Lukáš Jansa, Petr Otevřel, Jiří Čermák, Petr Mališ,
Petr Hostaš, Michal Matějka, Ján Matejka

Internetové právo

Praktický průvodce

Domény, hosting
a internetové stránky

Uzavírání smluv
a obchodování
na Internetu

Vyhledávače, reklama,
spam a sociální sítě

Ochrana autorských děl
na Internetu

Internetová kriminalita
a kybernetická bezpečnost



computer press

Internetové právo

Vyšlo také v tištěné verzi

Objednat můžete na
www.computerpress.cz
www.albatrosmedia.cz



Lukáš Jansa, Petr Otevřel, Jiří Čermák, Petr Mališ,
Petr Hostaš, Michal Matějka, Ján Matejka
Internetové právo – e-kniha
Copyright © Albatros Media a. s., 2017

Všechna práva vyhrazena.
Žádná část této publikace nesmí být rozšiřována
bez písemného souhlasu majitelů práv.

ALBATROS MEDIA a.s.

**Lukáš Jansa, Petr Otevřel, Jiří Čermák, Petr Mališ,
Petr Hostaš, Michal Matějka, Ján Matejka**

Internetové právo

**Computer Press
Brno
2016**

Obsah

O autorech **15**
Poděkování **17**
Řekli o knize **18**
Předmluva **19**

KAPITOLA 1
Úvod do problematiky internetového práva **21**

Právo informačních technologií **21**
Internetové právo 22
Softwarové právo 22
Právní předpisy internetového práva **23**
Právní předpisy ČR a ostatní závazná pravidla 23
Právní předpisy EU 24
Shrnutí kapitoly **25**

KAPITOLA 2
Domény a doménová jména **27**

Klasifikace a využití domén **27**
Pojmy doména a doménové jméno 27
Základní podmínky registrace domén 31
Správa doménového systému **33**
Vznik sítě Internet 34
IP adresy 34
Správci domén nejvyšší úrovně 35
Registr doménových jmen 36
Technické zajištění správy domény 37
Doména CZ 37
Jak funguje DNS? 37
Právní povaha domén **38**
Vznik doménového jména 38
Zánik doménového jména 39
Převod doménového jména 40
Zástava doménového jména 40
Exekuce doménového jména 40
Kolize domén s právy třetích osob **41**
Kolize doménových jmen navzájem 43
Ochranné známky 43

Název právnické osoby 45
Ochrana názvu veřejnoprávních korporací 46
Přednost doménového jména před ochrannou známkou nebo názvem právnické osoby 47
Jména fyzických osob 48
Kolize z důvodu nekalé soutěže 49
Vícečetné kolize 52
Dobrá a zlá víra 53
Odpovědnost za porušení práv třetích osob 53

Doménové spory 54
Doménové spory řešené obecnými soudy 54
Prostředky nápravy v řízení před obecnými soudy 57
Mimosoudní (alternativní) řešení doménových sporů 60
Sudiště nabízející alternativní řešení sporů 67
Předběžná opatření v doménových sporech 68
Výkon rozhodnutí ve věcech doménových sporů 71

Shrnutí kapitoly 72

KAPITOLA 3
Internetové stránky, jejich obsah, zhotovení a hosting 73

Internetové stránky 73

Ochrana internetových stránek 74
Preventivní ochrana internetových stránek 76
Následná ochrana internetových stránek 79
Jednotlivé způsoby ochrany internetových stránek 80

Obsah internetových stránek 84
Texty jako součást internetových stránek 84
Fotografie jako součást internetových stránek 85
Katalogové fotografie výrobců a užití jejich ochranných známek 88
Fotobanky jako zdroj fotografií 91
Grafická díla jako součást internetových stránek 92
Videa jako součást internetových stránek 92

Nároky z porušení práv provozovatele internetových stránek 92
Aktivní legitimace – oprávněný (žalobce) 93
Pasivní legitimace – povinný (žalovaný) 94
Rozhodné právo a příslušnost soudu 94
Nároky z porušení práv k internetovým stránkám 96
Soudní řízení 98
Správněprávní odpovědnost 99
Trestněprávní odpovědnost 99

Typy smluv související s internetovými stránkami 100

Smlouva o registraci domény a jejím obnovování 101

Smlouva o vytvoření internetových stránek **102**
Základní obsahové náležitosti smlouvy o vytvoření internetových stránek 104
Ostatní obsahové náležitosti smlouvy o vytvoření internetových stránek 108
Licence a licenční smlouva k autorsky chráněným prvkům **110**
Pojem licence 110
Výhradní a nevýhradní licence 111
Omezení rozsahu licence 113
Licenční smlouva k autorským dílům užitým na internetových stránkách 113
Základní obsahové náležitosti licenční smlouvy 114
Ostatní obsahové náležitosti licenční smlouvy 115
Zánik licence a licenční smlouvy 116
Licenční smlouva k redakčnímu systému **116**
Smlouva o servisu a údržbě redakčního systému **117**
Incidenty a vady 117
Servis, údržba a customizace 118
Obsahové náležitosti servisní smlouvy 120
Forma servisní činnosti 120
Kategorizace vad/incidentů 120
Reakční doba a doba odstranění vady 123
Odstranění vady – vyřešení incidentu 124
Odpovědnost za škodu a sankce 125
Doba trvání smlouvy a způsoby jejího ukončení 126
Odstoupení od smlouvy 126
Výpověď smlouvy 127
Vypořádání při ukončení servisní smlouvy 128
Smlouva o správě internetových stránek **129**
Smluvní úprava webhostingu a telekomunikačních služeb **130**
Bezpečnost webových stránek 133
Smlouva o poskytování webhostingových služeb 134
Smlouva o poskytování telekomunikačních služeb 136
Shrnutí kapitoly **138**

KAPITOLA 4
Odpovědnost za vlastní obsah zpřístupněný prostřednictvím internetu **139**

Jaký je rozdíl mezi vlastním a cizím obsahem **139**
Původní obsah 141
Převzatý obsah 141
Embedded link a převzetí cizího obsahu 143
Příklady nepřijetí a přijetí cizího obsahu za vlastní 144
Povaha odpovědnosti za vlastní obsah **145**
Trestněprávní odpovědnost 146

Správněprávní odpovědnost 146
Soukromoprávní odpovědnost 147
Rozsah odpovědnosti za vlastní obsah a nároky z ní vyplývající 147
Nárok na náhradu škody 148
Nárok na vydání bezdůvodného obohacení 149
Vyčíslení škody a bezdůvodného obohacení 150
Poskytnutí přiměřeného zadostiučinění 151
Opatření k nápravě 151
Právo na informace 152
Shrnutí kapitoly 152

KAPITOLA 5
Odpovědnost za cizí obsah zpřístupněný prostřednictvím Internetu 153
Osoby odpovědné za cizí obsah 153
Povaha odpovědnosti za cizí obsah 154
Odpovědnost trestněprávní a správní 154
Odpovědnost soukromoprávní 155
Omezení odpovědnosti za cizí obsah 157
Osoby, na které se omezení odpovědnosti za cizí obsah vztahuje 157
Rozsah omezení odpovědnosti za cizí obsah 158
Rozpor mezi ZNSIS a Směrnicí o elektronickém obchodu 159
Vyloučení povinnosti zkoumat nebo kontrolovat cizí obsah 161
Odpovědnost poskytovatelů prostoru za jimi ukládaný cizí obsah (hosting) 162
Vymezení služby spočívající v ukládání cizího obsahu 162
Podmínky vzniku neodpovědnosti za cizí obsah („vplutí do bezpečného přístavu“) 163
Podmínky zachování neodpovědnosti za cizí obsah („udržení se v bezpečném přístavu“) 166
Zánik podmínky nevědomosti - oznámení o protiprávnosti obsahu 166
Odstranění či znepřístupnění obsahu 167
Pravidlo následné prevence 168
Významná soudní rozhodnutí - odpovědnost poskytovatelů prostoru za jimi ukládaný cizí obsah 169
Odpovědnost poskytovatelů přístupu za přenášený cizí obsah (prostý přenos - mere conduit) 174
Co je a co není prostým přenosem 175
Hranice odpovědnosti 176
Další podmínky odpovědnosti 176
Vybraná rozhodnutí k odpovědnosti za přenos cizího obsahu (mere conduit) 177
Odpovědnost za cizí obsah ukládaný do vyrovnávací paměti („caching“) 182
Co se rozumí cachingem 182
Hranice odpovědnosti poskytovatele 183
Rozhodnutí vztahující se ke službě „caching“ 184

Odpovědnost spojená s poskytováním a využíváním odkazu na cizí obsah 185
Nepřímá odpovědnost za poskytování prostého odkazu na cizí obsah 185
Nepřímá odpovědnost za cizí obsah v případě využívaní tzv. embedded linku 186
Soudní rozhodnutí zabývající se odpovědností za poskytování odkazu 186
Přehled odpovědností za cizí obsah 187
Shrnutí kapitoly 188

KAPITOLA 6
Uzavírání smluv, obchodování na internetu, e-commerce, aukční portály 189

Uzavírání smluv prostředky komunikace na dálku 189
Obecně k uzavírání smluv 189
Sjednávání smluv, nabídka a její přijetí 190
Rozdíl mezi uzavíráním smluv prostřednictvím e-mailu a webových stránek 191
Vážnost projevu vůle v prostředí internetu 192
Obecně k obchodním podmínkám 193
Připojení obchodních podmínek k nabídce 194
Odkaz na obchodní podmínky, seznámení se s nimi 194
Neúčinnost obsahu obchodních podmínek 196
Konflikt obchodních podmínek 197
Jednostranné změny obchodních podmínek 198
Spotřebitelské a adhezní smlouvy 200
Definice spotřebitele 201
Slabší strana a spotřebitel 204
Adhezní (formulářové) smlouvy 205
Ochrana slabší strany 206
Uzavření spotřebitelské smlouvy 208
Informační povinnost vůči spotřebiteli 208
Následky neposkytnutí informací spotřebiteli 212
Nepřípustná ujednání v obchodních podmínkách 213
Práva a povinnosti z uzavřené spotřebitelské kupní smlouvy 214
Práva a povinnosti z uzavřené spotřebitelské smlouvy o poskytování služeb 220
Elektronické aukce 221
Obecně 221
Dražba v elektronické podobě 222
Aukce provozovaná zájemcem o uzavření smlouvy 223
Aukce prováděná prostřednictvím nezávislého aukčního portálu 223
Vznik kupní smlouvy na aukčním portále nezávislého provozovatele 224
Odpovědnost provozovatele aukčního portálu 226
Odpovědnost účastníků e-aukce 228
Platební styk, platební transakce v rámci e-commerce 231
Off-line platební metody 232
On-line platební metody 232

Platební služby 235
Opatření proti praní špinavých peněz 236
Shrnutí kapitoly 237

KAPITOLA 7
Internetová reklama a spam 239

Internetová reklama a její právní regulace 239
Definice reklamy dle vnitrostátních předpisů a předpisů EU 239
Právní předpisy upravující internetovou reklamu 240
Formy internetové reklamy 248
Banner (proužková reklama) 249
Kontextová reklama, reklama na vyhledávačích, sociálních sítích a PPC reklama 249
Diskuzní skupiny 250
Katalogové zápisy 250
Spotřebitelské loterie a marketingové soutěže 250
Problematika cookies v rámci internetové reklamy 254
Protiprávní formy internetové reklamy 255
Metatagy jako součást zdrojových kódů internetových stránek 255
Klíčová slova v inzerci vyhledávačů 257
Mousetrapping a Pop up reklama 258
Reklama v internetových diskuzích a na sociálních sítích 258
Reklamní trójské koně 259
Spam – nevyžádané obchodní sdělení 259
Pojem spam a hlavní důvody jeho šíření 259
Definice spamu dle předpisů EU a vnitrostátních předpisů 261
Právní podmínky šíření spamu v ČR, legální postup 266
Další právní předpisy upravující problematiku spamu 271
Správní postihování spamu v ČR 273
Přehled soukromoprávních prostředků ochrany proti spamu 277
Obrana proti spamu prostřednictvím institutu nekalé soutěže 278
Obrana proti spamu prostřednictvím institutu ochrany osobnosti 281
Obrana proti spamu prostřednictvím závazkového deliktního práva 282
Prokazování původce (šiřitele) spamu 283
Technologické a komunitní formy ochrany proti spamu 288
Shrnutí kapitoly 291

KAPITOLA 8
Internetové vyhledávače 293

Krátce k vývoji vyhledávačů směrem k jejich dnešní podobě 294
Aktuální problémy vyhledávačů 295

Ochrana duševního a průmyslového vlastnictví v rámci služeb poskytovaných vyhledávači 295
Rozhodnutí Google France (Google v. Louis Vuitton a další) 297
Závěrem k používání klíčových slov ve vyhledávačích 304
Metavyhledávače a ochrana databází 305
Ochrana osobních údajů v rámci vyhledávačů a právo „být zapomenut“ 307
Ochrana hospodářské soutěže a dominantní postavení Google 313
Odpovědnost vyhledávačů za vyhledávání a poskytování odkazů na protiprávní obsah 316
Shrnutí kapitoly 317

KAPITOLA 9
Problematika zpřístupňování (sdílení) a stahování autorských děl 319

Autorské dílo na Internetu a jeho ochrana 319
Autorskoprávní ochrana obsahu 320
Omezení dispozic chráněným obsahem 323
Výjimky ze zákonné ochrany 325
Zpřístupňování díla prostřednictvím internetu 327
Rozmnožování díla 328
Sdělování díla veřejnosti 329
Některé zvláštní případy zpřístupňování obsahu 331
Zpřístupňování prostřednictvím zvláštních služeb (YouTube) a serverů (Megaupload, Ulož.to) určených ke sdílení obsahu 331
Sdílení v rámci peer to peer sítí 333
Odpovědnost provozovatelů a uživatelů peer to peer sítí 338
Streaming, video na požádání (video on demand) a webcasting 339
Webcasting jako televizní a rozhlasové vysílání 340
Webcasting jako kabelová televize 341
Další přenos rozhlasového nebo televizního vysílání formou webcastingu (retransmise) 342
Veřejnoprávní regulace streamingu 342
Poskytování a využívání odkazu (hyperlink, embedded linking) 343
Prostý (klikatelný) odkaz 344
Embedded link 345
Legální vs. nelegální obsah 345
Stahování díla z internetu 347
Rozmnožování díla 347
Přechodné či technické kopie obsahu 348
Stahování pro osobní účely, volné užití 349
Shrnutí kapitoly 350

KAPITOLA 10
Vybrané právní aspekty sociálních sítí **351**

Obecně k sociálním sítím **351**
Sociální sítě jako nový fenomén 351
Založení účtu uživatelem **352**
Uzavření smlouvy s provozovatelem sociálních sítí 352
Rozhodné právo pro smlouvu s provozovatelem sociálních sítí 353
Rozhodný soud pro spory ze smlouvy s provozovatelem sociální sítě 354
Volba uživatelského jména 355
Zpřístupňování povinných informací o podnikateli v prostředí sociálních sítí 356
Zpřístupňování obsahu a autorská práva **356**
Zpřístupňování vlastního obsahu 356
Osobnostní práva na sociálních sítích 357
Práva provozovatelů sociálních sítí k obsahu uživatele 360
Vkládání cizího obsahu 361
Reklama prostřednictvím sociálních sítí **361**
Obecně 361
Formy reklamy 362
Spam a sociální sítě 362
Regulace reklamy a sociální sítě 363
Reklama a nekalá soutěž 364
Skrytá reklama na sociálních sítích 364
Pracovněprávní vztahy a sociální sítě **366**
Obecně 366
Stručně k relevantní právní úpravě zákoníku práce 366
Chování zaměstnance na sociálních sítích a pracovněprávní dopady 367
Vnitřní předpisy zaměstnavatele – Corporate Social Media Governance 370
Soukromí a osobní údaje na sociálních sítích **372**
Obecný úvod k soukromí na sociálních sítích 373
Stručně k právní úpravě osobní údajů 374
Možné porušení právní úpravy na ochranu osobních údajů ze strany provozovatele – případ Max Schrems 376
Dopady případu Max Schrems vs. Data Protection Comissioner na Safe Harbor 379
Porušení právní úpravy na ochranu osobních údajů ze strany uživatele 380
Shrnutí kapitoly **382**

KAPITOLA 11
Internetová kriminalita a kybernetická bezpečnost **383**

Internetová kriminalita pojem a geneze **383**
Co je to internetová kriminalita? **384**
Internetová kriminalita – jak a proč vznikla? **386**

Druhy internetové kriminality **387**

Trestná činnost proti počítači **390**

Obecná majetková kriminalita 390
Průmyslová špionáž 390
Hacking (pronikání do systémů) 391
Carding (zneužívání platebních karet na internetu) 393
Skimming (útoky na bankomaty či platební terminály) 395
Phishing (podvodné vylákávání informací) 395
Pharming (podvodné přesměrování DNS) 396
Sniffing (neoprávněné monitorování elektronické komunikace) 397
Malware (tvorba a šíření škodlivého software) 397
DoS a DDos útoky 398

Trestná činnost s využitím počítače **399**

Moderní počítačové pirátství a warez 399
Podvody a zpronevěry 402
Padělání a penězokazectví 403
Útoky na čest a pověst, elektronická msta, pomluvy 403
Šíření pornografie 404
Extremismus na Internetu 406
Spamming (zasílání nevyžádaných e-mailových zpráv) 407
Phreaking (zneužívání telekomunikačních služeb) 407
Cybersquatting (domain grabbing, doménové pirátství) 408
Counterfeiting 408
Cybergrooming 409
Cyberstalking 409
Hoaxes, Urban Legends, poplašné zprávy všeho druhu 410

Boj proti internetové kriminalitě **411**

Prevence v oblasti internetové kriminality 411
Represe v oblasti internetové kriminality 412

Odhalování a dokazování internetových trestných činů **414**

Kybernetická bezpečnost **416**

Shrnutí kapitoly **418**

Závěrem **419**

Použitá a doporučená odborná literatura **421**

Použitá odborná literatura 421
Dále doporučená literatura 422
Články v odborných časopisech a sbornících 422

Rejstřík **423**

„Právo, a stejně tak jeho výklad, má sloužit praxi, nikoliv naopak.“

Na knize INTERNETOVÉ PRÁVO se podíleli advokáti následujících advokátních kanceláří:



JUDr. Lukáš Jansa
jansa@lawyer.cz

Mgr. Petr Otevřel
otevrel@lawyer.cz

Mgr. et Mgr. Petr Mališ
malis@lawyer.cz



JUDr. Jiří Čermák
Jiri.Cermak@bakermckenzie.com

JUDr. Ing. Michal Matějka
Michal.Matejka@bakermckenzie.com



JUDr. Petr Hostaš
hostas@akch.cz



JUDr. Ján Matejka, PhD.
matejka@itpravo.cz

O autorech



JUDr. Lukáš Jansa je advokátem advokátní kanceláře Jansa, Mokrý, Otevřel & partneři a předním odborníkem práva informačních technologií. Publikoval celou řadu odborných textů na téma softwarové a internetové právo v časopisu IT Systems nebo na stránkách *www.pravoit.cz*. Přednáší na odborných konferencích a seminářích právní problematiku softwaru a internetu. Je spoluautorem odborné publikace „Softwarové právo". Autor kapitoly 1, 3 a spoluautor kapitoly 7; korektura kapitol 2, 9 a 11 a závěrečná korektura textu knihy. Vedoucí autorského kolektivu.



Mgr. Petr Otevřel je advokátem advokátní kanceláře Jansa, Mokrý, Otevřel & partneři a je předním odborníkem v oblasti práva informačních technologií. Je autorem několika desítek článků na téma softwarové právo v odborných časopisech a na specializovaných internetových portálech. Prezentuje zejména problematiku smluv v IT na konferencích a seminářích. Je spoluautorem odborné publikace „Softwarové právo". Autor kapitoly 10 a spoluautor kapitoly 6; korektura kapitoly 3 a závěrečná korektura textu knihy.



JUDr. Jiří Čermák je advokátem a partnerem advokátní kanceláře Baker & McKenzie se zaměřením na právo informačních technologií, právo duševního vlastnictví a řešení sporů. Je předním specialistou v oboru internetového práva u nás. Pravidelně přednáší k různým tématům týkajícím se práva informačních technologií, externě působí na právnické fakultě v Praze a na EPO v Mnichově. Zakladatel portálu itpravo.cz. Publikoval desítky odborných textů z oblasti internetového práva a je autorem publikace „Internet a autorské právo" a spoluautorem publikace „ International Encyclopaedia of Laws for Cyber Law – Czech Republic". Autor kapitoly 4 a 9 a spoluautor kapitoly 5; korektura kapitoly 8.



Mgr. et Mgr. Petr Mališ je advokátem advokátní kanceláře Jansa, Mokrý, Otevřel & partneři, ve které se specializuje na internetové právo. V této oblasti publikoval na stránkách pravoit.cz celou řadu odborných článků. Přednáší na odborných konferencích témata z oblasti internetového práva. Autor kapitoly 8 a spoluautor kapitoly 5 a 6; korektura kapitoly 2, 4 a 10.



JUDr. Petr Hostaš je advokátem advokátní kanceláře ČÍŽEK HOSTAŠ a předním odborníkem v oblasti doménových jmen a práv s nimi spojených. Rozhoduje spory o doménová jména CZ a EU a přednáší o této problematice na odborných konferencích a seminářích. Autor kapitoly 2.



JUDr. Ing. Michal Matějka je advokátem advokátní kanceláře Baker & McKenzie a specialistou na právo duševního a průmyslového vlastnictví, právo informačních technologií a mezinárodní obchodní právo; v těchto oborech se rovněž věnuje publikační činnosti. O problematice internetové a počítačové kriminality přednáší na odborných konferencích a je autorem publikace „Počítačová kriminalita". Na témata duševní a průmyslové vlastnictví, nekalá soutěž a počítačová kriminalita přednáší rovněž na Fakultě informačních technologií ČVUT. Autor kapitoly 11.



JUDr. Ján Matejka PhD. je advokátem a ředitelem Ústavu státu a práva Akademie věd ČR. Jako odborník na internetové právo a softwarové právo působí v akademické sféře a je publikačně činný jak v odborných časopisech, tak v rámci portálu itpravo.cz. Je autorem odborné publikace „Internet jako objekt práva". Spoluautor kapitoly 7.

Poděkování

V této souvislosti děkujeme všem klientům a kolegům, kteří se pohybují ve světě Internetu a díky nimž jsme získali cenné zkušenosti, bez nichž by tato kniha vůbec nevznikla. Stejně tak patří dík trpělivosti blízkých za čas věnovaný spoluautorům k sepsání této knihy.

Řekli o knize

„Knihu "Internetové právo" mohu s klidným svědomím označit za povinnou četbu nejen pro internetové podnikatele. Knihu doporučuji mít při ruce také všem majitelům e-shopů, provozovatelům informačních portálů, blogerům či administrátorům webových stránek. Ať už internet využíváte pro osobní nebo komerční účely, kniha "Internetové právo" bude neocenitelným průvodcem a rádcem. Vedle definice základních pojmů v knize najdete také řadu užitečných příkladů z praxe."

Václav Liška, CEO segment online cenových srovnávačů pro střední Evropu, Naspers

„Vydání nové publikace Internetové právo jsem uvítala jako velmi užitečný počin v oblasti, ve které stále chybí dostatek kvalitní a aktuální odborné literatury. Rozhodně by měla zajímat jak soukromé osoby, které prostřednictvím internetu činí běžně právní úkony, aniž si vždy uvědomují jejich právní dopad, tak právníky či manažery IT firem, kteří využívají internet ke svému podnikání a potřebují správně smluvně ošetřit jeho využívání. Kniha odbornou a přitom přehlednou a čtivou formou seznamuje čtenáře s důležitými fakty, novými informacemi, právními výklady i užitečnými návody, díky kterým každý její čtenář může získat znalost, která mu pomůže se lépe a mnohem bezpečněji orientovat v poměrně složité a dosud tak málo právně zpracované oblasti, jakou je internetové právo."

Mgr. Eva Freiburgová, právník ČSOB

„Kniha Internetové právo je povinné čtení pro každého, kdo podniká v oblasti internetu. Velmi stručným a hlavně jasným způsobem sumarizuje právní rámec podnikání na internetu a pomáhá se v této složité problematice zorientovat. Vřele doporučuji k přečtení."

Tomáš Braverman, CEO Heureka.cz

"*Veľmi pekný počin. Komplexná publikácia, ktorá prakticky popisuje zásadné témy internetového práva.*"

Gabriel Kalapoš, CEO PayU Czech Republic s.r.o. - PayU.cz

Předmluva

Internet dnes představuje neodmyslitelnou součást našeho života a v podstatě lze říci, že náš čas se už rozlišuje na on-line a off-line. A i ve stavu off-line jsme neustále obklopováni technologiemi závislými na internetu, které naše životy ovlivňují v rámci každodenního života. Z dnešního úhlu pohledu lze uzavřít, že historie začíná být psána Internetem na Internetu.

Jsem velice rád, že se podařilo dát dohromady tým předních odborníků, kteří se pohybují téměř každý den v právním světě internetu. Naším cílem bylo, abychom právní internetovou problematiku pojali a vysvětlili čtenářům srozumitelně k praktickému užitku. Záměrně jsme se vyhnuli některým oblastem internetového práva, jako je e-government či elektronický podpis, které by vydaly na samostatnou knihu, a rádi odkážeme v doporučené literatuře na publikace dalších autorů. Jsem si vědom složitostí, které s sebou nese sepsání jakéhokoliv prvního vydání, navíc v širším autorském kolektivu, jehož členové jsou extrémně časově vytíženi, proto věřím, že druhé vydání nenechá na sebe čekat řadu let a jakákoliv chybějící témata doplní a nedostatky odstraní.

Na úvod této knihy bych rád citoval z rozhovoru s polsko-britským předním sociologem Zygmuntem Baumanem: „*Žijeme ve dvojím světě. On-line a off-line, tedy na síti a v reálném světě. On-line je vše velmi jednoduché, stačí pár kliků a je to hotovo, a když se chcete vrátit, můžete se vrátit. Na Internetu si snadno uděláte přátele a snadno se jich zbavíte… Ale když trávíte devět hodin před obrazovkou, ztrácíte schopnosti potřebné k životu v reálném světě, off-line…V reálném světě nejste pánem nad situací, jako je tomu při používání počítače. Nemůžete vymazat či zavřít, co se vám nelíbí. Na Internetu si vytváříme ‚bublinu pohodlí'. Čteme to, co upevňuje náš pohled na svět, a vyhýbáme se informacím, které by nás nutily přehodnotit své názory. Na Internetu se – pokud chcete – můžete zcela vyhnout informacím, se kterými nesouhlasíte, a vyhledávat jen to, co vyhovuje vašemu pohledu na svět. Je vám něco nepohodlné? Klik – a je to pryč. Zkuste takhle řešit problémy v reálném světě – nejde to… Informační technologie povzbuzují lidi k tomu, aby z reálného světa utíkali do pohodlného světa, který si sami formují podle obrazu svého.*"[1] Z vlastní právní zkušenosti však víme, že i na Internetu celá řada jednání může mít pozitivní i negativní dopady do reálného života. Podceňovat tak internetové prostředí je velmi ošemetné. Svět Internetu není však vždy jednoduše ovládán jeho uživatelem a platí pro něj určitá pravidla, právní regulace, jejichž uvědomění si je pro každého přínosem. Pokud k tomuto uvědomění přispěje byť jen nepatrně tato kniha, pak naše práce nebyla zcela zbytečná.

V Ostravě 10. 10. 2015
Lukáš Jansa za kolektiv autorů

1 Citace z rozhovoru publikovaného na portálu Idnes.cz dne 26. 8. 2015 pod *http://technet.idnes.cz/zygmunt-bauman-rozhovor-sociolog-uprchlici-migrace-technologie-modernita-stesti-gjb-/veda.aspx?c=A150826_151023_veda_mla*

KAPITOLA 1

Úvod do problematiky internetového práva

Co se dozvíte v této kapitole

- Co spadá do oblasti práva informačních technologií, internetového a softwarového práva
- Jaké jsou základní právní předpisy dopadající na oblast internetu

Právo informačních technologií

Právo informačních technologií není omezeno pouze na internet. Internetové právo je vedle softwarového práva podoblastí práva informačních technologií. Někdy se hovoří také o rozšířené oblasti práva ICT (Information and Communications Technology), tzn. práva informačních a telekomunikačních technologií.

S internetovým právem velice úzce souvisí i právo telekomunikační, které umožňuje vzájemné propojení počítačů a sítí a existenci internetu, a lze ho tak zařadit do širšího pojmu práva informačních technologií.

Obor práva informačních technologií lze vyjádřit následovně:



Obrázek 1.1 Schéma obsahového pojetí práva informačních technologií

Je možné konstatovat, že stěžejním základem práva informačních technologií je právo softwarové a internetové.

Internetové právo

Internetové právo je tvořeno zejména problematikou:

- **Internetu a internetových stránek**
  Jde o témata jako Internet a internetové připojení (ISP), odpovědnost za obsah internetových stránek, ochrana osobních údajů, tvorba internetových stránek a jejich provoz, webhosting a sociální sítě apod.
- **Doménových jmen**
  Sem patří otázky tvorby a registrace doménových jmen a dispozic s nimi, spekulativních registrací a doménových sporů, problematika nekalé soutěže (parazitování na pověsti, nebezpečí vyvolání záměny) a ochrany názvu firmy a ochranných známek.
- **Internetového obchodování a komunikace**
  Do této kategorie lze zařadit uzavírání smluv na internetu, otázky spojené s e-shopy, internetovými aukcemi, platbami přes Internet a také reklamou v prostředí internetu, včetně spammingu. Internetovou komunikaci představují otázky spojené s emaily a komunikátory (skype, icq atd.).
- **Autorského práva na Internetu**
  Autorské právo na Internetu zahrnuje problémy spojené s užitím autorských děl v prostředí Internetu (fotografie, texty) a dále zejména otázky sdílení a stahování autorských děl (hudby, filmů atd.) atd.
- **E-governmentu**
  Elektronizace státní správy (vč. e-justice) je formou fungování a komunikace státní správy a samosprávy s občany a právnickými osobami. V širším pojetí lze podřadit do této oblasti i elektronické dokumenty a elektronický podpis.
- **Internetové kriminality**
  Internet je také prostředkem k páchání trestné činnosti, a to např. v podobě zásahu do autorských práv, formou phishingu, hackingu apod.

Softwarové právo

Softwarové právo je vymezeno následujícím okruhem témat:

- **Software a jeho vývoj**
  Předmětem je právní povaha softwaru (komerční SW a open source) a autorských práv k němu, problematika jeho vývoje zaměstnanci či na objednávku.

- **Licencování a distribuce softwaru a další dispozice**
  Udělování licencí k softwaru je základní formou, jak umožnit třetím osobám jeho užívání. Současně licence podléhají celé řadě forem distribuce směrem ke konečným zákazníkům, ať už přímo výrobci, tak prostřednictvím distributorů. Dalšími dispozicemi se rozumí jeho zveřejňování např. na internetu, převod výkonu autorských práv atd.
- **Dodání a implementace softwaru**
  S tím souvisí analýza softwaru a IT infrastruktury, právní úprava smluv o dodání a implementaci softwaru.
- **Servis a údržba softwaru**
  Servisní činnost softwaru je představována zejména odstraňováním incidentů. Pod pojmem údržba softwaru si lze představit otázky upgradu a customizace softwaru.
- **Outsourcing softwaru a Cloud Computing**
  Na základě těchto právních vztahů přebírá odpovědnost za funkčnost IT infrastruktury objednatele poskytovatel příslušné služby, v krajním případě jsou veškeré klíčové aplikace a data objednatele umístěny u poskytovatele.
- **Softwarové pirátství**
  Softwarovým pirátstvím se rozumí zásah do osobnostních či majetkových autorských práv k softwaru. Nároky z takového porušení či následky plynou jak z autorského zákona, tak z trestněprávních předpisů.
- **Bezpečnost a ochrana dat**
  Problematika bezpečnosti a ochrany dat získala na významu v souvislosti s rozvojem Cloud Computingu, kdy dochází k ukládání dat v datových centrech formou hostingu.

Spoluautoři této publikace Lukáš Jansa a Petr Otevřel se věnovali tématům softwarového práva v obdobně pojaté knize Softwarové právo, Praktický průvodce právní problematikou v IT, vydané v Computer Pressu v roce 2011 a v rozšířené a aktualizované podobě v roce 2014.

Právní předpisy internetového práva

Základní právní předpisy, které jsou v oblasti internetového práva použitelné, představuje následující přehled, který uvádí i dále v textu užívané zkratky předpisů.

Právní předpisy ČR a ostatní závazná pravidla

„AutZ“ nebo „autorský zákon“ – Zákon č. 121/2000 Sb., autorský zákon

„OZ“ nebo „občanský zákoník“ – Zákon č. 89/2012 Sb., občanský zákoník

„TrZ“ nebo „trestní zákoník“ – Zákon č. 40/2009 Sb., trestní zákoník

„ZEK“ – Zákon č. 127/2005 Sb., o elektronických komunikacích

„ZNSIS" – Zákon č. 480/2004 Sb., ze dne 29. července 2004, o některých službách informační společnosti a o změně některých zákonů

„ZoKB" – Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů

„ZOOÚ" – Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně dalších zákonů, ve znění pozdějších předpisů

„ZOZ" – Zákon č. 441/2003 Sb., o ochranných známkách, ve znění pozdějších předpisů

„ZP" – Zákon č. 262/2006 Sb., zákoník práce

„ZRR" – Zákon č. 40/1995 Sb., o regulaci reklamy

Zákon č. 221/2006 Sb., o vymáhání práv z průmyslového vlastnictví, ve znění pozdějších předpisů.

Zákon č. 64/1986 Sb., o České obchodní inspekci

Zákon č. 284/2009 Sb., o platebním styku

Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci trestné činnosti a financování terorizmu (zákon proti praní špinavých peněz)

Vyhláška Národního bezpečnostního úřadu č. 316/2014 Sb.

Pravidla registrace doménových jmen v ccTLD .cz

Pravidla alternativního řešení sporů Cz.NIC

Právní předpisy EU

„Směrnice o elektronickém obchodu" – Směrnice o určitých aspektech služeb v informační společnosti, zejména elektronického obchodu, v rámci vnitřního trhu (2000/31/ES)

Směrnice o harmonizaci autorského práva a práv s ním souvisejících v informační společnosti (2001/29/ES)

Směrnice o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí (2006/24/ES)

Směrnice o ochraně spotřebitele v případě smluv uzavřených na dálku (97/7/ES)

Směrnice o nekalých obchodních praktikách (2005/29/ES)

Směrnice o klamavé a srovnávací reklamě (2006/114/ES)

Směrnice o odpovědnosti za vadné výrobky (85/374/EHS)

Směrnice o nepřiměřených podmínkách ve spotřebitelských smlouvách (93/13/EHS);

Směrnice o dodržování práv duševního vlastnictví (2004/48/ES)

Směrnice o právní ochraně počítačových programů (2009/24/ES)

Směrnice o právní ochraně databází (96/9/ES)

Nařízení o zavedení domény nejvyššího řádu „.eu“ (733/2002)

Nařízení, kterým se stanoví obecná pravidla pro zavádění a funkce domény nejvyšší úrovně .eu, a zásady, jimiž se řídí registrace (874/2004)

Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. 11. 2001

Mezinárodní úmluva o ochraně výkonných umělců, výrobců zvukových záznamů a rozhlasových organizací ze dne 26. října 1961

Bernská úmluva o ochraně literárních a uměleckých děl, revidované znění

Všeobecná úmluva o autorském právu revidovaná v Paříži dne 24. července 1971

Smlouva Světové organizace duševního vlastnictví (WIPO) o právu autorském (Ženeva 1996)

Nařízení Evropského parlamentu a Rady (EU) č. 1215/2012 ze dne 12. prosince 2012 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech

Shrnutí kapitoly

- Právo informačních technologií je tvořeno internetovým a softwarovým právem, částečně právem databází a telekomunikačním právem.
- Základem internetového práva je autorský zákon a občanský zákoník, zákon o kybernetické bezpečnosti a elektronických komunikacích, zákon o některých službách informační společnosti, Směrnice o elektronickém obchodu a celá řada dalších souvisejících předpisů.

KAPITOLA **2**

Domény a doménová jména

Co se dozvíte v této kapitole

- Co jsou domény a jaké jsou jejich druhy
- Jak je spravována síť Internet
- Jak mohou práva k doménám kolidovat s jinými právy
- Jak řešit spory o domény a o porušování jiných práv doménami či jejich užíváním
- Příklady rozhodnutí ve sporech týkajících se domén

Klasifikace a využití domén

Každý počítač komunikující v počítačové síti musí mít přiřazenu číselnou adresu (IP[2] adresu), numerický kód vyjádřený v desítkové nebo dvojkové soustavě, který umožňuje identifikaci počítače zapojeného do struktury počítačových sítí a jeho komunikaci s jinými počítači zapojenými do příslušných sítí. K identifikaci přitom musí mít každý počítač zapojený do sítě jednu unikátní adresu odlišnou od adresy jakéhokoliv jiného počítače v téže síti.

K usnadnění komunikace prováděné uživateli se pak uvedená číselná adresa nahrazuje doménovým jménem, které je zpravidla zapamatovatelnější než prostý numerický kód.

Prvotní funkce identifikace jednotlivého počítače však z uživatelského hlediska není jedinou funkcí doménového jména. Doménové jméno má celou řadu dalších, druhotných funkcí, jež jsou z hlediska praktických potřeb uživatelů často důležitější než prvotní funkce identifikační.

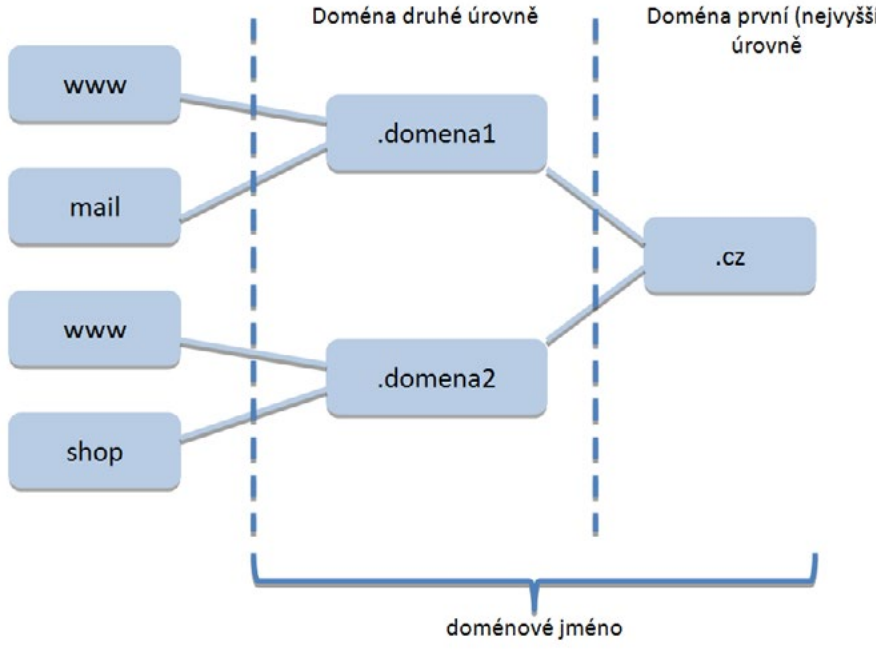
Pojmy doména a doménové jméno

Doménu (*domain*) ve smyslu, ve kterém je užívána v souvislosti s doménovými jmény, je třeba považovat za určitý uzavřený virtuální prostor v síti Internet.

Systém domén je konstruován na základě hierarchického principu: na nejvyšší úrovni hierarchie existují tzv. domény nejvyšší úrovně (označované též jako domény první úrovně nebo prvního stupně, *top level domains*, nebo jen *TLD*), v jejichž rámci jsou pak vytvářeny další domény, označované jako domény nižších úrovní. Každá doména je přitom spravována určeným správcem, který umožňuje v rámci své domény třetím osobám vytvářet domény nižších úrovní.

2 Internet Protocol – datový protokol používaný pro přenos dat přes tzv. paketové sítě

Doménové jméno je pak tvořeno souhrnem domén všech úrovní, které jsou spolu hierarchicky propojeny a jejichž spojení příslušní správci jednotlivých domén umožnili. Jednotlivé domény jsou přitom navzájem oddělovány tečkou a pořadí jednotlivých úrovní domén je dáno pořadím v sekvenci domén oddělených tečkou, a to počítáno zprava.



Obrázek 2.1 Struktura úrovní domén

Doménové jméno nelze ztotožňovat s doménou, neboť zatímco domény reprezentují určitý prostor v síti Internet, doménové jméno je jen označením souhrnu nejméně dvou a více domén uspořádaných v určité hierarchii. Pro účely této kapitoly však budeme za doménové jméno považovat, nebude-li výslovně uvedeno jinak, pouze souhrn dvou domén, a to domény druhé úrovně a domény nejvyšší úrovně. Je to proto, že teprve u souhrnu dvou domén se vůbec dá hovořit o doménovém jméně (za doménové jméno nelze považovat nižší počet domén než dvě) a především na této „úrovni" doménových jmen se řeší valná většina právních otázek, které existence a užití doménových jmen vyvolává.

Druhy domén nejvyšší úrovně (TLD – top level domains)

Domény nejvyšší úrovně jsou buď národní, nebo generické. Národní domény (označované jako *country code top level domains* nebo jen *ccTLD*) se prakticky kryjí s územím jednotlivých

států a jsou tvořeny dvoupísmenným ISO[3] kódem (např. CZ pro Českou republiku, DE pro Spolkovou republiku Německo, FR pro Francii apod.). Mezi národní domény je přitom obvykle řazena i EU doména Evropské unie, byť se jedná o výjimku, neboť doména EU není doménou státního útvaru, ale skupiny států.

Historicky starší generické domény (označované jako *generic top level domains* nebo jen *gTLD*) jsou nadnárodní. Generické domény byly zřizovány v několika vlnách. Tzv. původní generické domény jsou tvořeny třípísmenným kódem (např. COM, GOV, ORG, NET apod.), posléze vznikaly další domény (např. MUSEUM, AERO apod.). Generické domény se dále člení na domény určené výlučně některým subjektům (typicky např. doména GOV určená pro vládní instituce USA) nebo otevřené k volnému užití (typicky doména COM).

Z původních generických domén v podstatě pouze doména COM byla určena pro obecné komerční užití. Protože počet registrovaných domén prudce rostl, začaly se objevovat požadavky na zavedení nových generických domén, které by byly určeny výhradně určitému odvětví, prezentaci měst či dalším specifickým účelům.

Od roku 2013 je možné za přesně stanovených podmínek vytvářet další domény nejvyšší úrovně, které jsou označovány jako nové generické domény (*new gTLD*). V současnosti již bylo zřízeno několik set nových generických domén nejvyšší úrovně, včetně BERLIN, LONDON, BEER, CAR, AFRICA, VERSICHERUNG, GURU, XYZ a řady dalších.

Zvláštním druhem domén nejvyšší úrovně jsou tzv. IDN[4] domény. Doménový systém byl původně vytvořen pouze z písmen, která se nacházela v tzv. ASCII tabulce odpovídající svým obsahem anglické abecedě. Podstatnou je přitom skutečnost, že v této tabulce jsou výhradně znaky v latince a bez diakritiky. Když se diakritika a nelatinkové jazyky začaly používat v elektronické komunikaci, tj. v e-mailech nebo na webových stránkách, objevil se požadavek, aby bylo připuštěno používání nelatinkových jazyků či diakritiky i v názvech domén. Je tak umožněno zřizování domén nejvyšší úrovně (např. РФ) s diakritikou či v nelatinkových jazycích, přičemž připuštění registrace domén druhé úrovně s diakritikou (РОССИЯ.RU či РОССИЯ.РФ) záleží na správci každé domény nejvyšší úrovně. V České republice tato možnost zatím zavedena nebyla.[5]

Tvorba doménového jména

Doménové jméno je z technického hlediska sekvencí vybraných znaků, která představuje symbolické označení unikátní číselné adresy počítače, tedy IP adresy. V názvu domény může být použito 37 znaků, tedy pouze znaky obsažené v ASCII tabulce, a to písmena bez interpunkce (a–z), dále čísla od 0 do 9 a konečně spojovník neboli pomlčka (–).

3 ISO 3166-1 (seznam kódů jmen států a závislých území vydaný International Organization for Standardization, Ženeva)

4 Internationalized Domain Names

5 Průzkum „Internationalized Domain Names" publikovaný na *www.háčkyčárky.cz*

Přestože přirozený jazyk obsahuje znaky, které nejsou v ASCII tabulce obsaženy (interpunkce, nelatinkové znaky), neexistují univerzálně platná pravidla převodu těchto nelatinkových znaků do znění doménového jména. Pouze pravidla platná pro registraci doménových jmen pod doménou nejvyšší úrovně EU[6] stanoví, že zvláštní znaky: ~ @ # $ % ^ * ( ) + = { } | \ / : ; ‘ , . ?, mezery nebo interpunkce mají být v odpovídajícím doménovém jméně zcela eliminovány, nahrazeny spojovníkem (-) nebo, je-li to možné, přepsány odpovídajícím ekvivalentem (např. zvláštní znak „&“ se obvykle přepisuje jako „*a*“ v češtině, „*and*“ v angličtině nebo „*et*“ ve francouzštině). Analogicky lze tuto úpravu (která je jen právní normou stanoveným principem vyplývajícím z technických možností systému DNS) vztáhnout i na ostatní doménová jména, tedy např. i doménová jména v doméně nejvyšší úrovně CZ. Lze proto v této souvislosti konstatovat, že obsahuje-li označení (název, obchodní firma, ochranná známka) některé zvláštní znaky, které nelze použít v textu doménového jména, mezery nebo interpunkci, tyto budou při přepisu do textu doménového jména vypuštěny, nahrazeny spojovníkem nebo přepsány (tam, kde takový znak lze přepsat).

V rámci systému tzv. IDN domén je připuštěno i použití jiných znaků, tedy znaků nelatinkových abeced a znaků s diakritikou. IDN nicméně slouží pouze pro větší komfort uživatelů domén. Pro účely samotného internetového provozu dochází k překladu IDN domén na ASCII tvar domény, takže doménové jméno **háčkyčárky.cz**[7] se automaticky překládá na **xn--hkyrky-ptac70bc.cz**.

Doménové jméno skládající se z domény druhé úrovně a domény nejvyšší úrovně může mít nejvýše 64 znaků, přičemž při použití IDN domény se nepočítá počet znaků dle zápisu s diakritikou, ale počet znaků, který bude zjištěn po překladu na ASCII tvar domény. Doménové jméno **háčkyčárky.cz** tak má 22 znaků.

Z uvedeného tak vyplývá, že v doméně CZ je k dispozici 61 znaků pro použití v doméně druhé úrovně (znaky „.cz“ jsou u všech doménových jmen v doméně CZ stejné); celkový počet teoreticky možných doménových jmen v doméně CZ tak činí necelých 36^{61} a je představován číslem s 94 nulami za číslem 44. Jedno z několika málo doménových jmen, která v doméně CZ využívají plný potenciál znaků, je doménové jméno hryhryhryhryhryhryhryhryhryhryhryhryhryhryhryhryhryhryhryhryhryhry.cz[8].

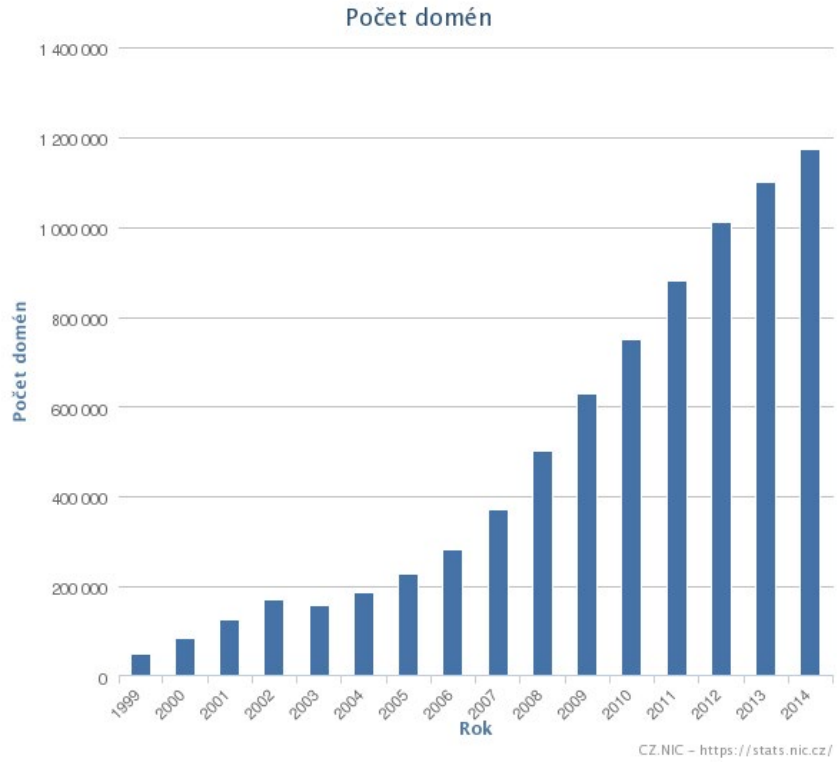
Pokud jde o celosvětově nejrozšířenější doménu COM, v červenci 2015 bylo v této doméně zaregistrováno cca 118,6 milionu domén[9]. V doméně CZ ve stejném období bylo zaregistrováno cca 1,2 milionu domén.

6 Článek 11 Nařízení Komise (EC) č.874/2004 ze dne 28. 4. 2004 vymezující pravidla veřejné politiky týkající se implementace a funkcí domény nejvyšší úrovně .eu a principů, jimiž se řídí registrace

7 IDN systém dosud v České republice nebyl zaveden a doménové jméno háčkyčárky.cz je jediným doménovým jménem s diakritikou v doméně nejvyšší úrovně CZ

8 Domain Report 2014 (*https://stats.nic.cz/reports/2014/*) vydaný sdružením CZ.NIC, z.s.p.o.

9 Údaj dle Domain Count Statistics for TLDs (*http://research.domaintools.com/statistics/tld-counts/*)



Obrázek 2.2 Nárůst registrací domén .cz

Základní podmínky registrace domén

Doménová jména neexistují „sama o sobě". Jedná se o záznamy v databázi správce domény nejvyšší úrovně, případně o záznamy v tzv. zónovém souboru na příslušném DNS[10] serveru. Doména je přitom zaregistrována a doménové jméno vzniká až zápisem záznamu do takové databáze.

Registrace domén se řídí celou řadou norem, přičemž valná většina z nich je územně univerzální, tj. musí být dodržovány v rámci všech domén nejvyšší úrovně, aby byla zajištěna technická funkčnost DNS systému. Tyto normy se v prostředí Internetu nazývají Requests For Comments (RFC), a ač jde převážně o neoficiální dokumenty, jsou obecně uznávány a dodržovány.

Jedinečnost doménového jména

Jedním z nejdůležitějších principů, který vyplývá z požadavku jednoznačné identifikace číselné adresy, a tím i unikátní identifikace jednotlivého počítače, a který tak velkou měrou ovlivňuje

10 Domain Name System

právní vztahy týkající se doménových jmen, je požadavek jedinečnosti doménového jména. Jestliže každý z počítačů zapojených do sítě počítačů musí mít unikátní IP adresu, která umožní komunikovat právě a jedině s tímto jediným počítačem, každé doménové jméno musí odkazovat právě na jednu unikátní IP adresu. Jen na okraj lze upozornit, že jedna unikátní IP adresa může být dostupná pod více doménovými jmény, tzn. že může existovat několik různých doménových jmen, přičemž všechna budou odkazovat na jednu unikátní IP adresu. Takové adresování je běžné zejména v případech, kdy jeden počítač má být dostupný pod více než jedním doménovým jménem.

V rámci jedné domény nejvyšší úrovně (TLD) nemohou existovat dvě nebo více stejných domén druhé úrovně. V národní doméně České republiky (CZ) tak nemohou existovat dvě identické domény tvořící doménové jméno. Na druhou stranu však identicky znějící doména může být zaregistrována v rámci různých domén první úrovně – vedle sebe tak mohou existovat doménová jména domena.cz, domena.com, domena.de apod., přičemž každé z doménových jmen může náležet jiné osobě a každé může (ale nemusí) odkazovat na jiný počítač.

Princip „first come, first served"

Registrace doménových jmen se ve většině domén nejvyšší úrovně řídí principem „kdo první o doménu požádá, dostane ji ", tedy registraci doménového jména získá ten, kdo o registraci jako první požádá. Historicky první registrace doménových jmen probíhaly prakticky v několika jednotkách případů denně, mimo zájem subjektů, které by se mohly cítit registrací doménového jména dotčeny. Teprve v okamžiku, kdy se začal rozvíjet obchodní potenciál doménových jmen, rapidně narostl počet registrovaných doménových jmen a začalo docházet ke střetům registrovaných doménových jmen s právy k ochranným známkám, obchodním firmám apod. Odbornou veřejností je proto argumentováno ve prospěch změny tohoto principu tak, aby přednost při registraci doménových jmen získaly subjekty, které mají jiné jim svědčící právo (např. k ochranné známce).

Z praktických důvodů je obtížné taková doplňující pravidla zavádět do existující domény nejvyšší úrovně, ve které jsou již registrovány statisíce či miliony doménových jmen. V těchto případech jsou práva třetích osoba ošetřena v rámci soudních sporů či alternativního řešení sporů, ve kterých se zkoumá případné porušení těchto práv registrací nebo užíváním doménového jména a stanoví se nápravné prostředky.

Jednodušší je pak situace u nově zaváděných domén nejvyšší úrovně, u kterých se většinou před otevřením přístupu k všeobecně dostupné registraci stanoví časově omezená lhůta, ve které lze zaregistrovat pouze doménová jména shodná s registrovanými ochrannými známkami nebo obchodními firmami s tím, že po uplynutí takové doby (většinou označována jako „Sunrise period") je další registrace možná na základě principu „kdo první o doménu požádá, dostane ji". V případě zavádění domény nejvyšší úrovně EU tak byla nařízena tzv. etapová registrace, když v první etapě bylo možné po dobu 2 měsíců registrovat domény pouze pro registrované ochranné známky, zeměpisná označení a jména, včetně jmen veřejných subjektů, a ve druhé etapě pak opět po dobu 2 měsíců domény pro označení, která mohla být zaregistrována v první etapě, i pro veškerá ostatní označení.

Omezení držby domény

Pro registrace domén v národní doméně nejvyšší úrovně CZ nejsou stanoveny žádné zvláštní podmínky, které by musel držitel domény splňovat, a to ani omezení územní. Držitelem CZ domény se tak může stát i zahraniční právnická či fyzická osoba, bez ohledu na to, zda má nějakou vazbu na území České republiky. Pouze na výzvu správce domény či soudu musí držitel, který má bydliště, sídlo či kontaktní adresu mimo území Evropské unie, poskytnout platnou doručovací adresu na území EU.

Naproti tomu např. na Slovensku platí, že držitelem domény v národní doméně nejvyšší úrovně SK může být pouze právnická osoba se sídlem na území Slovenské republiky, fyzická osoba, která je občanem Slovenské republiky a má na území Slovenské republiky trvalý pobyt, a konečně fyzická osoba, která je podnikatelem.[11] Obdobné omezení je stanoveno i pro domény nejvyšší úrovně EU, ve které mohou držet domény pouze subjekty se sídlem či bydlištěm v některém z členských států Evropské unie.

V případech některých domén nejvyšší úrovně, a to zejména domén generických, platí zvláštní pravidla. Generické domény nejvyšší úrovně lze dělit na tzv. sponzorované a nesponzorované. Sponzorované domény nejvyšší úrovně jsou určeny pro užití určitou komunitou, ať již národnostní, etnickou, územní, profesní či technickou, zatímco domény nesponzorované jsou určeny volnému použití.

Platí tak například, že domény v doméně AERO může držet pouze subjekt zabývající se leteckou přepravou, domény v doméně GOV jsou vyhrazeny pouze pro vládní instituce USA, domény v doméně CAT jsou vyhrazeny pouze pro použití komunitou hovořící katalánštinou či že domény v doméně XXX jsou určeny pro pornografické stránky. Seznam sponzorovaných generických domén se rozrůstá s novými generickými doménami (new gTLD), takže přibyly domény pro subjekty podnikající v pojištění (VERSICHERUNG), pro subjekty působící v určitém městě (LONDON, PARIS) či pro fanoušky piva (BEER) a podobně.

Správa doménového systému

Systém doménových jmen je spjat s počítačovými sítěmi, zjednodušeně se sítí Internet. Označení síť Internet, jak je běžně používáno, je však nepřesné, neboť síť Internet je v podstatě síť sítí, neboť vzniká až spojením jiných počítačových sítí. Internet jako takový proto není předmětem vlastnictví (ani soukromého, ani veřejnoprávního), nemá jednoho provozovatele ani jakoukoliv centrální správu, byť jsou jisté činnosti nezbytné k provozu některých z částí Internetu (např. systému doménových jmen) zajišťovány centrálně.

11 Článek 3.4 Pravidel poskytovania menného priestoru v internetovej doméne SK vydaných správcem domény SK, společností SK-NIC, a.s. (*www.sk-nic.sk*)

Vznik sítě Internet

Za rok vzniku Internetu je obvykle považován rok 1969, kdy v rámci experimentálního ověřování možností datových přenosů byla vytvořena síť ARPANET (podle financující armádní grantové agentury ARPA, Advanced Research Projects Agency). Přestože šlo o vládní výzkum financovaný z armádních zdrojů, byla síť po úspěšném otestování zkoumaných principů předána do správy akademické obci. Postupným připojováním dalších akademických sítí k původní síti ARPANET pak začal být propojený systém těchto sítí označován v 80. letech minulého století jako „Internet“[12].

V současnosti je Internet často považován pouze za soubor www stránek. Přitom však, jak bylo výše uvedeno, síť Internet, resp. její předchůdci, fungovala od 70. let minulého století až do roku 1991 bez služby World Wide Web (označované jako „www“). Ta je tedy službou podstatně mladší, než je celá síť Internet, a je jen jednou z jejích nadstaveb. Mezi další nadstavby (služby) se řadí elektronická pošta (e-mail), služba FTP[13] nebo spíše v minulosti užívané BBS nebo Gopher. Tuto skutečnost je přitom důležité brát v úvahu i v souvislosti s doménovými jmény. V drtivé většině případů jsou doménová jména užívána v souvislosti se službou www, a odkazují tedy na www prezentace, nejčastější „formu“ Internetu, kterou si v současnosti lze představit. I doménové jméno, které není využíváno pro službu www, však může být užíváno pro celou řadu dalších služeb, nejčastěji pro službu elektronické pošty (e-mail).

Pro fungování Internetu je zapotřebí dodržovat určité technické konvence číslování a nastavování parametrů. Přidělování a koordinování takovýchto numerických hodnot musí být jednotné, jinak by Internet nemohl fungovat univerzálně. V roce 1972 byl Ministerstvem obrany USA tento úkol přidělen (prostřednictvím již zmíněné grantové agentury ARPA) kalifornské univerzitě USC (University of Southern California) a jejímu Institutu informatiky (Information Sciences Institute). Role „správce identifikátorů“, která byla středisku ISI přidělena, nebyla zpočátku nějak formálně pojmenována. Teprve později, v roce 1987, se poprvé objevuje formální označení Internet Assigned Numbers Autority (IANA – Internetová autorita pro přidělování čísel) v souvislosti s internetovými funkcemi střediska ISI. Do její působnosti spadá i zastřešení distribuce číselných IP adres. Dalším úkolem organizace IANA je formální zastřešení správy systému DNS – faktická správa jednotlivých TLD domén je sice v rukou konkrétních správců, ale jejich vzájemná koordinace a dohled nad činností a správou kořenových jmenných serverů (DNS) byly úkolem právě organizace IANA.

IP adresy

Jak již bylo uvedeno výše, doménové jméno je z technického hlediska sekvencí vybraných znaků, která představuje symbolické označení unikátní číselné adresy počítače (IP adresa). Při konstruování technických protokolů, na kterých je postaven Internet, se počítalo s tím, že

12 Peterka, J.: Kolikáté narozeniny slaví Internet? citováno 6. 1. 2003, Dostupný z: *www.earchiv.cz/b03/b0106001.php3* (z tohoto zdroje jsou čerpány i další údaje o historii sítě Internet a její správy)

13 File Transfer Protocol

každý počítač bude vybaven svou vlastní číselnou adresou, která musí být odlišná od adres ostatních počítačů. Požadavek, aby každý uzlový počítač měl odlišnou adresu od všech ostatních uzlů, při dnešním rozsahu Internetu znamená celosvětovou unikátnost těchto adres – neboli celosvětově koordinovaný způsob distribuce těchto adres, který dokáže zajistit, že žádné dva uzly nedostanou přiděleny stejné adresy.

Původní IP protokol verze 4 (IPv4) umožňoval teoreticky přidělení 2^{32} unikátních adres (cca 4 miliardy IP adres). Vzhledem k prudkému růstu počtu zařízení, která musí mít pro komunikaci v síti Internet přidělenou IP adresu, byl zaveden IP protokol verze 6 (IPv6), který umožňuje přidělení cca 2^{128} unikátních adres, což představuje cca 66 trilionů IP adres na každý centimetr čtvereční zemského povrchu včetně oceánů.

Příklad IP adres ve verzi IPv4 a IPv6 a k nim přiřazené domény:

- IPv4 77.75.74.80
- IPv6 2a02:598:3333::3
- Doménové jméno: ans.seznam.cz (jeden se serverů Seznam.cz)

Z počátku se IP adresy přidělovaly z jednoho centra. Tím bylo od roku 1987 středisko DDN NIC, spadající pod rezort obrany USA. Později se faktické přidělování všech adres z jediného centra ukázalo být organizačně neúnosné, a tak se přistoupilo k delegaci distribučních pravomocí – z jediného centra se přidělovaly větší bloky IP adresy dalším „přidělovatelům" (označovaným jako IP registry) a ti pak v okruhu své působnosti zajišťovali distribuci „v malém".

O koordinaci přidělování IP adres po celém světě se v současné době starají tři koordinační střediska, formálně zastřešená organizací IANA: středisko RIPE (Reseaux IP Europeenne), s působností pro Evropu, středisko APNIC (Asia-Pacific NIC) pro oblast Asie a Pacifiku a středisko InterNic pro zbytek světa. Přidělování IP adres není totožné s registracemi doménových jmen a střediska koordinující přidělování IP adres nejsou zodpovědná za registrace doménových jmen.

Správci domén nejvyšší úrovně

V roce 1998 byla z podnětu organizace IANA, vykonávající z pověření vlády USA většinu praktických řídících funkcí sítě Internet, vytvořena nová nevýdělečná organizace jménem ICANN (Internet Corporation for Assigned Names and Numbers), která řízení sítě Internet převzala a drží je dosud. Její postavení je přitom velmi silné, o čemž svědčí mimo jiné skutečnost, že jejímu souhlasu podléhalo i vytvoření nové domény nejvyšší úrovně EU[14].

Pro jednotlivé domény nejvyšší úrovně jsou určeni jednotliví správci, označovaní též jako Registry (TLD Registry); pro doménu COM se jedná o VeriSign Global Registry Services, pro doménu CZ sdružení CZ.NIC, pro doménu DE organizaci DENIC eG apod. Protože Inter-

14 Bod 14 Preambule Nařízení Evropského parlamentu a Rady č. 733/2002 ze dne 22. 4. 2002 o implementaci domény nejvyšší úrovně. eu

net byl původně akademickou sítí, stávali se správci osoby z akademické obce (např. Polsko). V některých případech jsou správci soukromé podnikatelské subjekty (např. Slovensko) nebo nevýdělečné organizace ve formě nadací či sdružení poskytovatelů přístupu k síti Internet (např. Rakousko, Česká republika, Německo). V některých případech převzal registraci doménových jmen stát, který tuto činnost provozuje většinou v rámci správy telekomunikačního prostředí (např. Finsko, Španělsko).

Správa generických domén nejvyšší úrovně je dána smluvními vztahy mezi jednotlivými správci a organizací IANA, potažmo ICANN.

Jednotliví správci národních domén nejvyšší úrovně (ccTLD) odvozují své právo spravovat příslušnou doménu zpravidla historicky. Dá se říci, že v počátcích byla správa národních domén nejvyšší úrovně získávána „okupací", tj. obsazením dosud nefunkční a nikým nespravované domény nejvyšší úrovně zájemcem, který byl pro organizaci IANA (ICANN) natolik důvěryhodný, že mu bylo možno správu domény nejvyšší úrovně delegovat. V současnosti se organizace ICANN snaží, aby správa národní domény nejvyšší úrovně byla vykonávána důvěryhodnou organizací ve shodě s místní internetovou komunitou a místními státními orgány. Vztahy jednotlivých správců národních domén nejvyšší úrovně s organizací ICANN jsou proto postupně formalizovány cestou uzavírání smluv, dohod nebo memorand – taková smlouva byla kupříkladu v roce 2006 uzavřena sdružením CZ.NIC, které je správcem domény CZ.

Registr doménových jmen

Základní povinností správce domény nejvyšší úrovně je vedení registru doménových jmen, tedy seznamu, ve kterém je ke každému zaregistrovanému doménovému jménu zapsána osoba, která je jeho držitelem, a dále IP adresa počítače, ke které má být doménové jméno přiřazeno, resp. adresa DNS serveru, který obsahuje záznam o tom, ke které IP adrese je doménové jméno přiřazeno.

Ze samotné podstaty fungování systému doménových jmen pak vyplývá, že takový registr, který není ničím jiným než počítačovou databází, může být pro každou jednu doménu nejvyšší úrovně pouze jeden, protože jen tak je možné zajistit, že nedojde k zaregistrování dvou domén druhé úrovně v rámci jedné domény nejvyšší úrovně, a tedy k vytvoření dvou identických doménových jmen, přičemž každé by mohlo odkazovat na jinou IP adresu. V takovém případě by se totiž odkazování na jednotlivé počítače stalo nepredikovatelným a vedlo by ve svém důsledku ke znemožnění základní funkce systému doménových jmen, a totiž identifikace jednotlivých počítačů.

Z požadavku jedinečnosti registru doménových jmen pak vyplývá, že správcem domény nejvyšší úrovně může být pouze jediný subjekt, jehož postavení jako správce registru doménových jmen je tak ze své podstaty přirozeně monopolní.

Technické zajištění správy domény

Technické zajištění správy domén nejvyšší úrovně se u jednotlivých správců (Registrů) liší, nicméně v zásadě lze hovořit o dvou základních modelech. V prvním zajišťuje správce vedle správy samotného registru doménových jmen i registrační proces jako takový, a je tak jediným kontaktním místem pro „zákazníky", tedy osoby registrující doménová jména.

V ostatních případech si správce ponechává pouze správu registru doménových jmen a standardizuje registrační procedury (technické a právní parametry procesu) a samotné registrace (tedy primární kontakt se „zákazníky") přebírají tzv. registrátoři.

Na rozdíl od IP adres, které jsou uživatelům přidělovány, jak bylo popsáno výše, u doménových jmen se zpravidla jedná o jiný přístup. Zájemci o doménová jména si vytváří doménová jména sami z předem dané množiny povolených znaků a s takto vytvořenou kombinací žádají o zaregistrování vytvořené skupiny znaků v registru doménových jmen druhé úrovně. Správce domény nejvyšší úrovně tedy doménová jména nepřiděluje, ale jen zapíše do seznamu doménové jméno vytvořené osobou žádající o registraci.

Doména CZ

Doména nejvyššího stupně CZ, která „náleží" k České republice, vznikla v roce 1993 při vzniku samotné České republiky a nahradila do té doby používanou doménu CS. Jejím správcem je zájmové sdružení právnických osob CZ.NIC, z. s. p. o.

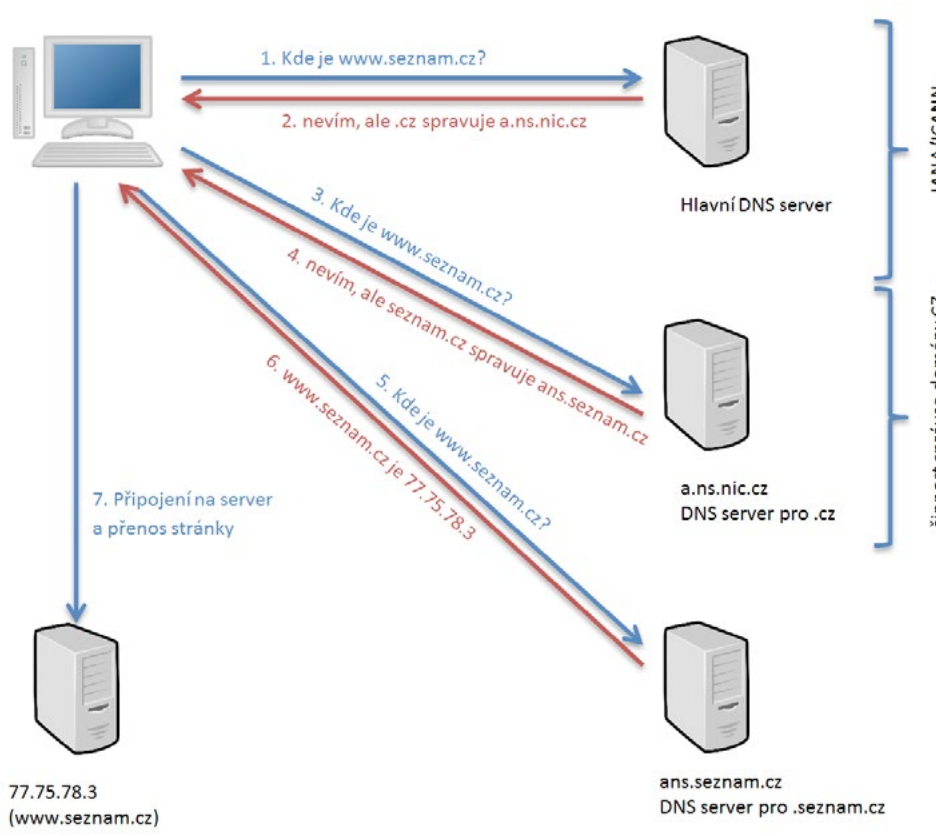
Těžiště činnosti CZ.NIC spočívá v provozování primárního jmenného (DNS) serveru, obsahujícího registr (databázi) doménových jmen a s nimi spojených technických a identifikačních údajů (technickými údaji jsou zejména informace o jednotlivých jmenných serverech, které jsou k doménovému přiřazeny, resp. na kterých je veden záznam o tom, jaká služba je jeho prostřednictvím poskytována; identifikačními údaji jsou zejména údaje o držitelích doménových jmen, kontaktních osobách, adresách apod.). Dále provozuje sekundární jmenné servery replikující základní databázi – tzv. zónu v různých zeměpisných zónách.

Sdružení CZ.NIC dále stanovuje pravidla pro registrace doménových jmen a zajišťuje správu a přístup k databázi, ve které jsou registrovaná doménová jména vedena. Samotné registrace domén pak provádějí smluvní partneři, tzv. registrátoři.

Ve světě i v České republice mívá správa doménových jmen povahu soukromé správy. Internetové adresy (domény) jsou vyňaty z veřejné správy adres vykonávané Českým telekomunikačním úřadem, proto ani doménová jména nepodléhají státní kontrole, a to na rozdíl od veřejné správy telefonních čísel jakožto znaků podléhajících veřejnoprávní regulaci.

Jak funguje DNS?

Ve zjednodušené podobě lze systém DNS popsat jako systém neustálé komunikace mezi počítači a DNS servery, které dotazující se počítač postupně směřují k vybranému cíli.



Obrázek 2.3 Systém DNS

Právní povaha domén

Doménová jména jsou soukromoprávním předmětem právních vztahů s povahou nehmotných věcí. Práva k nim jsou pak relativními majetkovými právy, tj. závazky, jež souvisí s využíváním služeb elektronických komunikací, nikoliv právy absolutními (věcnými právy a právem dědickým). Disponibilním předmětem právních vztahů k doménovým jménům je tak pohledávka ze smlouvy o registraci doménového jména. To v praxi nepřináší žádné problémy, protože i pohledávku, jež tvoří nehmotný majetek, resp. jmění, lze ocenit, postoupit, vložit do základního kapitálu či zastavit.

Vznik doménového jména

V prvé řadě je třeba určit, jak doménové jméno jako předmět právních vztahů vzniká. Doménové jméno je de facto jen určitým povoleným způsobem uspořádaná sekvence povolených

znaků, která před registrací (zápisem do registru/databáze) existuje jen jako jedna z možných kombinací, jak mohou být povolené znaky pro dané doménové jméno uspořádány. Doménové jméno jako takové tak vzniká až v okamžiku, kdy je z dostupných znaků vybrána konkrétní sekvence a tato sekvence je zaregistrována jako doménové jméno v odpovídajícím seznamu.

Za doménové jméno nelze považovat sestavení znaků do podoby odpovídající doménovému jménu před tím, než je tato sekvence zaregistrována v příslušném seznamu, neboť teprve zápisem do seznamu doménové jméno vzniká ve smyslu, který je předvídán systémem doménových jmen. Zápis zvolené sekvence znaků do příslušného registru, který může být označován též jako rejstřík, databáze nebo seznam, představuje konstitutivní akt, neboť zamýšlený účinek – vznik doménového jména – je dosažen právě a jedině tímto zápisem. Teprve provedením příslušného zápisu tak je doménové jméno objektivně zachyceno a je mu poskytnuta ochrana před registrací dalšího obsahově totožného doménového jména. Tato skutečnost nicméně nepředstavuje vznik absolutní ochrany označení, které je součástí doménového jména, neboť toto označení může kolidovat s jinými právními tituly.

Stejně tak teprve okamžikem zápisu doménového jména do odpovídajícího registru (tato skutečnost bude dále označována jako registrace doménového jména) vznikají k tomuto doménovému jménu práva osoby, která si je zaregistrovala, tedy zejména právo doménové jméno držet a užívat. Osoba, která si doménové jméno zaregistrovala, je zpravidla označována jako „držitel".

Z právního hlediska je vznik doménového jména představován uzavřením smlouvy o registraci doménového jména, kterou se správce domény nejvyšší úrovně zavazuje žadateli zaregistrovat doménu druhé úrovně a žadatel (budoucí držitel doménového jména) se zavazuje zaplatit odměnu ve výši tzv. registračního poplatku. Uzavřená smlouva je smlouvou adhezní, tj. smlouvou, která vychází ze standardních obchodních podmínek týkajících se příslušné domény nejvyšší úrovně a kterou nelze měnit. V doméně CZ jsou těmito obchodními podmínkami Pravidla registrace doménových jmen v ccTLD .cz.[15]

Smlouva o registraci doménového jména je smlouvou nepojmenovanou (§ 1746 odst. 2 OZ) a je uzavírána zpravidla distančním způsobem, tj. bez současné přítomnosti obou stran, a prostřednictvím elektronických prostředků, ať již ve formě výměny e-mailových zpráv nebo prostřednictvím webových formulářů.

Zánik doménového jména

Registrace doménového jména může trvat jen po dobu, po kterou doménové jméno splňuje technické podmínky pro doménová jména (v některých doménách nejvyšší úrovně se např. vyžaduje, aby každé registrované doménové jméno mělo přiřazeno funkční DNS servery), dokud držitel doménového jména splňuje stanovené požadavky (v některých doménách nejvyšší úrovně se vyžaduje, aby držitel měl sídlo na území příslušného státu) apod. Jednou z obvyklých podmínek je pak i pravidelné hrazení ceny za jednotlivá v příslušné doméně zúčtovatelná období. Jedná se zpravidla o období jednoho roku či jeho násobky. V důsledku nezaplacení poplatku na další zúčtovací období pak registrace doménového jména zaniká (expiruje).

15 *https://www.nic.cz/page/314/pravidla-a-postupy/*

Držitel doménového jména je oprávněn v rámci svého práva s doménovým jménem nakládat. Může kdykoliv zrušit registraci doménového jména (ať již opominutím uhradit cenu za další registrační, období nebo přímým pokynem ke zrušení registrace) a zrušením registrace doménové jméno zanikne. Nejedná se však o zánik absolutní, neboť doménové jméno s identickým zněním může být kdykoliv znovu „vytvořeno", ať již původním držitelem, nebo třetí osobou.

Zánikem registrace doménového jména by mělo zároveň docházet k zániku práv držitele k tomuto doménovému jménu. Z rozhodnutí Vrchního soudu v Praze ve věci doménového jména **cad.cz**[16] nicméně vyplývá, že zánikem registrace doménového jména pro nezaplacení poplatku na další období neztrácí původní držitel právo bránit třetí osobě v tom, aby si takové „uvolněné" doménové jméno pro sebe zaregistrovala, jestliže držiteli i nadále svědčí právo k označení, které bylo obsaženo v doménovém jménu.

Převod doménového jména

Doménové jméno může být předmětem převodu, byť formálně jde o nakládání s pohledávkou věřitele na majetkové plnění poskytované správcem domény nejvyšší úrovně jako dlužníkem. Ve skutečnosti tak dochází k postoupení pohledávky ze smlouvy o registraci doménového jména (§ 1879 OZ), jejímž obsahem je povinnost správce domény nejvyšší úrovně udržovat za sjednaných podmínek záznam o existenci doménového jména v registru doménových jmen, případně půjde i o možnost postoupení celé smlouvy (§ 1895 OZ)[17].

Zástava doménového jména

Zástavou může být každá věc, s níž lze obchodovat. Věcí v tomto smyslu je přitom vše, co je rozdílné od osoby a slouží potřebě lidí. Zástavou tak mohou být i pohledávky, tedy i pohledávka ze smlouvy o registraci doménového jména.

Protože registr doménových jmen, ve kterém jsou registrovaná doménová jména zapsána, není tzv. veřejným seznamem, nemůže zástavní právo k doménovému jménu vzniknout zápisem do tohoto registru (§ 1316 OZ). Správci domén nejvyšší úrovně přitom ani zápis údaje o tom, že doménové jméno je předmětem zástavního práva, do centrálního registru neumožňují. Zástavní právo k doménovému jménu, resp. k pohledávce ze smlouvy o registraci doménového jména, tak vznikne účinností zástavní smlouvy, strany si však mohou ujednat zápis zástavního práva do rejstříku zástav (§ 1335 odst. 2 OZ), který je veden Notářskou komorou ČR[18].

Exekuce doménového jména

Doménové jméno, resp. pohledávka ze smlouvy o registraci doménového jména, může být i předmětem výkonu rozhodnutí či exekuce.

16 Rozsudek Vrchního soudu v Praze ze dne 13. 9. 2006, sp.zn. 3 Cmo 114/2006, cad.cz

17 Telec, I.: Nový občanský zákoník ve společnosti sítí, Právní rozhledy č. 23–24/2012, s. 853

18 *www.nkcr.cz*

Zvláštní a v praxi dosud neřešenou otázkou nicméně může být, zda realizací výkonu rozhodnutí (exekuce), při kterém dojde ke zpeněžení doménového jména (pohledávky ze smlouvy o jeho registraci), nemůže dojít k porušení práv původního držitele (v exekučním řízení dlužníka).

Předmětné doménové jméno totiž mohlo odpovídat jménu či názvu (obchodní firmě) původního držitele nebo mohlo být totožné s jeho ochrannou známkou. V takovém případě ovšem osoba, která v rámci exekučního řízení doménové jméno získá, může začít okamžitě porušovat práva původního držitele k názvu či ochranné známce. Původní držitel pak má právo domáhat se ochrany svých práv, a to i proti osobě, která doménové jméno řádně získala v rámci exekučního řízení.

Realizace výkonu rozhodnutí (exekuce) by tak mohla vést k tomu, že nabyvateli, který doménové jméno získá v rámci výkonu rozhodnutí, může být zakázáno jeho užívání, pokud by soud dospěl k závěru, že jeho registrací či užíváním dochází k porušování práv původního držitele.

Takový závěr však považujeme za extrémní, neboť přiznat dlužníkovi, kterému bylo doménové jméno odebráno zákonným postupem k zajištění úhrady jeho dluhu, ochranu před tím, aby nabyvatel doménového jména mohl takové doménové jméno užívat, by bylo v rozporu se zásadou, že výklad a použití právního předpisu nesmí být v rozporu s dobrými mravy (§ 2 odst. 3 OZ) a že nikdo nesmí těžit ze svého nepoctivého nebo protiprávního činu (§ 6 odst. 2 OZ).

Samozřejmě není vyloučeno, aby předmětem exekuce byla současně jak např. ochranná známka, tak doménové jméno.

Kolize domén s právy třetích osob

Doménová jména jsou často v kolizi s jinými právními instituty, zejména s právy na označení. Vyplývá to především z požadavku jedinečnosti doménového jména, kdy v rámci jedné domény nejvyšší úrovně nelze zaregistrovat dvě (nebo i více) identické domény druhé úrovně.

Kolize doménových jmen s právy třetích osob může být neúmyslná, často je však vyvolána úmyslně, tj. osoba registrující doménové jméno ví nebo musí vědět o tom, že registrováním doménového jména poruší práva třetích osob, a při registrování doménového jména jí tak nesvědčí dobrá víra.

Dalším důvodem četných kolizí je fakt, že doménová jména (na rozdíl např. od práv na označení) nemají teritoriální povahu. I když je tedy doménové jméno registrováno v doméně nejvyšší úrovně COM, je dostupné z celého světa, tedy i z České republiky. I doménové jméno zaregistrované v doméně COM a zapsané v databázi vedené na počítačích umístěných např. v USA tak může kolidovat s ochrannou známkou zapsanou v České republice.

Za důvod kolizí lze pak považovat i princip „first come, first served", užívaný při registracích doménových jmen prakticky ve všech doménách nejvyšší úrovně. Tento princip má svůj význam, neboť za situace, kdy registrační proces probíhá takřka výlučně automatizovanými procesy, nelze očekávat, že by bylo technicky možné před registrací doménového jména provést kontrolu, zda doménové jméno nekoliduje s ochrannými známkami národními (tedy za-

psanými ve státu, v jehož doméně má být doménové jméno registrováno), zahraničními nebo mezinárodními. Kolize s právy k ochranným známkám je přitom jen jednou z mnoha kolizí, které připadají v souvislosti s doménovými jmény v úvahu, a na rozdíl od ochranných známek zpravidla tato jiná práva, se kterými může doménové jméno kolidovat, nejsou uvedena ve veřejně dostupných databázích (ostatně ani databáze ochranných známek všech zemí nejsou veřejně dostupné), a automatizované vyhledání možné kolize při registraci doménového jména tak nepřipadá v úvahu bez opuštění automatizovaného procesu registrace.

Celá řada práv, se kterými mohou doménová jména kolidovat, je kromě toho takového charakteru, že posouzení, zda dochází v důsledku registrace doménového jména k jejich porušení, je předmětem subjektivního hodnocení, které nelze přenechat automatizovanému procesu. Přechod na ruční zpracování registrací doménových jmen se zapojením subjektivního hodnocení možného porušení práv třetích osob, by tak představoval v prvé řadě několikanásobné zvýšení nákladů spojených s procesem registrace a dále podstatné prodloužení doby mezi podáním žádosti o registraci a jejím vyřízením. Kromě toho by se správce příslušné domény nejvyšší úrovně dostal do pozice, kdy bude nahrazovat zkoumání střetu doménového jména a dalších práv, které jinak provádí soudy nebo jiné nezávislé orgány. Z těchto důvodů je proto obecně přijímán a uplatňován princip „first come, first served", tedy s tím, že nejprve dojde k zaregistrování doménového jména a teprve poté se na základě podnětů dotčených osob hodnotí případné střety s jinými právy.

Mezi základní obecné principy uplatňované při posuzování kolizí práv a doménových jmen přitom patří to, že při posuzování zaměnitelnosti domén a ochranných známek, názvů či jmen se nepřihlíží k té části doménového jména, která je tvořena doménou nejvyšší úrovně. Je tak nerozhodné, že ochranná známka (název či jméno) neobsahuje označení domény nejvyšší úrovně (např. text „.cz"), neboť tento dovětek je sice důležitý z technického hlediska pro provoz počítačů, ale nemá rozlišovací způsobilost z hlediska běžného vnímání. Podstatné tak jsou dominantní prvky ochranných známek, názvů a jmen a to, zda v doménovém jménu jsou použity tyto dominantní prvky.[19]

Určitá typická jednání vedoucí ke kolizím doménových jmen získala své pojmenování:

- **Cybersquatting či domain-grabbing** – registrace a následné užívání doménového jména ve zlé víře na úkor ochranné známky, obchodní firmy názvu nebo jména jiné osoby. Typickým příkladem je registrace domény odpovídající ochranné známce, kterou si vlastník ochranné známky dosud nezaregistroval jako doménové jméno, nebo registrace domény, která je již zaregistrována pod jinou doménou nejvyšší úrovně. Příkladem je doménové jméno **komercnibanka.biz**, jehož registrace kolidovala s ochrannou známkou KOMERČNÍ BANKA a které bylo po skončení sporu převedeno na navrhovatele.
- **Typosquatting** – registrace doménových jmen využívající obvyklých překlepů při psaní na klávesnici, popřípadě jazykových neznalostí uživatelů (např. seynam.cz).
- **Domain hijacking** – únos či krádež doménového jména je buď jakékoliv jednání spočívající v registraci označení podléhajícího ochraně, tedy např. ochranné známky (viz

19 Např. Rozsudek Nejvyššího soudu ČR ze dne 3. 5. 2006, 32 Odo 447/2006

cybersquatting), nebo jednání využívající skutečnosti, že většina pokynů týkajících se doménových jmen je zadávána elektronicky. Podvržením e-mailů s pokynem k převodu domény může proto dojít ke změně držitele, a tedy k získání kontroly nad obsahem, který je prostřednictvím doménového jména dostupný. Toto jednání je nebezpečné zejména v tom, že uživatelé Internetu se mohou domnívat, že se nachází na oficiálních stránkách majitele práv k dotčenému označení, a je-li takové označení užíváno k obchodním aktivitám zahrnujícím např. zadávání platebních údajů, hesel apod., tedy jedná-li se např. o internetový obchod, útočník může v důsledku únosu doménového jména získat přístup k přihlašovacím údajům či číslům platebních karet uživatelů.

- **Reverse domain hijacking** – „obrácený" únos či krádež doménového jména představuje jednání, kterým se vlastník později zaregistrované ochranné známky či obchodní firmy domáhá v soudním či mimosoudním řízení převodu staršího doménového jména.

Kolize doménových jmen navzájem

Doménové jméno může v prvé řadě kolidovat s jiným doménovým jménem. V drtivé většině případů se jedná o registrace spekulativní, parazitující na jiném doménovém jménu. Může se jednat o záměnu fonetickou vycházející z předpokládané neznalosti cizího jazyka běžného uživatele Internetu nebo o tzv. překlepové doménové jméno využívající neznalosti přesného znění původního doménového jména (tam, kde původní doménové jméno např. obsahuje zdvojenou hlásku, je zaregistrováno doménové jméno s jednou hláskou) nebo typických překlepů při psaní na klávesnici počítače.

Překlepové doménové jméno se přitom nemusí od původního doménového jména odlišovat jen záměnou pořadí některých písmen, za překlepové doménové jméno lze považovat i případ doménového jména **wwwpaegas.cz**, využívajícího překlepu ve formě absence tečky (.) při zápisu kompletní adresy *www.paegas.cz*, která by jinak odkázala uživatele na prezentaci jednoho z operátorů mobilních sítí v České republice.

Ochranné známky

Ochrannou známkou může být označení schopné grafického znázornění, zejména slova, včetně osobních jmen, barvy, kresby, písmena, číslice, tvar výrobku nebo jeho obal, pokud je toto označení způsobilé odlišit výrobky nebo služby jedné osoby od výrobků nebo služeb jiné osoby. Ochrany přitom požívají na území České republiky ochranné známky

- národní, zapsané v rejstříku ochranných známek vedených Úřadem průmyslového vlastnictví,
- registrované známky mezinárodní, zapsané v rejstříku vedeném Mezinárodním úřadem duševního vlastnictví na základě mezinárodní přihlášky ve smyslu Madridské dohody o mezinárodním zápisu ochranných známek (1891) nebo Protokolu k Madridské dohodě (1989),