určují právní základ zpracování, aniž by mohly posoudit jeho vhodnost a musely doložit jeho soulad. Zároveň nutí jednat developery netransparentně vůči jednotlivcům, když vyžadují souhlas za účelem zpracování, které by se mohlo opírat o jiný právní základ, nejčastěji právě oprávněný zájem.

Z hlediska kontextu je důležité si uvědomit, že vzhledem ke specifikům technologického odvětví je souhlas vyžadován v průběhu instalace, u níž je kladen důraz na co nejkratší

[4] Mozilla. *Add-on Policies – User Interactions & Technical Data* [online]. [cit. 31.8.2020]. Dostupné z www.extensionworkshop.com/documentation/publish/add-on-policies/.

[5] Opera. *Acceptance Criteria* [online]. [cit. 31.8.2020]. Dostupné z https://dev.opera.com/extensions/acceptance-criteria/.

[6] Google. *Updated Privacy Policy & Secure Handling Requirements* [online]. [cit. 31.8.2020]. Dostupné z www.developer.chrome.com/webstore/user_data.

[7] Microsoft. *Microsoft Edge Addons Catalog Developer Policies* [online]. [cit. 31.8.2020]. Dostupné z https://docs.microsoft.com/en-us/microsoft-edge/extensions-chromium/store-policies/developer-policies.

[8] Apple. *App Store Review Guidelines* [online]. [cit. 31.8.2020]. Dostupné z www.developer.apple.com/app-store/review/guidelines/#legal.

[9] Amazon. *Privacy and Security Policy* [online]. [cit. 31.8.2020]. Dostupné z https://developer.amazon.com/docs/policy-center/privacy-security.html.

[10] POLČÁK, R. *Internet a proměny práva*. Praha: Auditorium, 2012, str. 130.

a uživatelsky nejpřívětivější průběh. Z tohoto důvodu je každý krok vážně zvažován, jelikož může vést ke zvýšení počtu nedokončených instalací a ztrátě uživatelů. Souhlas má navíc negativní podtext a v uživatelích vzbuzuje nedůvěru. V rámci záměrné ochrany soukromí proto developeři již při vývoji softwarového programu dbají na to, aby zpracování za účely odlišnými od funkčnosti programu, prošla balančním testem a bylo možné se spoléhat na oprávněný zájem. Vyžadování souhlasu v případech, kdy není nezbytný ani vhodný, má dalekosáhlé dopady na podnikání developerů.

Ať už jsou, nebo nejsou výše uvedené příklady pouze výjimkou, je třeba vlivu definičních autorit na developery věnovat pozornost a zajistit účinné prostředky na jejich ochranu, a to nejen z hlediska compliance v oblasti ochrany osobních údajů. Jedním z možných nástrojů je intenzivnější orientace státu na definiční autority a aktivní zásahy v případech rozporu definičních norem se základními účely práva.[11] Výše diskutovaný příklad souhlasů je pouze jedním z institutů v oblasti ochrany osobních údajů, které definiční autority mohou použít k posilování své pozice. Regulace jiných oblastí relevantních pro technologický průmysl skýtají další takové instituty. Je důležité si proto uvědomit, že podobné situace by mohly být řešeny rovněž soutěžním právem[12], které má horizontální povahu. Vedle *ex ante* kontroly spojování podniků a *ex post* zákaz zneužití dominantního postavení si v souvislosti s žalobou Fortnite proti Apple Store lze také představit kartel vzbouřenců-developerů proti podmínkám těchto definičních autorit, a to vše za předpokladu změn klíčových konceptů relevantního trhu a tržní síly tak, aby obstály v testu digitálního času.

[11] Tamtéž, str. 135.

[12] Úřady pro ochranu hospodářskou soutěž j se otázkami spojenými se zpracováním údajů aktivně zabývají. Francouzský úřad pro ochranu hospodářské soutěže („Autorité de la concurrence“) a německý úřad pro ochranu hospodářské soutěže („Bundeskartellamt“) prvně analyzovaly zpracování údajů v souvislosti s důsledky a výzvy analýzy big dat, a to zejména s ohledem na aplikační fázi, ve které jsou výsledky analýzy big dat využívány k profilování a cílení na jednotlivce prostřednictvím online reklamy, v případech proti Google (č. j. 10-MC-01 ze dne 30. června 2010) a Facebook (č. j. B6-22 / 16 ze dne 6. února 2019).