Kriminalita a kyberkriminalita - pojem

PŘEDNÁŠKA PRO STUDIUM LL.M. V PRÁVU INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ,

PROF. JUDR. JAROSLAV FENYK, PH.D., DSC.

5. 2. 2021

I. Základy trestní odpovědnosti

Trestní odpovědnost v ČR

- Trestní odpovědnost **fyzických osob** - trestní zákoník (zák. č. 40/2009 Sb., ve znění pozdějších předpisů – dále jen TZ), zákon o soudnictví ve věcech mládeže č. 218/2003 Sb., ve znění pozdějších předpisů
- Trestní odpovědnost **právnických osob** - zákon o trestní odpovědnosti právnických osob a řízení proti nim (zák. č. 418/2011 Sb., ve znění pozdějších předpisů – dole jen TOPOZ)

Působnost trestního zákoníku a TOPOZ

- Časová a místní působnost TZ a TOPOZ (částečně odlišná působnost u FO a PO)

Trestný čin

- „**Trestným činem** je protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně (§ 13 odst.1. TZ)“

Skutková podstata trestného činu

Zásada zákonnosti : (§ 12 odst. 1 TZ - nullum crimen, nulla poena sine lege)

- **4 obligatorní znaky trestného činu :**

- Objekt
- Objektivní stránka
- Subjekt
- Subjektivní stránka

+ protiprávnost

Trestný čin právnické osoby

Kromě znaků skutkové podstaty u osob fyzických, je třeba doplnit dále znaky uvedené v § 8 odst. 1, 2 TOPOZ…protiprávní čin spáchaný v jejím zájmu nebo v rámci její činnosti, jednal-li tak ….

II. Trestněprávní postih jako ultima ratio (subsidiarita trestní represe)

Zásada subsidiarity trestní represe

- Kontroverzní ustanovení § 12 odst. 2 TZ :

„Trestní odpovědnost pachatele a trestněprávní důsledky s ní spojené lze uplatňovat jen v případech **společensky škodlivých**, ve kterých nepostačuje uplatnění odpovědnosti podle jiného právního předpisu.“

Ultima ratio

- „Trestní právo má místo pouze tam, kde jiné prostředky z hlediska ochrany práv fyzických a právnických osob jsou nedostatečné, neúčinné nebo nevhodné.“

a) Legislativní prostředek
b) Interpretační prostředek???
c) Aplikační prostředek???

Ultima ratio

- **Společenská nebezpečnost** trestného činu podle § 3 odst. 1,2 a 4 trestního zákona č. 140/1961 Sb. a **společenská škodlivost** trestného činu podle § 12 odst. 2 trestního zákoníku č. 40/2009 Sb.
- § 39 odst. 2 trestního zákoníku
- § 172 odst. 2 písm. c) trestního řádu
- **Současná praxe** (stanovisko trestního kolegia NS ČR (srov. stanovisko trestního kolegia Nejvyššího soudu ze dne 30. 1. 2013, sp. zn. **Tpjn 301/2012**, uveřejněné pod č. 26/2013 Sbírky soudních rozhodnutí a stanovisek, rozh. tr.)

Stanoviska NS ČR k subsidiaritě a ultima ratio

- Každý protiprávní čin, který vykazuje všechny znaky uvedené v trestním zákoníku, je trestným činem. Tento závěr je však v případě méně závažných trestných činů korigován uplatněním zásady subsidiarity trestní represe ve smyslu § 12 odst. 2 tr. zákoníku, podle níž trestní odpovědnost pachatele a trestněprávní důsledky s ní spojené lze uplatňovat jen v případech společensky škodlivých, ve kterých nepostačuje uplatnění odpovědnosti podle jiného právního předpisu. Společenská škodlivost činu není zákonným znakem trestného činu, neboť má význam jen jako jedno z hledisek pro uplatňování zásady subsidiarity trestní represe ve smyslu § 12 odst. 2 tr. zákoníku. Společenskou škodlivost nelze řešit v obecné poloze, ale je ji třeba zvažovat v konkrétním posuzovaném případě spáchaného méně závažného trestného činu, u něhož je nutné ji zhodnotit s ohledem na intenzitu naplnění kritérií vymezených v § 39 odst. 2 tr. zákoníku, a to ve vztahu ke konkrétním znakům zvažované skutkové podstaty trestného činu. Úvaha o tom, zda jde o čin, který není trestným činem pro nedostatek škodlivosti pro společnost, se zásadně uplatní v případech, ve kterých posuzovaný skutek z hlediska spodní hranice trestnosti neodpovídá běžně se vyskytujícím trestným činům dané skutkové podstaty. Kritérium společenské škodlivosti případu je dále doplněno principem ultima ratio, z kterého vyplývá, že trestní právo má místo pouze tam, kde jiné prostředky z hlediska ochrany práv fyzických a právnických osob jsou nedostatečné, neúčinné nebo nevhodné.
- (Usnesení Nejvyššího soudu České republiky sp.zn. 11 Tdo 344/2017, ze dne 27.9.2017)

III. KYBERZLOČIN, RESP. KYBERKRIMINALITA

„Kyberzločin/ Kyberkriminalita“

- Jednotná definice dosud neexistuje, jen širší a užší pojetí

- **Prozatímních definic je celá řada- příklady**:

1. „ Trestný čin ohrožující informační a síťovou bezpečnost, využívající tuto síť k páchání trestné činnosti nebo trestný čin vztahující se k obsahu sítě“

(Kyberkriminalita a právo - Gřivna, Polčák eds. Auditorium, 2008).

Kyberzločin/ Kyberkriminalita

2. „ Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení včetně dat, nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě a to jako :

a) **předmět** trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem, jsou popsaná zařízení jako věci movité
b) **nástroj** trestné činnosti.“

(Porada V. a kol. Kriminalistika, technické, forenzní a kriminalistické aspekty, AČ, Plzeň 2019.)

§ 257a TZ (1961) - první skutková podstata PK – § 257a (hacking)

Poškození a zneužití záznamu na nosiči informací

(1) Kdo získá přístup k nosiči informací a v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch

a) takových informací neoprávněně užije,

b) informace zničí, poškodí, změní nebo učiní neupotřebitelnými, nebo

c) učiní zásah do technického nebo programového vybavení počítače nebo jiného telekomunikačního zařízení,

bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti nebo peněžitým trestem nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo

b) způsobí-li takovým činem značnou škodu nebo získá-li sobě nebo jinému značný prospěch.

(3) Odnětím svobody na jeden rok až pět let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu nebo získá-li sobě nebo jinému prospěch velkého rozsahu.

Informační/informatická kriminalita

- **Informační kriminalita** : prostředkem nebo cílem zločinného útoku jsou informace, jejich zpřístupňování, šíření, sdílení, shromažďování s cílem nelegálního využití (§ 180, §182- 184, § 191-192, § 248, § 250, § 288, § 352, § 354, § 355- § 357, § 364-365 TZ atd.)

- **Informatická kriminalita** : prostředkem nebo cílem zločinného útoku jsou informační systéme a jejich komponenty (počítač, program, data, telekomunikace (sítě a jiná zařízení)

(Porada V. a kol. Kriminalistika, technické, forenzní a kriminalistické aspekty, AČ, Plzeň 2019.)

Typické způsoby páchání kyberkriminality

Půjde často o následující neoprávněné :

- zásahy do vstupních dat
- změny v uložených datech
- pokyny k počítačovým operacím
- průniky do počítačů, počítačových systémů

Typickou formou páchání trestné činnosti je :

napadení cizího počítače, jeho programového vybavení a souborů dat v databázích.

Obtíže při dokazování kyberkriminality

- Nejednoznačná nebo mezerovitá právní úprava
- Nedostatečná připravenost orgánů činných v trestním řízení
- Nedostatečné technické vybavení orgánů činných v trestním řízení
- Složitost opatření elektronického důkazu (nehmotnost - latentnost digitální stopy, snadná odstranitelnost důkazu, nízká životnost digitální stopy, problémy s uchováváním stop, rychlý vývoj nových informačních systémů, přeshraniční element, vyžadující specifické formy přeshraniční spolupráce…)

Softwarové pirátství

- Zvláštní forma kyberkriminality, spočívající v porušování práv **duševního vlastnictví**
- Formy páchání – především tyto nelegální zásahy a :

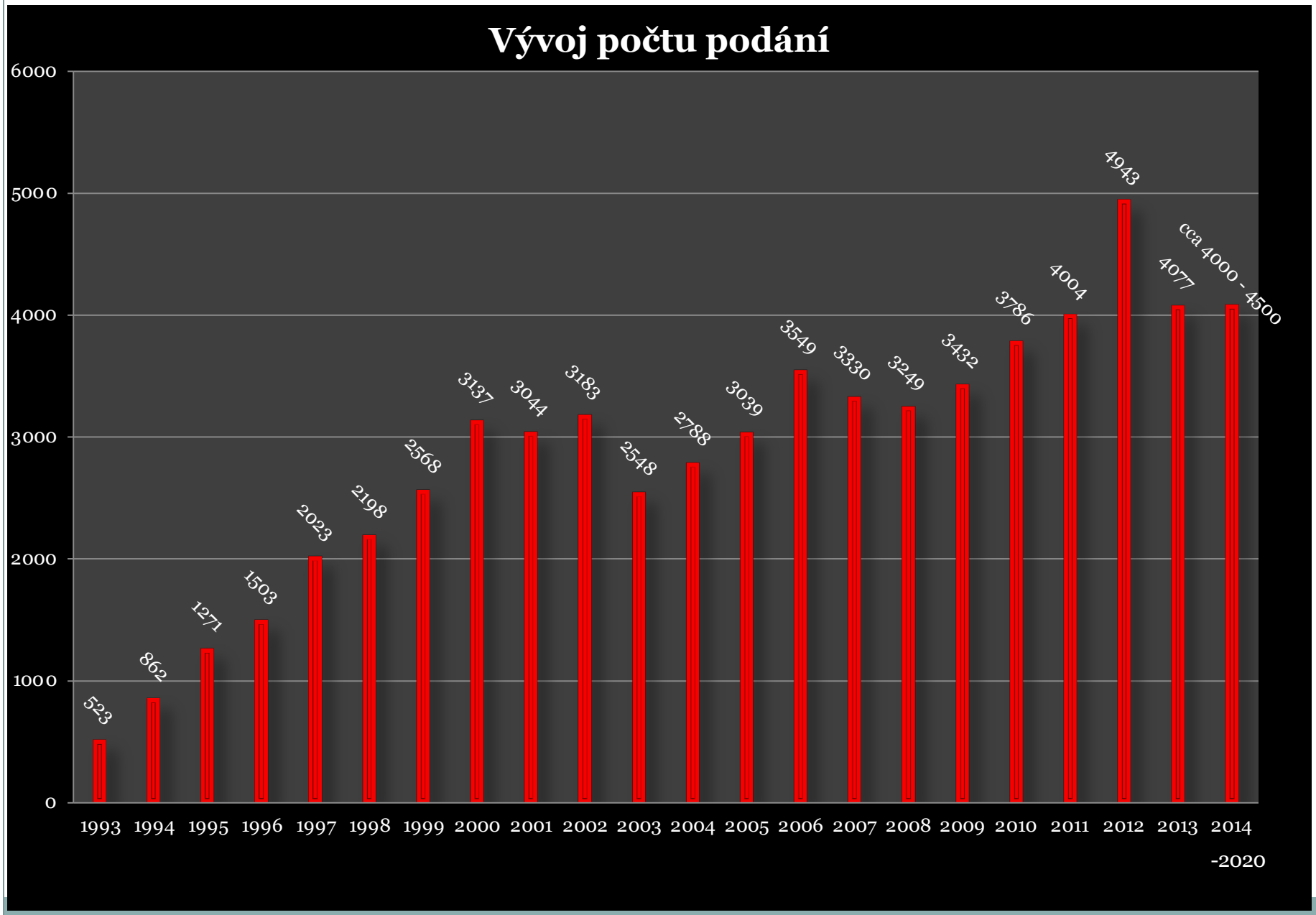
  a)šíření- užívání počítačových programů

  b)šíření - užívání audiovizuálních nebo jen audio děl

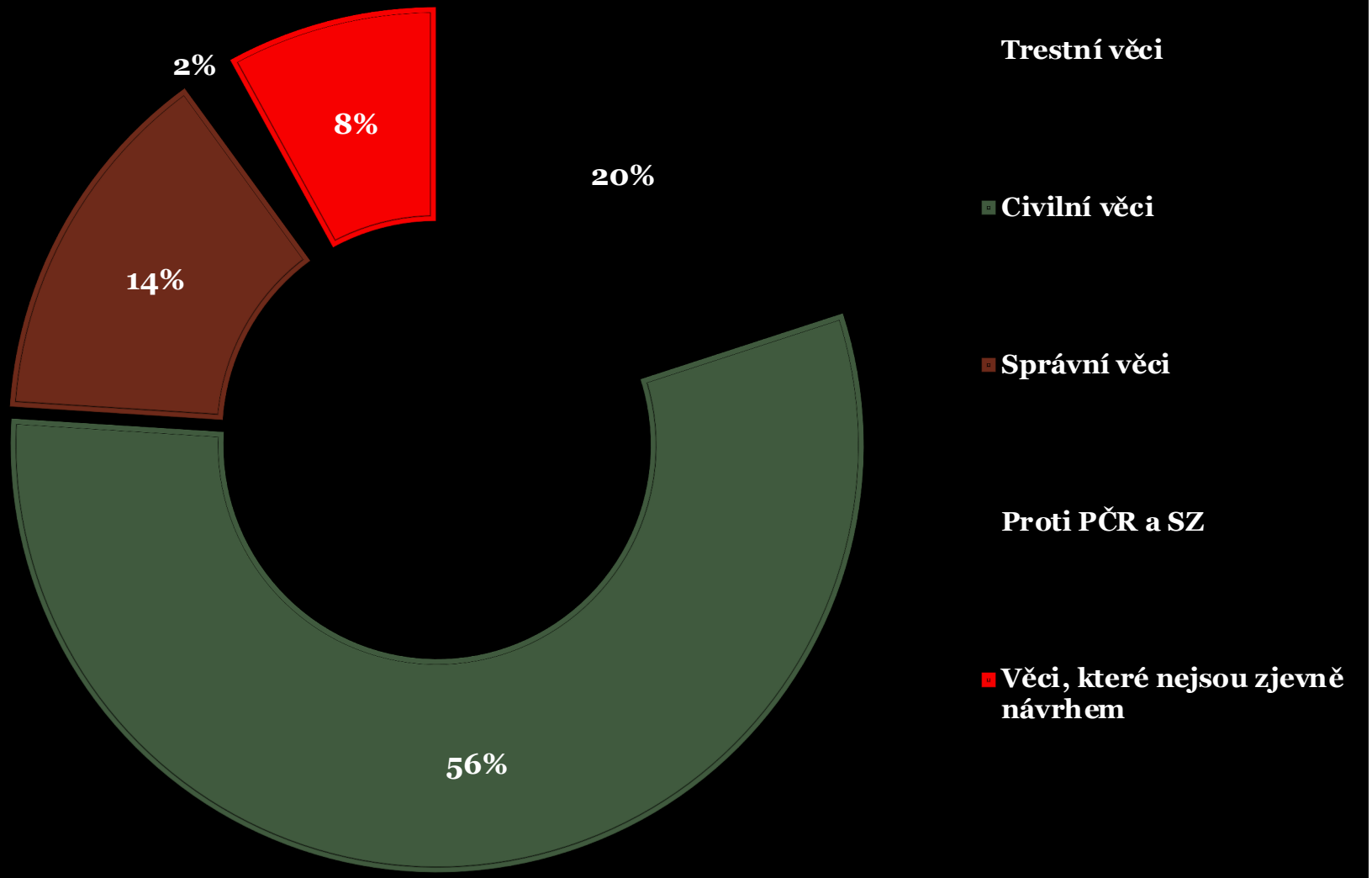
I. Kyberkriminalita v judikatuře Ústavního soudu

Ústavní soud ČR

- Chrání ústavnost
- Chrání základní lidská práva a svobody
- Garantuje ústavní charakter výkonu státní moci
- Je sice orgánem soudního typu, ale nepatří mezi obecné soudy
- Vytvořen přímo ústavou
- Činnost ÚS se řídí zákonem o ústavním soudu
- 15 soudců / 4 senáty/ plénum
- Může zrušit jakékoliv rozhodnutí orgánu veřejné moci
- Může zrušit jakýkoliv právní předpis
- Rozhodnutí jsou nezrušitelná a nezměnitelná
- Nálezy Ústavního soudu jsou závazné


Vývoj počtu podání
6000
5000
4000
3000
2000
1000
0
523
862
1271
1503
2023
2198
2568
3137
3044
3183
2548
2788
3039
3549
3330
3249
3432
3786
4004
4943
4077
cca 4000 - 4500
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
-2020

VĚCNÁ STRUKTURA NÁPADU ÚS



Usn. I. ÚS 3069/17

Rozsudkem okresního soudu v Ostravě byl stěžovatel uznán vinným přečinem šíření toxikomanie podle § 287 odst. 1, odst. 2 písm. c) TZ.

Stěžovatel jako jednatel obchodní společnost s vědomím a srozuměním, že svým jednáním může podněcovat a svádět široký okruh osob ke zneužívání návykové látky marihuany, s jejímiž účinky byl sám obeznámen, v kamenných obchodech a současně **prostřednictvím internetového obchodu XY** nabízel k prodeji jednak semena konopí setého, ze kterých lze vypěstovat konopí s vysokým obsahem THC, jednak i ucelený sortiment evidentně sloužící ke zneužívání rostliny konopí.

Spáchání uvedeného trestného činu **"veřejně přístupnou počítačovou sítí"** naplňuje kvalifikovanou skutkovou podstatu šíření toxikomanie, jak výslovně, srozumitelně a určitě stanoví § 287 odst. 2 trestního zákoníku.

Usn. IV. ÚS 530/18

Městský soud v Praze rozhodoval o návrhu státního zastupitelství na vydání stěžovatele do zahraničí ke dvěma trestním stíháním podle § 95 zákona č. 104/2013 sb., O mezinárodní justiční spolupráci ve věcech trestních. Dospěl přitom k závěru, že vydání k oběma trestním stíháním je přípustné a stěžovatel tedy může být vydán buď do spojených států amerických, kde se měl, stručně řečeno, dopustit **neoprávněného vniknutí do zabezpečené počítačové sítě několika obchodních společností a neoprávněně tak získat přístup k osobním údajům z účtů jejich klientů** (v počtu desítek milionů), jakož i do ruské federace, kde se měl, stručně řečeno, dopustit **odcizení majetku přes internet** v rámci organizované skupiny.

Podle názoru Ústavního soudu rozdílnost kulturního přístupu k některým obecně trestným jednáním (typicky například drogové delikty, sexuální napadání, **nebo právě informační kriminalita**) není sama o sobě důvodem nesplnění mezinárodních závazků. I osoba bez právnického vzdělání má v současné době dostatek informací, aby si uvědomovala, že v různých zemích platí různé právní řády odpovídající specifické historii konkrétní země a její společenské, ekonomické a kulturní vyspělosti, tedy i co se týče možné variability trestů za trestné činy.

Usn. IV. ÚS 2034/16

Stěžovatel byl prověřován policejním orgánem pro podezření ze spáchání přečinu neoprávněného přístupu k počítačovému systému a nosiči informací dle § 230 odst. 1, TZ, dílem dokonaného, dílem spáchaného ve stadiu pokusu dle § 21 TZ proto, že po **překonání bezpečnostního opatření** opakovaně neoprávněně získal přístup k počítačovému systému obchodní společnosti X. Přinejmenším jednou se pak stěžovateli podařilo získat z tohoto systému i data týkající se mj. veškerých nákupů, včetně seznamu dodavatelů, seznamu odběratelů, soubory obsahující osobní data všech zaměstnanců a členů orgánů uvedené obchodní společnosti, údaje o know-how či podnikatelský záměr pro rok 2016. Policejní orgán šetřením zjistil, že dílčí útoky byly vedeny z IP adresy přidělené poskytovatelem internetového připojení stěžovateli na adresu jeho bydliště.

Stěžovatel podle názoru Ústavního soudu věděl, že již není zaměstnancem obchodní společnosti X a že přístupovými údaji k počítačovému systému **nedisponuje oprávněně**, přesto se k počítačovému systému uvedené obchodní společnosti opakovaně připojil (překonal bezpečnostní opatření) a v jednom případě z tohoto systému zkopíroval data blíže specifikovaná v usnesení o zahájení trestního stíhání. Tvrzení stěžovatele, že absence vymezení tohoto znaku skutkové podstaty trestného činu brání v řádném uplatňování jeho obhajoby, nepovažuje ústavní soud za odůvodněné.

Usn. I. ÚS 2816/15

Okresní soud ke stěžovatelově argumentaci ohledně neodkladného a neopakovatelného úkonu odkázal na rozhodnutí nejvyššího soudu ze dne 15. 12. 2010 sp. Zn. 5 tdo 1312/2010, podle něhož ani chybějící odůvodnění neodkladného nebo neopakovatelného úkonu v příkazu k domovní prohlídce a časový odstup provedení tohoto úkonu nemá vliv na jeho zákonnost. Neodkladnost a neopakovatelnost úkonu, nebyly-li odůvodněny v příkazu k domovní prohlídce, musí alespoň vyplývat z povahy trestní věci, což je v nyní projednávaném případě splněno. **V případě počítačové kriminality** může zásah do softwarového či hardwarového vybavení počítače nebo úprava na něm uložených dat před tím, než by byl odborně zjištěn a zadokumentován jeho skutečný stav, znamenat zmaření objasňování skutečností závažných pro trestní stíhání. V projednávaném případě pak pokud by došlo k provedení domovní prohlídky až po zahájení trestního stíhání, obviněný by nepochybně odstranil věci, které se v rámci domovní prohlídky měly nalézt, zejména počítačovou techniku, razítka, šeky, padělané listiny.

Napadený příkaz skutečně explicitní odůvodnění domovní prohlídky jako neodkladného, respektive neopakovatelného úkonu neobsahuje. Avšak při širším, materiálním náhledu na napadené rozhodnutí je nutno konstatovat, že k porušení ústavně zaručených práv stěžovatele zde nedošlo. V napadeném příkazu je zřetelně uvedeno, z jakého trestného činu je stěžovatel podezřelým, jakým jednáním se jej měl dopustit a jaké věci související s prověřovanou trestnou činností by se v dotčených objektech měly nacházet, přičemž tyto věci jsou rovněž (typově) specifikovány zcela dostatečně. Jedná se přitom namnoze o věci, které lze snadno zničit, případně jejich obsah (záznamy v nich uložené) pozměnit či odstranit. Ústavní soud tak má za to, že v daném případě byla podmínka neodkladnosti domovní prohlídky splněna a tato skutečnost byla rovněž z odůvodnění napadeného příkazu interpretací seznatelná.

Usn. IV. ÚS 3001/09

Namítá-li stěžovatelka, že v rámci provedené prohlídky byly zajištěny i datové nosiče obsahující soukromou korespondenci zaměstnanců, je možno v zásadě uplatnit dvojí právní argumentaci, vedoucí však ke stejnému faktickému výsledku.

První linie argumentace vychází z toho, že samotné tvrzení stěžovatelky **o obsahu datových nosičů** nemůže zabránit jejich zajištění, pokud toto tvrzení nelze v průběhu prohlídky ověřit, případně není-li možné část nosičů, které jsou důležité pro vedení trestního řízení, oddělit. Důvodem je především ta skutečnost, že v opačném případě by byla ohrožena samotná podstata zajišťování datových nosičů. Uživatelům nosičů by pro jejich vyloučení z možnosti zajištění orgány činnými v trestním řízení v podstatě postačovalo uložit na ně vedle pracovních údajů i data soukromá a orgány činné v trestním řízení by byly nuceny zvolit procesní postup ušitý na míru každého zaměstnance stěžovatele. Dle náhledu ústavního soudu je třeba však vždy sledovat především cíl samotné prohlídky. Zajištění případných soukromých dat zaměstnanců bylo v tomto konkrétním případě pouhým vedlejším produktem prohlídky, kterému nebylo možno zabránit. Není v moci orgánů činných v trestním řízení, aby při provádění prohlídky v sídle stěžovatelky prohlížely každý počítačový soubor, zda-li neobsahuje údaje soukromé povahy. Dovedeno k závěrům ad absurdum by taková prohlídka neprobíhala v řádu hodin, ale spíše několika týdnů, což je vyloučeno. Podstatné je to, že se zde nejedná o záměrné získávání údajů, nejde o primární cíl prohlídky. Navíc pokud se zaměstnanec rozhodne využívat datových nosičů zaměstnavatele i pro soukromé účely, musí být s touto možností srozuměn.

Jiná linie argumentace, tentokrát procesněprávní, vychází z toho, že stěžovatelka je ve věci soukromých údajů svých zaměstnanců, uložených na datových nosičích, osobou zjevně neoprávněnou k podání ústavní stížnosti. Aktivně legitimováni jsou zde samotní zaměstnanci, neboť zasaženo by mohlo být případně do jejich práv a nikoli do práv stěžovatelky.

Usn. IV. ÚS 2798/17

Stěžovatel je stíhán pro přečin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 2 písm. a), odst. 3 písm. a) TZ, dále pro přečin zneužití pravomoci úřední osoby podle § 329 odst. 1 písm. a) TZ a pro zločin přijetí úplatku podle § 331 odst. 1 alinea první, odst. 3 písm. b) TZ. Tohoto jednání se měl (ve stručnosti řečeno) dopustit tím, že jako policista za úplatu vynášel **informace z interních policejních počítačových systémů** ve prospěch podezřelých osob. Stěžovatel byl vzat do vazby / § 67písm. b) TŘ/ a proti tomuto rozhodnutí podal ústavní stížnost.

S ohledem na povahu a charakter trestné činnosti, pro kterou byl obviněný stíhán, měl městský soud správně za to, že je u obviněného dána důvodná obava, že by mohl působit na dosud nevyslechnuté svědky (kolegy obviněného) tak, aby tito nevypovídali v jeho neprospěch, a mohl by tak mařit objasňování skutečností závažných pro trestní stíhání

Nález III. ÚS 3844/13

Policejním orgánem byla stěžovateli uložena pořádková pokuta ve výši 10 000,- Kč s odůvodněním, že svým jednáním pomocí sociální sítě facebook před ostatními svědky a poškozenými snižoval autoritu policejního orgánu, ohrožoval důvěru v jeho činnost a snižoval vážnost a důstojnost jeho funkce. Stěžovatel se dle usnesení policejního orgánu vůči němu chová urážlivě, jelikož je prověřován ve věci ohrožování výchovy dítěte dle ustanovení § 201 odst. 1 TZ.

Povaha sociální sítě facebook není dle názoru ústavního soudu jednoznačně soukromá či veřejná. Vždy záleží na konkrétních uživatelích, jakým způsobem si míru soukromí na svém profilu, případně přímo u jednotlivých příspěvků, nastaví. Teoreticky může uživatel prostřednictvím této sítě komunikovat pouze s jediným dalším uživatelem, a to aniž by tuto komunikaci mohli vidět, či do ní zasahovat, ostatní uživatelé. Taková komunikace by pak jistě mohla být považována za ryze soukromou, byť uskutečněnou prostřednictvím sociální sítě využívané miliardou uživatelů, stejně jako je za soukromou možno považovat emailovou komunikaci dvou osob, uskutečněnou např. Prostřednictvím emailové služby gmail (www.Gmail.Com), kterou taktéž využívají miliony uživatelů (obdobně v české republice např. Emailová služba dostupná na stránkách www.Seznam.Cz). Uživatel sociální sítě facebook však má možnost učinit svůj profil také zcela veřejným a tedy přístupným všem uživatelům sociální sítě facebook, případně i všem uživatelům sítě internet. Tato možnost je hojně využívána např. Politickými stranami, zájmovými skupinami, umělci, poskytovateli služeb, obchodníky a dalšími, jejichž cílem je prezentovat se prostřednictvím sociální sítě facebooku co nejširšímu počtu uživatelů internetu. Toto nastavení ale volí i část "běžných" uživatelů.

S ohledem na stále narůstající význam a rozsah využívání internetu, sociálních sítí a nejrůznějších mobilních aplikací v každodenním životě, se jedná o oblast, na kterou svou pozornost zaměřují také orgány činné v trestním řízení. Je nepopiratelné, že při odhalování trestné činnosti mohou být informace ze sítě internet velmi nápomocné a u některé trestné činnosti dokonce přímo nezbytné. Internet je zdrojem mnoha veřejně dostupných informací, které jsou tak přímo dostupné i orgánům činným v trestním řízení, ale stejně tak obsahuje množství informací soukromé povahy. Postupy aplikované příslušnými orgány při zjišťování těchto informací proto musí dodržovat rámec stanovený právními předpisy a musí respektovat obecné principy, na nichž je založena činnost státních orgánů, zejména v maximální možné míře šetřit ústavně zaručená práva a svobody dotčených osob.

Usn. I.ÚS 2878/14

Při výkonu prohlídky jiných prostor, pro jejíž nařízení byly splněny zákonné podmínky, lze jako věci důležité pro trestní řízení zajistit i výpočetní techniku a záznamová média, případně jejich kopie, i když existuje možnost, že zajištěné nosiče informací obsahují vedle záznamů o skutečnostech důležitých pro trestní řízení i informace o skutečnostech, které se netýkají probíhajícího trestního řízení a ke kterým se váže státem uložená nebo uznaná povinnost mlčenlivosti. Současně však zdůraznil, že je samozřejmé, že je třeba postupovat v souladu se zásadou přiměřenosti a zdrženlivosti (§ 2 odst. 1 a § 52 trestního řádu), kteréžto zásady spočívají v tom, že orgány činné v trestním řízení budou v míře co nejmenší zasahovat do základních práv a právem chráněných zájmů těch osob, vůči kterým není vedeno trestní řízení.

Pokud se v dispozici orgánů činných v trestním řízení nacházejí data nepřezkoumaná obecným soudem nahrazujícím souhlas zástupce ČAK k seznámení se s obsahem dat z datových uložišť (včetně tzv. cloudu) na základě nesprávného výkladu ustanovení § 85b odst. 1 trestního řádu, je třeba posoudit, zda existuje způsob nápravy, aniž by došlo ke zrušení napadeného rozhodnutí. S ohledem na probíhající trestní řízení ve věci existuje důvodné podezření, že se mezi zajištěnými daty nacházejí informace prokazující páchání trestné činnosti advokátem, a taková data žádnou ochranu přiznanou důvěrné komunikaci mezi advokátem a jeho klienty nepožívají. Tyto důkazy o trestné činnosti samotného advokáta tedy nejsou nijak chráněny a mohou být orgány činnými v trestním řízení použity, ačkoli k jejich získání došlo na základě nesprávného výkladu ustanovení § 85b odst. 1 trestního řádu.