

# DONÁT, J., TOMÍŠEK, J. PRÁVO V SÍTI. PRŮVODCE PRÁVEM NA INTERNETU

FRANTIŠEK KASL\*

**DONÁT, J., TOMÍŠEK, J. *Právo v síti. Průvodce právem na internetu.*  
1. vydání. Praha: C.H.Beck, 2016, 350 str., ISBN: 978-80-7400-610-4**

V létě letošního roku vyšla publikace Josefa Donáta a Jana Tomíška, praktikujících odborníků na oblast ochrany osobních údajů, jejímž proklamovaným cílem je přiblížení základních aspektů občanského soužití v prostředí internetu široké veřejnosti, a to z pohledu běžného uživatele. Autoři tak reagují na nedávné i očekávané změny v právní úpravě týkající se této problematiky a snaží se poskytnout široký ucelený přehled hlavních aspektů jednání a dění na internetu. Je na místě uvítat tuto příručku, která se svým přístupem vymyká většině dostupných odborných publikací z oblasti ochrany osobních údajů, jelikož je zaměřena na zpřístupnění obecného přehledu a praktických rad odborné, ale i laické veřejnosti.

Tato forma osvěty širší veřejnosti je značně potřebná, jelikož i samotnými autory je v závěru knihy zdůrazněno, že základní zásada, že práva náleží bdělým, je platná i v prostředí internetu. Čtenář by si po jejím přečtení, namísto pocitu nejistoty a bezmoci, při svém počínání v internetovém prostředí měl být schopen na jednu stranu uvědomit rizika spojená s pohybem v tomto virtuálním prostoru a na druhou stranu možnosti, které má k dispozici, aby jim čelil.

Knihla je tematicky rozdělena do čtyř kapitol, přičemž každá kapitola sleduje strukturu obecného úvodu následovaného nejprve technicky zamě-

---

\* Autor je prezenčním doktorským studentem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontaktní e-mail je frantisek.kasl@mail.muni.cz.

řeným rozbohem a poté též zasazením do právního kontextu. Krátká shrnutí na konci kapitol pak poskytují přehledný obsah dané kapitoly. Tento systematický přístup, spojený s na poměry právní publikace příjemně čtivým textem, umožňuje čtenáři snadný vstup do popisované problematiky a rychlou orientaci při potřebě řešení konkrétního problému. Nejen laický čtenář dozajista ocení četné příklady a vzorové situace, kterými je text protkán a díky kterým si může lépe uvědomit roli různých technických či právních instrumentů, ale též reálnou dimenzi řady popisovaných technických rizik či problematických situací, ve kterých se osoba v prostředí internetu může ocitnout. V tomto ohledu lze publikaci označit i za vhodný doplňkový studijní materiál pro vstup do oblasti práva informačních technologií a souvisejících právních oborů. Praktickou rovinu má též soubor vzorových dokumentů a podání, které mohou některým čtenářům usnadnit postup při obraně jejich práv a na které je vhodně odkazováno i v textu popisujícím příslušné situace.

První kapitola slouží jako úvod do ochrany soukromí na internetu. Autoři se hned na začátek snaží čtenáři osvětlit, proč je na místě této problematice věnovat pozornost. Osobní údaje jsou přirovnány k měně, kterou je v prostředí internetu placeno za zdánlivě bezplatné služby, a na případu Maxe Schremse proti společnosti Facebook je upozorněno na některá rizika, kterých bychom si měli být vědomi při používání sociálních sítí.

Technicky zaměřená část kapitoly hlouběji popisuje, co si představit pod profilováním uživatelů pro marketingové účely a jakou roli při tom hrají tzv. cookies a další údaje sloužící k identifikaci uživatele. Čtenářům jsou také obratem nabídnuty některé snadno dostupné cesty k omezení těchto metod sledování a profilování. Tato forma představení určitého varovného aspektu přítomnosti na internetu a obratem navazující nasměrování či rada ohledně možného řešení je přítomna skrze celou publikaci a lze ji hodnotit jako přehlednou a přínosnou především pro čtenáře, kteří hledají příručku pro řešení praktických situací. Krátká zmínka je věnována také současnému rozmachu chytrých zařízení, tzv. internetu věcí, a to především v souvislosti s často zmiňovanými riziky pro soukromí a identitu uživatelů. Zdůrazněn je trend kombinace údajů z různých zařízení a jejich sdílení s třetími

subjekty, jako jsou např. pojišťovny, za účelem dosažení lepších služeb či smluvních podmínek. Autoři na závěr části představují specifika biometrických údajů, usnadnění, která nabízí jejich plošné užívání, ale také rizika spojená s jejich nezměnitelností.

V právně orientovaném segmentu je autory stručně představeno pojetí práva na soukromí jako komplexu dílčích práv, která se v prostředí internetu projevují především v možnosti kontrolovat dostupné informace o vlastní osobě. Po přehledu základních relevantních právních předpisů je čtenář seznámen s principem zákonného důvodu svolení ke zveřejnění osobních údajů a dalšími důvody, které umožňují zveřejnění i bez souhlasu subjektu údajů. Výklad je doplněn příklady situací, což napomáhá čtenáři v orientaci. Nutnost vyvažování práva na soukromí s jinými základními právy, jako je právo na svobodu projevu či právo veřejnosti na přístup k informacím, je vyložena na příkladech několika obecně známých soudních sporů z českého prostředí. Značná pozornost je věnována postupu při uplatnění občanskoprávních nároků na ochranu osobnosti. Čtenář je upozorněn na význam předžalobní výzvy, funkci předběžného opatření i na časté nedostatky žalob, které vedou k jejich neúspěchu. Odkazy na vzory podání nacházející se v závěru publikace pak umožňují lepší orientaci v popisovaném postupu. Na výklad týkající se práva na soukromí navazuje představení právní úpravy ochrany osobních údajů. Po seznámení se se základními právními pojmy je čtenáři nabídnut přehled právních základů zpracování osobních údajů. Nejsou opomenuty ani základní principy nakládání s osobními údaji a další instituty, které tvoří nezbytné jádro pro pochopení této právní úpravy. V rámci výkladu je bohatě zohledňována relevantní judikatura a je také přihlédnuto k nadcházející úpravě ve formě Obecného nařízení o ochraně osobních údajů, která přinese řadu nových institutů, práv a povinností. Prostředí internetu není vázáno státními hranicemi, a proto je vysoce relevantní problematika předávání osobních údajů do zahraničí a její dramatický vývoj v posledních letech. Čtenáři jsou srozumitelně objasněna základní práva subjektu údajů, jako je např. právo být zapomenut, zdůrazněné Soudním dvorem ve věci Google Spain. Vyložena je i kontrolní činnost Úřadu pro ochranu osobních údajů a její nedostatky, soubor relevantních

správních deliktů a přestupků i rozšíření možností vymáhání práv z ochrany osobních údajů v budoucím režimu Obecného nařízení. Značně relevantní je také téma digitální pozůstalosti, ve kterém autoři objasňují omezení příkazů v závěti ve vztahu k online službám, vyjmutí osobních údajů zesnu-  
lé osoby z režimu ochranné zákonné úpravy i řadu nedostatků právní úpravy, které jsou dnes jen částečně kompenzovány technickými postupy poskytovatelů online služeb.

První kapitola byla podobně jako celá kniha dominována právním pohledem na předmětnou problematiku, to je však ve světle názvu publikace zcela na místě. Ve struktuře kapitoly se projevuje záměr autorů poskytnout široký přehled o velkém počtu dílčích aspektů internetového prostředí, čímž dochází k určité segmentaci dílčích témat, která na sebe ne vždy zcela plynule navazují. Přesto si publikace zachovává pevnou nosnou strukturu hlavních oblastí dílčích kapitol a čtenářsky přívětivou formu podání jak technické, tak právní problematiky.

V druhé kapitole se autoři věnují zábavě online a významu duševního vlastnictví. Úvodem je čtenář krátce seznámen s nedávným vývojem distribuce zábavy; od CD a DVD přes datová úložiště a peer-to-peer sítě po služby jako je iTunes. Rozebrány jsou základní formy vytváření digitálního obsahu na internetu, jakou roli při této tvůrčí činnosti hraje zpracování cizího autorského díla a jaká tomu klade autorské právo omezení.

Technická část začíná odlišením různých typů internetových odkazů, ozřejměním principů fungování peer-to-peer sítí a zdůvodněním jejich vysoké rizikivosti. Čtenář se dozví, na jaké bázi funguje placený přístup k digitálnímu obsahu, co se skrývá pod zkratkou DRM, či jak se projevuje geoblocking. Posledním technickým tématem je software, z čeho se skládá, jak vzniká, jaký je rozdíl mezi zdrojovým a strojovým kódem a co znamená pojem reverzní inženýrství.

Část právní se opět věnuje značně rozsáhlé problematice, tentokrát autorskému právu. Nejprve jsou systematicky vyloženy základní pojmy a instituty, poté jsou odlišeny osobnostní a majetková práva autora. Autoři následně popsanou právní úpravu vztahují na prostředí internetu a zaměřují se na posouzení různých běžných online činností z pohledu autorských práv

a jejich narušování. Čtenář se tak dozví o rozsahu výjimek z autorských práv, o rozdílném přístupu ke kvalifikaci stahování autorskoprávně chráněného obsahu z internetu v německém a českém právu, či o právních rizicích spojených s využíváním peer-to-peer sítí. Na základě představené judikatury Soudního dvora i českého Nejvyššího soudu jsou načrtnuty současné hranice mezi autorskoprávně přípustným a nepřípustným jednáním. Formě příručky pro běžného uživatele je pak v této části nejbližší popis práv a povinností spotřebitele při nákupu digitálního obsahu. Za zmínku stojí, že autoři neopomněli zdůraznit problematické oblasti, jako je např. sdílení účtu a nakoupeného obsahu mezi více uživateli či nevyjasněná otázka přechodu oprávnění z licence na dědice. Zvýšená pozornost je věnována podmínkám tvorby vlastního online obsahu, přičemž je nutné ocenit snahu autorů o podrobnější rozbor funkce a významu veřejných licencí, s jejichž existencí je na místě širokou veřejnost trvale seznamovat. Nadto je čtenáři poskytnut stručný přehled dalších forem licencí, včetně řady příkladů jejich uplatnění. Z autorskoprávního hlediska je specifická situace počítačových programů a autoři tato specifika neopomněli zmínit. Srozumitelnou formou je vysvětlen rozdíl mezi proprietárním software a open source software i význam veřejných licencí pro open source software. Závěr této části se věnuje právním nástrojům ochrany autorskoprávních nároků a civilněprávním i veřejnoprávním sankcím hrozcím za porušení autorských práv. Tato kapitola má za cíl vytvořit určitý základní přehled funkcí a rozsahu autorskoprávní ochrany v prostředí internetu, na základě kterého si čtenář snáze zhodnotí, při jakých činnostech dochází k porušení jakých práv, jaké jsou účelné a adekvátní metody obrany a jaké postihy v případě porušení hrozí.

Třetí kapitola se věnuje internetovým službám a nakupování na internetu. Úvod kapitoly se opět snaží nastínit kontury dílčích témat, která jsou následně řešena v technické či právní části. Zmíněna jsou tedy specifika nákupu online, projevující se v úpravě kupní smlouvy na dálku, v potřebě zvýšené důvěry při elektronických transakcích i v důsledcích anonymity internetu pro soukromoprávní jednání.

Hlavním tématem technické části je fungování elektronického podpisu, datové schránky a dalších technických řešení zajišťujících důvěru při elektronické komunikaci. Čtenáři je také nabídnut praktický návod na založení a používání datové schránky. Druhým technickým tématem je objasnění fungování nákupu v internetovém obchodě či na internetové aukci a specifiky různých způsobů doručení a platby. Nebyly opomenuty ani internetové služby, kde je zdůrazněna častá přítomnost obchodního modelu bezplatnosti, která je kompenzována zpracováváním osobních údajů, důležitost pečlivé volby poskytovatele i některá rizika specifická pro služby poskytované na dálku pomocí internetové sítě.

Právní část je na rozdíl od předchozích částí knihy napsána náročnější formou právního výkladu, jelikož se autoři poměrně detailně věnují elektronickému právnímu jednání a změnám, které přineslo nařízení eIDAS účinné od letošního léta. Na jejich obranu je však nutno vyzdvihnout použití řady příkladů aplikace vykládaných právních institutů, což dává čtenáři možnost lepšího pochopení a jejich vztahení na životní situace, ve kterých se může vyskytnout. V části týkající se datových schránek je čtenář varován před určitými aspekty jejich užívání, jako je např. fikce doručení či závazek k jejímu povinnému užívání pro daňová přiznání. Tématem kapitoly jsou internetové služby a nakupování na internetu, není tudíž opomenuta jejich právní úprava a úprava ochrany spotřebitele. Nabídnut je užitečný průřez spotřebitelským právem, který, i přes menší stylistickou toleranci k laickým čtenářům, za pomoci příkladů dobře osvětluje tuto právní problematiku. Za praktické lze označit především přehledné seznámení s možnými postupy pro řešení spotřebitelských sporů jak na národní, tak na evropské úrovni.

V poslední tematické kapitole se autoři věnují jednomu z nejpálčivějších témat ve vztahu k online prostředí, a to je bezpečnost na internetu. Hned v úvodu výstižně vztahují lehkovážnost řady uživatelů ohledně internetových hrozeb k odlišnosti pocitu nebezpečí při pohybu v nebezpečném prostředí fyzického a virtuálního světa.

Nezvykle rozsáhlá technická část je zaměřena na řadu velmi aktuálních a významných rizik pohybu na internetu, která jsou čtenáři vysvětlena přívetivou formou, za pomoci vzorových příkladů nebo skutečných situací. Po

výkladu pojmů jako je malware, trojský kůň, ransomware, keylogger a další, se čtenář seznámí s hlavními lákadly a nebezpečími webových stránek s rizikovým obsahem, se specifickými riziky vztahujícím se k chytrým telefonům nebo s principy, na kterých jsou založeny podvodné e-maily a sociální inženýrství. Zvýšená pozornost je věnována nedostatečnému zabezpečení uživatelských účtů a systémů před únikem dat, krádežemi identity či neoprávněnými přístupy k finančním prostředkům, ale také bezpečnostním politikám zaměstnavatelů a jejich slabým článkům: zaměstnancům. Na tuto poměrně temnou část navazuje důsledný přehled možností obrany běžného uživatele proti většině ze zmíněných rizik, který dobře vystihuje autory definované zlaté pravidlo internetu; nic není zadarmo, je tedy nutno dbát obezřetnosti před podezřelým obsahem. Podrobněji jsou rozebrány některé dílčí složky, jako je vhodný přístup k zabezpečení internetové komunikace, benefity a limity šifrování, pravidla pro bezpečné heslo, účelnost vícestupňového ověřování identity nebo základy obezřetného zacházení s platebními prostředky online.

Výklad právní úpravy kybernetické kriminality je zahájen seznámením čtenáře s Budapeštskou úmluvou Rady Evropy o počítačové kriminalitě z roku 2001, popisem skutkových podstat tzv. ryzích počítačových trestných činů a příklady trestné činnosti v kontextu rizik zmíněných v předchozí části. Následně je pozornost věnována narušení soukromí a důvěrnosti komunikace, krádežím identity, internetovým podvodům na bázi sociálního inženýrství a problematice kyberstalkingu a kyberšikany.

Příručka přístupným jazykem seznamuje čtenáře s širokým okruhem dílčích témat souvisejících s přítomností a jednáním na internetu. Vzhledem k důrazu na právní aspekty výkladu lze dovodit cílení spíše na právně vzdělanou, či vzdělávající se, veřejnost, které může posloužit jako souborný přehled právní úpravy popisované problematiky. Je na místě ocenit i zohlednění nejnovějšího vývoje evropského práva ochrany osobních údajů i judikatury Soudního dvora v této oblasti. Pro zbylou veřejnost lze v knize shledávat základní vodítko pro rozumnou míru vědomého jednání v prostředí internetu a orientaci v právních nástrojích, které jim jsou k dis-

pozici v případě potřeby. Vzorové dokumenty i časté odkazy na relevantní zdroje a služby pak jen dále zvyšují její praktické využití.

---

*Toto dílo lze užít v souladu s licenčními podmínkami Creative Commons BY-SA 4.0 International (<http://creativecommons.org/licenses/by-sa/4.0/legalcode>).*

---