

Obsah

Předmluva	15
------------------------	-----------

Právní vědy	17
--------------------------	-----------

1 Budování právního státu a vývoj právního řádu v České republice po roce 1989	19
---	-----------

1.1 Úvod	19
----------------	----

1.2 Státoprávně-politická dimenze změn.....	19
---	----

1.3 Nový hodnotový základ a jeho bezprostřední projevy v právním řádu.....	20
---	----

1.4 Vyrovnání se s minulostí a napravení křivd	25
--	----

1.5 Změny v organizaci justice.....	27
-------------------------------------	----

1.5.1 Soudnictví.....	27
-----------------------	----

1.5.2 Státní zastupitelství.....	30
----------------------------------	----

1.5.3 Svobodná právnická povolání	31
---	----

1.5.4 Ombudsman.....	33
----------------------	----

1.6 Reakce na vývoj po roce 1989 a další významné milníky v českém právním řádu.....	33
---	----

1.6.1 Právo Evropské unie.....	33
--------------------------------	----

1.6.2 Další významné změny v právním řádu	35
---	----

1.7 Současná situace a možné perspektivy	38
--	----

2 Několik poznámek a rozhodnutí Nejvyššího soudu ČR ke kybernetické kriminalitě.....	41
---	-----------

2.1 Úvodem	41
------------------	----

2.2 K tomu, co lze považovat za kybernetickou kriminalitu	41
---	----

2.3 Aktuální judikatura Nejvyššího soudu k některým případům kybernetické kriminality.....	46
---	----

2.4 Několik procesních souvislostí.....	49
---	----

2.5 Závěrem	51
-------------------	----

3 Význam kriminalistiky z pohľadu ochrany slobody človeka	52
3.1 Úvod.....	52
3.2 Kriminalistika a ochrana slobody človeka.....	54
3.3 Zákonnosť procesu dokazovania	57
3.4 Zákonnosť a prípustnosť dôkazu	62
3.5 Záver	64
4 Právo neobviniť sa v podmínkách zákona o kybernetickej bezpečnosti.....	65
4.1 Úvod.....	65
4.2 Analýza vzťahu povinností ukládaných ZKB a súvisiacimi predpisy vzhľadom k právu neobviniť sa.....	66
4.3 Závěr	78
5 Právny rámec pre trestnoprávny postih neoprávnených prístupov a zásahov do počítačových systémov a údajov v Slovenskej republike.....	81
5.1 Úvod.....	81
5.2 Účel a význam trestnoprávneho postihu neoprávnených prístupov a zásahov do počítačových systémov a údajov, ako spôsobov kybernetickej kriminality	82
5.3 Trestné činy postihujúce neoprávnené prístupy a zásahy do počítačových systémov a údajov v Trestnom zákone Slovenskej republiky	84
5.4 Záver	93
6 Záludnosti informačných technológií	95
6.1 Úvod.....	95
6.2 Distanční smlouvy	95
6.3 Elektronizace justice	96
6.4 Elektronický spis.....	97

6.5	Distanční řízení.....	98
6.6	Dokazování a informační technologie.....	100
7	Odpovědnost poskytovatelů služeb informační společnosti na Internetu – současnost a perspektiva ...	104
7.1	Úvod	104
7.2	Současný právní stav	105
7.3	Blíží se plíživě povinnost obecného dohledu?	108
7.4	Návrh nařízení o jednotném trhu digitálních služeb a jeho vliv na současný stav	111
7.5	Návrh mechanismu oznamování nezákonného obsahu a opatření s tím spojená	112
7.6	Závěr.....	114
8	Zamyšlení nad možnostmi prevence kybernetické kriminality.....	115
8.1	Úvod	115
8.2	Kriminalita v kyberprostoru	116
8.3	Pachatelé kybernetické kriminality	117
8.4	Odhalování a dokazování kybernetické kriminality	119
8.5	Hmotněprávní úprava	121
8.6	Závěr.....	122
9	Trestnoprávní ochrana súkromia v kybernetickom priestore.....	123
9.1	Úvod	123
9.2	Právo na súkromie ako základné ľudské právo	124
9.3	Kybernetický priestor	125
9.4	Hmotnoprávne garancie ochrany práva na súkromie	128
9.5	Trestnoprocesné garancie ochrany práva na súkromie.....	130
9.6	Záver.....	132
10	Quo vadis, Data Retention?	134

10.1	Úvod – povinnost Data Retention v právním řádu ČR.....	134
10.2	Dosavadní vývoj právní úpravy Data Retention.....	135
10.2.1	Počátky povinnosti Data Retention v právním řádu ČR.....	135
10.2.2	Prohlášení neplatnosti Data Retention směrnice	136
10.2.3	Další rozhodování Soudního dvora EU	138
10.2.4	Rozhodnutí národních soudů.....	139
10.2.5	Výjimky ze zákazu plošného uchovávání provozních a lokalizačních údajů.....	142
10.3	Klíčové právní otázky a problémy úpravy Data Retention.	143
10.3.1	Sledovaný cíl – boj proti terorismu, či proti (závažné) trestné činnosti?.....	143
10.3.2	Rozsah povinnosti Data Retention, oprávněné orgány..	145
10.4	Závěr: možné varianty dalšího vývoje právní úpravy Data Retention	147
10.4.1	Dopady aktuálních závěrů Soudního dvora.....	147
10.4.2	Možná změna právní úpravy ZoEK	148
10.4.3	Zachování stávající právní úpravy.....	150
11	Přestupky podle zákona o zpracování osobních údajů	151
11.1	Úvodem.....	151
11.2	Implementace unijní úpravy	152
11.3	Koncept zákonné úpravy.....	155
11.4	Zákaz zveřejnění osobních údajů.....	156
11.5	Přestupky za porušení nařízení 2016/679	158
11.6	Přestupky za porušení povinností podle hlavy III adaptačního zákona	159
12	Otazníky nad trestní politikou uplatňovanou v době pandemie v oblasti vězeňství	161
12.1	Úvod.....	161
12.2	Problémy české trestní a sankční politiky.....	162

12.3	Aktivity trestní justice, jednotlivců a nestátních neziskových organizací.....	164
12.4	Závěr	167
13	Digitální novoty v návrhu novely autorského zákona	170
13.1	Úvod	170
13.2	Vybrané digitální novoty	171
14	Nesnáze autorského práva	179
15	Soutěživá agrese z hlediska teorie her.....	184
15.1	Úvodní úvahy	184
15.2	Teorie her a soupeřivé chování.....	187
15.3	Sociální psychologie o soupeřivém chování	188
15.4	Český psycholog o agresivním chování	190
15.5	Agresivní chování a speciální skutkové podstaty nekalé soutěže	191
15.6	Agresivní chování a generální klauzule proti nekalé soutěži	193
15.7	Agresivní obchodní praktiky a evropská směrnice č. 2005/29/ES	194
16	Kybernetická bezpečnost, právo na štěstí a Nakatani-san v českém občanském zákoníku.....	197
16.1	Pojem práva na štěstí	197
16.2	Distributivní formy práva na štěstí	200
16.3	Nedistributivní formy práva na štěstí	202
16.4	Právo na štěstí a legitimita kybernetické bezpečnosti	204
16.5	Závěrečná poznámka	207
Kriminalistika.....		209

17 Základní parametry teorie a metodologie klasického a systémového pojetí kriminalistické identifikace 211

17.1	Úvod.....	211
17.2	Základní pojmy z oblasti kriminalistiky	213
17.3	Identifikace jako proces ztotožňování objektů, schéma systémového přístupu, stav a struktura systému	215
17.3.1	Kritérium shody objektu s modelovým objektem	218
17.3.2	Stochastická shoda	219
17.4	Kriminalistická znalecká identifikace.....	220
17.4.1	Komplexní struktura kriminalistické identifikace	222
17.4.2	Realizace řešení kriminalistického problému kriminalistickou identifikací	223
17.4.3	Systémové pojetí identifikace	224
17.5	Identifikace	226
17.5.1	Identifikace objektová	226
17.5.2	Identifikace systémů.....	229
17.6	Závěr	232

18 Pravděpodobnostní charakter závěrů znaleckých zkoumání 233

18.1	Úvod.....	233
18.2	Identifikace	233
18.3	Subjektivní charakter znaleckých závěrů.....	235
18.4	Věrohodnostní poměr	237
18.5	Doporučení ENFSI	240
18.6	Závěr	243

19 Digitálne dôkazné prostriedky v trestnom konaní 245

19.1	Úvodom	245
19.2	K podstate a aplikačnému využívaniu FDA pri odhaľovaní a objasňovaní trestnej činnosti.....	246

19.3	Digitálne dôkazné prostriedky – osobitosti ich zisťovania, zaisťovania, skúmania	248
19.4	Screenshoty – printscreeny ako digitálne dôkazné prostriedky	248
19.5	Komprimácia obsahu odpočúvania a záznamu telekomunikačnej prevádzky	251
19.6	Záver	253

20 Digitální stopy z pohledu kriminalistické kategorizace stop 254

20.1	Úvod	254
20.2	Paměťové a materiální stopy	259
20.2.1	Stopy obsahující informaci o základní struktuře působících objektů.....	260
20.2.2	Stopy převažujících charakteristik odraženého objektu nebo subjektu	261
20.2.3	Stopy dle předmětu zkoumání informačního obsahu ...	261
20.2.4	Stopy dle objemu, hmotnosti, rozměrů nebo viditelnosti	262
20.2.5	Stopy interakce při jejich vzniku	262
20.2.6	Sdružené stopy.....	264
20.3	Kategorizace stopy	264
20.4	Zařazení digitální stopy	265

21 Význam digitální stopy pro skutkový stav v trestní věci 268

21.1	Úvod	268
21.2	Skutkový stav v trestní věci.....	270
21.3	Digitální stopa jako důkaz?	271
21.4	Význam digitální stopy pro skutkový stav v trestní věci....	275
21.5	Závěr	278

22 Adolph Quetelet – polyhistor v kriminologii..... 279

22.1	Úvod.....	279
22.2	Život a dílo Adolpha Queteleta.....	279
22.3	Přínos pro rozvoj kriminologického bádání.....	280
Kybernetika		285
23 Myšlení 4.0, virtuální svět, společnost a stát		286
23.1	Internet vstupuje do našich životů	286
23.2	Vize Průmyslu 4.0 jako modelu uvažování	288
23.3	Paradigmata virtuálního světa.....	291
23.4	Stát a internetová revoluce.....	296
23.5	Jak dál?	300
24 Hodnocení kvality eGovernmentu a bezpečnost informačních systémů		303
24.1	Úvod.....	303
24.2	Kvalita eGovernmentu	305
24.3	Hodnocení výkonnosti eGovernmentu	309
24.4	Hodnocení bezpečnosti eGovernmentu	314
24.5	Ekonomické aspekty bezpečnosti eGovernmentu	316
24.5.1	Počáteční náklady	316
24.5.2	Průběžné náklady	317
24.6	Závěr	319
25 Kryptologie a kyberprostor		320
25.1	Úvod.....	320
25.2	Informace, informatika, informační technologie	320
25.2.1	Alan Mathison Turing	321
25.2.2	Claude Elwood Shannon	322
25.3	Kyberprostor	323
25.4	Kryptologie	324
25.5	Kryptologie v kyberprostoru.....	330

25.6	Závěr.....	332
26	Využití podvrhů biometrických charakteristik v praxi.....	333
26.1	Úvod do problematiky biometrických systémů.....	333
26.2	Podvrhy biometrických charakteristik.....	336
26.2.1	Podvrhy otisků prstů.....	339
26.2.2	Podvrhy obličeje.....	340
26.2.3	Podvrhy charakteristik oka	342
26.2.4	Podvrhy charakteristik ruky	343
26.2.5	Podvrhy dalších biometrických charakteristik.....	344
26.3	Závěr.....	345
27	Řešení dynamického modelu detekce kybernetických útoků	346
27.1	Úvod	346
27.2	Dynamický model požadavků a odpovědí.....	347
27.3	Konstrukce řešení	349
27.4	Ilustrativní příklad	351
27.4.1	Případ 1.....	352
27.4.2	Případ 2.....	353
27.4.3	Případ 3.....	353
27.4.4	Případ 4.....	354
27.5	Závěr.....	355
28	Fuzzy množiny jako nástroj detekce kybernetických útoků v mobilních systémech	357
28.1	Úvod	357
28.2	Motivace pro použití fuzzy množin.....	359
28.3	Základní aparát fuzzy množin potřebný pro detekci mobilního malwaru	359

28.4	Mechanismus detekce mobilního malwaru pomocí fuzzy množin	362
28.5	Výsledky provedených experimentů.....	364
28.6	Omezení a budoucí výzkum	366
29	Řízení kybernetických rizik	367
29.1	Principy fuzzy logiky	367
29.2	Princip modelu	368
29.3	Sestavení fuzzy modelu	368
29.4	Interpretace výsledků	369
29.5	Závěr	371
30	Politika informační a kybernetické bezpečnosti ve výrobních firmách v České republice.....	372
30.1	Úvod.....	372
30.2	Literární rešerše	374
30.3	Metodologie	376
30.4	Analýza informační a kybernetické bezpečnosti	376
30.5	Závěr	380
31	Využití neuronových sítí v rozhodovacích procesech podniku.....	381
31.1	Earnings Management – správa zisku podniku	381
31.2	Řízení nákladů podniku	382
31.3	Správa výdělků a její vztah k technologické progresivitě podniku	383
31.3.1	Výzva pro R&D: Průmyslová revoluce čtvrté generace (Industry 4.0)	384
31.3.2	Kyberfyzické systémy jako hlavní médium průmyslové revoluce čtvrté generace a jejich bezpečnost	385
31.3.3	Kybernetické systémy – přínos neuronových sítí (NN)	387
31.4	Závěr	388

Resumé	391
Summary	395
Seznam použité literatury.....	399
Prof. Ing. Vladimír Smejkal, CSc., LL. M., DrSc.	431
Osobnost prof. Smejkal.....	433
Seznam vybraných publikací prof. Smejkal	445
Monografie	445
Kapitoly ve vědeckých monografiích vydaných v zahraničních vydavatelstvích.....	446
Kapitoly ve vědeckých monografiích vydaných v domácích vydavatelstvích.....	446
Kapitoly ve vysokoškolských učebnicích vydaných v domácích vydavatelstvích.....	447
Vědecké práce v zahraničních časopisech	448
Vědecké práce v domácích časopisech.....	448
Publikované příspěvky na zahraničních vědeckých konferencích	450
Publikované příspěvky na domácích vědeckých konferencích ..	454
Legislativní dokumenty	459
Výzkumné studie a průběžné zprávy	459
Vybrané ohlasy na publikace.....	460
Rejstřík	461