

Ochrana osobních údajů v kontextu poskytování digitálních dat spotřebitelům

Štěpán Richter*

Anotace: Autor analyzuje ochranu osobních údajů při poskytování digitálních dat spotřebitelům, primárně komparací Obecného nařízení o ochraně osobních údajů, směrnice 2019/770 ze dne 20. května 2019 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb, směrnice 2019/771 ze dne 20. 5. 2019 o některých aspektech smluv o prodeji zboží a návrhu novely občanského zákoníku, který implementuje uvedené směrnice do českého právního řádu. Komparací právní úpravy bylo zjištěno, jakým způsobem na sebe jednotlivé předpisy reagují a jaká je jejich terminologická provázanost. Autor se dále věnuje problémům, které při interakci jednotlivých předpisů vznikají. Zde dochází k závěru, že, byť je vztah právních norem ochrany osobních údajů a norem soukromoprávních dobře a konkrétně vytyčen, vzniklo v rámci úpravy několik praktických problémů, které nelze vyřešit prostou interpretací. Konkrétně smlouvy, kde je jednou ze stran nezletilý a instituty následného odmítnutí plnění a práva na výmaz mají v kontextu obou úprav vážné nedostatky. Autor se rovněž zamýšlí nad hypotetickými důsledky striktní a důsledné aplikace nové úpravy na praxi trhu. Autor dospívá k závěru, že mezi ochranou osobních údajů a soukromoprávní úpravou poskytování dat spotřebitelům existuje hodnotová mezera, která má potenciál vytvářet praktické problémy, se kterými bude třeba se nějak vypořádat.

Klíčová slova: digitální obsah, digitální služby, smluvní protiplnění, ochrana osobních údajů, GDPR, právo na výmaz, double opt-in

Úvod: ochrana osobních údajů a nová právní úprava digitálního trhu

Ochrana osobních údajů není v právu ani ve společnosti novým fenoménem. První moderní právní akt ochrany osobních údajů vznikl, podobně jako mnoho progresivních legislativních aktů, ve Švédském království již v roce 1973.¹ Do podvědomí širokého okruhu spotřebitelů ovšem koncepcie ochrany osobních údajů začala skutečně pronikat až s účinností 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, populárně známého jako GDPR. To stanovilo pro členské státy Evropské unie konkrétní univerzální pravidla zpracování osobních údajů, stejně jako povinnost zpracovatelů si od subjektu, jehož údaje jsou zpracovávány, vyžádat jasný a explicitní souhlas, pokud ke zpracování jeho osobních údajů neexistuje jiný zákonem předvídaný důvod. Sekundárním přínosem GDPR byl právě fakt, že se díky němu právo na ochranu osobních údajů zapsalo do povědomí laických adresátů práva, kteří si uvědomili, že mají právo na to, aby jejich osobní údaje nebyly svévolně vyžadovány, zpracovávány a obchodovány jinými osobami. Díky účinnosti GDPR se problematice ochrany osobních údajů v soukromoprávní sféře začala hlouběji věnovat i literatura.

* Mgr. Štěpán Richter, interní doktorand na katedře občanského práva hmotného, Právnická fakulta Masarykovy univerzity, Brno. E-mail: stp.rich@gmail.com, <https://orcid.org/0000-0002-8057-6047>. Výzkum, jehož závěry obsahuje tento článek, byl realizován v rámci projektu specifického výzkumu Grantové agentury Masarykovy univerzity s názvem *Výzkum smluvní praxe poskytování digitálních dat spotřebitelům*, MUNI/A/1296/2020.

¹ DEAKIN, A. GDPR Timeline: A History of Data Protection. In: *vutu.re*. [online]. Červenec 2017 [cit. 2020-01-23].

Zpracování osobních údajů se v moderním digitalizovaném světě zcela vyhnout nelze.² Každá transakce provedená v digitálním prostředí má tzv. osobnostní deficit, tedy že subjekty uzavírající smlouvu komunikují spolu na dálku, a tedy si nejsou zcela jisty totožností druhé strany, kterou je třeba ověřit.³ Nejekonomičtější způsobem, jak se tohoto v praxi dosahuje, je právě poskytnutí osobních údajů spotřebitelem a jejich následné zpracování obchodníkem. Osobní údaje tedy plní v obchodním styku, jehož předmětem plnění jsou digitální data, roli nástroje kontraktace. Není to ovšem jediná role, kterou plní.

Nedlouho po účinnosti GDPR byla po dlouhém politicko-legislativním procesu schválena nová evropská právní regulace poskytování digitálních dat spotřebitelům, tvořená dvěma sekundárními právními akty: směrnicí Evropského parlamentu a Rady (EU) 2019/770 ze dne 20. května 2019 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb (dál jen „směrnice 770“) a Směrnicí Evropského parlamentu a Rady EU 2019/771 ze dne 20. 5. 2019 o některých aspektech smluv o prodeji zboží (dál jen „směrnice 771“). Směrnice 770 upravuje poskytování digitálního obsahu a služeb, což jsou ve své podstatě data vytvořená a uchovaná v digitální podobě⁴ a nehmotné věci. Oproti tomu směrnice 771 upravuje koupi a prodej zboží s digitálními prvky, což jsou hmotné věci, jejichž integrální součástí je digitální obsah nebo digitální služba [čl. 2 odst. 5 písm. b) směrnice 771].

S platností směrnic byl právem vytvořen nový koncept, a sice že spotřebitel místo zaplacení ceny za poskytnutá data poskytne obchodníkovi přístup k datům svým, přičemž velká část těchto dat jsou osobní údaje, které může obchodník následně shromažďovat a zpracovávat a jejichž prodejem následně dosahuje zisku. Tato alternativa ke standardnímu peněžnímu modelu transakcí je již v praxi hojně využívána,⁵ nicméně právní řád neměl pro tento model až do platnosti směrnice žádnou speciální úpravu, vyjma právě ustanovení GDPR. Nabízí se pak stěžejní právněteoretická i praktická otázka, jakým způsobem je nová koncepce „platby osobními údaji“ provázána s již existující úpravou ochrany osobních údajů, zejména s GDPR.

V současné době je již právní úprava GDPR, účinná od roku 2018, obstojně zažitá v právní praxi České republiky. Proces implementace shora uvedených směrnic právě probíhá a s největší pravděpodobností bude mít podobu novely Občanského zákoníku. Návrh novely zákona je ve fázi projednávání v poslanecké sněmovně, prozatím nebyl ale ani v prvním čtení.⁶ Jedná se tedy o vysoce aktuální téma jak pro legislativu, tak pro odbornou veřejnost, neboť nový koncept osobních údajů jako obchodovatelné komodity zásadně změní chápání významné části závazkového práva. Článkem se tak může inspirovat zákonodárce při inkorporaci směrnice 770, stejně jako praxe během procesu porozumění novým normám a odborná veřejnost při vytváření nové právní teorie.

² MATES, P. – VALOUŠEK, M. – FIALOVÁ, E. a kol. *Ochrana osobnosti, soukromí a osobních údajů*. Praha: Leges, 2019, s. 33.

³ MAŠTALKA, J. *Osobní údaje, právo a my*. Praha: C. H. Beck, 2008, s. 11.

⁴ PRAŽÁK, Z. a kol. *Závazky z právních jednání podle občanského zákoníku. Komentář k § 1721–2893 OZ*. Praha: Leges, 2017, s. 160.

⁵ K tomuto závěru dospěl autor při svém předchozím výzkumu. Srov. RICHTER, Š. *Mobilní aplikace ve smluvním právu*. In: *Dopady digitalizace do oblasti soukromého práva*. Brno: Masarykova univerzita, 2019, s. 55–70, s. 15.

⁶ ÚŘAD VLÁDY ČESKÉ REPUBLIKY. *Návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů*. Dostupné z: Elektronická knihovna legislativního procesu (VeKLEP) [právní informační systém].

Cílem tohoto článku je analyzovat vztah právní úpravy poskytování digitálního obsahu a digitálních služeb a ochrany osobních údajů. V návaznosti na to budou analyzovány praktické problémy, které mohou při poskytování dat spotřebitelům z pohledu ochrany osobních údajů nastat, se závěrem v podobě polemiky *de lege ferenda*.

1. Právní rámec poskytování digitálních dat spotřebitelům, ochrany osobních údajů, a styčné body těchto odvětví

1.1 Systematický vztah unijních předpisů

Pro pochopení vztahu mezi směrnicemi 770 a 771 a GDPR je nutné analyzovat provázanost těchto aktů ve vztahu k teorii i korelaci jednotlivých ustanovení.

Směrnice 771 vůbec s pojmem osobní údaje nepracuje ani jinak nenavazuje na regulaci jejich ochrany. To je, vzhledem k povaze předmětu její úpravy, přirozené; směrnice 771 upravuje koupi a prodej zboží s digitálními prvky, tedy hmotných věcí, jejichž neoddělitelnou součástí jsou digitální data. Za koupi této věci spotřebitelé, alespoň prozatím, platí výhradně penězi. To samozřejmě neznamená, že by pomocí zboží s digitálními prvky, jako jsou například smartphony, obchodníci neshromažďovali osobní údaje uživatelů. Nicméně tyto osobní údaje nejsou primární hodnotou, kterou obchodník získá od spotřebitele oproti koupi zboží samotného; spotřebitel za zboží vždy zaplatí kupní cenu. V praxi rovněž není zboží s digitálními prvky, které by obchodníci prodávali pouze za sběr osobních údajů spotřebitele.⁷ Pokud aplikace ve spotřebitelově *smartphonu* o něm shromažďuje osobní údaje za účelem zisku, jedná se právně o samostatný právní vztah, který je poskytnutím digitálního obsahu podle směrnice 770. Tento právní názor není v souladu s názory Německého Internetového institutu,⁸ nicméně jejich analýza nezohledňuje rozdělení poskytovaných dat do tří kategorií stanovených směrnicemi 770 a 771 a zároveň nezohledňuje aspekty smluvní praxe. Další analýza v článku se tedy bude věnovat výhradně úpravě vyplývající ze směrnice 770, která je s úpravou ochrany osobních údajů obsahově výrazně více provázána.

Ze systematiky směrnice 770 je patrné, že evropský zákonodárce zamýšlel navázat na předchozí úpravu digitálních dat, včetně úpravy ochrany osobních údajů. Toto vyplývá nejvíce z faktu, že směrnice 770 ohledně definice osobních údajů přímo odkazuje na GDPR, místo toho, aby obsahovala vlastní definiční ustanovení (čl. 2 odst. 8 směrnice 770). Dokonce GDPR výslovně zmiňuje v recitálu.⁹ GDPR definuje osobní údaje jako „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě*“ (čl. 4 odst. 1 GDPR). Tato definice v sobě zahrnuje pojmové znaky osobních údajů. Jedná se o veškeré informace, tedy není důležitý jejich faktický obsah nebo technická forma. Tyto informace se musí přímo týkat fyzické osoby, která je pomocí těchto údajů identifikovaná nebo identifikova-

⁷ Tuto informaci autor zjistil analýzou smluvní praxe poskytování digitálních dat, v rámci projektu specifického výzkumu Grantové agentury Masarykovy univerzity s názvem *Výzkum smluvní praxe poskytování digitálních dat spotřebitelům*, MUNI/A/1296/2020.

⁸ METZGER, A. – EFRONI, Z. – MISCHAU, L. – METZGER, L. Data-Related Aspects of the Digital Content Directive. *Journal of Intellectual Property, Information Technology and E-Commerce Law* [online]. 29. 5. 2018. [cit. 2020-01-15], s. 101. Dostupné z: <<https://www.jipitec.eu/issues/jipitec-9-1-2018/4682>>.

⁹ Recitál 37 Směrnice Evropského parlamentu a Rady EU 2019/770 ze dne 20. 5. 2019 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb.

telná. Identifikovatelná fyzická osoba je osobou, kterou lze přímo i nepřímo identifikovat na základě identifikátorů jako je jméno, identifikační číslo, lokační údaje nebo jeden či více zvláštních prvků identity fyzické osoby.

Vzhledem k tomu, že jsou zákonné definice vymezeny velmi obecně, lze prakticky veškerá data zpřístupněná obchodníkovi spotřebitelem klasifikovat jako osobní údaje. Ne všechna data poskytnutá spotřebitelem jsou na první pohled osobními údaji podle GDPR, nicméně při praktické analýze je jimi valná většina, zejména s ohledem na množství údajů, které obchodník od jednoho spotřebitele obvykle shromažďuje: poloha, registrační údaje, dokonce historie používání programu jsou způsobilé identifikovat osobu, zejména pokud se těchto informací sejde více najednou.¹⁰ Maštalka definuje osobní údaj jako sdělení pojednávající o určité skutečnosti, jejímž předmětem je určitá fyzická osoba,¹¹ a tuto definici data poskytnutá spotřebitelem nepochybně splňují. Moderní technologie navíc rozšiřují okruh údajů, které naplňují pojem soukromí, za určitých okolností stačí jen IP adresa.¹²

Potřeba stanovit univerzální pravidla pro zpracování osobních údajů vyplynula primárně z praxe, na kterou GDPR v době svého vzniku reagovalo.¹³ Věcná působnost GDPR zahrnuje jak automatizované, tak ruční zpracování osobních údajů. Není přitom rozhodný množství ani časový rozsah zpracování, ani jeho způsob – nařízení explicitně stanoví, že ochrana osobních údajů je technologicky neutrální.¹⁴ GDPR je, jakožto Nařízení Evropského parlamentu a Rady, přímo použitelné, tedy jeho ustanovení platí všeobecně pro všechny členské státy EU. GDPR je všeobjímajícím univerzálním předpisem, který připouští ze své působnosti jen minimum výjimek a i ty je třeba dle ustálené judikatury ESD vykládat restriktivně.¹⁵ Žádná z těchto výjimek se neuplatní na poskytování osobních údajů vůči digitálnímu obsahu nebo službám.

Směrnice 770 se vztahuje na veškeré smlouvy, na jejichž základě spotřebitel poskytne nebo se zaváže poskytnout obchodníkovi osobní údaje.¹⁶ To platí v případech, kdy spotřebitel poskytne osobní údaje aktivně, stejně jako pasivně – tedy pouze umožní jejich sběr. Jedná se například o situaci, kdy spotřebitel založí účet na sociální síti, kde uvede své jméno, věk a e-mailovou adresu, které jsou poté zpracovány a použity obchodníkem pro cílenou reklamu. Rovněž reguluje případy, kdy spotřebitel dá souhlas k tomu, aby obchodník dosahoval zisku zpracováváním materiálů představujících osobní údaje, jako např. fotografie nebo recenze nahrané spotřebitelem. Souhlas se zpracováním musí být výslovný, konkrétní a informovaný, jak judikoval Tribunál.¹⁷ To ovšem neznamená, že souhlas nemůže být ve formulářové podobě, například prostého kliknutí v programu, které je v praxi nejčastější.

¹⁰ MATES, P. – VALOUŠEK, M. – FIALOVÁ, E. a kol. *Ochrana osobnosti, soukromí a osobních údajů*, s. 85.

¹¹ MAŠTALKA, J. *Osobní údaje, právo a my*. Praha: C. H. Beck, 2008, s. 5.

¹² MATES, P. – VALOUŠEK, M. – FIALOVÁ, E. a kol. *Ochrana osobnosti, soukromí a osobních údajů*, s. 34.

¹³ DVOŘÁKOVÁ, H. – POKORNÁ, A. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek*. Praha: Wolters Kluwer, 2020, s. 5.

¹⁴ Recitál 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.

¹⁵ Srov. Rozsudek SDEU ze dne 10. července 2018. č. j. C-25/17 (*Jehovan Todistajat*) a Rozsudek SDEU ze dne 14. prosince 2014. č. j. C-212/13 (*Ryneš*).

¹⁶ Recitál 24 Směrnice Evropského parlamentu a Rady EU 2019/770 ze dne 20. 5. 2019 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb.

¹⁷ Rozsudek Tribunálu ze dne 3. prosince. 2015. č. j. T 343/13 (*CN proti Evr. Parlamentu*).

GDPR pracuje v kontextu ochrany osobních údajů s pojmy správce a zpracovatel. Správce je osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení (čl. 4 odst. 7 GDPR). Zpracovatel je pak osoba nebo jiný subjekt, který zpracovává osobní údaje pro správce (čl. 4 odst. 8 GDPR). Směrnice 770 s těmito termíny neoperuje. Zato stanoví velmi obecnou a širokou kategorii tzv. obchodníků jako osob, které jednájí v souvislosti se smlouvami o poskytování digitálního obsahu a služeb za účelem, který lze považovat za obchodní činnost, podnikání, řemeslo nebo povolání. Toto platí i v případě, že za tuto osobu jedná jiná osoba v zastoupení (čl. 2 odst. 5 směrnice 770). Jinými slovy, obchodníci podle směrnice jsou poskytovatelé digitálního obsahu a služeb spotřebitelům neohledně na vnější okolnosti. V praxi se jedná v drtivé většině případů o právnické osoby. V kontextu poskytování digitálního obsahu a služeb spotřebitelům, což je záležitost čistě práva soukromého, splývají zpracovatel, správce a obchodník do jedné osoby, která zastává všechny tyto role. Vedle toho jsou subjekt zpracování podle GDPR a spotřebitel podle směrnice 770 rovněž toutéž osobou. Za zmínku stojí, že novela Občanského zákoníku, která inkorporuje normy směrnice 770 do českého právního řádu, se terminologicky vrátila k pojmům poskytovatel a uživatel.¹⁸ Tyto pojmy, byť specifitější pro odvětví informačních technologií, ovšem nevyjadřují dostatečně fakt, že regulace směrnice 770 se vztahuje pouze na spotřebitelské právní vztahy. V konečném důsledku, při současném zohlednění systematiky o. z., by mohla některá ustanovení novely dopadnout i na vztahy B2B. Případná analýza novely v tomto směru by byla hodna dalšího zkoumání.

Na základě faktů uvedených v této kapitole je zjevné, že na poskytování dat, která jsou osobními údaji spotřebitelem obchodníkovi zpřístupněna či poskytována, se normy GDPR uplatní v plném rozsahu. Vzhledem k povaze GDPR jako veřejnoprávního předpisu je aplikace jeho norem nezávislá na aplikaci práva soukromého. Subjekty operující s osobními údaji při poskytování digitálního obsahu a služeb musí ctít požadavky práva ochrany osobních údajů, neohledně na vlastní zájmy nebo ustanovení soukromoprávních předpisů.

1.2 Osobní údaje – základní lidská hodnota nebo měna?

Systematicky a jazykově je právní regulace poskytování digitálního obsahu a služeb oproti osobním údajům ucelená a stabilní. Pokud bychom právní řád oprostili od jakýchkoli mimoprávních morálních hodnot, což není v právní teorii zcela neslýchaný koncept,¹⁹ dichotomie osobních údajů by nebyla koncepčně problémem – ano, ochrana osobnosti a osobních údajů je ústavním pořádkem chráněnou hodnotou a zároveň jsou osobní údaje komoditou digitálního světa. Dichotomie vzniká nikoli díky textům předpisů samotných, nýbrž v rovině hodnotové, koncepční a právněteoretické.

Předně, ochrana osobních údajů je hodnotou chráněnou ústavním pořádkem. Základem pro současnou právní úpravu osobních údajů je Úmluva o ochraně lidských práv

¹⁸ Tyto byly používány v předchozích návrzích úpravy. Srov. Návrh Směrnice Evropského parlamentu a Rady KOM (2015) 634 v konečném znění 2015/0287 (COD), ze dne 9. 12. 2015 o některých aspektech smluv o poskytování digitálního obsahu.

¹⁹ Srov. např. Kelsenovu *Ryzí nauku právní* nebo Weyrovu *Normativní právní teorii*.

a základních svobod, která je součástí právního řádu skrz čl. 8 Ústavy.²⁰ Rovněž Listina základních práv a svobod stanoví, že každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě (čl. 10 odst. 3 Listiny). Jedná se tedy o hodnotu, jejíž ochraně je přikládána mimořádná váha, která nemůže být snadno omezována, modifikována či snižována.²¹ Toto je ovšem v přímém rozporu s rolí osobních údajů jako komodity stanovenou novými právními předpisy. Jak je možné přisuzovat hodnotě ústavněprávní váhu, pokud jí její nositelé platí v běžných, každodenních transakcích?

Unijní odborníci zastávají názor, že osobní údaje mají kapacitu sloužit jako smluvní protiplnění navzdory jejich lidskoprávnímu aspektu.²² Jejich argumentace se opírá především o to, že i v jiných právních disciplínách je praxí, že práva vztahující se k osobě (např. autorská) mají i peněžní dimenzi, se kterou mohou jejich držitelé volně nakládat. Směrnice 770 reguluje pouze obchodní a spotřebitelské aspekty nakládání s osobními údaji, a úprava podle GDPR tak zůstává nezasažena. V souvislosti s tím je třeba počítat i s opačným efektem, kdy úprava ochrany osobních údajů zasahuje do smluvního práva.

Odborníci z oblasti ekonomie obvykle posuzují zpřístupnění osobních údajů jako cenu na základě subjektivních kritérií; jedná se o cenu jen v případě, že je to konkrétnímu uživateli subjektivně k tíži.²³

Je důležité poznamenat, že unijní zákonodárce si je evidentně této dichotomie vědom. Odborná veřejnost poukazovala na tento problém již u předchozích návrhů úpravy,²⁴ přičemž tyto předchozí návrhy hovořily explicitně o smluvním protiplnění.²⁵ V aktuální úpravě se ovšem termín protiplnění neobjevuje, a to ani v recitálech. Lze dovodit, že unijní zákonodárce se s ohledem na komplexnost legislativního procesu EU rozhodl problémem vyplývajícím z klasifikace poskytování osobních údajů jako smluvního protiplnění vyhnout a její případné teoretické vyřešení přenechal členským státům nebo odborné veřejnosti.

V případě České republiky se prozatím nezdá, že by se zákonodárce koncepční otázkou osobních údajů jako smluvního protiplnění hlouběji zabýval. Implementace směrnic probíhá toliko v rovině novelizace zvláštních ustanovení Občanského zákoníku, konkrétně § 1811 a násl., a dále transplantací norem směrnic do nových paragrafů o. z.²⁶ Obecná ustanovení o plnění (§ 1721 a násl. o. z.) zůstávají nezměněna, navzdory tomu, že některá ustanovení by přinejmenším zasloužila reflexi nové právně teoretické situace. Zejména ustanovení § 1747 o. z., které stanoví, že „[j]e-li smlouva bezúplatná, má se za to,

²⁰ MAŠTALKA, J. *Osobní údaje, právo a my*. Praha: C. H. Beck, 2008, s. 5.

²¹ MATES, P. – VALOUŠEK, M. – FIALOVÁ, E. a kol. *Ochrana osobnosti, soukromí a osobních údajů*, s. 66.

²² METZGER, A. – FRONI, Z. – MISCHAU, L. – METZGER, L. Data-Related Aspects of the Digital Content Directive. *Journal of Intellectual Property, Information Technology and E-Commerce Law* [online]. 29. 5. 2018 [cit. 2020-01-15], s. 94. Dostupné z: <<https://www.jipitec.eu/issues/jipitec-9-1-2018/4682>>.

²³ GRAEF, I. a kol. Assessing data access issues in online platforms. In: *Telecommunications Policy* [online]. Únor 2015 [cit. 2020-01-23], s. 5. Dostupné z: <<https://www.researchgate.net/publication/273509086>>.

²⁴ Návrh Směrnice Evropského parlamentu a Rady KOM (2015) 634 v konečném znění 2015/0287 (COD), ze dne 9. 12. 2015 o některých aspektech smluv o poskytování digitálního obsahu. Srov. dále METZGER, A. *Data-Related Aspects of the Digital Content Directive*, s. 90.

²⁵ Čl. 3 odst. 1. Návrhu Směrnice Evropského parlamentu a Rady KOM (2015) 634 v konečném znění 2015/0287 (COD), ze dne 9. 12. 2015 o některých aspektech smluv o poskytování digitálního obsahu.

²⁶ ÚŘAD VLÁDY ČESKÉ REPUBLIKY. Návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Dostupné z: Elektronická knihovna legislativního procesu (VeKLEP) [právní informační systém].

že se dlužník chtěl zavázat spíše méně než více“, by mělo být poměřováno s čl. 2 odst. 7 směrnice 770, který definuje cenu jako „peněžní částka nebo digitální vyjádření hodnoty, jež mají být poskytnuty za poskytnutí digitálního obsahu nebo digitální služby“, což zcela evidentně míří na osobní údaje.

Pro komplexní představu o právním rámci poskytování digitálního obsahu a služeb je vhodné poznamenat, že toto poskytování je službou informační společnosti. SDEU judikoval, že „[s]lužby informační společnosti zahrnují smlouvy a jiné služby, jež se uzavírají nebo přenášejí online“.²⁷ Služba informační společnosti je termín původně rovněž práva EU, který je v národní úpravě promítnut zákonem č. 480/2004 Sb., zákon o některých službách informační společnosti, ve znění pozdějších předpisů. Podobně jako ochrana osobních údajů je koncept služeb informační společnosti doménou práva veřejného. Analýza práv a povinností osob ve vztahu k úpravě služeb informační společnosti ovšem není předmětem tohoto článku: postačí říci, že obchodníci nejsou trestně či jinak odpovědní za obsah vytvořený uživateli v rámci poskytnutého digitálního obsahu nebo služby.²⁸

2. Praktické problémy duality právní regulace

2.1 Nakládání s osobními údaji nezletilých

Nezletilé osoby, byť nenabyté plnou svéprávností, mohou figurovat na digitálním trhu jako spotřebitelé, neboť k zajišťování si přístupu k obsahu např. pro zábavu nebo vzdělání jsou jistě volně i rozumově vyspělí, ve smyslu § 31 o. z.

Významný koncepční problém nastává v situaci, kdy je spotřebitelem nezletilý, který sice může uzavřít smlouvu, avšak jeho osobní údaje požívají zvláštní ochrany. Osobní údaje nezletilých požívají zvláštní ochrany (čl. 8 GDPR), jelikož děti jsou si s ohledem na svůj věk méně vědomy rizik, důsledků, záruk a práv při jejich zpracování.²⁹ Toto se v oblasti poskytování obsahu projeví nejvíce v tom, že v případě zpracování na základě souhlasu musí být nezletilému alespoň 16 let, aby byl takový samostatný souhlas platný. Český zákon č. 110/2019 Sb., zákon o zpracování osobních údajů (dále jen z. o. o. ú.), tuto hranici v souladu s možností GDPR snížil na 15 let. Pro případ nižšího věku nezletilého jsou zákonem stanoveny další podmínky: musí jít o službu informační společnosti a tato musí být nabízena přímo dítěti (tedy být i zamýšlena pro používání nezletilými), a zároveň musí být souhlas vyjádřen nebo schválen osobou, která vykonává rodičovskou zodpovědnost k dítěti. Jak již bylo řečeno výše, velká část poskytovaného obsahu cílí přímo na nezletilé, zejména v zábavním odvětví.³⁰ GDPR upřesňuje, že „tato zvláštní ochrana by se měla zejména vztahovat na používání osobních údajů dětí pro účely marketingu nebo vytváření osobnostních či uživatelských profilů a shromažďování osobních údajů týkajících se dětí při využívání

²⁷ Rozsudek SDEU ze dne 2. prosince 2010 č. j. C-108/09, (*Ker-Optika*), odst. 22 a 28.

²⁸ KORBEL, F. Ne-odpovědnost poskytovatelů služeb informační společnosti v digitálním světě. *Právní prostor* [online]. 17. 5. 2018 [cit. 2020-02-20]. Dostupné z: <<https://www.pravniprostor.cz/clanky/pravo-it/ne-odpovednost-poskytovatelu-sluzeb-informacni-spolecnosti-v-digitalnim-svete>>.

²⁹ Recitál 32 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.

³⁰ Jako typický příklad lze zmínit platformu Youtube, která nedávno spustila program Youtube Kids, specificky cílený na prepubertální děti. Srov. dále ALBA, D. Google Launches ‚YouTube Kids‘, a New Family-Friendly App. In: *wired.com* [online]. 23. 2. 2015 [cit. 2020-02-20]. Dostupné z: <<https://www.wired.com/2015/02/youtube-kids/>>.

služeb nabízených přímo dětem“.³¹ Dále pak má nezletilý právo na výmaz osobních údajů, které se ho týkají a byly shromážděny v souvislosti s nabídkou služeb informační společnosti podle čl. 8 odst. 1 GDPR [čl. 17 odst. 1 písm. f) GDPR]. Problematice nemožnosti/zbytečnosti následného výmazu osobních údajů se věnuje kapitola *Nakládání spotřebitelů s osobními údaji*. U souhlasu nezletilého pak vyvstávají praktické problémy, a sice, že je třeba každý individuální případ posuzovat podle toho, zda byl obsah nabízen dětem. Právní řád ČR nezná nic jako dělení obsahu do kategorií podle věku, mimo speciální případy.³² Z praktického hlediska existuje obsah, který zjevně není (respektive by neměl být) nezletilým přístupný, nicméně podstatná část digitálního trhu nezletilým přístupná je.

Systémové řešení by mohlo spočívat v individuální aplikaci široké škály neformálních dělení přístupných spotřebiteli, např. hodnocení ESRB používaného v USA. Vzhledem k tomu, že podstatná část obsahu je z USA,³³ kde je toto hodnocení stanovené zákonem, lze snadno argumentovat pro použití tohoto hodnocení i zde – alespoň co amerického obsahu se týče. Jako dobré interpretační východisko lze použít i technologické limity samotné: nezletilý, který nemá rozumovou a volní vyspělost k uzavření smlouvy o poskytnutí digitálního obsahu, není obvykle vůbec schopen operovat s příslušným zařízením natolik, aby vědomě smlouvu uzavřel.

Ochrana osobních údajů požaduje, aby správce údajů ověřil, že souhlas ke zpracování osobních údajů dítěte vyjádřila nebo schválila osoba vykonávající k nezletilému rodičovskou odpovědnost. Pokud toto neučiní, porušuje tím článek 8 GDPR, přičemž za porušení norem v čl. 8 GDPR může být uložena sankce až do výše 10 milionů euro [čl. 83 odst. 4 písm. a) GDPR], což je dozajista sankce, kterou nechce riskovat žádný racionální obchodník. V praxi poskytování obsahu se toto ovšem až na čestné výjimky³⁴ neděje. V případech, kdy ano, má ověřování dvě formy: uvedení věku v rámci systému obchodníka a odstavec ve smluvním ujednání potvrzující souhlas rodiče.

Tento problém má přirozeně i praktický přesah, neboť ve shora uvedených situacích by bylo možné argumentovat, že nezletilá osoba není dostatečně svéprávná k poskytování svých osobních údajů jako smluvního protiplnění, a tedy je jakákoli jimi uzavřená smlouva neplatná ve smyslu § 581 o. z.

2.2 Následné odmítnutí plnění

Další praktický problém, již diskutovaný jak na akademické, tak na zákonodárné půdě, vyvstává v situaci, kdy ve spotřebitelské smlouvě spotřebitel plní pouze poskytnutím přístupu k osobním údajům. Následně ovšem odvolá souhlas s jejich zpracováním podle GDPR.

³¹ Recitál 38 Nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

³² Např. obsah, který je hazardní hrou podle zákona č. 186/2016 Sb., o hazardních hrách, nebo obsah, který by mohly ohrozit fyzický, psychologický nebo mravní vývoj dětí a mladistvých podle § 32 odst. 1 písm. g) zákona č. 231/2001 Sb. o provozování rozhlasového a televizního vysílání.

³³ Commission staff working document. A Digital Single Market Strategy for Europe – Analysis and Evidence Communication from the Commission. In: *EUR-Lex* [online]. Úřad pro publikace Evropské unie. Evropská Komise (2015b), 2015 COM(2015) 192 final [cit. 2020-02-28]. Dostupné z: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015SC0100>>.

³⁴ *Epic Games store End User License Agreement* [online]. 2021 [cit. 2021-02-10]. Epic Games International, Sà r.l. Dostupné z: <<https://www.epicgames.com/store/en-US/eula>>.

Pro zpracování osobních údajů za účelem jejich zpeněžení potřebuje obchodník spotřebitelův souhlas, jelikož smluvní vztah o poskytování obsahu a služeb za osobní údaje nenaplnuje jiné podmínky podle čl. 6 GDPR.³⁵ Takovýto souhlas může spotřebitel dle čl. 7 odst. 3 GDPR kdykoli bez dalších podmínek odvolat. V návaznosti na to má spotřebitel právo na výmaz osobních údajů, které o něm obchodník posbíral. Toto právo spotřebitele ve smluvním vztahu explicitně potvrzuje i směrnice 770,³⁶ která dokonce přímo stanoví, že tím není dotčeno právo spotřebitele na ukončení smlouvy podle čl. 15 směrnice. Je vhodné připomenout, že odvolání souhlasu nemá vliv na předchozí legální sběr údajů.³⁷

V situaci, kdy toto spotřebitel učiní, je ovšem zásadním způsobem zasaženo do uzavřené smlouvy, jelikož fakticky přestává mít obchodník z právního vztahu užitek; pokud přestane mít možnost sbírat a zpracovávat osobní údaje spotřebitele, pozbude tím pro obchodníka smlouva primární účel – dosažení zisku. Zde se dichotomie opět projevuje; na jedné straně je veřejné právo jedince na ochranu jeho hodnot, na straně druhé soukromoprávní kontraktační vztah, do kterého se tentýž jedinec dobrovolně zavázal.

Směrnice 770 neupravuje důsledky odvolání souhlasu se zpracováním osobních údajů. Tato povinnost je tedy ponechána na vnitrostátním právu.³⁸ Novelizace o. z. ovšem na tuto otázku nijak neodpovídá.³⁹ Současné platné znění o. z. upravuje speciálně otázku poskytování digitálního obsahu zcela minimálně,⁴⁰ jediným východiskem tedy zůstává obecná úprava závazků. Ze závazku je povinen věřitel, mimo jiné, něco strpět (§ 1789 o. z.), což je případ spotřebitele, který strpí sběr a zpeněžení svých osobních údajů. Ustanovení o. z. už ovšem konkrétně nestanoví, jak postupovat, když se strpění dlužníka stane nemožným v důsledku právního jednání dlužníka, které znemožní věřiteli konat věc, která má být strpěna.

V případě odvolání souhlasu se zpracováním osobních údajů připadá rovněž v úvahu institut neúměrného zkrácení (§ 1793 o. z.), jelikož plnění stran v situaci, kdy spotřebitel odvolá souhlas ke zpracování svých osobních údajů, by bylo nepochybně v hrubém nepoměru. Zároveň je tu ale vždy varianta, že institut v této situaci nebude vůbec možné použít, vzhledem k plné harmonizaci úpravy směrnice 770. Nicméně jsem názoru, že zde se pravidlo plné harmonizace neuplatní, jelikož se jedná o situaci, kdy směrnice na vnitrostátní úpravu výslovně odkazuje, a tedy je i použití institutu neúměrného zkrácení přípustné.

Jak je patrné z právní analýzy, pozitivní právo uspokojivou odpověď nenabídne. Odborná veřejnost se již otázkou rovněž zabývala. Hugh Beale zastává striktní pozici, že v případě, kdy spotřebitel znemožní obchodníkovi zisk odvoláním souhlasu se zpracováním osobních údajů, přestává tím fakticky plnit svůj závazek a měly by z toho být vyvozeny příslušné občanskoprávní následky.⁴¹ K tomuto názoru se připojují i někteří kontinentální odborníci, např. Gerald Spindler a Pia Kalamees.⁴²

³⁵ Mimo osobní údaje, které musí obchodník zpracovávat ze zákona nebo pro splnění smlouvy.

³⁶ Čl. 39 Recitálu směrnice 770.

³⁷ METZGER, A. – EFRONI, Z. – MISCHAU, L. – METZGER, L. Data-Related Aspects of the Digital Content Directive. *Journal of Intellectual Property, Information Technology and E-Commerce Law* [online]. 29. 5. 2018 [cit. 2020-01-15], s. 93. Dostupné z: <<https://www.jipitec.eu/issues/jipitec-9-1-2018/4682>>.

³⁸ Čl. 40 Recitálu směrnice 770.

³⁹ ÚŘAD VLÁDY ČESKÉ REPUBLIKY. Návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Dostupné z: Elektronická knihovna legislativního procesu (VeKLEP) [právní informační systém].

⁴⁰ Např. § 1811 odst. 3 b). Ten je navíc v rozporu se Směrnicí 770 a nadcházející novelou bude změněn.

⁴¹ BEALE, H. Digital consumer conference. Tallin Estonia, listopad 2020.

⁴² SPINDLER, G. – KALAMEES, P. et al. *Digital consumer conference*. Tallin Estonia, listopad 2020.

Protiargument k tomuto přístupu předkládají odborné orgány věnující se primárně ochraně osobních údajů, konkrétně Evropský sbor pro ochranu osobních údajů. Při posuzování toho, zda je souhlas se zpracováním osobních údajů svobodný, musí být důsledně zohledněna skutečnost, zda je mimo jiné plnění smlouvy, včetně poskytnutí služby, podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné (čl. 7 odst. 4 GDPR). Slovo „svobodný“ implikuje skutečnou možnost volby a kontrolu nad situací pro subjekt zpracování osobních údajů.⁴³ Obecně platí, že pokud subjekt zpracování nemá skutečnou volbu a cítí se nucen souhlasit se zpracováním svých údajů, nebo ponese negativní následky pokud souhlasit nebude, nebude jeho souhlas svobodný, a tedy platný podle GDPR.⁴⁴ Pokud ovšem udělený souhlas nebyl platný, nemá obchodník v první řadě vůbec právo na sběr dat spotřebitele. Evropský sbor pro ochranu osobních údajů ilustruje tento koncept na následujícím příkladu: mobilní aplikace na editaci fotografií požaduje po svých uživateli přístup k lokalizaci pomocí GPS, pro používání aplikace. Spotřebitel je informován, že sbíraná data budou použita pro cílenou reklamu. Ani lokalizace pomocí GPS ani cílená reklama nejsou nutné k tomu, aby byla aplikace funkční, tedy editovala fotografie. Jelikož spotřebitel nemůže aplikaci použít bez souhlasu se sdílením své polohy, nelze souhlas vnímat jako svobodný.⁴⁵ Nutno poznamenat, že metodika, která se daným tématem zabývá, byla Evropským sborem pro ochranu osobních údajů přijata 4. května 2020 – tedy dávno po účinnosti směrnice 770. Sbor si tedy musel být této dichotomie dobře vědom, a přesto se k tomuto závěru přiklonil.

Pohledem čistě systematickým je třeba se přiklonit k závěru Beala a Spindlera, tedy, že odvoláním souhlasu se zpracováním osobních údajů spotřebitel fakticky přestává plnit a nastupují z toho vyplývající občanskoprávní následky. Tento přístup je logický a z pohledu soukromého práva spravedlivý, nicméně se zde opět projevuje hodnotová kolize GDPR a směrnice 770. Na jednu stranu by měla osoba mít právo rozhodnout, jak budou zpracovávány její osobní údaje, na stranu druhou se jedná o hodnotu, kterou osoba může a musí disponovat, pokud chce využívat služeb digitální společnosti. Zde je ovšem potřeba připomenout, že spotřebitel často reálně nemá možnost volby – jeho jedinou alternativou je daný obsah nepoužít. A za takovýchto podmínek je reálně vnímat spotřebitelův souhlas se zpracováním osobních údajů jako nesvobodný a tedy neplatný. Nabízí se reflexe s adhezními smlouvami, kde je spotřebitel rovněž zákonem významně zvýhodněn, aby byla dorovnána materiální nerovnost stran.

Spotřebitel nemá obvykle ohledně svého plnění ani možnost volby; poskytovatelům sociálních sítí ani nelze za jejich služby platit peníze. U těch mála případů, kde to možné je, přestane být sice spotřebitel vystaven reklamám, ale souhlas se zpracováním osobních údajů si obchodník stejně vyžádá a ponechá.⁴⁶ Ostatně je to pro něj dodatečný zisk. V případě, kdy lze volbu skutečně učinit (např. u her, které využívají modelu placeného i modelu „zdarma“) se pak osoba musí rozhodnout, zda přijít o peníze, nebo své soukromí.

⁴³ Evropský sbor pro ochranu osobních údajů. Guidelines 05/2020 on consent under Regulation 2016/679. 4. května 2020, s. 7.

⁴⁴ Opinion 15/2011 on the definition of consent. 13. 7. 2011. Evropský sbor pro ochranu osobních údajů – pracovní skupina 29.

⁴⁵ Evropský sbor pro ochranu osobních údajů. Guidelines 05/2020 on consent under Regulation 2016/679. 4. května 2020, s. 8.

⁴⁶ YOUTUBE. *Podmínky poskytování služeb* [online]. 22. července 2019 [cit. 2021-02-10]. Dostupné z: <<https://www.youtube.com/static?template=terms>>.

Takovýto systém fakticky zvýhodňuje v otázkách ochrany osobních údajů majetné, což lze v konečném důsledku považovat až za nepřímou diskriminaci. Dokonce by bylo možné argumentovat, že i v případě, kdy spotřebitel možnost volby má (tedy buďto za obsah zaplatí nebo poskytne přístup ke svým osobním údajům), by neměl být *de lege ferenda* souhlas se zpracováním považován za svobodný. Znamenalo by to totiž právní posvěcení praktiky, že si osoba může připlatit za to, že nebude narušeno její soukromí, čímž by byly v konečném důsledku monetizovány právem chráněné hodnoty. Ochrana soukromí není neomezená, ovšem v moderním právním státě, který skutečně ctí hodnoty deklarované svým ústavním pořádkem, by neměla být omezována ekonomickými faktory.

Okénko ze smluvní praxe: čl. 7 odst. 3 GDPR stanoví, že: odvolat souhlas musí být stejně snadné jako jej poskytnout. Poskytnutí souhlasu se téměř výlučně děje „proklikáním se“. Odvolat souhlas v rámci instalačního programu/procesu registrace samotného nelze z povahy věci vůbec (pokud je obsah nainstalován, program se již nespouští, pokud je uživatel zaregistrován a obsah zpřístupněn, uživatel se již neregistruje). Teleologickým výkladem normy bychom ovšem mohli pravidlo zobecnit, a sice, že odvolání souhlasu by mělo být stejně jednoduché jako jeho dání. Obchodníci ovšem k odvolání souhlasu navíc jednoduchou cestu nenabízí; pokud je vůbec odvolání možné v rámci prostředí poskytovaného obsahu nebo služby, je často velice dobře skryté.⁴⁷

Jak bylo zjištěno, platí, že normy GDPR jsou speciální vůči normám vyplývajícím z norem směrnice 770, a tedy i důsledky vyplývající z norem GDPR jsou nadřazeny důsledkům vyplývajícím z norem směrnice 770. Za této situace se přikláním k závěrům odborníků na ochranu osobních údajů, a sice, že souhlas se zpracováním osobních údajů daný pod ekonomickým nátlakem faktického používání poskytnutého obsahu není svobodný, a tedy není platný. Z právního hlediska pak, pokud spotřebitel takovýto „souhlas“ odvolá, nejedná se o akt znemožňující jeho plnění, neboť plnění v rovině osobních údajů od počátku možné nebylo. Nelze pak, s ohledem na ochranu spotřebitele, toto odvolání přičítat spotřebiteli k tíži a připustit variantu, že by mu obchodník mohl odmítnout nadále poskytovat plnění.

2.3 Právo na výmaz

Další problematika a novou úpravou uspokojivě nevyřešená situace vyvstává z technologické povahy osobních údajů a dat obecně. Osobní údaje, na rozdíl od peněz, mají trvalý charakter a data lze donekonečna kopírovat. Z praktického pohledu to znamená, že pokud spotřebitel poskytne své osobní údaje nebo k nim udělí přístup, neztrácí je tím, na rozdíl od peněz nebo jiné věci. Problém nastává v situaci, kdy spotřebitel uplatní své právo na výmaz podle čl. 17 GDPR, respektive podle příslušných ustanovení z. o. o. ú. Spotřebitel jakožto subjekt zpracování má tzv. právo na výmaz, a sice, že správce bez zbytečného odkladu musí vymazat osobní údaje, které se daného subjektu údajů týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat, pokud subjekt údajů odvolá souhlas se zpracováním a žádný další právní důvod pro zpracování neexistuje nebo byly tyto údaje zpracovány protiprávně.

⁴⁷ VALVE CORPORATION. *Steam Subscriber Agreement* [online]. 28. srpna 2020 [cit. 2021-02-10]. CHYBÍ ODKAZ. Srov. dále EPIC GAMES INTERNATIONAL. *Epic Games store End User License Agreement* [online]. 2021 [cit. 2021-02-10]. Dostupné z: <<https://www.youtube.com/static?template=terms>>.

Jak již bylo řečeno, ochrana soukromí je dána ústavním pořádkem. Ochranu osobnosti člověka a právo se domáhat neoprávněného zásahu do osobnosti či odstranění následků stanoví § 83 o. z. V případě práva na výmaz při poskytování digitálních dat spotřebitelům (tedy čistě soukromoprávní styk) se ovšem aplikují speciální ustanovení GDPR, specificky k tomu určené. Právo na výmaz ve veřejnoprávním styku upravuje přímo z. o. o. ú. Spotřebitel nemá dle pozitivního práva nárok na to, aby třetí osoby, kterým obchodník poskytne jeho zpracované osobní údaje, tyto údaje vymazaly.⁴⁸ Má ovšem právo vědět, kterým třetím osobám byly jeho osobní údaje poskytnuty (čl. 15 a 19 GDPR). Toto by měl obchodník činit automaticky, tedy bez žádosti spotřebitele.⁴⁹

Tento problém přímo navazuje na otázku kapitoly výše, avšak uplatní se v obou variantách jejího vyřešení: pokud spotřebitel může souhlas odvolat, může se zároveň domáhat práva na výmaz, pokud je jeho souhlas od počátku neplatný, byly osobní údaje zpracovány protiprávně a může se domáhat práva na výmaz.

Při poskytování digitálního obsahu a služeb ovšem z praktického hlediska může být, a obvykle je, na právo na výmaz příliš pozdě. Technologie současnosti dovolují automatizovaný sběr a zpracování osobních údajů pouhé milisekundy poté, co je uzavřena smlouva a spotřebiteli zpřístupněn obsah.⁵⁰ Spotřebitel, který se z jakéhokoli důvodu rozhodne využít svého práva, v mnoha případech již nemá faktickou šanci ochránit své soukromí, které již bylo prolomeno. Třeba i v případě, že se rozhodne odstoupit od smlouvy ve čtrnácti dnech bez udání důvodu. Jakmile jsou osobní údaje jednou obchodníkovi poskytnuty, ten je sesbírá a prodá dále reklamní společnosti, je soukromí spotřebitele nevyhnutelně narušeno a spotřebitel se nemůže již vrátit do situace, kdy tomu tak nebylo.

2.4 Double opt-in

Problémy okolo ochrany osobních údajů při poskytování digitálního obsahu a služeb spotřebitelům nejsou neznámé odborné veřejnosti ani praxi, které se již prakticky od vzniku úpravy snaží nabídnout vhodná řešení. Jako jedna z vhodných metod pro udělení souhlasu se zpracováním osobních údajů je často zmiňována tzv. *double opt-in*, spočívající v procesu, kdy spotřebitel udělí souhlas prostřednictvím softwaru a je zároveň požádán o sdělení e-mailu, na který následně přijde ověřovací e-mail s unikátním odkazem, na který musí kliknout, aby souhlas dokončil. Tuto metodu považuje za dobrou odborná veřejnost⁵¹ i evropské instituce spolupracující na vytvoření úpravy samotné.⁵² *Double opt-in* byl dokonce patentován ve Spojených státech amerických.⁵³ Přestože je tato metoda

⁴⁸ V terminologii GDPR se jedná o „příjemce“ dle čl. 4 odst. 9 GDPR.

⁴⁹ Recitál 61 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.

⁵⁰ SØRENSEN, J. – VAN DEN BULCK, H. Public service media online, advertising and the third-party user data business: A trade versus trust dilemma? In: *Convergence* [online]. 13. 8. 2018 [cit. 2020-01-10]. Dostupné z: <https://journals.sagepub.com/doi/full/10.1177/1354856518790203?casa_token=plmr-gC19VwAAAAA%3Aekoe-ult1hNY1vIXREK2NcKJbwNdyGx6bHvMr1SrW45BRPO7UE93MJ1zbbHqcb-4iy47N5vpo-dpOl#articleCitationDownloadContainer>.

⁵¹ DVOŘÁKOVÁ, H. – POKORNÁ, A. *Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek*. Praha: Wolters Kluwer, 2020.

⁵² Skupina WP29. Guidelines 05/2020 on consent under Regulation 2016/679. Verze 1.1. 4. května 2020. Evropský sbor pro ochranu osobních údajů, s. 25.

⁵³ IFI CLAIMS Patent Services. Double opt-in™ method and system for verifying subscriptions to information distribution services.

v podstatě ideálním kompromisem, jelikož naplňuje podmínky právní úpravy ochrany osobních údajů při současném zohlednění specifík poskytování digitálního obsahu, nese s sebou stejný problém, který provází mnoho uspokojivých technicko-smluvních řešení; je časově i úkonově neekonomická. Zejména v případě obsahu malého rozsahu, typicky mobilních aplikací, může i takto jednoduchý proces zcela odradit spotřebitele od pořízení aplikace, zatímco obchodník, který bude souhlas získávat jednodušším způsobem nebo vůbec, může být zvýhodněn, protože jeho instalační proces bude jednodušší.

2.5 Nakládání spotřebitelů s osobními údaji

Právní úpravy ochrany osobních údajů a poskytování digitálního obsahu a služeb spotřebitelům mají společné to, že jejich primárním účelem je ochrana práv fyzických osob – subjektů zpracování údajů/spotřebitelů. Při posuzování toho, nakolik nová právní úprava skutečně své subjekty chrání, tedy nelze pominout ekonomickou analýzu práva. Právní řád je stavěn na systému brání se o vlastní práva; pokud jsou práva osoby porušována, musí to být v první řadě osoba samotná, která se svých práv bude domáhat. Toto je ovšem v případě poskytování digitálního obsahu a digitálních služeb problematické, protože pro data malého rozsahu a nízké ceny, což je většina trhu,⁵⁴ je úprava často nedostatečně vymahatelná, neboť práva porušená při poskytování dat spotřebiteli z ekonomického hlediska nestojí často ani za komunikaci s obchodníkem, natož za soudní řízení. To platí tím víc u obsahu, oproti kterému spotřebitel zpřístupňuje své osobní údaje, neboť u těch musí spotřebitel jako fyzická osoba poměřovat, zda mu jeho soukromí stojí za jeho peníze.

Je těžké říct, kolika osobám je milejší platit za software svým soukromím oproti penězům. Vzhledem k hojnému počtu uživatelů sociálních sítí a jiného obsahu a služeb „zdarma“ ovšem lze tvrdit, že jim tento model přinejmenším nevádí.

Je třeba poukázat na fakt, že stěžejní hodnotou demokratické společnosti není ochrana soukromí, nýbrž svoboda jednotlivce. Ať je právní situace jakákoli, spotřebitelé se dnes a denně svobodně rozhodují poskytnout své osobní údaje oproti jiným hodnotám. Model obsahu „zaplaceného“ osobními údaji nevznikl s účinností nové úpravy, ale je běžně užíván již léta. Na základě právní analýzy výše je možné dojít k legitimnímu závěru, že souhlas se zpracováním osobních údajů může spotřebitel kdykoli odvolat a nedostane se tím do situace, že neplní své závazky ze smlouvy. Dokonce v případě, kdy je jedinou alternativou spotřebitele smlouvu neuzavřít, by bylo možné uvažovat o neplatnosti smlouvy podle § 580 odst. 1 o. z., neboť takovýto nesvobodný souhlas odporuje smyslu a účelu GDPR. Takovýto autoritativní právní zásah do zavedené praxe by ovšem mohl významně narušit plynulost digitálního trhu, který již léta funguje, a v konečném důsledku by stanovení možnosti spotřebitelů kdykoli odvolat souhlas se zpracováním svých údajů mohlo uškodit jim samotným. Ne z pohledu ochrany jejich osobních údajů, ale z pohledu ekonomického. Pokud by spotřebitel měl právo souhlas se zpracováním svých osobních údajů kdykoli odvolat (zde připomínám, že podle zákona musí být odvolání souhlasu stejně jednoduché jako jeho dání) a odvoláním by se neocitl v prodlení s vlastními závazky, významně by se

⁵⁴ Ceny digitálního obsahu či služeb málokdy překročí částku 2 000 Kč. Pro srovnání: Licence antiviru NOD32, nejdražšího antivirového software na českém trhu, stojí 1 203 Kč na jeden rok. Srov. dále Právní informace [online]. 2021 [cit. 10. 7. 2021] ESET software spol. s. r. o.

zvýšilo riziko pro poskytovatele obsahu, kteří by se v konečném důsledku museli spoléhat na to, že spotřebitel svých práv podle GDPR nevyužije. Toto by přirozeně vedlo ke snížení používání modelu zpracování osobních údajů jako smluvního protiplnění a transakce na digitálním trhu by se mohly začít vracet ke starému peněžnímu modelu.

Nelze uspokojivě odpovědět na právněfilozofickou otázku, nakolik by měl systém chránit osoby před nimi samotnými, třeba i ku jejich ekonomickému neprospěchu. V rámci aplikace a interpretace práva se ovšem obávám, že důsledná ochrana soukromí osob, třeba i za cenu narušení praxe trhu, by se nesečkala s pochopením ani u těch osob, které chránit má.

Závěr – kolize ochrany osobních údajů a soukromého práva

Mezi právem ochrany osobních údajů a soukromoprávní úpravou poskytování digitálního obsahu a digitálních služeb existuje propast. Ačkoli se to nemusí na první pohled takto jevit, neboť systematický vztah obou právních úprav je pevně daný, jasný a snadno interpretovatelný, při hlubší analýze konkrétních institutů a praktických situací vyvěrá na povrch mnoho problémů, a hodnotový rozpor mezi těmito pododvětvími právní úpravy se stává zjevným.

Unijní právní úprava ochrany osobních údajů je na systematické úrovni precizní, bezrozporná a svojí obecností nadčasová. Ostatně myšlenka technologické neutrality zákona je klíčem k udržení aktuálnosti nejen úpravy osobních údajů, ale jakéhokoli právního předpisu. S odstupem času se ovšem začínají objevovat koncepční a praktické trhliny. Výše analyzované praktické problémy jsou důkazem faktu, že obecná evropská úprava dostatečně nezohledňuje specifika digitálního trhu. To není z povahy věci zřejmě možné, jelikož těchto specifik je obrovské množství a na úrovni evropského práva, jehož tvorba je notoricky dlouhá a komplikovaná, prakticky nelze regulovat veškeré možné situace speciálními normami. Unijní akty samotné ovšem dávají široký prostor národním zákonodárcům právo dotvořit, nicméně alespoň v prostředí ČR se toto obvykle neděje, nestalo se tak v případě ochrany osobních údajů a s největší pravděpodobností ani nestane v případě poskytování dat spotřebitelům. Národní právní řády nicméně mohou nabídnout východiska v obecných ustanoveních, ustálené interpretaci a hodnotách chráněných právním řádem. Nezbyvá tak než vyčkat, jak se s konkrétními problémy nové úpravy vypořádá praxe a judikatura.

Problematiku ochrany osobních údajů při poskytování digitálních dat spotřebitelům není jednoduché rozklíčovat, zejména proto, že celý koncept zpřístupnění osobních údajů jako smluvního protiplnění je v právu stále velmi nový (ostatně ani moderní ochrana osobních údajů není tak stará). Problematika jako celek je vysoce aktuální a být na mnou vytyčené problémy odborná veřejnost občas poukázala, nikdo ještě nenabídl uspokojivé a komplexní řešení. Tomu se nelze divit, na složité otázky neexistují jednoduché odpovědi.

Personal Data Protection in the Context of Supply of Digital Data to the Consumer

Štěpán Richter (<https://orcid.org/0000-0002-8057-6047>)

Abstract: The article analyses personal data protection in the context of supply of digital data to the consumer mostly by the way of comparing the General data protection regulation, Directive 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, Directive 2019/771 of 20 May 2019 on certain aspects concerning contracts for the sale of goods and the draft of Civil code novelization, which implements said directives to the Czech law. The comparison determined how these legal acts interact and how their terminology is intertwined. The author then analyses issues stemming from the interaction of the two regulations and concludes that while the relationship between data protection and supply of digital content and digital services is well defined, several problems have still arisen, which cannot be dealt with by simple interpretation. Specifically, contracts with minors, cases of refusal of counter-performance and the right to be forgotten can be severely problematic. The author also considers the digital market practice and hypothetical impact of strict and thorough application of the new regulations on it. In the end, the author concludes that there is a value gap between data protection and private law of supply of digital data to the consumer, which can create practical problems, that will need to be dealt with somehow.

Keywords: digital content, digital service, counter-performance, personal data protection, GDPR, the right to erasure, double opt-in