

OBSAH

ZOZNAM SKRATIEK A ZNAČIEK.....	14
ÚVOD	18
I. ČASŤ – ÚVOD DO TRESTNÉHO PRÁVA EURÓPSKEJ ÚNIE	
KAPITOLA 1 – POJEM „TRESTNÉ PRÁVO EURÓPSKEJ ÚNIE“	21
1.1 Vymedzenie pojmu	21
1.2 Vzťah trestného práva Európskej únie s vnútroštátnym trestným právom	22
1.3 Úloha vrcholových inštitúcií Európskej únie v oblasti trestného práva	24
1.3.1 Európska rada	24
1.3.2 Rada Európskej únie	25
1.3.3 Európsky parlament	26
1.3.4 Európska komisia	26
1.3.5 Súdny dvor Európskej únie	27
KAPITOLA 2 – VÝVOJ TRESTNÉHO PRÁVA EURÓPSKEJ ÚNIE	28
2.1 Úvod	28
2.2 Európska integrácia	28
2.3 Trestné právo v rámci práva Európskych spoločenstiev, t. j. trestné právo pred vznikom Európskej únie (do roku 1993)	30
2.3.1 Spoločný boj proti terorizmu a skupina TREVI	32
2.3.2 Schengenská spolupráca a jej trestnoprávne otázky	32
2.3.3 Výkon cudzích trestných rozsudkov	33
2.3.4 Spoločný boj proti praniu špinavých peňazí	33
2.4 Trestné právo od založenia Európskej únie (od roku 1993)	34
2.4.1 Dopad nadobudnutia platnosti Zmluvy o Európskej únii na trestné právo	34
2.4.2 Právne predpisy europeizujúce trestné právo	35
2.5 Trestné právo po prvej revízii Zmluvy o Európskej únii, vykonanej Amsterdamskou zmluvou (roky 1999 až 2003)	36

2.5.1 Zmena trestného práva a posilnenie jeho pozície v Európskej únii	36
2.5.2 Výmena (aktualizácia) právnych predpisov europeizujúcich trestné právo	37
2.6 Trestné právo po druhej revízii Zmluvy o Európskej únii, vykonanej Zmluvou z Nice (roky 2003 až 2009)	38
2.7 Trestné právo po tretej revízii Zmluvy o Európskej únii, vykonanej Lisabonskou zmluvou (rok 2009 až súčasnosť)	38

KAPITOLA 3 – PRAMENE TRESTNÉHO PRÁVA

EURÓPSKEJ ÚNIE	40
3.1 Úvod	40
3.2 Systém prameňov	40
3.3 Druhy prameňov, ich povaha a vnútroštátne účinky	43
3.3.1 Smernica	43
3.3.2 Nariadenie	45
3.3.3 Rámcové rozhodnutie	45
3.3.4 Medzinárodná zmluva	47
3.3.5 Rozhodnutie Rady Európskej únie alebo Európskej komisie ...	48
3.3.6 Spoločná pozícia	48
3.3.7 Jednotná pozícia	49
3.3.8 Jednotná akcia	49
3.3.9 Rozhodnutie Súdneho dvora Európskej únie	50
3.3.10 Nelegislatívne dokumenty	51
3.4 Postoj členských štátov k prameňom trestného práva Európskej únie	51
3.4.1 Slabé povedomie o práve Európskej únie	52
3.4.2 Nedostatočné zavedenie (implementácia) rámcových rozhodnutí a smerníc	53
3.4.3 Nesprávny preklad právnych aktov a výklad ich pojmov	54
3.4.4 Komplikované „nápady“ Európskej únie	57
3.4.5 Dvojrýchlostná Európska únia pri legislatívnych nástrojoch justičnej spolupráce v trestných veciach	57
3.5 Akceptácia práva Rady Európy	58
3.6 Akceptácia práva Organizácie Spojených národov	60

II. ČASŤ – HMOTNÉ PRÁVO

KAPITOLA 4 – TRESTNÁ ZODPOVEDNOSŤ	63
4.1 Fyzické osoby	63
4.2 Právnické osoby	63
4.3 Jurisdikcia členských štátov Európskej únie	64
4.4 Výmena informácií z registrov trestov medzi členskými štátmi Európskej únie	65
KAPITOLA 5 – EURÓPSKE TRESTNÉ ČINY – ÚVOD	67
5.1 Vnútroštátne trestné činy považované za európske trestné činy	67
5.2 Právna úprava európskych trestných činov a jej „minimálne pravidlá“	68
5.3 Spoločné črty	71
5.3.1 Potlačanie trestnej činnosti na spoločnom základe v podobe spoločných pravidiel	71
5.3.2 Aproximácia a harmonizácia trestných činov a sankcií	72
5.3.3 Dôraz na trestnú zodpovednosť právnických osôb a ich sankcionovanie	73
5.3.4 Nestabilita právnej úpravy Európskej únie	73
5.3.5 Nadväznosť na právnu úpravu Rady Európy a OSN	74
KAPITOLA 6 – TERORIZMUS	75
6.1 Úvod	75
6.2 Právna úprava	76
6.3 Vymedzenie trestných činov	76
6.3.1 Teroristické trestné činy	76
6.3.2 Trestné činy týkajúce sa teroristických skupín	77
6.3.3 Trestné činy spojené s teroristickými aktivitami	78
KAPITOLA 7 – OBCHODOVANIE S LUĎMI A SEXUÁLNE ZNEUŽÍVANIE ŽIEN A DETÍ	79
7.1 Úvod	79
7.2 Právna úprava	80

7.3	Vymedzenie trestných činov	81
7.3.1	Obchodovanie s ľuďmi	81
7.3.2	Sexuálne zneužívanie detí	82
KAPITOLA 8 – OBCHODOVANIE S DROGAMI		86
8.1	Úvod	86
8.2	Právna úprava	87
8.3	Vymedzenie trestných činov	88
KAPITOLA 9 – PRANIE ŠPINAVÝCH PEŇAZÍ (LEGALIZÁCIA PRÍJMU Z TRESTNEJ ČINNOSTI) ...		90
9.1	Úvod	90
9.2	Právna úprava	91
9.3	Vymedzenie trestných činov	92
KAPITOLA 10 – KORUPCIA		93
10.1	Úvod	93
10.2	Právna úprava	94
10.3	Vymedzenie trestných činov	95
10.3.1	Korupcia v súvislosti s finančnými záujmami Európskej únie	95
10.3.2	Korupcia úradníkov Európskej únie	95
10.3.3	Korupcia v súkromnom sektore	96
KAPITOLA 11 – FALŠOVANIE PLATOBŇÝCH PROSTRIEDKOV		97
11.1	Úvod	97
11.2	Právna úprava	97
11.3	Vymedzenie trestných činov	98
11.3.1	Trestné činy týkajúce sa platobných nástrojov	98
11.3.2	Trestné činy týkajúce sa počítačov	99
11.3.3	Trestné činy týkajúce sa zvláštne upravených zariadení	100
KAPITOLA 12 – POČÍTAČOVÁ KRIMINALITA		101
12.1	Úvod	101
12.2	Právna úprava	103

12.3	Vymedzenie trestných činov	105
12.3.1	Protiprávny prístup do informačných systémov.....	105
12.3.2	Protiprávny zásah do systému	106
12.3.3	Protiprávny zásah do údajov	106
12.3.4	Protiprávne zachytávanie údajov	106
KAPITOLA 13 – ORGANIZOVANÁ TRESTNÁ ČINNOSŤ (ORGANIZOVANÁ KRIMINALITA)		108
13.1	Úvod	108
13.2	Právna úprava	109
13.3	Vymedzenie trestných činov	110
KAPITOLA 14 – RASIZMUS A XENOFÓBIA		112
14.1	Úvod	112
14.2	Právna úprava	112
14.3	Vymedzenie trestných činov	113
KAPITOLA 15 – POŠKODZOVANIE ŽIVOTNÉHO PROSTREDIA ...		115
15.1	Úvod	115
15.2	Právna úprava	115
15.3	Vymedzenie trestných činov	116
KAPITOLA 16 – POŠKODZOVANIE FINANČNÝCH ZÁUJMOV EURÓPSKEJ ÚNIE		118
16.1	Úvod	118
16.2	Právna úprava	118
16.3	Vymedzenie trestných činov	119
III. ČASŤ – PROCESNÉ PRÁVO		
KAPITOLA 17 – ZÁKLADNÉ PRÁVA V TRESTNOM KONANÍ V EURÓPSKEJ ÚNII		123
17.1	Úvod	123
17.2	Právo na spravodlivý proces	125
17.2.1	Úvod	125
17.2.2	Medzinárodné záruky Rady Európy a OSN	126
17.2.3	Záruky Európskej únie	127

17.3	Prezumpcia nevinny	128
17.3.1	Úvod	128
17.3.2	Medzinárodné záruky Rady Európy a OSN	128
17.3.3	Záruky Európskej únie	129
17.4	Právo nebyť trestne stíhaný dvakrát v tej istej veci (<i>ne bis in idem</i>)	130
17.4.1	Úvod	130
17.4.2	Medzinárodné záruky Rady Európy a OSN	131
17.4.3	Záruky Európskej únie	131
17.5	Právo na informácie	136
17.5.1	Úvod	136
17.5.2	Medzinárodné záruky Rady Európy a OSN	136
17.5.3	Záruky Európskej únie	137
17.6	Právo na tlmočenie a preklad	141
17.6.1	Úvod	141
17.6.2	Medzinárodné záruky Rady Európy a OSN	141
17.6.3	Záruky Európskej únie	142
17.7	Právo na obhajobu (právo na právnu pomoc, právo na prístup k advokátovi)	144
17.7.1	Úvod	144
17.7.2	Medzinárodné záruky Rady Európy a OSN	145
17.7.3	Záruky Európskej únie	146
KAPITOLA 18 – OCHRANA OBETÍ TRESTNÝCH ČINOV		149
18.1	Úvod	149
18.2	Záruky v Európskej únii	149
18.3	Európsky ochranný príkaz	151
18.3.1	Právny základ	151
18.3.2	Pojem	152
18.3.3	Vydanie	153
18.3.4	Vykonanie	154
KAPITOLA 19 – SPOLUPRÁCA V TRESTNÝCH VECIACH V RÁMCI EURÓPSKEJ ÚNIE		156
19.1	Úvod	156

19.2	Formy spolupráce	156
19.2.1	Vzájomná pomoc prostredníctvom žiadosti o pomoc	157
19.2.2	Prístupnosť	158
19.2.3	Vzájomné uznávanie	158
19.3	Vzájomné uznávanie ako oporná forma justičnej spolupráce v trestných veciach	158
19.3.1	Základná idea	158
19.3.2	Rozsah vzájomného uznávania	159
19.3.3	Právna úprava vzájomného uznávania	160
19.3.4	Európsky zatýkací rozkaz	165

KAPITOLA 20 – SPOLUPRÁCA V TRESTNÝCH VECIACH V RÁMCI SCHENGENSKÉHO PRIESTORU

20.1	Úvod	175
20.2	Právny základ	175
20.3	Policajná spolupráca	176
20.3.1	Sledovanie osôb	177
20.3.2	Prenasledovanie osôb	178
20.3.3	Výmena informácií	178
20.3.4	Vysielanie styčných dôstojníkov	178
20.4	Justičná spolupráca	179
20.4.1	Právna pomoc v trestných veciach	179
20.4.2	Zákaz dvojitého trestu (zásada <i>ne bis in idem</i>)	180
20.4.3	Vydávanie osôb (extradícia) prostredníctvom medzinárodného zatýkacieho rozkazu	181
20.4.4	Zabezpečenie výkonu rozsudku	181
20.5.5	Spolupráca v oblasti omamných látok (drog) a strelných zbraní a streliva	181
20.5	Schengenský informačný systém	182
20.5.1	Úvod	182
20.5.2	Zriadenie	182
20.5.3	Právny základ	183
20.5.4	Informácie (údaje) v schengenskom informačnom systéme a ich archivovanie	183

20.5.5 Národná ústredňa SIRENE	184
KAPITOLA 21 – SPOLUPRÁCA V TRESTNÝCH VECIACH S NEČLENSKÝMI ŠTÁTMI EURÓPSKEJ ÚNIE	186
21.1 Úvod	186
21.2 Spojené štáty americké	186
21.3 Japonsko	187
21.4 Čína	188
KAPITOLA 22 – SPOLOČNÉ VYŠETROVACIE TÍMY	189
22.1 Úvod	189
22.2 Vznik	190
22.3 Právny základ	190
22.4 Zostavenie spoločného vyšetrovacieho tímu	191
22.5 Prípadové štúdie	193
22.5.1 Organizovaná trestná činnosť	193
22.5.2 Obchodovanie s drogami	193
IV. ČASŤ – ORGÁNY A JEDNOTKY PODPORUJÚCE SPOLUPRÁCU ČLENSKÝCH ŠTÁTOV EURÓPSKEJ ÚNIE V TRESTNÝCH VECIACH	
KAPITOLA 23 – EUROJUST (JEDNOTKA PRE SÚDNU SPOLUPRÁCU EURÓPSKEJ ÚNIE)	195
23.1 Úvod	195
23.2 Vznik, právny základ a pomenovanie	196
23.3 Ciele, úlohy a právomoci	197
23.4 Národný člen Eurojustu	202
23.5 Spolupráca a vzťahy s partnermi	203
23.5.1 Europol (Agentúra Európskej únie pre spoluprácu v oblasti presadzovania práva)	203
23.5.2 Európska justičná sieť	204
23.5.3 OLAF (Európsky úrad pre boj proti podvodom)	205
23.5.4 Nečlenské štáty Európskej únie a medzinárodné organizácie	206

23.6	Prípadové štúdie	206
23.6.1	Falšovanie platobných prostriedkov	206
23.6.2	Obchodovanie s drogami	207
23.6.3	Pranie špinavých peňazí	207
KAPITOLA 24 – EUROPOL (AGENTÚRA EURÓPSKEJ ÚNIE PRE SPOLUPRÁCU V OBLASTI PRESADZOVANIA PRÁVA)		
		209
24.1	Úvod	209
24.2	Vznik, právny základ a pomenovanie	210
24.3	Ciele, úlohy a právomoci	211
24.4	Národné ústredne Europolu a styční dôstojníci Europolu	214
24.5	Spolupráca a vzťahy s partnermi	214
24.5.1	Eurojust (Jednotka pre súdnu spoluprácu Európskej únie)	215
24.5.2	OLAF (Európsky úrad pre boj proti podvodom)	215
24.5.3	Nečlenské štáty Európskej únie a medzinárodné organizácie ...	216
24.6	Prípadové štúdie	216
24.6.1	Obchodovanie s drogami a obchodovanie so zbraňami	216
24.6.2	Nedovolené prevádzacstvo imigrantov	216
24.6.3	Obchodovanie s ľuďmi	217
24.6.4	Falšovanie peňazí	217
24.6.5	Počítačová kriminalita	217
KAPITOLA 25 – EURÓPSKE CENTRUM BOJA PROTI POČÍTAČOVEJ KRIMINALITE		
		219
25.1	Úvod	219
25.2	Vznik	219
25.3	Právny základ	220
25.4	Úlohy a ciele	220
25.5	Prípadové štúdie (prvé úspechy)	221
25.5.1	High-tech kriminalita (kybernetické útoky, malvér)	222
25.5.2	Sexuálne vykorisťovanie detí online	222
25.5.3	Podvod v oblasti platobného styku	223

KAPITOLA 26 – OLAF (EURÓPSKY ÚRAD PRE BOJ PROTI PODVODOM)	224
26.1 Úvod	224
26.2 Vznik a právny základ	224
26.3 Úlohy	225
26.4 Vyšetrovanie	226
26.5 Spolupráca vrcholových inštitúcií Európskej únie pri vyšetrovaniach OLAFu	228
26.6 Spolupráca a vzťahy s partnermi	229
26.6.1 Eurojust (Jednotka pre justičnú spoluprácu Európskej únie) ...	229
26.6.2 Europol (Agentúra Európskej únie pre spoluprácu v oblasti presadzovania práva)	229
26.7 Koordinačná služba pre boj proti podvodom – AFCOS	229
26.8 Prípadové štúdie	231
26.8.1 Nezrovnalosti pri financiách z Európskeho fondu regionálneho rozvoja	231
26.8.2 Pašovanie cigariet a pranie špinavých peňazí	231
KAPITOLA 27 – SIETE JUSTIČNEJ SPOLUPRÁCE V TRESTNÝCH VECIACH	232
27.1 Úvod	232
27.2 Európska justičná sieť	232
27.2.1 Vznik, právny základ a názov	232
27.2.2 Charakter a spôsob fungovania	234
27.3 Európska sieť na predchádzanie trestnej činnosti	236
27.4 Sieť kontaktných osôb na boj proti korupcii	237
27.5 Európska sieť kontaktných miest, pokiaľ ide o osoby zodpovedné za genocídu, zločiny proti ľudskosti a vojnové zločiny	238
27.6 Sieť pre legislatívnu spoluprácu ministerstiev spravodlivosti Európskej únie	239
POUŽITÉ PRAMENE	240
O AUTOROVI	265

POČÍTAČOVÁ KRIMINALITA

12.1 Úvod

Počítače sú súčasťou nášho každodenného života, ba niekedy až nevyhnutnosťou. Na jednej strane, sú komunikačným nástrojom spájajúcim celý svet neprekonateľnou rýchlosťou (napr. e-mail či Skype), neoceniteľným pomocníkom pri životných povinnostiach (napr. platenie výdavkov prostredníctvom internet bankingu), ideálnym prostriedkom na trávenie voľného času (napr. pozeranie filmov či fotografií) či v mnohých prípadoch štandardným pracovným nástrojom.

Na druhej strane, človek prišiel so „skvelým“ nápadom – uškodiť inému prostredníctvom počítača (a internetu). Nemožno povedať, že človek začal konať trestnoprávne, ale až pri vybraných závažných konaniach spoločnosť usúdila, že je vhodné ich vymedziť ako trestné činy. Navyše, človek prišiel s ďalším „skvelým“ nápadom – uľahčiť si už existujúcu trestnú činnosť, ktorá pomocou počítača (a internetu) je jednoduchšia, efektívnejšia a najmä anonymnejšia.

Počiatky počítačovej kriminality možno datovať do obdobia 60-tych a 70-tych rokov minulého storočia. Prirodzene, v tých časoch bola odlišná od dnešnej. Počítače boli úplne iné od dnešných. Ich cena predstavovala milióny amerických dolárov, zaberali celú miestnosť, vyžadovali si špeciálny klimatický systém a v neposlednom rade tím špecialistov, ktorí sa starali o ich chod. Vlastníkom počítačov boli spravidla len veľké spoločnosti, ako napríklad banky. Navyše, počítače neboli pripojené do sietí a v žiadnom prípade nemožno hovoriť o prítomnosti internetového pripojenia, ako ho poznáme dnes.

Počítačová kriminalita je v súčasnosti najrýchlejšie sa rozvíjajúca forma kriminality. V celosvetovom meradle je počet obetí počítačovej kriminality viac ako milión ľudí denne. Ide o výnosnejší druh kriminality ako celosvetový obchod s marihuanou, kokaínom a heroínom dohromady. Je mimoriadne široká, zahŕňa napríklad *hacking*, *cracking*, *warez*, *phishing*, *sniffing* či *skimming*. Ide o trestnú činnosť, ktorá bežnému človeku mnoho nevraví. V mnohých prípadoch je veľmi sofistikovaná a jej objasnenosť hraničí s nulou.

Pojem **počítačová kriminalita** má niekoľko alternatív v slovenskom jazyku – napríklad **kybernetická kriminalita** alebo **kyberkriminalita**. V anglickom jazyku nachádzame oveľa viac alternatív, napríklad *computer crime*, ktorý je časovo najstarším pojmom, alebo novšie alternatívy *cyber crime*, resp. *cybercrime* alebo *cyber-crime*, zriedkavo taktiež pojmy *high-tech crime*, *virtual crime* alebo výnimočne *e-crime*.

Za súčasného stavu poznania je definovanie počítačovej kriminality mimoriadne náročná úloha, ba priam nemožná. Praktickejšie je poukázať na **skupiny počítačových trestných činov**:

1. trestné činy, ktorých cieľom je počítač,
2. trestné činy, pri ktorých je počítač používaný ako nástroj na ich spáchanie,
3. trestné činy, pri ktorých má počítač len vedľajšiu príležitostnú úlohu pri ich páchaní.

Ad 1) V prvom prípade je **počítač cieľom či terčom útoku**. Konanie spočíva napríklad v prieniku do počítača za účelom „krádeže“ dát, súborov či dokumentov, v neoprávnenom zásahu do informačných systémov alebo aj vo vydieraní založenom na hrozbách zo zverejnenia odcudzeného obsahu. V tomto prípade dochádza k neoprávnenému prístupu k počítaču, t. j. k hackerstvu. Keďže počítač je majetkom/vlastníctvom, neoprávnený prístup k počítaču je podobný nepovolenému vkročeniu na cudzí pozemok. Avšak, kým neoprávnené vkročenie na cudzí pozemok či do obydli sa týka reálneho sveta, neoprávnený prístup k cudziemu počítaču sa týka kyberpriestoru. V princípe túto skupinu trestných činov možno prirovnať k barbarstvu.

Ad 2) V prípade trestných činov, pri ktorých **počítač je používaný ako nástroj**, počítač slúži ako pomocník na uľahčenie trestnej činnosti. Ide napríklad o falšovanie peňazí, falšovanie úradných listín, výroba a distribúcia detskej pornografie na internete, porušovanie autorských práv výrobou nelegálnych kópií hudobných CD nosičov, filmových nosičov v najrôznejších podobách – DVD disk, HD DVD disk, Blu-ray disk alebo v neposlednom rade ide o výrobu nelegálnych kópií počítačových programov.

Ad 3) V poslednom prípade, keď **počítač má len vedľajšiu príležitostnú úlohu pri páchaní trestných činov**, počítač zohráva malú úlohu a nie je potrebný na spáchanie trestného činu. Príkladom je napísanie vydieračského alebo výhražného listu, ktorý je napísaný na počítači, ale mohol byť napísaný aj na písacom stroji alebo rukou, taktiež ohováranie prostredníctvom internetu,

ekonomická kriminalita či ilegálny predaj drog prostredníctvom internetu. Táto skupina počítačových trestných činov nepredstavuje počítačovú kriminalitu v pravom slova zmysle.

12.2 Právna úprava

Práva úprava EÚ v oblasti počítačovej kriminality sa týka štyroch oblastí, a to a) podvody a falšovanie bezhotovostných platobných prostriedkov, b) útoky na informačné systémy, c) detská pornografia na internete a kontaktovanie detí na účely ich sexuálneho zneužitia a d) porušovanie právnej ochrany počítačových programov. Podvody a falšovanie bezhotovostných platobných prostriedkov sú upravené v samostatnej kapitole ako samostatný európsky trestný čin (bližšie pozri kapitolu 11). Detská pornografia na internete a kontaktovanie detí na účely ich sexuálneho zneužitia sú upravené taktiež v samostatnej kapitole (bližšie pozri kapitolu 7). Právna úprava porušovania právnej ochrany počítačových programov (smernica 2009/24/ES o právnej ochrane počítačových programov) neobsahuje sama osebe trestnoprávne prvky. V dôsledku toho sa nasledujúci text tejto kapitoly zameriava len na útoky na informačné systémy.

Vedúcim právnym predpisom EÚ ochrany proti útokom na informačné systémy je **smernica 2013/40/EÚ o útokoch na informačné systémy**. Táto smernica vymedzuje trestné činy a sankcie v oblasti útokov na informačné systémy. Jej cieľom je tiež uľahčiť predchádzanie takýmto trestným činom a zlepšiť spoluprácu medzi justičnými a inými príslušnými orgánmi.

Smernica chráni **informačný systém**. Na účely smernice sa ním rozumie zariadenie alebo skupina navzájom prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré automaticky spracúvajú počítačové údaje podľa programu, ako aj počítačové údaje, ktoré toto zariadenie alebo skupina zariadení ukladá, spracúva, opätovne získava alebo prenáša na účely svojho fungovania, používania, ochrany a údržby [čl. 2 písm. a) smernice 2013/40/EÚ]. Príkladom môže byť internetové bankovníctvo banky alebo univerzitný informačný systém, ktorý slúži na internú potrebu zamestnancov, ale aj študentov danej inštitúcie. Aj napriek tomu, že ich účelom je zjednodušenie a zefektívnenie komunikácie, nie všetci ich vnímajú rovnako. Na jednej strane, väčšina ľudí ich používa spôsobom, ktorý je im prínosný a zároveň pre iných nezávadný. Na druhej strane, možno sa stretnúť aj so škodlivými útokmi na informačné systémy. Úmyselne

škodlivé útoky môžu mať mnoho podôb, napríklad neoprávnený prístup, t. j. hackerstvo, alebo šírenie škodlivého kódu (vírusov).

Smernica zohľadňuje nové metódy páchania počítačových trestných činov, najmä použitie botnetov. Tie sú v poslednom období pravdepodobne najväčšou hrozbou, ktorej čelí internet, ako aj jeho bezpečnosť. Pojem „botnet“ je pomenovaním siete „robotov-počítačov“, ktoré boli infikované škodlivým počítačovým vírusom. Vírus sa za účelom preniknutia dostane do počítača veľmi jednoducho, ak počítač nie je zabezpečený ochrannými mechanizmami (napr. antivírusový systém alebo „FireWall“). Pojem „botnet“ pramení v anglickom jazyku. Je spojením slov *bot* a *net* ako skrátený tvar spojenia *robot network* alebo *network of robots*. Slovo *bot* je skrátený tvar slova *robot*, čo v slovenskom jazyku znamená rovnomenne pomenovanie robot a *net* je skrátený tvar slova *network*, čo v slovenskom jazyku znamená sieť. Infikovaný počítač je pomenovaný ako *bot* alebo v nedávnej minulosti *zombie*. Takéto siete sú riadené a kontrolované iným počítačom, často aj bez vedomia ich užívateľov. Osoba, ktorá ho riadi a kontroluje, je pomenovaná ako *bot herder* alebo *bot master*.

Sieť botnet môže byť aktivovaná na vykonávanie špecifických činností. Každý počítač siete môže pracovať samostatne, napríklad za účelom krádeže osobných údajov z počítača ako sú e-mailové adresy, heslá, údaje týkajúce sa licencií k počítačovým programom počítača, údaje k elektronickému bankovníctvu a pod. Počítače môžu pracovať taktiež spolu, napríklad zasielaním záplav správ alebo dát za účelom „odmietnutia služby“, čím sa sleduje ohrozenie internetovej stránky. Ohrozenie spočíva v tom, že napadnutá stránka je nefunkčná alebo nedostupná pre užívateľov internetu. Iným účelom je odosielanie spamu prostredníctvom e-mailu. Takmer všetok spam pramení práve z činnosti botnetov. Omnoho závažnejšou činnosťou sú podvody s kreditnými kartami či útoky na informačné systémy.

Je ťažké definovať takéto siete čo do veľkosti, avšak boli spozorované siete s odhadom 40 000 až 100 000 infikovaných počítačov za 24 hodín (počet pripojení za 24 hodín je bežne používaná meracia jednotka na odhad veľkosti botnetov). Možno teda konštatovať, že útoky sú rôzne. Osoby, ktoré riadia a kontrolujú botnety, majú byť považované za páchatelov trestného činu.

Smernica dopĺňa už pred ňou existujúce medzinárodné nástroje. Smernica nadväzuje na Dohovor o počítačovej kriminalite z roku 2001, prijatý Radu Európy. Tento dohovor je na medzinárodnej úrovni považovaný za najúplnejšiu

súčasnú medzinárodnú normu v oblasti boja proti počítačovej kriminalite. Poskytuje komplexný a ucelený rámec zahŕňajúci viaceré aspekty počítačovej kriminality v medzinárodnom európskom kontexte.

12.3 Vymedzenie trestných činov

Smernica 2013/40/EÚ o útokoch na informačné systémy predstavila konkrétne **trestné činy týkajúce sa informačných systémov**, a to:

- protiprávny prístup do informačných systémov,
- protiprávny zásah do systému,
- protiprávny zásah do údajov a
- protiprávne zachytávanie údajov.

Na druhej strane, je vhodné vopred poukázať, že smernica neukladá trestnoprávnu zodpovednosť v prípadoch, keď trestné činy v nej vymedzené sú spáchané, ale boli spáchané bez úmyslu. Príkladom je, ak osoba nevie o neoprávnenosti prístupu alebo v prípade povereného testovania alebo ochrany informačných systémov, napríklad ak osobu poverí spoločnosť alebo predajca, aby otestovala silu jej bezpečnostného systému.

12.3.1 Protiprávny prístup do informačných systémov

Protiprávny prístup do informačných systémov je *hacking* resp. hackerstvo. *Hacking* je najstarším spôsobom páchania počítačovej kriminality. Ide o neoprávnené preniknutie do cudzieho systému (napr. počítačového, informačného, riadiaceho) inou ako štandardnou cestou, a to prostredníctvom prelomenia alebo obídenia jeho bezpečnostnej ochrany. Pre jeho páchatelov – hackerov – často nie je ničím iným ako intelektuálnou výzvou. Obeťami hackingu boli napríklad Pentagon, NASA, Yahoo či Google. V Slovenskej republike bolo najznámejšou kauzou hackerstva preniknutie do systému Národného bezpečnostného úradu Slovenskej republiky, teda ostro výsmešná kauza prelomenia hesla „nbusr123“.

V zmysle smernice za trestný čin je považované úmyselné získanie prístupu do celého informačného systému alebo akejkoľvek jeho časti bez oprávnenia, ak bolo spáchané porušením bezpečnostného opatrenia, a to aspoň v prípadoch, ktoré nie sú menej závažné [čl. 3 smernice 2013/40/EÚ o útokoch na informačné systémy].

Konaním bez oprávnenia sa na účely smernice rozumie konanie vrátane prístupu, zásahu alebo zachytávania údajov, ktoré nie je povolené zo strany vlastníka či iného držiteľa práv systému alebo jeho časti alebo ktoré nie je povolené vnútroštátnym právom.

Za menej závažný prípad sa má považovať, keď došlo k protiprávnemu prístupu menšieho významu alebo keď porušenie dôverného charakteru informačného systému je menšieho stupňa. Ide o možnosť uplatnenia materiálneho korektívu.

12.3.2 Protiprávny zásahu do systému

V prípade protiprávneho zásahu do systému, ktorého zmyslom je ochrana celistvosti informačných systémov, za trestný čin je považované úmyselné závažné bránenie fungovaniu informačného systému alebo prerušenie jeho fungovania vložением počítačových údajov, prenosom, poškodením, vymazaním, zhoršením, pozmenením alebo potlačením takýchto údajov alebo ich zneprístupnením bez oprávnenia, a to aspoň v prípadoch, ktoré nie sú menej závažné [čl. 3 smernice 2013/40/EÚ o útokoch na informačné systémy].

Za menej závažný prípad sa má považovať, keď samotný zásah do systému má menší význam alebo keď sa do celistvosti informačného systému zasiahlo len v menšej miere. Aj tu ide o možnosť uplatnenia materiálneho korektívu.

12.3.3 Protiprávny zásah do údajov

V prípade protiprávneho zásahu do údajov je za trestný čin považované úmyselné vymazanie, poškodenie, zhoršenie, pozmenenie, potlačenie počítačových údajov v informačnom systéme alebo zneprístupnenie takýchto údajov bez oprávnenia, a to aspoň v prípadoch, ktoré nie sú menej závažné [čl. 3 smernice 2013/40/EÚ o útokoch na informačné systémy].

12.3.4 Protiprávne zachytávanie údajov

V neposlednom rade, za trestný čin je považované taktiež úmyselné zachytávanie údajov prostredníctvom technických prostriedkov, neverejného prenosu počítačových údajov do informačného systému, z informačného systému alebo v rámci neho vrátane elektromagnetického vysielania z informačného systému

nesúceho takéto počítačové údaje, ak je spáchané bez oprávnenia, a to aspoň v prípadoch, ktoré nie sú menej závažné [čl. 6 smernice 2013/40/EÚ].

Zachytávanie zahŕňa získavanie obsahu údajov buď priamo, a to prostredníctvom prístupu a využívania informačného systému, alebo nepriamo, a to prostredníctvom využívania elektronického odpočúvania alebo odpočúvacieho zariadenia technickými prostriedkami.

ORGANIZOVANÁ TRESTNÁ ČINNOSŤ (ORGANIZOVANÁ KRIMINALITA)

13.1 Úvod

Páchatelia trestných činov sa neraz zoskupujú do organizovaných skupín, čím vytvárajú organizovanú trestnú činnosť, ktorá v porovnaní so „sólo páchatelom“ je omnoho efektívnejšia.

Najzávažnejšie organizované skupiny pochádzajú napríklad z Ruska, Talianska, Spojených štátov amerických, Číny, Japonska, Mexika, Izraela či Kolumbie. Ako najznámejšie organizované skupiny možno uviesť napríklad taliansku skupinu Cosa Nostra, japonskú Yakuzu, čínske Triády alebo „ruskú mafiu“. Niektoré organizácie majú dlhú tradíciu – napríklad história Yakuzy siaha až do 17. storočia. V extrémnom prípade, počet členov organizácií presahuje aj stotisíc členov. Neobmedzujú sa len na jednu krajinu, ale ich aktivity sa prejavujú aj v medzinárodnom rozmere. Napríklad talianska Cosa Nostra pôsobí aj v Spojených štátoch amerických, čínske Triády v Európe alebo „ruská mafia“ pôsobí v desiatkach krajín celého sveta.

Organizovaná trestná činnosť sa prejavuje najmä v oblastiach, ktoré sú finančne výnosné. Ide spravidla o výrobu a obchodovanie s drogami, obchodovanie s ľuďmi, sexuálne vykorisťovanie žien na účely prostitúcie, obchodovanie so zbraňami a muníciou, obchodovanie s kradnutými autami, obchodovanie s diamantmi a drahými kovmi, pašovanie cigariet, falšovanie peňazí, vydieranie/výpalníctvo či podvody najrôznejšieho charakteru. V neposlednom rade ide aj o pranie špinavých peňazí, ktorým organizované skupiny legalizujú svoje nelegálne príjmy, napríklad v reštauračných zariadeniach, disco podnikoch alebo v hoteloch, ktoré vykazujú neexistujúce tržby, resp. faktúry za neexistujúce služby.

Ak organizovaná trestná činnosť nadobúda cezhraničný rozmer, môže byť prirovnávaná k **medzinárodnému podnikaniu**. Spoločným im je cieľ – dosahovanie zisku bez obmedzenia aktivít len v jednej krajine. Avšak zásadným rozdielom medzi nimi je spôsob k jeho dosiahnutiu – organizované skupiny nie sú

vždy viazané zákonnými spôsobmi výkonu ich činností. Navyše, berúc do úvahy nemožnosť obmedzení monopolov či zdanenia ich ziskov, sú v značnej výhode.

Do polovice 80-tych rokov minulého storočia bola organizovaná trestná činnosť považovaná za problém, ktorý sa týkal len obmedzeného počtu krajín – predovšetkým Spojených štátov amerických a Talianska, s eventuálnym pridaním Japonska, Číny a Kolumbie. O dvadsať rokov neskôr sa obraz organizovanej trestnej činnosti dramaticky zmenil.

Zmeny sa prejavili aj v Európe. V rámci EÚ malo vplyv na rozmach organizovanej trestnej činnosti dokončenie vnútorného trhu a zrušenie kontrol na vnútorných hraniciach. Tým bol organizovaným skupinám uľahčený pohyb v rámci celej EÚ a taktiež došlo k otvoreniu priestoru pre ich nelegálne aktivity. Okrem toho, po páde železnej opony v roku 1989 sa otvorili územia ďalších krajín, najmä v strednej Európe vrátane Slovenskej republiky.

V súčasnosti na európskom území vykonávajú svoje aktivity rôzne organizácie – napríklad v Holandsku skupiny zaoberajúce sa drogami, v Nemecku skupiny zaoberajúce sa nelegálnym prístahovalectvom, v Poľsku skupiny zaoberajúce sa prepravou kradnutých áut z Nemecka do Ruska alebo v Litve skupiny pašujúce cigarety z Ukrajiny do baltických a nordických krajín. Možno hovoriť aj o organizáciách z neeurópskych krajín, ktoré v Európe pôsobia – napríklad čínske Triády alebo ruská mafia.

Boj proti organizovanej trestnej činnosti nie je jednoduchý. Dosať si vyžiadal nemálo ľudských obetí. Známymi príkladmi sú talianski sudcovia Giovanni Falcone a Paolo Borsellino, aktívne bojujúci proti Cose Nostre, ktorí boli v roku 1992 obeťami bombových atentátov.

V rámci legislatívnej činnosti EÚ boli prijaté legislatívne akty za účelom boja proti organizovanej trestnej činnosti. Možno hovoriť napríklad o obchodovaní s ľuďmi, obchodovaní s drogami alebo o praní špinavých peňazí. Tieto oblasti spadajú do oblasti európskych trestných činov a sú spracované v samostatných kapitolách tejto učebnice. Avšak ako samostatný trestný čin je považovaná už len samotná účasť v zločineckej organizácii.

13.2 Právna úprava

Vedúcim právnym predpisom EÚ v boji proti organizovaným zločineckým skupinám je **rámčové rozhodnutie 2008/841/SVV o organizovanom zločine**.