Univerzita Palackého v Olomouci

Právnická fakulta

Michal Pisklák

Ochrana osobních údajů v prostředí internetu

Diplomová práce

Olomouc 2018

Čestné prohlášení:

Prohlašuji, že jsem diplomovou práci na téma Ochrana osobních údajů v prostředí internetu vypracoval samostatně a citoval jsem všechny použité zdroje podle směrnice děkanky č. 2/2010, kterou se stanoví náležitosti kvalifikačních prací na Právnické fakultě Univerzity Palackého v Olomouci.

V Olomouci dne 29. března 2018 Podpis: ……

Poděkování:

Děkuji panu JUDr. Bc. Marianu Kokešovi za trpělivé vedení a korekci mé diplomové práce. Dále děkuji rodině a přátelům za podporu v průběhu studia a vypracovávání této práce.

OBSAH

ÚVOD

K výběru tématu pro svou diplomovou práci jsem se naklonil po praktických zkušenostech se zpracováním a analýzou dat obsahujících osobní údaje fyzických osob získaných na internetu a s rozhodovací praxí Úřadu pro ochranu osobních údajů. Chtěl bych tak využít jak mých zkušeností, tak mého zájmu o tuto oblast ústavního práva.

Jako konkrétní oblast, ve které hodlám ústavně zaručenou ochranu osobních údajů (jako součást práva na soukromí) zkoumat, jsem si vybral prostředí internetu, které se neustále dynamicky mění, a jehož rychle se střídající obsah umožňuje vznik nových způsobů obcházení, nebo dokonce porušování tohoto práva. Téma datového obsahu na internetu je v posledních letech ožehavé a diskutované téma, a jeho praktický význam pociťuje i široká laická veřejnost. Proto bych chtěl zhodnotit jak právní, tak praktickou stránku ochrany osobních údajů ve webovém prostředí a dopracovat se k odpovědím na otázky, jak je ochrana osobních údajů na internetu realizována, a jestli je činnost orgánů pro ochranu osobních údajů získaných na webu v současné době dostatečná.

Nejdříve bych rád definoval pojem osobního údaje a zařadil ho v systému ústavního práva, respektive výčtu základních práv obsažených v Listině základních práv a svobod. Následovat bude krátký historický exkurz do dob vzniku ochrany osobních údajů. Také bych v rád zhodnotil, jaký je standard garance tohoto základního práva a upozornil na to, jakým způsobem se do právního řádu České republiky promítá ochrana tohoto práva z komunitárního práva Evropské unie. V této souvislosti zmíním i obecné nařízení o ochraně osobních údajů (anglicky General Data Protection Regulation, zkráceně GDPR), jehož účinnost je stanovena na 25. května 2018, a také systémy předávání osobních údajů do zemí mimo Evropskou unii a jejich nedávné změny.

Dále budu pokračovat samotnými osobními údaji, které se nejčastěji vyskytují nebo získávají na internetu. V tomto ohledu poukážu na postupy největších hráčů na poli internetové sítě, co do obsahu dat o svých uživatelích, jakými jsou například společnosti Google LLC nebo Facebook Inc. Do této kapitoly také zařadím pojednání o datech cookies, listovním tajemství a úpravě nevyžádaných obchodních sdělení, to vše v prostředí internetu.

Další analýzu věnuji rozhodovací praxi orgánů, které by měly sloužit jako ochránci tohoto základního práva, ať už je to český Úřad pro ochranu osobních údajů, obecné vnitrostátní soudy, Ústavní soud ČR, štrasburský Evropský soud pro lidská práva (ESLP), nebo lucemburský Soudní dvůr Evropské unie (SDEU). Za zmínku zde stojí nedávné rozsudky ESLP i SDEU, které potvrdily, že statická i dynamická IP adresa osoby procházející web je

osobním údajem s patřičnou úrovní ochrany. Ze spojení konkrétních rozhodnutí se budu snažit vysledovat moderní způsob ochrany osobních údajů, které se týkají internetového prostředí, a směr, jakým se tato ochrana bude vydávat.

V závěru práce bude třeba především odpovědět na mnou položené výzkumné otázky. Dále se pokusím shrnout současné problémy ochrany osobních údajů na internetu a jejich úpravu *de lege lata,* a také najít možná východiska pro úpravu *de lege ferenda* v souvislosti s nařízením GDPR, které bude přímo závazné bez nutnosti transpozice a zároveň nahradí jak předchozí směrnici, tak ve velké míře změní český zákon o ochraně osobních údajů.

1. OCHRANA SOUKROMÍ NA ÚSTAVNÍ ÚROVNI

1.1 Ústavní úroveň ochrany

Lze snadno souhlasit s výrokem soudce amerického Nejvyššího soudu A. Scalii, který prohlásil, že *„by bylo bláznovstvím tvrdit, že míra soukromí zůstala technickým pokrokem zcela nedotčena"*[1]. Technologický pokrok vytvořil nové problémy, které zpochybňují konzistenci aplikace ochrany soukromí a ohrožují její aplikaci v prostředí doby internetové. Dobu internetovou lze charakterizovat především rozšířeností sociálních sítí, neregulovaného toku dat v kyberprostoru a novými metodami trestné činnosti.[2] J. Matejka představuje ve své monografii[3] čtyři zásadní problémy ochrany soukromí na internetu, a to následovně:

1. větší propast mezi mírou ochrany soukromí, kterou očekává jednotlivec v prostředí informační společnosti, a tím, co je „společnost" (tj. soud) ochotna uznat za přiměřené,
2. smluvní podmínky a povaha poskytování služeb v tomto prostředí, které podkopávají důležité dílčí principy práva soukromí,
3. nevídaný nárůst případů, jejichž předmětem je zejména rozsah možnosti vzdát se práva na ochranu soukromí (např. dobrovolné poskytnutí informací, limity autonomie člověka v oblasti vědomého se vystavení ztrátě soukromí apod.),
4. nekompetentnost soudní i výkonné moci, která postrádá technické znalosti potřebné k tomu, aby mohla efektivně a přiměřeně vymezit ochranu soukromí v digitálním prostředí.

V České republice je na ústavní úrovni zakotveno právo na soukromí v článku 10 Listiny základních práv a svobod[4] (dále jen „Listina"). Odstavec 3 tohoto článku zní *„Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě."* Citovaný odstavec pojednává o ochraně osobních údajů v podobě termínu tzv. práva na informační sebeurčení. Toto právo výstižně zařazuje Ústavní soud ČR jako součást práva na soukromí, když uvádí, že „*právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení, zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny*

[1] *Kyllo v. United States,* 533 U.S. 27, 33–34 (2001)
[2] KOKEŠ, Marian. Několik poznatků k problematice konkrétních konfliktů mezi právem na informační sebeurčení a ochranou národní bezpečnosti v tzv. době internetové. In ŠIMÍČEK, Vojtěch. *Právo na soukromí.* Brno: MUNI Press, 2011.
[3] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. 1. vydání. Praha: CZ.NIC, 2013. s. 39
[4] ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů

jiným subjektům. Jde o aspekt práva na soukromí v podobě práva na informační sebeurčení, výslovně garantovaný čl. 10 odst. 3 Listiny."[5]

Tato ochrana je zajištěna jak mezi občany navzájem, tak mezi občanem a státním orgánem a chrání osobní údaje o subjektu, přímo či nepřímo identifikovatelného na základě čísla, kódu nebo jednoho či více prvků specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.[6]. Jako základní právo je tedy třeba právo z čl. 10 odst. 3 Listiny vyvažovat v poměru k ostatním základním právům.

Protože lidé jsou nositeli základních práv a zároveň disponují různými zájmy a praktikují různé způsoby chování, může výkon základních práv jednotlivých členů společnosti vzájemně kolidovat. U mnohých základních práv obsažených v ústavním pořádku je možnost jejich omezení zákonem výslovně zmíněna. Jde o pověření zákonodárce přijmout zákonnou úpravu, která většinou umožňuje omezit to které základní právo z určitého důvodu anebo bez jeho uvedení (např. čl. 7, 8, 11, 12, 13, 14, 16 Listiny). Vedle toho nalezneme v ústavním pořádku i taková základní práva, u nichž zmíněné zákonné omezení není předvídáno. Tím je např. právě čl. 10 pojednávající o ochraně soukromí. To ovšem neznamená, že by tato práva nebyla omezitelná.[7] K tomu viz kapitola 3.2 pojednávající o judikatuře Ústavního soudu ČR.

Ochrana osobních údajů, jež je součástí ochrany soukromí ve výše uvedeném čl. 10 odst. 3 Listiny, je podrobně rozvedena v zákoně o ochraně osobních údajů[8] (dále jen „ZOÚ"). I bez legálních definic tam obsažených by ale tato součást práva na soukromí byla chráněna na ústavní úrovni.

1.2 Pojem osobní údaj

Pro tuto práci je klíčovým pojmem tzv. osobní údaj. Pro jeho definici nemusíme chodit daleko a stačí nahlédnout do ZOÚ. Ten ve svém § 4 písm. a) definuje osobní údaj jako *„jakoukoli informaci týkající se určeného nebo určitelného subjektu údajů"*. Tato definice je až na drobné slovní odlišnosti stejná s tou, která je obsažena v Úmluvě č. 108 na ochranu osob se zřetelem na automatizované zpracování osobních dat, přijaté Radou Evropy 28. ledna 1981[9],

[5] Nález Ústavního soudu ze dne 2. listopadu 2009, sp. zn. II. ÚS 2048/09 (N 232/55 SbNU 181). Dostupné na www.nalus.usoud.cz. Shodně Nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl.ÚS 24/10 (N 52/60 SbNU 625). Dostupné na www.nalus.usoud.cz

[6] KLÍMA, Karel et al. *Komentář k Ústavě a Listině. 2. díl. 2. rozš. vyd.* Plzeň: Nakladatelství a vydavatelství Aleš Čeněk, 2009. s. 1036

[7] WAGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch., LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer, 2012. s. 23

[8] zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů

[9] Úmluva č. 108, na ochranu osob se zřetelem na automatizované zpracování osobních dat, přijatou Radou Evropy 28. ledna 1981, vyhlášená pod č. 115/2001 Sb. m. s.,

která nabyla pro Českou republiku účinnosti dne 1. listopadu 2001 (dále jen „Úmluva č. 108“) a ve Směrnici Evropského parlamentu a Rady Evropské unie 95/46/ES[10] ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů (dále jen „Směrnice“). Subjektem[11] údaje je pak dle § 4 písm. d) ZOÚ *„fyzická osoba, k níž se osobní údaje vztahují“*. Cílem veškerých legislativních snah směřujících k ochraně takto definovaných osobních údajů, je zabránit jejich zneužití a zároveň umožnit zpřístupnění osobních údajů k legálním účelům. Takovéto legální využívání se obecně nazývá „volný tok“, obvykle ve spojení s tokem přes hranice států.

Za zmínku stojí i pojem tzv. „citlivého osobního údaje“. ZOÚ v § 4 písm. b) vyjmenovává taxativně okruhy citlivých osobních údajů a to následovně: údaje o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu, sexuálním životě, a také biometrické nebo genetické údaje. Citlivé údaje požívají zvláštní ochrany dle § 9 ZOÚ.

Dalším často skloňovaným pojmem je správce, což je osoba, která určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele. Zpracovatelem je ten, kdo na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje. ZOÚ dále vyjmenovává a popisuje povinnosti správce a zpracovatele, kterým ale není pro účely této práce třeba věnovat prostor.

Zpracováním údajů je jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů je zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.

Pod pojem osobní údaj spadá i dnes už hojně využívaný elektronický podpis, který je definován zákonem o elektronickém podpisu[12]. Tento zákon definuje elektronický podpis jako údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby ve vztahu k datové zprávě.

[10] Směrnice Rady Evropské unie 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů. Úř. věst. L 281, 23. listopadu 1995, s. 31 a násl.
[11] První český zákon na ochranu osobních údajů č. 256/1992 Sb. ve svém § 10 používal pojem dotčená osoba a stanovil, že „Dotčenou osobou se rozumí jednotlivá fyzická osoba, o které informace vypovídá“.
[12] zákon č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů

Elektronický podpis obsahuje jednak informace o obsahu zprávy, k níž je připojován, jednak osobní údaje jako informace o odesílateli datové zprávy.[13]

1.3 Vývoj ochrany osobních údajů na území České republiky

Poté, co jsme si osobní údaj jako právní termín definovali, je na místě stručně shrnout historii ochrany, jež se ve společnosti osobním údajům poskytovala. Ochrana osobních údajů je novým právním i společenským problémem. První právní předpisy k ochraně osobních údajů vznikly v 70. letech 20. století; ale významné případy využití dříve shromážděných osobních údajů proti právům a životům jiných lidí jsou v podmínkách střední Evropy spojeny už s obdobím druhé světové války a nacismem, především za účelem zjišťování židovského původu obyvatel.[14]

V období po druhé světové válce lze z pohledu mezinárodního práva nalézt jako první krok k ochraně osobních údajů Úmluvu č. 108. Jedná se o mezinárodní smlouvu dle čl. 10 Ústavy ČR[15]. V článku 1 tato smlouva uvádí jako svůj předmět a účel *„zaručit na území každé smluvní strany každé fyzické osobě, ať je jakékoli národnosti nebo pobývá kdekoli, úctu k jejím právům a základním svobodám, a zejména k jejímu právu na soukromý život, se zřetelem k automatizovanému zpracování osobních údajů, které se k ní vztahují“*. Zkušenosti z praxe však přinesly poznání, že nelze v ochraně osobních údajů oddělovat automatizované a neautomatizované zpracování osobních údajů, ale naopak je nezbytné dívat se na způsob zpracování dat jako rovnocennou volbu odpovědného subjektu.[16]

K provedení Úmluvy č. 108 byl vydán zákon. č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech. Zákon měl ovšem jeden velký nedostatek. Z důvodu rozpadajícího se Československa nedošlo ke zřízení nezávislého dozorového orgánu nad zpracováním osobních údajů (dříve „nakládáním s osobními údaji“), který tento zákon předpokládal v ustanovení § 24. Díky tomuto nedostatku zákon v praxi nebyl příliš respektován, neboť neexistoval úřad, který by na dodržování povinností z tohoto zákona dohlížel a sankcionoval jejich porušení.[17]

S dalším obdobím vývoje ochrany osobních údajů se pojí tzv. internetová revoluce, tedy rozmach internetu, který probíhal přibližně v následujících dvou dekádách po vzniku

[13] MATOUŠOVÁ, Miroslava, HEJLÍK Ladislav. *Osobní údaje a jejich ochrana*. Vyd. 2. Praha: Aspi, 2008, s. 102
[14] tamtéž, s. 9
[15] ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů
[16] KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů – komentář.* Praha: Nakladatelství C. H. Beck, 2012. s. 4
[17] MAŠTALKA, Jiří. *Osobní údaje, právo a my*. Vyd. 1. Praha: C.H. Beck, 2008, xiv, s. 11

samostatné České republiky. Tato revoluce je dnes prakticky ukončena tím, že dle průzkumu společnosti Adobe k roku 2016 většina lidí, která má možnost se k internetu připojit, už na síti je. Internet má nyní pouze minimální potenciál přilákat nové uživatele.[18] Dobu po této revoluci lze popsat jako dobu internetovou, definovanou v kapitole 1.1.

K vývoji komunitárního práva je nutno uvést základní dokument Evropské unie k ochraně osobních údajů, a to výše uvedenou Směrnici. Tato Směrnice je ale ke dni 25. května 2018 nahrazena přímo účinným Nařízením (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů – též nazýváno „obecné nařízení o ochraně osobních údajů, angl. General Data Protection Regulation (dále jen „GDPR“)[19]. Více o GDPR v kapitole 1.5.1.

1.4 Zákonná úprava

Hlavním předpisem k ochraně osobních údajů v České republice je v současné době ZOÚ. Tento zákon kromě vymezení práv a povinností při zpracování osobních údajů vymezuje také postavení a působnost Úřadu pro ochranu osobních údajů, o jehož činnosti je dále pojednáno v kapitole 3.1. Jeho působnost je stanovena v ustanovení § 3, a to kombinací pozitivního i negativního vymezení. Následuje vymezení stěžejních pojmů pro účely tohoto zákona v § 4, která ovšem překračují jeho hranice a používají se ve vztahu k osobním údajům obecně. Lze zde nalézt definici pojmů jako např. již zmíněný osobní údaj, citlivý osobní údaj, anonymní údaj, subjekt údaje, shromažďování, zpracování a dále také definici osob správce a zpracovatele. Opisovat tyto definice ze zákona se pro účely této práce jeví jako nepotřebné.

V rámci občanského práva je chráněno soukromí a projevy osobní povahy obecným ustanovením § 81 odst. 2 občanského zákoníku[20] (dále jen „OZ“). Následuje podrobnější ochrana v § 84 až 90 OZ týkající se podoby a soukromí fyzické osoby. Po listopadu roku 1989 se při aplikaci ochrany osobnosti podle předchozího občanského zákoníku[21] vycházelo z toho, že úkolem úpravy práva na ochranu osobnosti je v občanskoprávní oblasti zabezpečit respektování osobnosti fyzické osoby a tím její všestranný svobodný rozvoj. Současně bylo zdůrazňováno, že jde též o jedno z důležitých rozvedení a konkretizací čl. 7, 8, 10, 11, 13 a 14 Listiny zakotvujících pro právní řád jako celek právo na ochranu osobnosti jako základní lidské

[18] TOMEŠ, Michal. *Rozmach internetu končí, noví uživatelé přibývají jen pomalu* [online].e15.cz, 28. září 2016 [cit. 19. března 2018]. Dostupné na <http://e-svet.e15.cz/internet/rozmach-internetu-konci-novi-uzivatele-pribyvaji-jen-pomalu-1323056>.
[19] Nařízení (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). Úř. věst. L 119, 4. května 2016, s. 1 a násl.
[20] zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
[21] zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů

právo a v tomto jednotném rámci práva na ochranu osobnosti existujících dílčích práv, která zabezpečují občanskoprávní ochranu jednotlivých hodnot, resp. stránek osobnosti fyzické osoby, jako neoddělitelných součástí její celkové fyzické a psychickomorální integrity osobnosti. OZ sleduje jusnaturalistický koncept celé kodifikace, zajišťuje ochranu osobnosti člověka v zásadě (pouze s drobnými diferencemi) ve stejném rozsahu jako předchozí občanský zákoník, přičemž jsou zásady, na jejichž základě je zbudován, ve své podstatě identické těm, na nichž byla již v "polistopadové" době vykládána ochrana osobnosti fyzické osoby.[22]

Z hlediska obsahu získávaných a shromažďovaných informací není samo o sobě rozhodující, zda se jedná o údaje ryze soukromé či získané na veřejnosti.[23] Rovněž je pro potřeby OZ bez významu, zda jde o osobní údaje ve smyslu ZOÚ či nikoli. Sám ZOÚ bohužel neřeší vztah k OZ a ani naopak.[24] Okruh údajů je v ZOÚ vymezen autonomně pro vlastní veřejnoprávní účely. Nelze proto dovozovat, že tyto údaje bez dalšího tvoří součást osobnosti člověka, a tedy předmět absolutního osobnostního práva podle OZ, nebo naopak.[25]

Postup při náhradě způsobené škody se bude řídit obecnou úpravou odpovědnosti za škodu dle OZ. Shodně je uveden v ustanovení § 21 odst. 3 ZOÚ odkaz na zvláštní zákon, konkrétně na § 12 OZ (§ 13 předchozího občanského zákoníku) pro případ, že vznikne v důsledku zpracování osobních údajů subjektu údajů jiná než majetková újma.

Ochrana osobních údajů je dále respektována i zákonem o svobodném přístupu k informacím[26]. V České republice platí princip publicity veřejné správy, který udává povinným osobám povinnost poskytnout na žádost veškeré informace s výjimkou těch, o kterých zákon stanoví výslovně, že se neposkytují.[27] Jedná se o opak principu diskrétnosti, který v tehdejším Československu platil před listopadem 1989. Právě výše uvedené výjimky z povinnosti poskytnout informaci plynou ze zájmu ochrany taxativně vyjmenovaných hodnot, kam (mimo např. obchodní tajemství a utajované informace) spadá právě i ochrana osobních údajů v § 8a zmiňovaného zákona. Aby se na informaci vztahovala tato výjimka, je nutné, aby splňovala znaky uvedené v § 4 písm. a) ZOÚ.[28]

---

[22] ŠVESTKA, Jiří a kol. *Občanský zákoník - Komentář - Svazek I (obecná část).* 1. vydání. Praha: Wolters Kluwer, 2014 (§ 81 občanského zákoníku).
[23] Rozsudek ESLP ze dne 4. května 2000, *Rotaru v. Rumunsko* (stížnost č. 28341/95)
[24] NONNEMANN, František. Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů, *Právní rozhledy* 13-14/2012, s. 505
[25] LAVICKÝ, Petr a kol. *Občanský zákoník.* 1. vydání. Praha: C. H. Beck, 2014, s. 509 - 523
[26] zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
[27] LIBERDOVÁ, Eva. *Právo na dobrou správu jako princip veřejné správy v EU* [online]. epravo.cz, 21. července 2015 [cit. 16. února 2018]. Dostupné na <https://www.epravo.cz/top/clanky/pravo-na-dobrou-spravu-jako-princip-verejne-spravy-v-eu-98220.html>.
[28] Rozsudek Nejvyššího správního soudu ze dne 10. 8. 2004, sp. zn. 2 As 6/2004-49

Mezi další právní předpisy, které obsahují ochranu osobních údajů lze zařadit z oblasti veřejnoprávní zákony upravující provoz informačních registrů veřejné správy, jako je katastr nemovitostí, obchodní nebo živnostenský rejstřík, registr evidence obyvatel, insolvenční rejstřík apod. V oblasti soukromoprávní se pak jedná o zákon o bankách, zákon o pojišťovnictví, zákon o zdravotních službách i zákoník práce.[29]

Ochranu osobních údajů reflektuje i české trestní právo, kdy v trestním zákoníku[30] stanoví v § 180 skutkovou podstatu trestného činu neoprávněného nakládání s osobními údaji. Toho se dopustí ten, kdo, byť i z nedbalosti, neoprávněně zveřejní, sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje, které byly o jiném shromážděné v souvislosti s výkonem veřejné moci, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají, bude potrestán odnětím svobody až na tři léta nebo zákazem činnosti. Ve druhém odstavci tohoto ustanovení je obsažena druhá skutková podstata, podle které hrozí stejný trest tomu, kdo, byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce, a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají. Ustanovení obsahuje další dva odstavce tzv. kvalifikovaných skutkových podstat, dle kterých se trestní sazba za tento trestný čin zvyšuje, např. s rostoucí způsobenou škodou.

Velmi nevyjasněný je vztah mezi odpovědnostní právnických osob za výše uvedené jednání dle trestního práva[31], a zda by v těchto případech nepostačovaly prostředky správního práva.[32]

1.5 Mezinárodní hledisko ochrany osobních údajů

1.5.1 Evropská úprava

Evropský, resp. mezinárodní charakter ochrany osobních údajů je zdůrazněn již v ustanovení § 1 ZOÚ, který mluví o souladu s právem Evropských společenství a s mezinárodními smlouvami. V roli *„ústavního nástroje evropského pořádku“*[33] byl a nadále

[29] KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů – komentář.* Praha: Nakladatelství C. H. Beck, 2012. s. 2
[30] zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
[31] zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů
[32] NONNEMANN, František. *Trestní odpovědnost právnické osoby za neoprávněné nakládání s osobními údaji,* Právní rozhledy 20/2016, s. 697
[33] Rozsudek Velkého senátu ESLP ze dne 30. června 2005, *Bosphorus Hava Yollari Turizm ve Ticaret Anonim Şirketi v. Ireland* (stížnost č. 45036/98)

zůstává dokument Rady Evropy s názvem Úmluva o ochraně lidských práv a základních svobod (dále jen „Úmluva“). O ochraně soukromí pojednává čl. 8 Úmluvy. Úmluva od počátku své existence sjednocuje minimální standard ochrany základních práv v Evropě. V tomto ohledu plní funkci skutečné evropské ústavy základních práv a ESLP jako roli soudu ústavního.[34] Stejně jako vnitrostátní ústavy, i Úmluva je „živoucím dokumentem“, vykládaným s ohledem na a v kontextu dynamiky základních práv v Evropě.[35]

Mezi právní základy ochrany osobních údajů v EU patří čl. 16 Smlouvy o fungování Evropské unie[36] a čl. 7 a 8 Listiny základních práv Evropské unie[37]. Kromě již zmíněné Směrnice Evropského parlamentu a Rady Evropské unie 95/46/ES je rozhodně nejvíce skloňovaným dokumentem poslední doby v oblasti ochrany osobních údajů nařízení GDPR. Evropská unie ho definitivně přijala až po několikaletém vyjednávání a nařízení vstoupilo v platnost dne 24. května 2016.[38] Důvodem pro přijetí nového a přímo účinného předpisu byl bezesporu nárůst přeshraničních toků osobních údajů, rychlý technologický rozvoj a globalizace, jak ostatně tvrdí i GDPR v bodech 5 až 7 svého recitálu.[39]

Členské státy a osoby, jichž se úprava bude týkat, dostaly k dispozici poměrně dlouhou dvouletou legisvakanční dobu a GDPR vstoupí do účinnosti ke dni 25. května 2018. Dosavadní Směrnice bude s účinností GDPR zrušena a dosavadní národní zákony budou zrušeny. Odstraní se tak rozdíly v právní regulaci ochrany osobních údajů v členských státech EU, která se nyní v mnohém liší, přestože je ochrana osobních údajů harmonizována Směrnicí.

GDPR si klade za cíl, aby stejná pravidla v něm obsažená platila i pro subjekty (nyní nemyšleno jako dotčené osoby ochrany osobních údajů dle GDPR, ale obecně) ve vztahu ke třetím zemím a mezinárodním organizacím. Dosavadní Směrnice obsahuje úpravu předávání v čl. 25 až 26, kdy stanovila, že předání je možné pouze, *„pokud dotyčná třetí země zaručí odpovídající úroveň ochrany“*. Ta je zajištěna buď právními předpisy nebo mezinárodními závazky.[40]

---

[34] WAGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch., LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer, 2012. s. 33

[35] Rozsudek ESLP ze dne 15. března 1978, *Tyrer v. United Kingdom* (stížnost č. 5856/72)

[36] 2012/C 326/01 Smlouva o fungování Evropské unie. Úř. věst. C 326, 26. října 2012, s. 47 a násl.

[37] 2012/C 326/02 Listina základních práv Evropské unie. Úř. věst. C 326, 26. října 2012, s. 391 a násl.

[38] KARTNER, Martin, PROUZA, Jiří. *Evropská unie schválila konečnou podobu obecného nařízení o ochraně osobních údaj* [online]. epravo.cz, 15. června 2016 [cit. 8. února 2018]. Dostupné na <https://www.epravo.cz/top/clanky/evropska-unie-schvalila-konecnou-podobu-obecneho-narizeni-o-ochrane-osobnich-udaju-101825.html>.

[39] MILT, Kristiina. *Fakta a čísla o Evropské unii - Ochrana osobních údajů* [online]. europarl.europea.eu., únor 2017. Dostupné na <http://www.europarl.europa.eu/atyourservice/cs/displayFtu.html?ftuId=FTU_4.2.8.html>.

[40] BURIAN, David, RADIČOVÁ, Zuzana. *Mezinárodní předávání osobních údajů z pohledu nové regulace ochrany osobních údajů* [online]. pravniprostor.cz, 13. dubna 2016 [cit. 8. února 2018]. Dostupné na

V článcích 44 až 50 GDPR rozšiřuje podmínky pro předávání osobních údajů, a to konkrétně na základě rozhodnutí o odpovídající ochraně nebo na vhodných zárukách. Dále jsou v této kapitole obsaženy závazná podniková pravidla a samozřejmě i taxativní výčet výjimek z podmínek pro předávání. Za účelem prohlášení o dostatečných zárukách vydává Komise „rozhodnutí o odpovídající ochraně osobních údajů" v příslušných zemích (např. Švýcarsko, Argentina, Kanada). Provozovatelé sociálních sítí, které jsou vystavěny skoro bezvýhradně na osobních údajích, běžně shromažďují a ukládají tyto údaje ve svých domovských zemích, nejčastěji v USA. USA ale nejsou považovány za zemi s odpovídající ochranou osobních údajů, a proto s nimi byla uzavřena dohoda, jejímž předmětem je umožnit volné předávání osobních údajů ze zemí EU do USA, pokud se na straně příjemce jedná o společnosti zařazené na tzv. Safe Harbor List, který vede Ministerstvo obchodu Spojených států amerických. Podrobnosti byly uvedeny v rozhodnutí Evropské komise č. 520/2000/ES[41]. Společnosti zařazené do Safe Harbor List by měly splňovat stejné standardy ochrany osobních údajů, jaké platí v EU. Proto byl seznam veřejně přístupný[42] a každý si mohl ověřit zapsání příslušné společnosti a platnost její certifikace. Tento seznam dovoloval předávání osobních údajů do USA pro více jak tři tisíce společností, jakými jsou např. Google, Facebook nebo Apple.[43] Nicméně Soudní dvůr Evropské unie v říjnu 2015 označil celé rozhodnutí Komise č. 520/2000 za neplatné právě v návaznosti na přípravu GDPR a v důsledku sporu Maximillian Schrems vs. Data Protection Commissioner[44]. O obsahu tohoto sporu pojednává kapitola 3.5.3.

Vedle Směrnice a nařízení GDPR se podílely v průběhu existence Evropských společenství na ochraně osobních údajů i další dokumenty. Jedná se o Směrnici 200/31/ES o určitých aspektech služeb informační společnosti, zejména elektronického obchodního styku v rámci vnitřního trhu (více o problematice nevyžádaných obchodních sdělení v kapitole 2.4). Dále se jedná o Směrnici Evropského parlamentu a Rady 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (tato směrnice byla změněna Směrnicí Evropského parlamentu a Rady 2006/24/ES o uchovávání údajů vytvářených nebo

<https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/mezinarodni-predavani-osobnich-udaju-z-pohledu-nove-regulace-ochrany-osobnich-udaju>.

[41] Rozhodnutí Komise 2000/520/ES ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad bezpečného přístavu a s tím souvisejících často kladených otázek vydaných Ministerstvem obchodu Spojených států. Úř. věst. L 215, 25. srpna 2000, s.7 a násl.

[42] U.S.-Swiss Safe Harbor pro předávání osobních údajů mezi USA a Švýcarskem nadále platí. Dostupné na <https://www.export.gov/safeharbor_swiss>.

[43] KENNEDY, John. *The Interview: Max Schrems, privacy activist* [online]. Siliconrepublic.com, 28. ledna 2015 [cit. 15. února 2018]. Dostupné na <https://www.siliconrepublic.com/enterprise/the-interview-max-schrems-privacy-activist-video>.

[44] Rozsudek ze dne 6. října 2015, *Maximillian Schrems vs. Data Protection Commissioner, Digital Rights Ireland Ltd*, C-362/14, zveřejněný v elektronické Sbírce rozhodnutí.

zpracovávaných v souvislosti s poskytováním dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně Směrnice 2002/58/ES, a také Směrnicí Evropského parlamentu a Rady 2009/136/ES, kterou se mění Směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací). Také je dlužno zmínit Nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele, Rámcové rozhodnutí Rady 2008/977/SVV o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech a Doporučení Komise 2009/387/ES o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence.[45]

Snahu založit přesah ochrany i mimo Evropskou unii velice vítám, zejména z důvodu, který souvisí s tématem této práce. V prostředí internetu osobní údaje obíhají planetu v neuvěřitelném množství a rychlosti, zejména mezi obřími korporacemi v čele s nadnárodními e-shopy a sociálními sítěmi. Bohužel si nemyslím, že se tato snaha setká s velkým úspěchem, neboť pravomoci EU vůči subjektům z nečlenských zemí jsou velice omezené, často skoro nulové.

1.5.2 Mezinárodní smlouvy

Safe Harbor byl v důsledku rozhodnutí Soudního dvora EU o zrušení rozhodnutí Komise č. 520/2000 zrušen. Rezort obchodu USA proto vypracoval jako jeho náhrady tzv. EU-U.S. a Swiss-U.S. Privacy Shield Framework, které slouží také k poskytnutí záruk při předávání osobních údajů z EU a Švýcarska do USA. 12. ledna 2017 byl schválen Švýcarskem a stejně tak 12. července 2017 vyslovila Evropská komise adekvátnost tohoto programu ze strany EU. Privacy Shield je řízen International Trade Administration v rámci amerického rezortu obrany a umožňuje společnostem se sídlem v USA přidat se do jednoho nebo obou z těchto programů. Veřejným a dobrovolným závazkem řídit se požadavky programu pro společnost začíná platit americké právo na ochranu osobních údajů.[46]

V průběhu roku 2017 byla pro program Privacy Shield předjímána nejistá budoucnost z důvodu směřování americké legislativy směrem k podpoře dohledu pod vedením prezidenta

[45] KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů – komentář.* Praha: Nakladatelství C. H. Beck, 2012. s. 3

[46] Privacy Shield Program Overview [online]. Dostupné na < https://www.privacyshield.gov/Program-Overview>.

Trumpa.[47] K březnu 2018 je Privacy Shield soudně napaden a čeká se na posouzení přípustnosti žalob.[48]

[47] ALLISON, Matt. *A Template for Adequacy: EU Pitches for Data Protection Gold Standard*. [online]. circleid.com, 9. února 2017 [cit. 19. března 2018]. Dostupné na <http://www.circleid.com/posts/20170209_template_for_adequacy_eu_pitches_for_data_protection_gold_standard/>.

[48] Žaloby *Digital Rights Ireland v Commission* (T-670/16), *La Quadrature du Net and Others v Commission* (T-738/16).

2. NAKLÁDÁNÍ S OSOBNÍMI ÚDAJI NA INTERNETU

2.1 Problematika poskytnutí souhlasu se zpracováním na internetu

Z nauky ústavního práva je známo, že základní práva (včetně práva na soukromí) jsou nezadatelná a nezcizitelná[49]. Těžko by ale dnes někdo namítal, že nemůže uzavřít smlouvu, kterou se vzdává části svého práva na ochranu soukromí. Pravda je taková, že je tento stav zcela běžným jevem v pracovních smlouvách, smlouvách s mobilními operátory, smlouvách s poskytovateli služeb informační společnosti a smlouvách o užívání kreditních karet. Obvykle je vzdávání se těchto práv postaveno na dobrovolnosti, často je ale rozsah poskytnutých údajů rozšířen za účelem zkvalitnění poskytovaných služeb, a to daleko za míru nezbytně nutnou k plnění předmětu smlouvy druhou stranou.

V případě smluv uzavíraných online bývá vzdání se části ochrany soukromí nazýváno různě, často jako „licenční smlouvy s koncovým uživatelem, „lhůty a podmínky“ nebo jen „podmínky“. Jejich obsah může být zobrazen v podobě tzv. „clickwrap“ smluv, tedy smluv odsouhlasených kliknutím na políčko „souhlasím“, nebo jim podobných „browsewrap“ smluv, které se považují za uzavřené pouhým procházením určitých stránek (objeví se oznámení ve spodní části stránky, které uživatele zaváže k dodržování podmínek a jeho souhlas se považuje za udělený, pokud stránku dále prochází), a případně i tzv. „cookiewrap“ smluv, kdy se souhlas uživatele ukládá v podobě cookies a použije se při další návštěvě stránek. Více o pojmu cookies v následující kapitole č. 2.2.

2.2 Pojem tzv. *„cookies“* a obdobných dat o uživatelích internetu

V knize Právo v síti: průvodce právem na internetu[50] jsou osobní údaje velice příhodně přirovnávány k jakési virtuální měně, kterou je v internetovém prostředí placeno za zdánlivě bezplatné služby. Přístupem k internetu vytváříme velké množství dat, která jsou tvořena především (ne-li výhradně) osobními údaji, a která o nás mohou mnoho prozradit. Tato data nemusí být a často ani nejsou přístupná jen nám. Některá z těchto dat jsou ukládána přímo do zařízení, které používáme pro přístup k internetu. Jsou využity při příští návštěvě webových stránek ukladatele a nazývají se cookies.

Jako cookie (anglicky koláček, oplatka, sušenka) se v protokolu HTTP označuje malé množství dat, které WWW server pošle prohlížeči, který je uloží na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru. Cookies běžně slouží

[49] PAVLÍČEK, Václav a kol., *Ústavní právo a státověda, II.díl*, 1. vydání, Olomouc: Leges 2011, s. 503 - 565
[50] DONÁT, Josef, TOMÍŠEK Jan. *Právo v síti: průvodce právem na internetu.* Vyd. 1. Praha. C.H. Beck, 2016, xi, s. 5

k rozlišování jednotlivých uživatelů, ukládají se do nich např. obsah „nákupního košíku“ v elektronických obchodech, uživatelské předvolby apod. Myšlenku cookies navrhl v 90. letech dvacátého století Lou Montulli, pracující tehdy u firmy Netscape Communications. O původu názvu cookies dlouho panovala nejistota.[51] Pravda ale byla vyřčena samotným vynálezcem internetových cookies jako název plynoucí z tzv. magic cookies, což byly kousky informací o provedení nějaké operace, které byly vytvořeny programátory systémů Unix počínaje sedmdesátými lety dvacátého století.[52]

Jak bylo uvedeno na začátku této kapitoly, dá se říci, že uživatelé platí za návštěvu a využívání většiny webových služeb a stránek právě daty cookies. Často je souhlasem k využívání cookies podmíněno samo využívání služby, a tak uživatel má při neochotě cookies poskytovat už jen jednu možnost – službu nevyužívat. Pokud není souhlas s ukládáním a využíváním cookies obsažen v podmínkách služeb (viz kapitola 2.1), používá se dnes snad všudypřítomná lišta umístěná většinou na horní či spodní okraj webové stránky, kde uživatel odklikne, že s využíváním cookies souhlasí. Aplikaci tohoto souhlasu jako čistě výstřední vtip lze nalézt na některých webových stránkách, která uvádí pouze, že „Tato lišta slouží k tomu, aby se lidé v Evropské unii naučili bezmyšlenkovitě odklikávat cokoli.“[53]

2.3 E-mailová a jiná internetová komunikace

2.3.1 Listovní tajemství

Kromě jednostranného působení jedince na internetu se logicky objevuje internetová komunikace mezi osobami a ochrana její důvěrnosti. Při posuzování případů ochrany listovního tajemství na internetu musíme vycházet především z čl. 13 Listiny, který stanoví, že *„nikdo nesmí porušit listovní tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí nebo zasílaných poštou, anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon“*. Výjimky jsou stanoveny zvláštními zákony, jako např. případy vyšetřování trestného činu. Stejná ochrana se zaručuje i tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným způsobem.

---

[51] Původ názvu cookies byl objektem několika teorií, např. asociaci zvyklosti ze Spojených států nebo Velké Británie nabídnout účastníkům při návštěvě určitého zájmového spolku nebo skupiny jejich oblíbenou sušenku pro vytvoření příjemnější atmosféry, slangový výraz pro žeton obdržený pro vyzvednutí určitého kusu oděvu v šatně (stejně jako se data cookies párují s konkrétním zařízením) nebo z malých čínských sušenek zvaných „fortune cookies“ (šťastné sušenky) podávaných v asijských zemích po hlavním jídle a obsahujících malý papírek se zprávou nebo věštbou (stejně jako data cookies obsahují krátké kousky informací o cílovém zařízení).
[52] STUART, Andrew. *Where do cookies come from* [online]. dominopower.com, 2. července 2002 [cit. 15. února 2018]. Dostupné na <http://dominopower.com/article/where-cookie-comes-from/>.
[53] V době psaní práce k vidění při navštívení např. <http://www.spr-rsc.cz/> či <https://phpfashion.com/>.

ESLP od rozsudku Klass proti Německu[54] (který podporuje další judikatura ESLP, např. rozsudek Malone proti Spojenému království[55], rozsudek Kruslin proti Francii[56] a další), v němž šlo o telefonní odposlechy a jejich záznamy, rozšířil dopad práva na soukromí na všechny další způsoby komunikace, které jsou vnitrostátně regulovány podobným způsobem, jako tradiční dopisní přeprava. Chráněna je tak komunikace prováděná mailem, přes pager a další.[57]

Dále listovní tajemství chrání i trestní zákoník v ustanovení § 182, když stanoví, že trestného činu porušení tajemství dopravovaných zpráv se dopustí ten, *„kdo úmyslně poruší tajemství uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením, datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníkovi nebo uživateli, který zprávu přijímá, nebo neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového sytému, přenášející taková počítačová data"*. Stejně jako pachatel tohoto trestného činu bude potrestán ten, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu, telefonního hovoru nebo přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo takového tajemství využije. Z výše uvedeného plyne podstatný závěr pro téma této práce, a to sice že tato ochrana se nevztahuje pouze na přenos písemností, ale i na jakýkoliv neveřejný přenos dat na internetu.

S tímto závěrem pracuje i judikatura, kdy *„přečinu porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b) trestního zákoníku se lze dopustit již tím, že poškozený je v důsledku neoprávněného zásahu pachatele zcela vyloučen z dispozice s obsahem své e-mailové schránky, přičemž se k trestní odpovědnosti za citovaný přečin nevyžaduje, aby se s tímto obsahem seznámila kromě pachatele i další osoba"*[58]. Při nahlédnutí do občanského práva zjistíme, že z ustanovení § 562 odst. 1 OZ plyne, že i elektronická komunikace je písemností a na její ochranu slouží ustanovení § 86 OZ o ochraně písemností osobní povahy.

[54] Rozsudek ESLP ze dne 6. září 1978, *Klass and others v. Germany* (stížnost č. 5029/71)
[55] Rozsudek ESLP ze dne 2. srpna 1984, *Malone v. The United Kingdom* (stížnost č. 8691/79)
[56] Rozsudek ESLP ze dne 24. dubna 1990, *Kruslin v. France* (stížnost č. 11801/85)
[57] WAGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch., LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer, 2012
[58] Usnesení Nejvyššího soudu ČR ze dne 16. listopadu 2016, sp. zn. 3 Tdo 1214/2016

2.3.2 Stanovisko Úřadu č. 2/2009

Otázku souborů přiložených k e-mailové zprávě upřesnil Úřad pro ochranu osobních údajů, stejně jako otázku monitoringu elektronické pošty obecně, svým Stanoviskem č. 2/2009[59] nazvaným Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště (dále jen „Stanovisko“). Zde se uvádí, že *„elektronické dokumenty (např. soubory typu docx, xlxs, pdf či jpeg) jsou písemností, byť nejsou listinami. Proto pro ně platí stejná pravidla jako pro ostatní písemnosti“.*

Dle Stanoviska je-li složena e-mailová adresa ze jména a příjmení zaměstnance (např. jan.novak@domena.cz), je e-mail doručený na ni vždy soukromou elektronickou poštou a adresa sama o osobě vždy osobním údajem. Ke zpracování tohoto osobního údaje je ale zaměstnavatel oprávněn. Oproti tomu věcně složená adresa jako např. info@domena.cz, objednavky@domena.cz nebo stiznosti@domena.cz je úřední elektronickou adresou, a to i v případě, že jí spravuje pouze jeden zaměstnanec.

Dále Stanovisko uvádí, že zaměstnavatel také nesmí sledovat, zpracovávat a monitorovat obsah korespondence svých zaměstnanců, ale pouze počet došlých a odeslaných e-mailů včetně hlavičky (tedy odesílatele a adresáta), zejména pokud vznikne podezření ze zneužití pracovních prostředků nebo využití k jiným než pracovním účelům.

2.3.3 Kontrola zaměstnanecké elektronické pošty

Na otázku, zda je soukromá zpráva doručená zaměstnanci pomocí elektronické komunikační sítě i po doručení soukromou, nám odpoví bod 24 recitálu Směrnice Evropského parlamentu a Rady z roku 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, kterou Česká republika promítla do svého právního řádu před vstupem do EU[60]. Zde je řečeno, že *„koncové zařízení uživatelů elektronických komunikačních sítí a jakékoliv informace uchovávané na takovém zařízení tvoří součást soukromí uživatelé, které je chráněno v souladu s Evropskou úmluvou na ochranu lidských práv a základních svobod. Tzv. špehovací software, webové štěnice, skryté identifikátory a jiné podobné nástroje mohou pronikat do koncového zařízení uživatele bez jeho vědomí s cílem získat přístup k informacím, uchovávat skryté informace nebo sledovat činnost uživatele a mohou vážně narušit soukromí těchto uživatelů. Použití takových nástrojů by mělo být povoleno pouze k oprávněným účelům s vědomím uživatelů, kterých se dotýká“*. Ve smyslu této Směrnice je

[59] https://www.uoou.cz/files/stanovisko_2009_2.pdf
[60] Seznam zákonů a novel zákonů provádějících tuto směrnici dostupný na <http://eur-lex.europa.eu/legal-content/CS/NIM/?uri=CELEX:32002L0058>.

uživatelem jakákoli fyzická osoba používající veřejnou elektronickou komunikační službu pro soukromé či obchodní účely, přičemž není nezbytně nutné, aby byla účastníkem této služby.

Český zákoník práce[61] (dále jen „ZP“) obsahuje zákaz sledování a kontroly zaměstnance zaměstnavatelem v ustanovení § 316 odst. 2, kdy *„zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci“*.

Proti této ochraně soukromí zaměstnance stojí právo zaměstnavatele sledovat u svých zaměstnanců dodržování pracovní doby a jejího využití. Doktor Bartík a doktorka Janečková uzavírají, že pokud by zaměstnavatel svou činností systematicky monitoroval e-mailovou komunikaci svých zaměstnanců a získané údaje by dále zpracovával, jednalo by se o zpracování osobních údajů ve smyslu ZOÚ a tento zákon by na tuto situaci v plném rozsahu dopadal. V případě, že by zaměstnavatel elektronickou poštu zaměstnance jen nahodile prohlédl (např. z důvodu dlouhodobé nepřítomnosti nebo nemoci zaměstnance a potřeby vyřídit pracovní korespondenci), pak by se o zpracování osobních údajů a porušení citovaného ustanovení § 316 odst. 2 ZP zřejmě nejednalo. Stále by ale mohlo dojít k zásahu do listovního tajemství a do rodinného a soukromého života dle čl. 10 odst. 2 Listiny.[62]

Jedná se dnes o zcela běžnou praxi, že zaměstnanci užívají firemní e-maily také pro své soukromé účely, stejně jako je tomu u firemních telefonů nebo automobilů. Striktní zákazy pravděpodobně nejsou nejlepším řešením. Řešení tohoto problému lze nalézt pravděpodobně pozorováním praxe a snahou stanovovat průběžně mantinely pro řádné jednání zaměstnavatelů a zaměstnanců. Ideálním východiskem se jeví firemní přístup k monitorování soukromé korespondence zaměstnanců, včetně monitorování e-mailů stanovený zaměstnavatelem v interním předpise nebo v pracovní smlouvě.[63]

Příkladem může být stanovisko britského regulátora osobních údajů Information Commissioner's Office s názvem The Employment Practises for Data Protection Code: Part 3: Monitoring at Work[64], podle nějž je vhodné stanovit okolnosti, za jakých je zaměstnanec

[61] zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
[62] BARTÍK, Václav, JANEČKOVÁ, Eva. *Ochrana osobních údajů v aplikační praxi: (vybrané otázky)*. Praha: Linde Praha, 2009, s. 145
[63] LOEBL, Zbyněk, HAJNÝ, Filip, FRYNTOVÁ, Jarmila. *Monitorování e-mailů zaměstnanců* [online]. epravo.cz, 12. prosince 2003 [cit. 11. února 2018]. Dostupné na <https://www.epravo.cz/top/clanky/monitorovani-e-mailu-zamestnancu-22444.html>.
[64] https://www.igt.hscic.gov.uk/KnowledgeBaseNew/ICO%20Employment%20Practices%20Code_Part3-Monitoring%20at%20Work.pdf

oprávněn užívat prostředky zaměstnavatele k soukromým účelům. Stejně tak je možné upřesnit i rozsah a typ užívání, např. zákaz mezinárodních hovorů, vymezení rozsahu prohlížení internetu nebo povinnost označování soukromých e-mailů.

2.4 Zasílání obchodních sdělení

K využívání internetové komunikace se pojí i poskytování obchodu a služeb. Právě nabídky takových služeb jsou značně ulehčeny, pokud poskytovatel služeb získá osobní údaje osob za účelem jejich kontaktování. Zákonodárce proto reagoval přijetím zákona o některých službách informační společnosti a o změně některých zákonů[65](dále jen „ZInfS“), kterým byla do českého právního řádu transponována Směrnice 2000/31/ES o elektronickém obchodu[66]. Šíření tohoto obsahu elektronickými prostředky je upraveno v ustanovení § 7 ZInfS. Je také nutné uvést, že ZInfS se vztahuje i na činnost obchodních zástupců, která spočívá v kontaktování potenciálních zájemců v nemasovém měřítku. Tudíž masovost není kritériem ZInfS a i odeslání jediného nevyžádaného obchodního sdělení je porušením zákona.[67]

Pokud poskytovatel získá osobní údaje jako jméno nebo datum narození či jiný významný datum subjektu osobního údaje, neváhá jej kontaktovat např. s přáním k svátku, narozeninám či na ples společnost. Ale i zdánlivě nevinná zpráva ovšem spadá do tzv. sdělení k podpoře image dle § 2 písm. f) ZInfS.

Podle hlavního dělení ZInfS na „neklienty“ a „klienty“ se také liší možnosti zasílání obchodních sdělení.[68] U neklientů je možno zasílat obchodní sdělení pouze po jejich souhlasu a u této skupiny se tedy využívá tzv. opt-in systém. Nabídka neklientovi tedy musí být formulována pouze jako žádost o zasílání obchodních sdělení bez znaků samotného obchodního sdělení dle § 2 písm. f) ZInfS. U klientů je naopak nastavený opačný systém tzv. opt-out jako u klasického marketingu dle § 5 odst. 5 až 9 ZOÚ. Tento systém funguje tak, že pokud poskytovatel získá osobní údaje spočívající v kontaktu elektronické komunikace na zákazníka v souvislosti s prodejem nebo poskytnutí služby a v souladu s ochranou osobních údajů dle zvláštního předpisu, může zákazníkovi bez jeho souhlasu zasílat obchodní sdělení související

[65] zákon č. 450/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů
[66] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)
[67] BARTÍK, Václav, JANEČKOVÁ, Eva. *Ochrana osobních údajů v aplikační praxi: (vybrané otázky)*. Praha: Linde Praha, 2009, s. 209
[68] OTEVŘEL, Petr. *Spamming a některé otázky šíření obchodních sdělení.* [online]. pravoit.cz, 12. srpna 2008 [cit. 11. února 2018]. Dostupné na <http://www.pravoit.cz/novinka/spamming-a-nektere-otazky-sireni-obchodnich-sdeleni>.

nebo týkající se obdobného plnění. To ale za předpokladu, že má zákazník v každé jednotlivé zprávě jasnou a zřetelnou možnost, zdarma na účet poskytovatele odmítnout souhlas s takovým využití svého elektronického kontaktu.[69]

Lze se setkat s častou argumentací některých společností, které tvrdí, že v seznamu e-mailových adres, které získají z otevřených zdrojů na internetu nebo nákupem databází, nevedou jméno a příjmení. Argumentace spočívající v tvrzení, že se v tomto případě nejedná o osobní údaj je dle dr. Bartíka a dr. Janečková chybná, neboť osobním údajem může být v závislosti na souvislostech jakýkoli údaj.[70] Plně se ztotožňuji s tímto vysloveným názorem, neboť se v tomto případě jedná o e-mailové adresy vztažené k určitým osobám, které jsou předmětem obchodního zájmu. Buď e-mailová adresa osoby obsahuje její jméno a příjmení a není zde o povaze údaje sporu. V druhém případě jméno a příjmení neobsahuje a je identifikovatelná nepřímo, např. jen určitým okruhem osob. ZOÚ nestanovuje, pro koho musí být osoba identifikovatelná, a tedy i v tomto případě nepřímé identifikovatelnosti je e-mailová adresa osobním údajem s jeho patřičnou ochranou.

3. ČINNOST ORGÁNŮ CHRÁNÍCÍCH OSOBNÍ ÚDAJE

3.1 Úřad pro ochranu osobních údajů

Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“ nebo „Úřad“) byl zřízen ke dni 1. června 2000 ustanovením § 2 odst. 1 ZOÚ. Zbytek ustanovení o Úřadu jako např. jeho postavení a působnost jsou obsažené dále v hlavě IV ZOÚ (ustanovení § 28 a násl.). Úřad vznikl přeměnou dosavadního odboru ochrany osobních údajů Úřadu pro státní informační systém (ÚSIS). Zbytek Úřadu pro státní informační systém byl přejmenován na Úřad pro veřejné informační systémy (ÚVIS) a později začleněn do Ministerstva informatiky.[71]

Zástupci ÚOOÚ se ve velké míře angažují v nezávislé poradní skupině Evropské komise složené z předsedů dozorových úřadů pro ochranu osobních dat, tzv. Working Party 29 pojmenované podle článku 29 Směrnice 95/46/EC, kterým byla zřízena. Z WP29 se s účinností nařízení GDPR stane tzv. European Data Protection Board (EDPB). Tato skupina dále obsahuje 8 podskupin zaměřených na dílčí témata ochrany soukromí a osobních údajů. Jedna z těchto

[69] BARTÍK, Václav, JANEČKOVÁ, Eva. *Ochrana osobních údajů v aplikační praxi: (vybrané otázky)*. Praha: Linde Praha, 2009, s. 212
[70] tamtéž, s. 211
[71] *Historie Úřadu pro ochranu osobních údajů* [online]. uoou.cz [cit. 8. prosince 2017]. Dostupné na <https://www.uoou.cz/historie%2Duradu%2Dpro%2Dochranu%2Dosobnich%2Dudaju/ds-1061/archiv=0&p1=1059>.

skupin jménem Technology Subgroup se v současné době věnuje právě vývoji technologických a internetových opatření ochrany jako jsou např. Do Not Track standardy, získávání informací a udělování souhlasů na chytrých zařízeních, e-Privacy Directive nebo Digital Single Market.[72]

Činnosti Úřadu jsou vymezeny v ustanoveních § 35 a násl ZOÚ, která popisují registr, výroční zprávu Úřadu, oprávnění a povinnosti kontrolujících a ukládání pořádkových pokut. Úřad je dále zákonem zmocněn k vedení klasického správního řízení ve věcech ochrany osobních údajů dle § 2 odst. 2 a § 46 ZOÚ ve spojení s § 10 správního řádu[73]. V těch jsou možnosti trestání (udělení pokuty) rozděleny dle kategorií na maximální hranici 100.000,- Kč (porušení mlčenlivost), 1.000.000,- Kč (jiné porušení jako např. zpracování osobních údajů bez souhlasu subjektu nebo nestanovení účelu zpracování) a dokonce 5.000.000,- Kč za předchozí porušení při ohrožení většího počtu osob nebo porušení povinnosti při zpracování citlivých údajů.

Objem činností Úřadu významně roste, jak lze vypozorovat z oficiálních čísel. Z výročních zpráv Úřadu vyplývá, že v roce 2007 přijal mimo jiné celkem 574 podnětů dle ZOÚ. V roce 2017 to bylo už 1684 podnětů.[74] Za posledních 10 let činnosti se tedy počet přijatých podnětů dle ZOÚ každým rokem zvyšoval, a celkem se téměř ztrojnásobil.

3.2 Ústavní soud ČR

3.2.1 Kolize základních práv

Samozřejmostí je, že právo na ochranu osobnosti a soukromého života se může a často bude dostávat do střetu s jinými základními právy. Především je právo na soukromí stavěno do kolize s právem na informace. K tomuto střetu uvedl Ústavní soud ČR, že *„při střetu práva na informace a jejich šíření s právem na ochranu osobnosti a soukromého života, tedy základních práv stojících na stejné úrovni, je především věcí obecných soudů, aby s přihlédnutím k okolnostem každého případu zvážily, zda jednomu právu nebyla bezdůvodně dána přednost před právem druhým“*[75]. To znamená, že Ústavní soud provádí při střetu těchto práv tzv. test proporcionality, který byl odvozen z principu materiálního právního státu[76].

---

[72] *The WP29 will become the EDPB – but what does that mean?* [online]. iabeurope.eu, 25. července 2016 [cit. 8. prosince 2017]. Dostupné na <https://www.iabeurope.eu/policy/data-protection/the-wp29-will-become-the-edpb-but-what-does-that-mean/>.

[73] zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů

[74] Výroční zprávy za jednotlivé roky dostupné na <https://www.uoou.cz/vyrocni-zprava/ds-2089/p1=2089>.

[75] Nález Ústavního soudu ze dne 2. února 1998, sp. zn. IV. ÚS 154/97 (N 17/10 SbNU 113). Dostupné na www.nalus.usoud.cz, shodně Usnesení Nejvyššího soudu ze dne 28. června 2007, sp. zn. 30 Cdo 664/2007

[76] Rozhodnutí německého Spolkového ústavního soudu 2 BvR 933/82, BVerfGE 76, 256 (359)

Při řešení takového střetu je stěžejní role státu, v našem případě jednajícího skrze soudy. Stát má povinnost nejen základní práva respektovat, ale rovněž zajišťovat jejich realizaci. Druhá jmenovaná povinnost znamená, že proti sobě nestojí jen dvě osoby, jejichž základní práva kolidují, ale je vytvořena trojúhelníková konstelace, v níž má stát povinnost poskytnout ochranu oběma právům.[77] Tuto ochranu poskytuje pomocí poměřování za použití výše zmíněného testu proporcionality, který se skládá ze tří kroků a to:

(a) vhodnost (způsobilost),

(b) potřebnost (nutnost)

(c) proporcionalita v užším smyslu (v poslední době po Evropě nazývána jako únosnost nebo spravedlivá požadovatelnost)[78].

3.2.2 Případ tzv. data retention

Pro přiblížení ochrany osobních údajů Ústavním soudem se pokusím stručně rozebrat problematiku uchovávání dat o telefonních a datových přenosech (SMS, e-mail) z databází soukromých telefonních společností a mobilních operátorů, které je běžně nazýváno z angličtiny jako data retention. Právně bylo data retention zakotveno přijetím směrnice č. 2006/24/ES o uchování dat[79], jež byla následně transponována do jednotlivých právních řádů členských států EU. V ČR se jednalo o § 97 zákona o elektronických komunikacích[80] a prováděcí vyhlášku o rozsahu provozních a lokalizačních údajů[81]. Ustanovení § 97 odst. 3, ukládal poskytovatelům internetového připojení uchovávat provozní a lokalizační údaje po dobu šesti měsíců. Současně zákon ukládal 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[82], Bezpečnostní informační službě, Vojenskému zpravodajství a České národní bance.

---

[77] WAGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch., LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer, 2012. s. 29

[78] tamtéž, s. 27

[79] Směrnice Evropského parlamentu a Rady č. 2006/24/ES ze dne 15. března 2006, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí (směrnice o uchovávání údajů). Úř. věst. L 105, 13. dubna 2006, s. 54 a násl.

[80] zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů

[81] vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchování a formě a způsobu jejich předávání orgánům oprávněných k jejich využívání, ve znění pozdějších předpisů

[82] zákon č. 273/2008, o Policii ČR, ve znění pozdějších předpisů.

Tato směrnice umožňovala preventivní a bezdůvodné uchovávání dat v délce 6 měsíců při podezření z možného spáchání v ní vyjmenované „závažné“ trestné činnosti. Proto se směrnice stala po celé Evropě terčem kritiky a byla předmětem několika řízení před ústavními soudy členských států, včetně českého Ústavního soudu[83], který zrušil ustanovení § 97 odst. 3 a 4 zákona o elektronických komunikacích a celou vyhlášku o rozsahu provozních a lokalizačních údajů.[84] Nakonec i Soudní dvůr EU dne 8. dubna 2014 směrnici zrušil pro rozpor s právem na soukromí.[85]

Ústavní soud v řízení o zrušení výše uvedených ustanovení citoval německý Spolkový ústavní soud, který při posouzení ústavnosti zákonné úpravy procesu sběru a uchovávání dat za účelem sčítání lidu (Volkszählung) mimo jiné konstatoval, že „*v moderní společnosti, charakterizované i obrovským nárůstem informací a dat, musí být ochrana jednotlivce před neomezeným sběrem, uchováváním, užitím a zveřejňováním dat o její/jeho osobě a soukromí poskytována v rámci obecnějšího, ústavně garantovaného práva jednotlivce na soukromí. Pokud jednotlivci nebude garantována možnost hlídat a kontrolovat obsah i rozsah osobních dat a informací jím poskytnutých, jež mají být zveřejněny, uchovány či použity k jiným než původním účelům, nebude-li mít možnost rozpoznat a zhodnotit důvěryhodnost svého potenciálního komunikačního partnera a případně tomu uzpůsobit i své jednání, pak nutně dochází k omezení až potlačování jeho práv a svobod, a nelze tak již nadále hovořit o svobodné a demokratické společnosti. Právo na informační sebeurčení (informationelle Selbstbestimmung) je tak nezbytnou podmínkou nejen pro svobodný rozvoj a seberealizaci jednotlivce ve společnosti, nýbrž i pro ustavení svobodného a demokratického komunikačního řádu. Zjednodušeně řečeno, v podmínkách vševědoucího a všudypřítomného státu a veřejné moci se svoboda projevu, právo na soukromí a právo svobodné volby chování a konání stávají prakticky neexistujícími a iluzorními*“[86].

Do zákona se ustanovení o uchování a zpřístupnění předmětných údajů dostalo v revidované podobě znovu. Ovšem i nyní se lze setkat s odbornými názory, že i v této podobě porušuje Listinu základních práv Evropské unie, především neobsahuje výjimku pro osoby

[83] KOSAŘ, David a kol. *Ústavní právo. Casebook.* Praha: Wolters Kluwer, a. s., 2014. s. 527
[84] Nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl.ÚS 24/10 (N 52/60 SbNU 625). Dostupné na www.nalus.usoud.cz
[85] Rozsudek Soudního dvora EU ze dne 8. dubna 2014 ve spojených věcech, *Digital Rights Ireland Ltd (C-293/12) proti Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irsku, The Attorney General, za přítomnosti: Irish Human Rights Commission, a Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl a další*, C-293/12 a C-594/12, zveřejněný v elektronické Sbírce rozhodnutí.
[86] rozhodnutí Spolkového ústavního soudu SRN ze dne 15. 12. 1983, BVerfGE 65, 1 (Volkszählungsurteil)

vázané profesním tajemstvím a nečiní rozdíl mezi osobami spojenými s trestnou činností a ostatními.[87]

3.3 Obecné soudy

I v českých reáliích se může stát, že se sociální sítě nebo internet obecně stanou prostředkem, který bude uživatelem použit (ať už úmyslně nebo neúmyslně) k narušení práv subjektů údajů. Následující rozbor se věnuje mediálně velmi sledovanému sporu, který se týkal zveřejnění fotografie zloděje vystřižené z kamerového video záznamu poškozeného podnikatele. Ačkoliv šlo o skutečného a potrestaného pachatele trestného činu, Úřad pro ochranu osobních údajů uložil poškozenému podnikateli pokutu z důvodu porušení příslušných ustanovení ZOÚ, podle kterých je správce povinen zpracovávat osobní údaje pouze k účelu, k němuž byly shromážděny, a dále z důvodu, že neoznámil Úřadu svůj záměr zpracovávat osobní údaje prostřednictvím kamerového systému před zahájením zpracování.

Podnikatel podal nejdříve rozklad proti rozhodnutí Úřadu k jeho předsedovi, a ten rozhodnutí úřadu a uložení pokuty potvrdil. Podnikatel tedy podal správní žalobu k Městskému soudu v Praze a požadoval zrušení rozhodnutí. Úřad argumentoval přípustností kamerového systému v prodejně za předpokladu, že nedochází k nepřetržitému sledování zaměstnanců ani k tomu, že provozovatel bude bez varování natáčet všechny osoby a *„dle svého úsudku označovat za zloděje nebo jinak nevhodné či závadné osoby“*. Přípustné dle Úřadu by bylo pouze předat záznamy Policii ČR, která je oprávněna podobiznu zveřejnit. Správní soud se s argumentací Úřadu neztotožnil a vycházel při tom z ustanovení § 5 odst. 2 písm e) ZOÚ a nezbytnosti zpracování bez souhlasu v případech ochrany práv a právem chráněných zájmů. Podnikatel chránil svůj majetek a na dveřích prodejny měl upozornění na střežení prostoru kamerovým systémem. Rozhodnutí Úřadu tedy správní soud zrušil a zdůraznil nutnost provedení testu proporcionality mezi ochranou osobních údajů a práva žalobce na ochranu vlastního majetku.[88] V návaznosti na podání kasační stížnosti spor projednal Nejvyšší správní soud, zrušil rozhodnutí správního soudu a vrátil mu věc k dalšímu řízení. Argumentoval přitom ohledně testu proporcionality následovně:

„ …za této situace není dán žádný prostor pro test proporcionality tak, jak ho provedl Městský soud v Praze. Za dané situace totiž k žádnému konfliktu mezi právem na ochranu majetku žalobce a právem na ochranu osobních údajů třetích osob nedochází a testem proporcionality není co poměřovat. Zákon sám totiž stanoví, kudy vedou hranice mezi právem na ochranu

[87] HARAŠTA Jakub, MYŠKA Matěj: *Budoucnost data retention,* Trestněprávní revue 10/2015, s. 238
[88] JANSA, Lukáš a kol. *Internetové právo*. Brno: Computer Press, 2016. s. 381

majetku na straně jedné a právem na ochranu osobních údajů na straně druhé. Právo na ochranu majetku je přitom dostatečně saturováno právem žalobce na instalaci a používání kamerového systému za zákonem stanovených podmínek a na případné další použití údajů získaných snímáním sledovaného prostoru státními orgány k tomu určenými. Jakékoliv další nakládání s osobními údaji takto shromážděnými bez souhlasu dotčených subjektů nelze ničím odůvodnit.“

Následně rozhodl Městský soud v Praze finálně a pravomocně jako soud vázaný výše uvedeným právním názorem Nejvyššího správního soudu velice kontroverzně tak, že žalobu v celém rozsahu jako nedůvodnou zamítl. [89]

3.4 Evropský soud pro lidská práva

ESLP se ve svých rozhodnutích opakovaně vyjádřil ve smyslu, že svou rozhodovací praxi staví na dynamické interpretaci Úmluvy[90], protože samy oblasti lidských práv, o kterých rozhoduje, prochází dynamickým vývojem.[91] Je vrcholně důležité, aby Úmluva byla vykládána a aplikována způsobem, který činí její práva praktickými a účinnými, nikoli teoretickými a iluzorními. Pokud by ESLP neudržoval dynamický a evolutivní přístup, hrozilo by, že by se stal překážkou reforem a vylepšení.[92]

K otázce tzv. dynamické IP adresy (neboli adresy internetového protokolu) jako osobního údaje se vyjádřil ESLP už v roce 2008. IP adresa jako unikátní číselná adresa počítače byla navržena tak, aby byl každý počítač v síti vybaven svou vlastní unikátní adresou. Při dnešním rozsahu a růstu internetu funguje určitý systém distribuce těchto adres. Od roku 1987 IP adresy přidělovalo jedno centrum spadající pod rezort obrany USA, dnes je to úkol celkem tří středisek po světě. Ty dostávají k dispozici větší bloky IP adres a ty dále přerozdělují dalším „přidělovatelům“ (např. lokálním poskytovatelům internetového připojení) a ti dále zajišťují distribuci v malém měřítku.[93] Dynamická IP adresa znamená, že je počítači přidělena jiná vždy, když navštíví webovou stránku. Na rozdíl od statické IP adresy není možné za použití pouze veřejně přístupných souborů vytvořit identifikovatelné propojení mezi počítačem uživatele a fyzickým připojením k síti poskytovatele internetu.[94]

---

[89] Rozsudek Městského soudu v Praze ze dne 25. srpna 2016, sp. zn. 11 A 77/2012
[90] Rozsudek ESLP ze dne 16. dubna 2002, *Société Colas Est and others v. France* (stížnost č. 37971/97)
[91] Rozsudek ESLP ze dne 3. listopadu 2011, *S. H. and others v. Austria* (stížnost č. 57812/00)
[92] Rozsudek Velkého senátu ESLP ze dne 11. července 2002, *Christine Goodwin v. The United Kingdom* (stížnost č. 28957/95)
[93] JANSA, Lukáš a kol. *Internetové právo*. Brno: Computer Press, 2016. s. 35
[94] DEMMEL, Annette. *IP Addresses Constitute Personal Data According to Court of Justice of European Union* [online]. natlawreview.om, 20. října 2016 [cit. 8. února 2018]. Dostupné na <https://www.natlawreview.com/article/ip-addresses-constitute-personal-data-according-to-court-justice-european-union>.

Ve věci *K. U. proti Finsku* (8. 12. 2008, stížnost č. 2872/02) ESLP rozhodl, že Finsko porušilo svůj závazek vyplývající z článku 8 Evropské úmluvy o ochraně lidských práv tím, že neposkytlo nezletilému chlapci K. U. a jeho otci efektivní prostředky, kterými by se mohli bránit proti neznámému pachateli, jehož bylo možné zjistit právě na základě jeho dynamické IP adresy. Skutkově šlo o situaci, kdy pachatel umístil na internetovou seznamku inzerát, prostřednictvím kterého uveřejnil jménem tehdy dvanáctiletého chlapce nabídku na seznámení s chlapcem ve stejném věku. Chlapec K. U. na inzerát přišel, když ho v reakci na falešný inzerát e-mailem kontaktoval cizí muž s nabídkou na seznámení. V daném případě poskytovatel internetového připojení odmítl při vyšetřování sdělit identitu uživatele dynamické IP adresy s odvoláním na tehdejší finská pravidla ochrany důvěrnosti elektronické komunikace. Na tomto případě jde vidět, kdy poprvé začal ESLP vnímat dynamickou IP adresu jako údaj, na jehož základě je možné dospět k identifikaci pachatele. Přitom ESLP logicky poznamenal, že ani svoboda projevu a důvěrnost elektronické komunikace není absolutní a v žádném případě nemůže působit na úkor práv a svobod druhých.[95]

3.5 Soudní dvůr Evropské unie

3.5.1 Google Spain v AEPD and Mario Costeja González (C-131/12)

K našemu každodennímu působení na internetu neodmyslitelně patří i používání internetových vyhledávačů, které používají tzv. fulltextové vyhledávání na bázi klíčových slov a indexují pro nás výsledky v podobě internetových stránek rozmístěných po internetu. Není proto divu, že může docházet (a už od dob zrození internetových vyhledávačů dochází) ke zneužívání klíčových slov v procesu vyhledávání. Společnosti jako např. Google LLC (v době sporu Google Inc., nyní vlastněný holdingovou společností Alphabet Inc.) provozují vyhledávače primárně za účelem zisku a zdroj tohoto zisku pramení z reklamy. Zneužíváním klíčových slov v reklamních systémech vyhledávačů řešil Soudní dvůr Evropské unie (dále jen „SDEU“ nebo „Soud“) již v případě Louis Vuitton[96]. Přelom v otázce soukromí a osobních údajů na internetu přivedl až rozsudek ve věci Google Spain[97].

---

[95] NEŠPŮREK, Robert. *Rozhodnutí Breyer a dynamická IP adresa jako osobní údaj* [online]. pravniprostor.cz, 24. května 2017 [cit. 8. února 2018]. Dostupné na <https://www.pravniprostor.cz/clanky/obcanske-pravo/rozhodnuti-breyer-a-dynamicka-ip-adresa-jako-osobni-udaj>.

[96] Rozsudek ze dne 23. března 2010, *Google France SARL, Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA, Luteciel SARL (C-237/08), a Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08),* C-236/08, C-237/08, C-238/08, Sb. rozh. s. I-02417

[97] Rozsudek ze dne 13. května 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* C-131/12, zveřejněný v elektronické Sbírce rozhodnutí.

Hlavní otázkou zde byla odpovědnost provozovatele vyhledávače v případě, že výsledky fulltextového vyhledávání odkazují na obsah, který se nachází na cizích internetových stránkách, a který obsahuje informace představující zásah do práva osob na jejich soukromí nebo na ochranu jejich osobních údajů.[98] Skutkově se jednalo o španělského občana pana Gonzálese a jeho dluh na sociálním pojištění, který vyústil v prodej jeho nemovitosti v dražbě. Tato skutečnost byla v souladu s místními právními předpisy uvedena v katalánském deníku La Vanguardia a v rámci internetových stránek tohoto deníku byla dlouhodobě dostupná. Dluhy pana Gonzálese byly výtěžkem z prodeje nemovitosti uhrazeny, nicméně ještě deset let po uhrazení dluhů prodejem nemovitosti byla tato informace v archivu deníku dostupná online. Po zadání jména pana Gonzálese byla mezi prvními výsledky ve vyhledávači Google. To nebyl ideální stav pro pana Gonzálese, který byl mimo jiné sám advokátem a jeho pověst pro něj měla obzvlášť velký význam.

Obrátil se proto na španělský úřad na ochranu osobních údajů (označovaný zkratkou „AEPD“) s žádostí o nařízení odstranění výše uvedených informací z internetových stránek deníku a tvrdil porušení jeho práva na ochranu osobních údajů. AEPD jeho žádost zamítl z důvodu oprávněného zveřejňování informací požadovaného nařízením ministerstva práce a sociálních věcí za účelem co nejširší informovanosti o dražbě. Španělsko má navíc zakotvenou zákonnou výjimku pro zpracování osobních údajů pro žurnalistické a literární účely, což výslovně umožňuje Směrnice č. 95/46. Pan Gonzáles se na AEPD obrátil s druhou žádostí, která směřovala tentokrát proti samotnému Googlu ve vztahu k výsledkům vyhledávání, konkrétně proti americké mateřské společnosti Google Inc. (dnes Google LLC) a její španělské pobočce Google Spain. AEPD vyslovil názor, že provozovatelé vyhledávačů jsou správci osobních údajů, protože tyto údaje zpracovávají a určují účel tohoto zpracování. Tímto závěrem se dále zabýval SDEU v žalobě proti rozhodnutí AEPD, kterou podal Google. Rozhodování o tomto sporu stálo na třech základních pilířích.

Za prvé se musel SDEU vypořádat s otázkou, zda je Google při práci s obsahem internetu při poskytování fulltextového vyhledávání správcem osobních údajů. S odkazem na svá dřívější rozhodnutí potvrdil, že samotní provozovatelé webových stránek, které Google následně indexuje, jsou správci osobních údajů. Google však tvrdil, že je v naprosto jiné pozici a nemůže být správcem osobních údajů, neboť informace zpracovává jako celek a ani neví a nemůže vědět o osobních údajích nacházejících se na indexovaných stránkách. Soud zde ale

[98] JANSA, Lukáš a kol. *Internetové právo*. Brno: Computer Press, 2016. s. 307

následujícím způsobem potvrdil názor vyslovený dříve AEPD a pozici Googlu jako správce osobních údajů. Soud zvolil velmi širokou definici „zpracování osobních údajů“ dle čl. 2 písm. b) Směrnice č. 95/46[99], které dle něj obsahují činnosti prováděné Googlem jako vyhledávání, uspořádávání, zaznamenávání, následné shromažďování, uchovávání a zpřístupňování třetím osobám (uživatelům vyhledávače). Jelikož provozovatel vyhledávače při své činnosti pracuje s osobními údaji a toto nemůže vyloučit, je nutno jej dle názoru Soudu považovat za správce osobních údajů se všemi patřičnými právy a povinnostmi.

Druhá klíčová otázka, se kterou se SDEU vypořádal, se týkala územní pravomoci AEPD vůči americké společnosti Google Inc. Mateřská společnost sice sama poskytuje v celém rozsahu vyhledávání a místní odnože se zakládají pouze za účelem podpory prodeje reklamy, ale Soud vzal opět velice striktně v potaz úzkou vazbu reklamy jako hlavního zdroje příjmů vyhledávače. Prostřednictvím takové podpůrné činnosti je prakticky v členském státě založena provozovna, skrze kterou je prováděno zpracování osobních údajů. Soud tedy uzavřel, že zpracování osobních údajů probíhá na území EU tak, jak požaduje Směrnice č. 95/46.

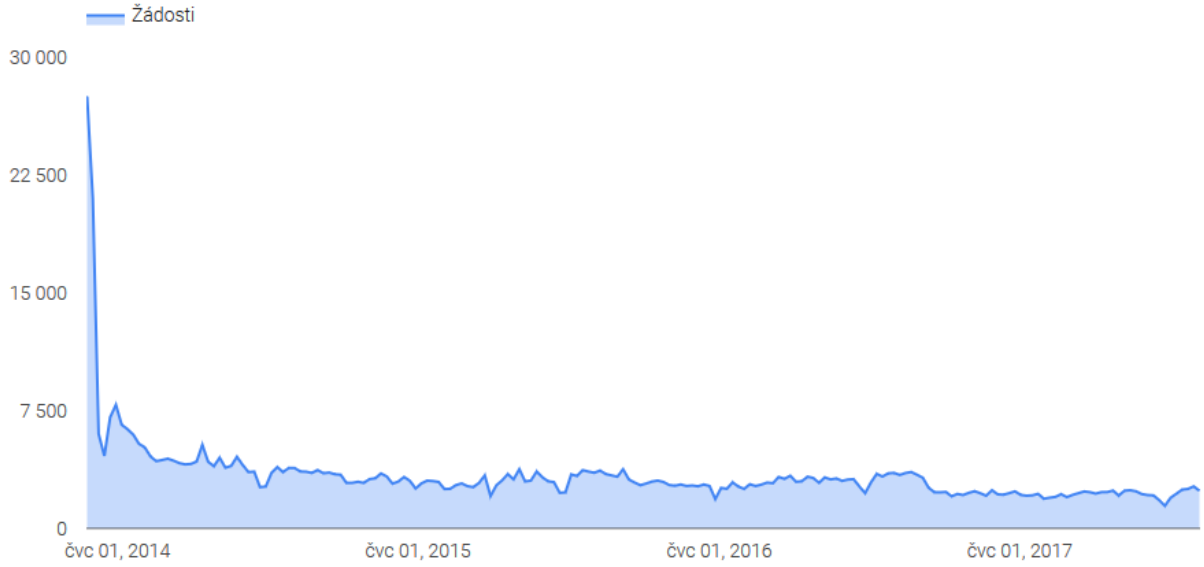
Třetí a poslední otázka se týkala možnosti požadovat výmaz jména subjektu údaje ze zobrazovaného seznamu. Směrnice hovoří o zpracování osobních údajů, které bylo původně oprávněné a v souladu s právními předpisy, a které se může časem stát neslučitelným se Směrnicí, pokud se takové údaje stanou nepřiměřenými, nepodstatnými nebo přesahujícími míru nezbytnou pro účel zpracování. V tomto konkrétním případě je informace o více jak 10 let starých (a navíc splacených) dluzích citlivá a už dle SDEU není dostatečný důvod požadovat, aby byla tato informace zobrazována veřejnosti. Při použití klasického testu proporcionality lze spatřit, že individuální zájem pana Gonzálese na ochraně jeho základních práv (ochrana osobních údajů jako součást práva na soukromí) převyšuje nad zájmem třetích osob na nalezení informace prostřednictvím vyhledávače. Soud ale připustil, že mohou existovat případy, kdy naopak zájem na informovanosti veřejnosti nebo zájem na dosažení ekonomického výsledku ze zobrazování co nejširšího spektra informací ve výsledcích vyhledávání převýší zájem na ochranu základních práv. V takovém případě by byl požadavek odstranění informace vyloučen.

V návaznosti na tento naprosto klíčový rozsudek v oblasti ochrany osobních údajů na internetu Google zveřejňuje počet přijatých a vyřízených žádostí o odstranění adres URL ze služby Vyhledávání Google kvůli ochranně soukromí. Od data 29. května 2014, kdy Google začal přijímat žádost na základě předmětného rozsudku, až ke dni 13. února 2018, byl celkový počet žádostí 2.059.275. Z toho 891.252 z nich bylo vyhověno, což představuje 43,3 %

[99] Obdobně také § 4 písm. e) ZOÚ

z celkového počtu. Pro ČR se jedná o celkem 28.591 žádostí, z čehož bylo 14.765 (51,6 %) vyhověno.

Z následujícího grafu lze vypozorovat, že celkový počet přijatých žádostí v průběhu času byl nejvyšší v létě 2014, tedy čerstvě po předmětném rozsudku, a pak prudce klesal a dále prakticky stagnuje. Z tohoto pohybu i celkového počtu žádostí lze vyvodit, jak velký dopad mělo rozhodnutí ve věci Google Spain.



Obrázek: Žádosti přijaté v průběhu času[100]

Důkazem, jak klíčové bylo toto rozhodnutí pro ochranu osobních údajů, může být fakt, že nové nařízení GDPR účinné od 25. května 2018 (viz kapitola 1.4.1) obsahuje ustanovení čl. 17 pojednávající o tzv. „právu být zapomenut“, k jehož výslovnému zakotvení vydláždil cestu právě rozsudek ve věci Google Spain.

3.5.2 Max Schrems v Facebook Ireland Limited (C-498/16)

Tento mediálně proslavený případ se týká odpovědnosti provozovatelů sociálních sítí ve vztahu k osobním údajům a jejich shromažďování. Sociální sítě mají ve svých smluvních podmínkách souhlasy se zpracováním osobních údajů formulovány velice široce. Tyto ustanovení jsou již dlouho pod tlakem veřejnosti pro rozpor s příslušnými vnitrostátními zákony nebo předpisy EU. Dosud nejpodstatnější kauzou v této věci je případ Max Schrems vs

[100] *Odstranění z vyhledávání na základě evropských předpisů na ochranu soukromí* [online]. transparencyreport.google.com. Dostupné na <https://transparencyreport.google.com/eu-privacy/overview>.

Facebook, na které lze ukázat argumenty obou stran ohledně ukládání osobních údajů provozovateli většiny sociálních sítí.

Max Schrems je rakouský právník, který se začal zajímat o ochranu osobních údajů ve spojitosti se sociální sítí Facebook už jako student právnické fakulty. Na sedmé výroční konferenci Annual Data Protection Conference v Dublinu uvádí, že jako posluchač přednášky zástupců technologických společností při studiu v USA byl svědkem sdělení v duchu *„kašlete na evropské regulace, nic se vám nikdy nestane, pokud je porušíte“*. To byl pro něj okamžik zlomu. Také uvádí, že dle jeho názoru se odhalení učiněná Edwardem Snowdenem ve spojitosti s americkým vládním špehovacím programem PRISM[101] rovná stejně zlomovému okamžiku v debatě o ochraně osobních údajů na internetu, jako byla černobylská havárie z roku 1986 pro debatu o atomové energii. Dále Schrems uvedl, že pro něj jako pro právníka jsou digitální svět a technický základ problému v pozadí nerozluštitelný, že současný systém implicitního souhlasu s nakládáním s osobními údaji je nepostačující a nefér k uživatelům, a že četl opakovaně zásady soukromí Facebooku a stále není schopný říct, jak s jeho osobními údaji Facebook nakládá. Poskytuje analogii, že zaměstnanci poštovní služby také neotvírají dopisy za účelem zkvalitnění poskytovaných služeb, a že přesně toto dělá Google se svojí e-mailovou službou.[102]

Spor začal žádostí o informace o zpracování osobních údajů Facebooku z pozice subjektu údajů. Podobná žádost je upravena v ustanovení § 12 českého ZOÚ. Schrems uvedl, že si Facebook vybral z několika společností, proti kterým mohla jeho žádost směřovat. Facebook skutečně Schremsovi poskytl odpověď v souboru PDF o cca 1200 stranách. Schrems tvrdí, že z odpovědi vyplynulo, že Facebook stále shromažďuje i ty osobní údaje, které už předtím on jako uživatel ze svého profilu vymazal. Ve své žádost se také dotazoval, kde jsou osobní údaje uloženy, avšak odpověď na tuto otázku mu zpřístupněna nebyla.

Následně Schrems podal celkem 22 stížností na společnost Facebook k irskému úřadu pro ochranu osobních údajů (Irish Data Protecion Commissioner, dále jen „IDPC“). V těchto stížnostech uváděl mimo výše uvedené např. i čerpání osobních údajů Facebookem z mobilních aplikací pro vlastní účely bez souhlasu, a napadal i „Podmínky užívání dat“ pro jejich nejasnost

[101] Tajný bezpečnostní program Národní bezpečnostní agentury USA fungující od roku 2007 proslavený především díky úniku informací o jeho existenci přičiněním Edwarda Snowdena. Více o programu na <https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>.
[102] KENNEDY, John. *The Interview: Max Schrems, privacy activist* [online]. Siliconrepublic.com, 28. ledna 2015 [cit. 15. února 2018]. Dostupné na <https://www.siliconrepublic.com/enterprise/the-interview-max-schrems-privacy-activist-video>.

či rozpor s právními předpisy[103]. Mimo jiné se Schrems nechal slyšet, že měl důvěru, že nově ustanovený IDPC bude mít díky novým prostředkům (konkrétně 3,63 milionů liber, nového sídla v Dublinu a personálu o 45 zaměstnancích) větší moc ve vymáhání ochrany osobních údajů.[104]

IDPC všechny stížnosti projednal a uložil Facebooku některá opatření k nápravě. Schrems je ale nepovažoval za dostačující a v červnu roku 2014 všech 22 stížností vzal zpět, protože podle něj IDPC odmítl ve věci rozhodnout. Zde je dlužno poznamenat, že v roce 2013 podal Schrems ještě jednu, dvacátou třetí stížnost, která se vztahovala k předávání osobních údajů do zahraničí (konkrétně do USA). Tento případ vedl až k SDEU a vedl k prohlášení rozhodnutí Komise č. 520/2000 za neplatné a zrušení Safe Harbor List systému poskytování vhodných záruk. Více o tomto případu v následující kapitole č. 3.5.3.

Dále podal Schrems 31. července 2014 žalobu přímo u vídeňského soudu. Z většiny se týkala stejných bodů jako předešlých 22 stížností k IDPC. Žaloba byla podána jako hromadná s více jak 25 tisíc uživatelů, kteří své nároky postoupili na Maxe Schremse. Vedení celého sporu je financováno soukromou společností, které v případě úspěchu náleží 20 % z celé vysouzené částky.[105] Petit hromadné žaloby zahrnuje mimo jiné určení:

- že správcem osobních údajů pro své osobní účely (tedy profil timeline, novinky, akce, fotky, skupiny, stránky, osobní zprávy, seznam přátel a aplikací), je žalobce jakožto uživatel, zatímco Facebook je pouze zpracovatelem, tudíž veškeré nakládání s osobními údaji je podmíněno souhlasem uživatele,
- že Facebook je správcem (pouze) osobních údajů shromážděných Facebookem pro svou osobní potřebu (v případech, kdy data kompiluje, shromažďuje, využívá pro funkci vyhledávání nebo pro účely reklamy, administraci uživatelů apod.),
- stanovil, že Facebook je povinen nakládat s osobními údaji žalobce jen dle jeho pokynů a zdržet se nakládání s osobními údaji, které by bylo v rozporu s pokyny žalobce,
- určil, že Facebook je povinen zajistit technicko-organizační ochranu osobních údajů žalobce zejména ve smyslu čl. 17 Směrnice 95/46,
- určil, že věta první čl. 3 („Naší maximální snahou je zajistit bezpečnost Facebooku, ale nemůžeme ji zaručit“) a další vybraná ustanovení jsou neúčinná,

[103] Stížnosti stejně jako další podrobnosti o celém případu jsou dostupné na <http://europe-v-facebook.org/EN/en.html>.
[104] KENNEDY, John. *The Interview: Max Schrems, privacy activist* [online]. Siliconrepublic.com, 28. ledna 2015 [cit. 15. února 2018]. Dostupné na <https://www.siliconrepublic.com/enterprise/the-interview-max-schrems-privacy-activist-video>.
[105] MAREK, Tomáš. Autonomie vůle a soukromí na Facebooku. *Právní rozhledy*, 6/2015, s. 196

- určil, že souhlas žalobce neopravňuje Facebook užívat osobní údaje žalobce pro své vlastní účely (zejména pro účely reklamy, agregace a analýzy dat),
- stanovil, že Facebook je povinen zdržet se jakéhokoliv spojování dat žalobce s jinými daty od třetích osob (např. od jiných uživatelů nebo firem) nebo vytěžování a analyzování dat žalobce či obdobných technik využívaných Facebookem pro své komerční účely, ledaže by od žalobce obdržel předchozí informovaný souhlas (Opt-In),
- stanovil, že Facebook je povinen zdržet se zpracování a užívání osobních údajů žalobce prostřednictvím poskytovatelů služeb, kteří nenabízejí žádné garance, že budou tyto osobní údaje sledovány třetími státy (v návaznosti na program PRISM),
- stanovil, že Facebook je povinen podat žalobci během čtrnáctidenní lhůty písemně a bezúplatně úplnou zprávu o jeho zpracovávaných osobních údajích, včetně přesného účelu a původu osobních údajů (je-li to možné), a případně také o příjemcích osobních údajů.

Místo pojmu „žalobce" je možné dosadit pojem „uživatel", protože i částečné vyhovění žalobě by mělo dalekosáhle důsledky pro všechny provozovatele sociálních sítí. Součástí petitu je i povinnost Facebooku uhradit peněžitou částku[106] jako újmu způsobenou žalobcům nesprávným nakládáním s osobními údaji.[107]

Soud prvního stupně ve Vídni však rozhodl tak, že žaloba je nepřípustná a označil Schremse v souladu s argumentací Facebooku jako osobu, která nevystupuje jako spotřebitel, ale jako profesionálního aktivista, který provozuje vlastní internetové stránky pouze za účelem vlastní prezentace a za účelem dosažení přímého i nepřímého ekonomického výnosu, i s ohledem na dvě publikované knihy, obdržená ocenění, založení spolku na ochranu osobních údajů a přednáškovou činnost. Mimo to byla jako problematická označena otázka volby rozhodného soudu ve Vídni (z pozice spotřebitele), protože spousta uživatelů připojených k hromadné žalobě nemá bydliště ve Vídni či dokonce ani v EU. Volba rozhodného soudu postupitele se na postupníka nevztahuje.

Ze stanoviska generálního advokáta Soudního dvora EU Michala Bobka v této věci vydaného dne 14. listopadu 2017[108] plynou dva stěžejní závěry:

---

[106] KENNEDY, John. *The Interview: Max Schrems, privacy activist* [online]. Siliconrepublic.com, 28. ledna 2015 [cit. 15. února 2018]. Dostupné na <https://www.siliconrepublic.com/enterprise/the-interview-max-schrems-privacy-activist-video>.

[107] Celý text hromadné žaloby v původním německém jazyce a v anglickém překladu dostupný na <http://europe-v-facebook.org/sk/sk.pdf>.

[108] Stanovisko generálního advokáta Michala Bobka přednesené dne 14. listopadu 2017. Věc C-498/16 Maximilian Schrems proti Facebook Ireland Limited. Digitální Sbírka rozhodnutí (obecná Sbírka rozhodnutí, část „Informace o nezveřejněných rozhodnutích") Identifikátor ECLI: ECLI:EU:C:2017:863.

1) Článek 15 odst. 1 nařízení Rady (ES) č. 44/2001 ze dne 22. prosince 2000 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech je třeba vykládat v tom smyslu, že vykonávání činností, jako je vydavatelská a přednášková činnost, provozování internetových stránek nebo získávání finančních prostředků za účelem vymáhání nároků, neznamená v případě nároků týkajících se vlastního účtu na Facebooku užívaného pro soukromé účely ztrátu postavení jako spotřebitel.

2) Na základě čl. 16 odst. 1 nařízení č. 44/2001 se spotřebitel nemůže současně se svými vlastními nároky dovolávat také nároků se stejným předmětem postoupených jinými spotřebiteli s bydlištěm na jiných místech téhož členského státu, v jiných členských státech nebo ve třetích zemích.[109]

V návaznosti na toto stanovisko vydal Soudní dvůr EU dne 25. ledna 2018 rozhodnutí, ve kterém připouští individuální žalobu Schremse proti Facebooku ve Vídni, ale vylučuje možnost hromadné žaloby.[110] Ke dni dokončení této práce byl již vydán rozsudek o předběžné otázce[111], ale na finální rozsudek ve věci stále čeká. Schrems se ale na svém účtu Twitter nechal slyšet, že poslední rozhodnutí o přípustnost bere jako dobrou zprávu a zásah pro Facebook, který bude muset zpřísnit svá pravidla pro nakládání s osobními údaji.[112]

3.5.3 Max Schrems v Data Protection Commissioner (C-362/14, Safe Harbor)

Jak je uvedeno v předchozí kapitole, z odhalení amerického tajného programu PRISM vyplynulo, že americká bezpečnostní agentura NSA sleduje a ukládá elektronickou komunikaci, aniž by si toho byli uživatelé vědomi. Irský úřad pro ochranu osobních údajů (IDPC) dvacátou třetí stížnost Maxe Schremse zamítl s odkazem na Safe Harbor a rozhodnutí Komise č. 2000/520/ES. Více o tomto rozhodnutí a Safe Harbor v kapitole 1.4.1. IDPC také dovodil, že USA zajišťují odpovídající ochranu předávaných osobních údajů. Tento případ se dostal až k Soudnímu dvoru EU ve formě předběžné otázky:

- zda jsou jednotlivé úřady pro ochranu osobních údajů v členských zemích absolutně vázány rozhodnutím Komise při posuzování stížnosti, ve které stěžovatel tvrdí, že

[109] KENNEDY, John. Max Schrems can sue facebook, but only as a customer [online]. Siliconrepublic.com, 14. listopadu 2017 [cit. 15. února 2018]. Dostupné na <https://www.siliconrepublic.com/enterprise/shrems-facebook-eu-court>.
[110] TANNAM, Ellen. *EU court allows Max Schrems' individual case against Facebook to proceed in Austria* [online]. Siliconrepublic.com, 26. ledna 2018 [cit. 15. února 2018]. Dostupné na <https://www.siliconrepublic.com/enterprise/facebook-max-schrems-eu>.
[111] Rozsudek ze dne 25. ledna 2018, *Maximilian Schrems v Facebook Ireland Limited*, C-498/16, zveřejněný v elektronické Sbírce rozhodnutí.
[112] Zpráva (tzv. tweet) z 25. ledna 2018 dostupná na <https://twitter.com/maxschrems/status/956447080033259520>.

dochází k předávání osobních údajů do jiné, třetí země (v tomto případě do USA), jejíž právní předpisy a praxe údajně nezajišťují odpovídající ochranu pro subjekty údajů

- nebo zda naopak úřad pro ochranu osobních údajů může či musí provést ve věci vlastní šetření s ohledem na vývoj faktické situace, ke kterému došlo od prvotního zveřejnění rozhodnutí Komise.

Soudní dvůr EU konstatoval, že žádné ustanovení Směrnice 95/46/ES nevyjímá z pravomoci vnitrostátních orgánů dozoru dohled nad předáváním osobních údajů do třetích zemí, na které se rozhodnutí Komise vztahuje. Tyto orgány dozoru jsou oprávněny nezávisle posoudit, zda předání osobních údajů dotyčné osoby do třetí země splňuje požadavky stanovené směrnicí. Opačný výklad by byl v rozporu s účelem příslušných článků Směrnice a takové odepření práva obrátit se na vnitrostátní orgány dozoru by představovalo zásah do základních práv zakotvených v čl. 8 odst. 1 a 3 Listiny základních práv Evropské unie. Ve druhé a větší části rozsudku Soudní dvůr EU vyslovil neplatnost Rozhodnutí komise 2000/520/ES, protože připouští omezení práva na ochranu osobních údajů plošně, *„bez jakéhokoliv rozlišení, omezení nebo výjimky v závislosti na sledovaném cíli“*. Dotčené osoby tedy nemají žádnou možnost získat přístup k osobním údajům, které se jich týkají, nebo dosáhnout opravy či výmazu[113], a tudíž rozhodnutí Komise nerespektuje podstatu základního práva na účinnou právní ochranu.[114]

V návaznosti na aféru okolo PRISM a NSA se již některé nadnárodní společnosti jako např. Microsoft[115] nebo Amazon[116] rozhodly vytvořit nová datová úložiště po Evropě, která budou provozována evropskými dceřinými společnostmi. Snaží se tak dostat pod jurisdikci evropských orgánů a dokázat tak klientům vetší bezpečnost jejich osobních údajů.

3.5.4 Patrick Breyer v Bundesrepublik Deutschland (C-582/14)

Soudní dvůr Evropské unie se stejně jako ESLP (viz kapitola 3.4) již k otázce dynamické IP adresy jako osobního údaje vyjádřil. Učinil tak v rozhodnutí ve věci C-70/10 Scarlet Extended[117]. Jednalo se o výklad několika předpisů EU ve smyslu, že s ohledem na

[113] Obě tyto práva už výslovně obsahuje nové nařízení pro ochranu osobních údajů (EU) 2016/679 (GDPR). Více o něm v kapitole 1.4.1.
[114] JANSA, Lukáš a kol. *Internetové právo*. Brno: Computer Press, 2016. s. 379
[115] ČÍŽEK, Jakub. Microsoft otevře nové datové centrum. NSA se do něj nedostane [online]. zive.cz, 11. listopadu 2015 [cit. 15. února 2018] Dostupné na https://www.zive.cz/bleskovky/microsoft-otevre-nove-datove-centrum-nsa-se-do-nej-nedostane/sc-4-a-180363/default.aspx.
[116] bru. Amazon předchází obavám ze špehování, otevře datové centrum v Německu [online]. e15.cz, 23. října 2014 [cit. 15. února 2018]. Dostupné na <http://e-svet.e15.cz/it-byznys/amazon-predchazi-obavam-ze-spehovani-otevre-datove-centrum-v-nemecku-1130920>.
[117] Rozsudek ze dne 24. listopadu 2011, *C-70/10 Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Sb. rozh. s I-11959, bod 51.

ochranu příslušných základních práv není možné, aby byla poskytovateli připojení uložena povinnost zavést systém plošné, preventivní a časově neomezené filtrování všech elektronických sdělení, zejména za použití programů „peer-to-peer“ (také jako „p2p“). Zde vyjádřil, že v situaci, kdy bude možné na základě IP adresy určit konkrétního uživatele, představuje tato adresa osobní údaj podle Směrnice. Odborný názor se už před datem rozsudku ve věci Scarlet Extended ustálil na tom, že hromadný sběr IP adres uživatelů posílajících si data přes p2p za účelem zjištění skutečné identity osoby porušující autorská práva, je v rozporu s evropskými zásadami ochrany osobních údajů.[118]

V nadepsané věci po odvolání pana Breyera i Spolkové republiky Německo proti prvostupňovému rozhodnutí německého soudu poukázal v odvolacím řízení německý Spolkový soud na pojetí osobního údaje dle dvou odlišných kritérií. Při uplatnění objektivního kritéria je možné dynamické IP adresy vnímat jako osobní údaje i v situaci, kdy by bylo možné subjekt údajů po ukončení připojení ke konkrétní internetové stránce určit pouze třetí osobou. Tu v projednávaném případě představuje poskytovatel připojení. Podle relativního kritéria by se naopak o osobní údaje jednalo pouze v případě poskytovatele připojení, neboť pouze tento mohl Breyera v daném případě přesně identifikovat.[119]

SDEU v rozhodnutí ve věci Breyera[120] odkázal na své rozhodnutí ve věci Scarlet Extended a upozornil na to, že u Breyera uchovával IP adresy uživatelů poskytovatel obsahu a ne poskytovatel připojení.[121] Soudní dvůr vyšel z relativního kritéria a uvedl, že i když má odlišná osoba od poskytovatele obsahu (např. poskytovatel připojení) informace k identifikaci uživatele, bude dynamická IP adresa i pro poskytovatele obsahu osobním údajem, pokud ten má k dispozici právní prostředky[122], které mu umožní subjekt údajů určit na základě dalších přidaných údajů. Tyto právní prostředky SDEU nespecifikoval, protože se v praxi budou lišit

[118] OKECHUKWU, Benjamin Vincents. When Rights Clash Online: The Tracking of P2p Copyright Infringements Vs. the EC Personal Data Directive. *International Journal of Law and Information Technology*, 2008, roč. 16, č. 3, s. 270 – 296. Dostupné online na <https://academic.oup.com/ijlit/article/16/3/270/710115>.
[119] NEŠPŮREK, Robert. *Rozhodnutí Breyer a dynamická IP adresa jako osobní údaj* [online]. pravniprostor.cz, 24. května 2017 [cit. 8. února 2018]. Dostupné na <https://www.pravniprostor.cz/clanky/obcanske-pravo/rozhodnuti-breyer-a-dynamicka-ip-adresa-jako-osobni-udaj>.
[120] Rozsudek ze dne 19. října 2016, *Patrick Breyer v Bundesrepublik Deutschland,* C-582-14, zveřejněný v elektronické Sbírce rozhodnutí.
[121] *Tisková zpráva č. 126/11, Unijní právo brání tomu, aby vnitrostátní soud uložil poskytovateli internetového připojení povinnost zavést systém filtrování za účelem zamezení protiprávnímu stahování souborů* [online]. curia.europa.eu, 24. listopadu 2011 [cit. 8. února 2018]. Dostupné na <https://curia.europa.eu/jcms/upload/docs/application/pdf/2011-11/cp110126cs.pdf>.
[122] Např. vyžádání doplňujících údajů od poskytovatele připojení.

stát od státu v závislosti na vnitrostátní legislativě a výkladu místních dozorových orgánů.[123] Takovými právními prostředky pro určení subjektu údajů mohou být např. provozní a lokalizační údaje ve smyslu čl. 5 odst. 2 bodu iii) zrušené směrnice o uchování dat. K tomu viz kapitola 3.2.2.

Český trestní řád[124] ve svém ustanovení § 88a umožňuje prostřednictvím soudu nařídit 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), který dopadá mimo jiného právě na případy kyberútoků proti webovým stránkám (resp. serverům, na nichž jsou umístěny).[125] 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).[126] Závěrem je vhodné uvést, že účinnost GDPR 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 jejichž základě lze subjekt údajů identifikovat.[127]

3.6 Závěry judikatury a její další směřování

Podrobný rozbor rozhodovací činnosti na ochranu osobních údajů z posledních let ukázal, že rozhodující orgány se snaží co nejpružněji reagovat na technologický pokrok. Velké nadnárodní společnosti jako např. Google a Facebook jsou nyní nově pod tlakem vnitrostátních úřadů a Evropské unie i v oblasti ochrany osobních údajů, a nejen jako již tradičně v oblasti porušování soutěžních pravidel.[128] V evropském prostředí pozoruji snahy chránit zájmy

[123] NEŠPŮREK, Robert. *Rozhodnutí Breyer a dynamická IP adresa jako osobní údaj* [online]. pravniprostor.cz, 24. května 2017 [cit. 8. února 2018]. Dostupné na <https://www.pravniprostor.cz/clanky/obcanske-pravo/rozhodnuti-breyer-a-dynamicka-ip-adresa-jako-osobni-udaj>.
[124] zákon č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů
[125] ŠÁMAL, Pavel a kol., *Trestní zákoník (EVK)*. 2.vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 2301 - 2315.
[126] KUBA, Jaroslav. *IP adresa osobním údajem?* [online]. epravo.cz, 6. prosince 2016 [cit. 16. února 2018]. Dostupné na <https://www.epravo.cz/top/clanky/ip-adresa-osobnim-udajem-104204.html>.
[127] Čl. 4 odst. 1 GDPR
[128] HARAŠTA Jakub: *Google opět před Evropskou komisí – může být open-source proti soutěži?* Obchodněprávní revue 10/2016, s. 282

fyzických osob a používat individuální přístup ke každému případu, neboť internetové prostředí v kolizi s tradičními právními principy vytváří ještě nikdy neřešené situace.

Další z příčin vzniku nových situací v ochraně osobních údajů na internetu spatřuji v jejím úzkém spojení s vědou informačních technologií. Kladně proto hodnotím přístup ESLP i SDEU spočívající ve snaze pochopit do hloubky technologický základ problematiky a nezaleknout se spousty odborných termínů. Jedná se často o termíny a principy fungování internetového světa, se kterými se většina laických uživatelů internetu nikdy nesetká.

Mimo Evropu lze spatřit směřování společnosti v ochraně soukromí na internetu jiným směrem. USA a její mentalita mohou být dle mého názoru už od přelomu tisíciletí ovlivněny teroristickými útoky ve spojení se stálou imigrací. Evropa se na rozdíl od amerického právního prostředí vydává jiným směrem, a to i na úkor oslabení nástrojů ochrany autorského práva nebo plošné prevence před terorismem a jinou trestnou činností. Znamením dynamiky rozhodovací činnosti vidím především ve zrušení rozhodnutí Komise o předávání údajů na základě Safe Harbor a směrnice o data retention pro rozpor se zásadami ochrany osobních údajů občanů EU. V podmínkách našeho prostředí toto hodnotím jako krok správným směrem, byť správnost výběru tohoto směru ukáže až čas a další vývoj internetového prostředí.

4. ZÁVĚR

Pojednání o tématu mé práce jako osvěta ochrany osobních údajů se mi jevila jako značně potřebná, neboť jedna ze základních právních zásad, že práva náleží bdělým (*vigilantibus iura scripta sunt*), je platná i v prostředí internetu. Úkolem této práce bylo vyjevit problematiku ochrany osobních údajů jako dvojsečnou zbraň. Značně usnadňuje a zrychluje naše působení na internetu, ať už pracovní nebo volnočasové, zároveň ale umožňuje a láká porušovat právo novými a moderními způsoby. Ve své práci jsem se z jedné strany snažil upozornit na rizika spojená s pohybem ve virtuálním internetovém prostoru a na druhou stranu představit možnosti, které má člověk k dispozici, aby těmto rizikům čelil.

S dnešní nezbytností pohybovat se v prostředí internetu se pojí i potřeba existence pravidel stanovujících jednoznačné podmínky nakládání s útržky našeho působení na internetu, které za sebou zanecháváme, a zajištění, že nedojde k jejich zneužití a poškození práv dotčených osob. Základním pilířem úpravy takového zajištění by dle mého názoru měl být naprostý důraz na preventivní účinek, jehož je v tomto odvětví třeba. Žádnému zneužití dat a údajů o nás by nemělo dojít, neboť následky již jednou uskutečněného zásahu do soukromí lze obvykle zhojit jen velmi obtížně nebo vůbec.

Existují opodstatněné obavy, že se ochrana osobních údajů a soukromí obecně bude zmenšovat a přibližovat se tak systému USA, např. v návaznosti na teroristické útoky po Evropě a snahy jim preventivně a efektivně zabraňovat. Závěrem ale vyslovuji názor, že tyto obavy nesdílím, a naopak vítám změny, které se snaží reagovat na dynamiku informačních technologií, ať už se jedná o pečlivě připravované nařízení GDPR nebo rozhodovací činnost Soudního dvora EU posledních let zrušující nevyhovující předpisy jako rozhodnutí Komise o předávání údajů do USA nebo směrnici o data retention. Nařízení je vystavěno na extrémním preventivním účinku díky hrozbě vysokých pokut stanovených u velkých společností procenty ze zisku, a vytvoření postavení pověřence pro ochranu osobních údajů jako osoby specializující se na tuto činnost. Judikatura Soudního dvora EU vedle toho dle mého názoru ukazuje, že si hodlá zachovat logické argumentační pochody i individuální přístup k ochraně osobních údajů, navzdory nezastavitelnému pokroku a někdy i výčitek ztěžování efektivnějšího bránění práv duševního vlastnictví na internetu.

SEZNAM ZDROJŮ

Komentáře

KLÍMA, Karel et al. *Komentář k Ústavě a Listině. 2. díl. 2. rozš. vyd.* Plzeň: Nakladatelství a vydavatelství Aleš Čeněk, 2009. 901 s.

WAGNEROVÁ, Eliška, ŠIMÍČEK, Vojtěch., LANGÁŠEK, Tomáš, POSPÍŠIL, Ivo a kol. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer, 2012. 906 s.

KUČEROVÁ, Alena a kol. *Zákon o ochraně osobních údajů – komentář.* Praha: Nakladatelství C. H. Beck, 2012. 536 s.

ŠVESTKA, Jiří a kol. *Občanský zákoník - Komentář - Svazek I (obecná část).* 1. vydání. Praha: Wolters Kluwer, 2014 (§ 81 občanského zákoníku).

LAVICKÝ, Petr a kol. *Občanský zákoník.* 1. vydání. Praha: C. H. Beck, 2014, s. 509 - 523

NOVÁK, Daniel. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Vyd. 1. Praha: Wolters Kluwer, 2014. 504 s.

ŠÁMAL, Pavel a kol., *Trestní zákoník (EVK)*. 2.vydání. Praha: Nakladatelství C. H. Beck, 2012, s. 2301 - 2315.

Monografie

MATOUŠOVÁ, Miroslava, HEJLÍK Ladislav. *Osobní údaje a jejich ochrana*. Vyd. 2. Praha: Aspi, 2008, 455 s.

MAŠTALKA, Jiří. *Osobní údaje, právo a my*. Vyd. 1. Praha: C.H. Beck, 2008, xiv, 212 s.

MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. 1. vydání. Praha: CZ.NIC, 2013. s. 39

PAVLÍČEK, Václav a kol., *Ústavní právo a státověda, II.díl*, 1. vydání, Olomouc: Leges 2011, s. 503 – 565

DONÁT, Josef, TOMÍŠEK Jan. *Právo v síti: průvodce právem na internetu.* Vyd. 1. Praha. C.H. Beck, 2016, xi, s. 5

BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: (vybrané otázky)*. Praha: Linde Praha, 2009, 277 s.

KOSAŘ, David a kol. *Ústavní právo. Casebook.* Praha: Wolters Kluwer, a. s., 2014. 636 s.

JANSA, Lukáš a kol. *Internetové právo*. Brno: Computer Press, 2016. s. 381

Příspěvky ve sborníku

KOKEŠ, Marian. Několik poznatků k problematice konkrétních konfliktů mezi právem na informační sebeurčení a ochranou národní bezpečnosti v tzv. době internetové. In ŠIMÍČEK, Vojtěch. *Právo na soukromí.* Brno: MUNI Press, 2011.

Právní předpisy

Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů

Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů

Úmluva č. 108, na ochranu osob se zřetelem na automatizované zpracování osobních dat, přijatou Radou Evropy 28. ledna 1981, vyhlášená pod č. 115/2001 Sb. m. s.,

Směrnice Rady Evropské unie 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů. Úř. věst. L 281, 23. listopadu 1995, s. 31 a násl.

Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech

Zákon č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů

Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů

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). Úř. věst. L 119/1, 4. května 2016, s. 1 a násl.

Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů

Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů

2012/C 326/01 Smlouva o fungování Evropské unie. Úř. věst. C 326, 26. října 2012, s. 47 a násl.

2012/C 326/02 Listina základních práv Evropské unie. Úř. věst. C 326, 26. října 2012, s. 391 a násl.

Rozhodnutí Komise 2000/520/ES ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad bezpečného přístavu a s tím souvisejících často kladených otázek vydaných Ministerstvem obchodu Spojených států. Úř. věst. L 215, 25. srpna 2000, s.7 a násl.

Směrnice Evropského parlamentu a Rady č. 2006/24/ES ze dne 15. března 2006, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí (směrnice o uchovávání údajů). Úř. věst. L 105, 13. dubna 2006, s. 54 a násl.
Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů
Zákon č. 450/2004 Sb., o některých službách informační společnosti a o změně některých zákonů
Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)
Zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů
Zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů
Vyhláška č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů, době jejich uchování a formě a způsobu jejich předávání orgánům oprávněných k jejich využívání, ve znění pozdějších předpisů
Zákon č. 273/2008, o Policii ČR, ve znění pozdějších předpisů.
Směrnice Evropského parlamentu a Rady č. 2006/24/ES ze dne 15. března 2006, o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí (směrnice o uchovávání údajů). Úř. věst. L 105, 13. dubna 2006, s. 54 a násl.
Stanovisko generálního advokáta Michala Bobka přednesené dne 14. listopadu 2017. Věc C-498/16 Maximilian Schrems proti Facebook Ireland Limited. Digitální Sbírka rozhodnutí (obecná Sbírka rozhodnutí, část „Informace o nezveřejněných rozhodnutích“) Identifikátor ECLI: ECLI:EU:C:2017:863.
Zákon č. 141/1961 Sb., o trestním řízení soudním, ve znění pozdějších předpisů

Časopisecké články

NONNEMANN, František. Právní úprava ochrany osobnosti v novém občanském zákoníku a její vztah k ochraně osobních údajů, *Právní rozhledy* 13-14/2012, s. 505
NONNEMANN, František. *Trestní odpovědnost právnické osoby za neoprávněné nakládání s osobními údaji,* Právní rozhledy 20/2016, s. 697
HARAŠTA Jakub, MYŠKA Matěj: *Budoucnost data retention,* Trestněprávní revue 10/2015, s. 238
MAREK, Tomáš. Autonomie vůle a soukromí na Facebooku. *Právní rozhledy*, 6/2015, s. 196

OKECHUKWU, Benjamin Vincents. When Rights Clash Online: The Tracking of P2p Copyright Infringements Vs. the EC Personal Data Directive. *International Journal of Law and Information Technology*, 2008, roč. 16, č. 3, s. 270 – 296. Dostupné online na <https://academic.oup.com/ijlit/article/16/3/270/710115>.

HARAŠTA Jakub: *Google opět před Evropskou komisí – může být open-source proti soutěži?* Obchodněprávní revue 10/2016, s. 282

Internetové zdroje

TOMEŠ, Michal. *Rozmach internetu končí, noví uživatelé přibývají jen pomalu* [online]. e15.cz, 28. září 2016 [cit. 19. března 2018]. Dostupné na <http://e-svet.e15.cz/internet/rozmach-internetu-konci-novi-uzivatele-pribyvaji-jen-pomalu-1323056>.

LIBERDOVÁ, Eva. *Právo na dobrou správu jako princip veřejné správy v EU* [online]. epravo.cz, 21. července 2015 [cit. 16. února 2018]. Dostupné na <https://www.epravo.cz/top/clanky/pravo-na-dobrou-spravu-jako-princip-verejne-spravy-v-eu-98220.html>.

KARTNER, Martin, PROUZA, Jiří. *Evropská unie schválila konečnou podobu obecného nařízení o ochraně osobních údaj* [online]. epravo.cz, 15. června 2016 [cit. 8. února 2018]. Dostupné na <https://www.epravo.cz/top/clanky/evropska-unie-schvalila-konecnou-podobu-obecneho-narizeni-o-ochrane-osobnich-udaju-101825.html>.

MILT, Kristiina. *Fakta a čísla o Evropské unii - Ochrana osobních údajů* [online]. europarl.europea.eu., únor 2017. Dostupné na <http://www.europarl.europa.eu/atyourservice/cs/displayFtu.html?ftuId=FTU_4.2.8.html>.

BURIAN, David, RADIČOVÁ, Zuzana. *Mezinárodní předávání osobních údajů z pohledu nové regulace ochrany osobních údajů* [online]. pravniprostor.cz, 13. dubna 2016 [cit. 8. února 2018]. Dostupné na <https://www.pravniprostor.cz/clanky/mezinarodni-a-evropske-pravo/mezinarodni-predavani-osobnich-udaju-z-pohledu-nove-regulace-ochrany-osobnich-udaju>.

KENNEDY, John. *The Interview: Max Schrems, privacy activist* [online]. Siliconrepublic.com, 28. ledna 2015 [cit. 15. února 2018]. Dostupné na <https://www.siliconrepublic.com/enterprise/the-interview-max-schrems-privacy-activist-video>.

Privacy Shield Program Overview [online]. Dostupné na <https://www.privacyshield.gov/Program-Overview>.

ALLISON, Matt. *A Template for Adequacy: EU Pitches for Data Protection Gold Standard.* [online]. circleid.com, 9. února 2017 [cit. 19. března 2018]. Dostupné na <http://www.circleid.com/posts/20170209_template_for_adequacy_eu_pitches_for_data_protection_gold_standard/>.

STUART, Andrew. *Where do cookies come from* [online]. dominopower.com, 2. července 2002 [cit. 15. února 2018]. Dostupné na <http://dominopower.com/article/where-cookie-comes-from/>.

LOEBL, Zbyněk, HAJNÝ, Filip, FRYNTOVÁ, Jarmila. *Monitorování e-mailů zaměstnanců* [online]. epravo.cz, 12. prosince 2003 [cit. 11. února 2018]. Dostupné na <https://www.epravo.cz/top/clanky/monitorovani-e-mailu-zamestnancu-22444.html>.

OTEVŘEL, Petr. *Spamming a některé otázky šíření obchodních sdělení.* [online]. pravoit.cz, 12. srpna 2008 [cit. 11. února 2018]. Dostupné na <http://www.pravoit.cz/novinka/spamming-a-nektere-otazky-sireni-obchodnich-sdeleni>.

Historie Úřadu pro ochranu osobních údajů [online]. uoou.cz [cit. 8. prosince 2017]. Dostupné na <https://www.uoou.cz/historie%2Duradu%2Dpro%2Dochranu%2Dosobnich%2Dudaju/ds-1061/archiv=0&p1=1059>.

The WP29 will become the EDPB – but what does that mean? [online]. iabeurope.eu, 25. července 2016 [cit. 8. prosince 2017]. Dostupné na <https://www.iabeurope.eu/policy/data-protection/the-wp29-will-become-the-edpb-but-what-does-that-mean/>.

DEMMEL, Annette. *IP Addresses Constitute Personal Data According to Court of Justice of European Union* [online]. natlawreview.om, 20. října 2016 [cit. 8. února 2018]. Dostupné na <https://www.natlawreview.com/article/ip-addresses-constitute-personal-data-according-to-court-justice-european-union>.

NEŠPŮREK, Robert. *Rozhodnutí Breyer a dynamická IP adresa jako osobní údaj* [online]. pravniprostor.cz, 24. května 2017 [cit. 8. února 2018]. Dostupné na <https://www.pravniprostor.cz/clanky/obcanske-pravo/rozhodnuti-breyer-a-dynamicka-ip-adresa-jako-osobni-udaj>.

Odstranění z vyhledávání na základě evropských předpisů na ochranu soukromí [online]. transparencyreport.google.com. Dostupné na <https://transparencyreport.google.com/eu-privacy/overview>.

KENNEDY, John. *The Interview: Max Schrems, privacy activist* [online]. Siliconrepublic.com, 28. ledna 2015 [cit. 15. února 2018]. Dostupné na <https://www.siliconrepublic.com/enterprise/the-interview-max-schrems-privacy-activist-video>.

KENNEDY, John. Max Schrems can sue facebook, but only as a customer [online]. Siliconrepublic.com, 14. listopadu 2017 [cit. 15. února 2018]. Dostupné na <https://www.siliconrepublic.com/enterprise/shrems-facebook-eu-court>.

TANNAM, Ellen. *EU court allows Max Schrems' individual case against Facebook to proceed in Austria* [online]. Siliconrepublic.com, 26. ledna 2018 [cit. 15. února 2018]. Dostupné na <https://www.siliconrepublic.com/enterprise/facebook-max-schrems-eu>.

ČÍŽEK, Jakub. Microsoft otevře nové datové centrum. NSA se do něj nedostane [online]. zive.cz, 11. listopadu 2015 [cit. 15. února 2018] Dostupné na https://www.zive.cz/bleskovky/microsoft-otevre-nove-datove-centrum-nsa-se-do-nej-nedostane/sc-4-a-180363/default.aspx.

bru. Amazon předchází obavám ze špehování, otevře datové centrum v Německu [online]. e15.cz, 23. října 2014 [cit. 15. února 2018]. Dostupné na <http://e-svet.e15.cz/it-byznys/amazon-predchazi-obavam-ze-spehovani-otevre-datove-centrum-v-nemecku-1130920>.

NEŠPŮREK, Robert. *Rozhodnutí Breyer a dynamická IP adresa jako osobní údaj* [online]. pravniprostor.cz, 24. května 2017 [cit. 8. února 2018]. Dostupné na <https://www.pravniprostor.cz/clanky/obcanske-pravo/rozhodnuti-breyer-a-dynamicka-ip-adresa-jako-osobni-udaj>.

Tisková zpráva č. 126/11, Unijní právo brání tomu, aby vnitrostátní soud uložil poskytovateli internetového připojení povinnost zavést systém filtrování za účelem zamezení protiprávnímu stahování souborů [online]. curia.europa.eu, 24. listopadu 2011 [cit. 8. února 2018]. Dostupné na <https://curia.europa.eu/jcms/upload/docs/application/pdf/2011-11/cp110126cs.pdf>.

KUBA, Jaroslav. *IP adresa osobním údajem?* [online]. epravo.cz, 6. prosince 2016 [cit. 16. února 2018]. Dostupné na <https://www.epravo.cz/top/clanky/ip-adresa-osobnim-udajem-104204.html>.

Judikatura

Nález Ústavního soudu ze dne 2. listopadu 2009, sp. zn. II. ÚS 2048/09 (N 232/55 SbNU 181)

Nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl.ÚS 24/10 (N 52/60 SbNU 625)

Rozsudek ESLP ze dne 4. května 2000, *Rotaru v. Rumunsko* (stížnost č. 28341/95)

Rozsudek Nejvyššího správního soudu ze dne 10. 8. 2004, sp. zn. 2 As 6/2004-49

Rozsudek Velkého senátu ESLP ze dne 30. června 2005, *Bosphorus Hava Yollari Turizm ve Ticaret Anonim Şirketi v. Ireland* (stížnost č. 45036/98)

Rozsudek ESLP ze dne 15. března 1978, *Tyrer v. United Kingdom* (stížnost č. 5856/72)

Rozsudek ze dne 6. října 2015, *Maximillian Schrems vs. Data Protection Commissioner, Digital Rights Ireland Ltd,* C-362/14, zveřejněný v elektronické Sbírce rozhodnutí.
Žaloby *Digital Rights Ireland v Commission* (T-670/16), *La Quadrature du Net and Others v Commission* (T-738/16).
Kyllo v. United States, 533 U.S. 27, 33–34 (2001)
Rozsudek ESLP ze dne 6. září 1978, *Klass and others v. Germany* (stížnost č. 5029/71)
Rozsudek ESLP ze dne 2. srpna 1984, *Malone v. The United Kingdom* (stížnost č. 8691/79)
Rozsudek ESLP ze dne 24. dubna 1990, *Kruslin v. France* (stížnost č. 11801/85)
Usnesení Nejvyššího soudu ČR ze dne 16. listopadu 2016, sp. zn. 3 Tdo 1214/2016
Nález Ústavního soudu ze dne 2. února 1998, sp. zn. IV. ÚS 154/97 (N 17/10 SbNU 113).
Usnesení Nejvyššího soudu ze dne 28. června 2007, sp. zn. 30 Cdo 664/2007
Rozhodnutí německého Spolkového ústavního soudu 2 BvR 933/82, BVerfGE 76, 256 (359)
Nález Ústavního soudu ze dne 22. března 2011, sp. zn. Pl.ÚS 24/10 (N 52/60 SbNU 625)
Rozsudek Soudního dvora EU ze dne 8. dubna 2014 ve spojených věcech, *Digital Rights Ireland Ltd (C-293/12) proti Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irsku, The Attorney General, za přítomnosti: Irish Human Rights Commission, a Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl a další*, C-293/12 a C-594/12, zveřejněný v elektronické Sbírce rozhodnutí.
Rozhodnutí Spolkového ústavního soudu SRN ze dne 15. 12. 1983, BVerfGE 65, 1 (Volkszählungsurteil)
Rozsudek Městského soudu v Praze ze dne 25. srpna 2016, sp. zn. 11 A 77/2012
Rozsudek ESLP ze dne 16. dubna 2002, *Société Colas Est and others v. France* (stížnost č. 37971/97)
Rozsudek ESLP ze dne 3. listopadu 2011, *S. H. and others v. Austria* (stížnost č. 57812/00)
Rozsudek Velkého senátu ESLP ze dne 11. července 2002, *Christine Goodwin v. The United Kingdom* (stížnost č. 28957/95)
Rozsudek ze dne 23. března 2010, *Google France SARL, Google Inc. v Louis Vuitton Malletier SA (C-236/08), Google France SARL v Viaticum SA, Luteciel SARL (C-237/08), a Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08)*, C-236/08, C-237/08, C-238/08, Sb. rozh. s. I-02417

Rozsudek ze dne 13. května 2014, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* C-131/12, zveřejněný v elektronické Sbírce rozhodnutí.

Rozsudek ze dne 25. ledna 2018, *Maximilian Schrems v Facebook Ireland Limited,* C-498/16, zveřejněný v elektronické Sbírce rozhodnutí.

Rozsudek ze dne 24. listopadu 2011, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, Sb. rozh. 2011 I-11959.

Rozsudek ze dne 19. října 2016, *Patrick Breyer v Bundesrepublik Deutschland*, C-582-14, zveřejněný v elektronické Sbírce rozhodnutí.

ABSTRAKT

Diplomová práce se zabývá ochranou osobních údajů na internetu. Pro udržení ochrany práva na soukromí musel reagovat na rychlý vývoj technologií jak zákonodárce, tak soudy. Úkolem práce bylo zjistit, jak je ochrana osobních údajů na internetu realizována, a jestli je a činnost orgánů pro ochranu osobních údajů získaných na webu v současné době dostatečná. Metody získání odpovědí na tyto otázky byly jednak analyzovat ochranu osobních údajů jako součást ochrany soukromí na všech úrovních (vnitrostátní, evropská, mezinárodní), a následně analýza všech orgánů chránících osobní údaje. Analyzována byla rozhodovací činnosti Úřadu pro ochranu osobních údajů, obecných soudů v ČR, Ústavního soud ČR, Evropského soudu pro lidská práva a Soudního dvora EU). Práce poskytuje závěry, že ochrana osobních údajů je na evropské úrovni vystavěna na snaze preventivně zamezovat zneužití osobních údajů primárně velkými společnostmi díky novému nařízení GDPR, a zároveň nesleduje trend stále narůstajícího dohledu státu, který lze pozorovat v USA. Činnost soudních a jiných institucí chrání osobní údaje získané z internetu dostatečně, neboť si zachovává individuální přístup, sleduje rychlý technologický pokrok a neprolomí právo na soukromí na internetu ani pod tíhou ochrany duševního vlastnictví.

Klíčová slova: soukromí, osobní údaj, internet, souhlas se zpracováním, listovní tajemství, cookies, úřad pro ochranu osobních údajů, nevyžádaná obchodní sdělení, proporcionalita, data retention, max schrems, google, facebook

ABSTRACT

The thesis deals with the protection of personal data on the Internet. In order to maintain the protection of the right to privacy, a response to the rapid development of technologies was needed from both the legislator and the courts. The task of the thesis was to find out whether the personal data on the Internet is being protected and whether the activity of the data protection authorities is sufficient at the present time. The methods of answering these questions were to analyze the protection of personal data as part of the protection of privacy at all levels (national, European, international), and then analyze all authorities protecting personal data. The analysis was made on the decision-making activities of the czech Office for Personal Data Protection, General Courts in the Czech Republic, the Czech Constitutional Court, the European Court of Human Rights and the Court of Justice of the EU. The thesis concludes that personal data protection is built at European level to prevent the prevention of misuse of personal data primarily by large companies thanks to the new GDPR regulation, while not following the trend of the ever-increasing state surveillance observed in the USA. The activity of judicial and other institutions protecting personal data obtained from the Internet is sufficient as it maintains an individual approach, follows the rapid technological progress and does not negate the right to privacy on the Internet for the sake of intellectual property protection.

Keywords: privacy, personal data, internet, consent to processing, letter secret, cookies, office for personal data protection, unsolicited commercial communications, proportionality, data retention, max schrems, google, facebook