Jan Kolouch

# CyberCrime

Edice CZ.NIC

**CYBERCRIME**
JUDr. Jan Kolouch, Ph.D.

Vydavatel:
CZ.NIC, z. s. p. o.
Milešovská 5, 130 00 Praha 3
Edice CZ.NIC
www.nic.cz

1. vydání, Praha 2016
Kniha vyšla jako 14. publikace v Edici CZ.NIC.
ISBN 978-80-88168-18-8

© 2016 Jan Kolouch
Toto autorské dílo podléhá licenci Creative Commons (http://creativecommons.org/licenses/by-nd/3.0/cz/), a to za předpokladu, že zůstane zachováno označení autora díla a prvního vydavatele díla, sdružení CZ.NIC, z. s. p. o. Dílo může být překládáno a následně šířeno v písemné či elektronické formě na území kteréhokoliv státu.

CZ.NIC | SPRÁVCE DOMÉNY CZ

Právní stav byl zohledněn ke dni 1. 8. 2016.

ISBN 978-80-88168-18-8

— Jan Kolouch

# CyberCrime

— Edice CZ.NIC

# Předmluva vydavatele

## Vážený čtenáři,

titulem, který právě držíte v ruce, se sdružení CZ.NIC vrací k problematice bezpečnosti. Po knize *Buď pánem svého prostoru*, která byla zaměřena především na teenagery a jejíž autoři se pohybovali v americkém prostředí, jsme se tentokrát rozhodli oslovit odborníka českého a vydat knihu zaměřenou komplexněji a odborněji.

Po přečtení knihy rád konstatuji, že Jan Kolouch ve své knize zúročil své bohaté zkušenosti pedagoga, právníka i odborníka na počítačovou bezpečnost a napsal knihu, která bude nejen ozdobou knihovniček, ale zřejmě mnoha lidem bude ležet na stole a budou v ní hojně listovat.

Autor vytvořil text, který obsahuje technické části, které čtenářům pomohou orientovat se ve světě malware, phishingu, darknetu, botnetů a dalších, pro ne zcela technicky zaměřeného uživatele matoucích a odstrašujících pojmů.

Zároveň ovšem kniha obsahuje i právní výklad: analyzuje kybernetickou kriminalitu z pohledu jednotlivých paragrafů, a umožňuje tak získat velké množství cenných informací i těm čtenářům, kteří sice ovládají všechny ty zvláštní technické pojmy, ale svět právních klasifikací, paragrafů a odstavců je jim cizí a neorientují se v něm.

Jsem rád, že máme příležitost vydat právě tento typ knihy. Věřím, že bude užitečná nejen studentům, ale i policistům, členům bezpečnostních týmů a koneckonců i právníkům, kteří přicházejí se světem kyberzločinu do styku stále častěji.

Příjemné čtení a spoustu nových a užitečných informací vám přeje

**Martin Peterka, CZ.NIC**
*Praha, 15. listopadu 2016*

# Předmluva autora

## Předmluva autora

Život bez informačních a komunikačních technologií je pro naši společnost již nemyslitelný. Ne, toto konstatování není zcela přesné. Dovolím si tvrdit, že ve stavu rozvoje společnosti, v jakém se nacházíme, bez zásadních změn, je dokonce nemožný.

Uvědomuji si, že toto vyjádření může pobouřit celou řadu lidí, kteří se rozhodli žít „off-line", avšak ani ti se v dnešní společnosti nemají šanci vyhnout průniku informačních technologií do svých životů. Virtuální, či rozšířená realita[1] a zejména pak jednotlivé prvky kyberprostoru[2] stále více prostupují do běžného života každého z nás.

Náš svět, ve kterém právě žijeme, a doba digitální, se všemi neodmyslitelnými klady i zápory a nezbytnými technologiemi, se kterými jsme denně spoutáni, mi vždy připomene úryvek z filmu Minority Report.[3] Konkrétně se jedná o průchod Johna Andertona obchodním centrem, při kterém John dostává nabídky na zboží, které je cíleno pouze na něj na základě jeho zvyků, jeho posledních nákupů, jeho zálib atd. Uvedené sci-fi sice má představovat realitu z roku 2054, ale ve skutečnosti se jedná o realitu dnešních technologicky vyspělých společností, ve kterých dochází k prostupu informačních a komunikačních technologií do života každého jedince. Běžně se můžete setkat s geomarketingem v podobě, kterou si sami mnohdy neuvědomujeme. Ivan Bartoš ve své přednášce na Security 2016[4] výstižně popsal stav, kdy se každý z nás stává produktem. Svým způsobem jsme zdrojem informací a dat pro někoho jiného. Otázkou je, kdo je tím „jiným". Mnoho z Vás si automaticky představí Velkého bratra v podobě KGB, CIA, FBI, NSA aj. Pravda je v současnosti mnohem prozaičtější, oněmi Velkými bratry jsou zpravidla společnosti (komerční či nekomerční organizace), které my, jakožto konzumenti informačních a komunikačních technologií a na ně nabalených aplikací využíváme, s pocitem, že je to „zdarma". Krásným příkladem předneseným právě v přednášce Ivana Bartoše jsou věrnostní (slevové) karty, přičemž nijak přitom nezáleží na tom, do jakého obchodu máte věrnostní kartu. Podstatou oné hry, kdy se sami stáváme produktem, je vlastní použití oné věrnostní (slevové) karty. Konkrétní obchodní řetězec je pak schopen například vyhodnocovat, jaké zboží se v jaké lokalitě prodává více, je schopen na Vás cílit konkrétní reklamu, či Vám zasílat letáky, samozřejmě s extra slevou, na zboží, které vy, zákazník, kupujete nejvíce. Tento příklad krásně demonstruje to, jak jsme ovlivňováni informačními a komunikačními technologiemi[5] a to i v okamžiku, kdy naše vzájemná interakce probíhá ve světě reálném, nikoli virtuálním.

1: Viz Oxford Dictionaries. *Augmented reality.* [online]. [cit. 10.7.2016].
Dostupné z: http://www.oxforddictionaries.com/definition/english/augmented-reality

2: Blíže k jednotlivým pojmům viz kap. 1.2.1 Kyberprostor (Cyberspace).

3: Minority Report je americký sci-fi film režiséra Stevena Spielberga z roku 2002.
Blíže k této konkrétní scéně např. [online]. [cit. 10.7.2016]. Dostupné z: https://www.youtube.com/watch?v=4bs9cAeOqZY

4: Přednáška: *„Souhlasím s VOP? Odkliknu a jedu..."* [online]. [cit. 10.7.2016]. Dostupné z: https://konferencesecurity.cz/

5: Dále jen: **ICT** či informační a komunikační technologie, **IT** či informační technologie, **IS** či informační systémy.

Nemyslím si, že je možné se oprostit od informačních a komunikačních technologií,[6] a rozhodně nemá být smyslem této knihy potlačovat či dehonestovat tyto technologie jako takové, či Vám tvrdit, že je máte přestat používat. Přínos těchto technologií pro společnost ve všech oblastech lidské činnosti (např. v lékařské vědě, výzkumné činnosti, bezpečnosti, dopravě aj.) je neoddiskutovatelný. Oblast informačních a komunikačních technologií je nejrychleji a nejvíce se rozvíjejícím odvětvím lidské činnosti.

To, co je třeba si uvědomit, je skutečnost, že informace či data a jejich využití v sobě zahrnují značný ekonomický i politický potenciál. Informace a jejich obsah mohou rozhodovat nejen o bytí či nebytí jednotlivce či firmy, ale ve své podstatě jsou schopny ovlivnit celosvětový vývoj.

Využití informačních a komunikačních technologií má však i stinné stránky. Jednou z nich je bezesporu i gigantický a dynamický nárůst „nového druhu" trestné činnosti, se kterou je třeba se vypořádat tak, aby nedocházelo k ohrožování a porušování zájmů společnosti. Tuto trestnou činnost lze souhrnně nazvat kyberkriminalitou.[7]

Je třeba zmínit, že v celosvětovém měřítku lze pozorovat značnou snahu jak na právní, tak i bezpečnostní úrovni, jejímž cílem je přijmout adekvátní opatření, která by byla schopna reagovat na tento nový a dynamický fenomén současnosti.[8]

Klíčovými body pro rozvoj kyberkriminality se dle mého názoru staly tři skutečnosti.[9] První

6: Vyjma případu, kdy se rozhodnete odcestovat na pustý ostrov... ale i tam si Vás Google Earth najde.

7: **Kyberkriminalita** je mnohdy označována různými názvy. Domnívám se, že nejvýstižnějším pojmem, označujícím toto protiprávní jednání, je právě pojem kyberkriminalita. V této monografii budou pro označení tohoto jevu používány i pojmy **kyberkriminalita, kybernetická kriminalita či kybernetická trestná činnost**. Blíže viz kap. 1.1 Kybernetická trestná činnost (Cybercrime).

Pokud bychom vycházeli z doslovného překladu anglického názvu **Cybercrime**, pak překlad kyberkriminalita není přesný, neboť doslovný překlad tohoto spojení dvou slov je možné přeložit jako: **kyber zločin** (případně **trestný čin**). Avšak i v prostředí České republiky je vžit a běžně užíván překlad **Convention on Cybercrime**, jako **Úmluva o kyberkriminalitě**, byť tento překlad není, jak je uvedeno výše, doslovný. Domnívám se proto, že i vzhledem k tomuto překladu není pochybením užívání pojmu kyberkriminalita.

Vymezení rozdílů mezi kriminalitou a trestnou činností na tomto úseku bude obsaženo v další části této publikace, stejně jako vymezení názorů různých autorů na přesné označení této trestné činnosti. V publikaci budou jako synonyma využívány zejména pojmy kybernetická trestná činnost a kyberkriminalita.

8: Např: *Fight against cyber crime: cyber patrols and Internet investigation teams to reinforce the EU strategy.* [online]. [cit. 10.7.2016]. Dostupné z: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827

9: Tyto skutečnosti pak byly podpořeny řadou dalších okolností (např. nedostatek právní úpravy ve vztahu k Internetu, neschopností vynutit právo, pocitem anonymity uživatelů aj.).

z nich je propojení čtyř univerzitních počítačů a vytvoření počítačové sítě určené ke sdílení dat.[10] Druhým vytvoření prvního osobního počítače (PC - Personal Computer) společností IBM na konci 80. let 20. století. Třetím a dle mého názoru nejvýznamnějším milníkem je zpřístupnění Internetu[11] široké veřejnosti, včetně úpravy jednotlivých aplikací do uživatelsky přívětivější podoby.[12]

Rozvoj současné digitální společnosti není založen přímo na hospodářském rozvoji spojeném s hmotnými zdroji, ale na rozvoji IT, na připojování stále většího počtu uživatelů do Internetu, ale zejména k aplikacím jako takovým a v neposlední řadě na zisku informací a dat od uživatelů samotných. Tyto změny související s rozvojem IT probíhajícím jak v sociální, tak i ekonomické rovině a jsou jednou z příčin kyberkriminality.

Kyberprostor je v současnosti nejúčinnější a nejnebezpečnější zbraní v rukou pachatelů kybernetické trestné činnosti. Nejde o to, že by byl kyberprostor, či Internet sám o sobě nebezpečný nebo nezabezpečený. Podstatou je, že systém je vždy tak silný, jak je silný jeho nejslabší článek. V tomto případě je tím nejslabším prvkem, víc než kdy jindy, uživatel. Uživatel je vlastně sám sobě a svému okolí největší „hrozbou", protože byť má právní osobnost,[13] tak často má jen minimální znalosti o svých právech a povinnostech.

Internet se stal součástí našeho každodenního života a zejména jeho multimediální aspekt se velmi rychle rozvíjí. Internet je, ať chceme či nechceme, silnějším a dravějším médiem než televize či jakékoli jiné masmédium. Už nyní může dokonce i prostý uživatel prostřednictvím jednoduchého rozhraní předat či vnutit celé světové populaci svou myšlenku, názory. A je jedno, zda jsou to myšlenky normální, či jakkoli zvrácené.

Na jedné straně Internet nabízí prakticky neomezené možnosti téměř komukoli v získávání a zpracovávání informací téměř o čemkoli, bez nutnosti trávení času v knihovnách či informačních centrech mimo domov (získání předmětných informací je otázkou několika vteřin). Google a Wikipedia se staly relevantním a mnohdy jediným zdrojem informací pro naše rozhodnutí. Internet umožňuje komunikaci sbližující lidi mezi sebou navzájem, usnadňuje řadu aktivit díky

10: Blíže viz ARPANET či NSFNET. Jedná se o období konce 60. let 20. století.
Srov. *Historical Maps of Computer Networks*. [online]. [cit. 10.7.2016]. Dostupné z:
https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html

11: Záměrně používám velké písmeno ve slově Internet, pokud jde o vlastní jméno (celosvětovou informační a komunikační síť) malé písmeno pak tam, kde píši o internetu ve smyslu propojených počítačových sítí.
K dalšímu vymezení viz blíže: MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. 1. vydání. Praha: CZ.NIC, 2013. ISBN: 978-80-904248-7-6.
Matejka dále uvádí, že: *„Je však nepochybné, že malé písmeno patří do trojice pojmů intranet – extranet – internet, užívané rovněž ve významu „komunikační médium", u nichž píšeme malé písmeno. Pokud jde o velké písmeno, mělo by vyznačovat samotný vlastní název jedinečného produktu, v tomto případě veřejně globálního Internetu."* Viz s. 19.

12: Aby se jednalo o kyberkriminalitu, je třeba, aby se toto protiprávní jednání odehrávalo v rámci počítačových sítí.

13: Mají práva a povinnosti. Uživatelé zakládají, mění a případně ruší právní vztahy.

možnosti nalezení řešení či návodu, nabízí množství různých informačních kanálů aj. Přitom to vše umožňuje dělat z prostředí domova a s pocitem téměř absolutní anonymity.

Na druhé straně může mít činnost v tomto virtuálním prostředí za následek těžké finanční ztráty, strach ze zásahů do svého soukromí cizími osobami, ztrátu cenných osobních dat, online komunikaci psychicky narušených osob (pedofilů, drogově závislých, filozoficky dezorientovaných apod.), komunikaci těchto osob s našimi vlastními dětmi za našimi zády, domlouvání kriminálních skupin na nezákonné činnosti bez možnosti odposlechu třetí stranou, podvody, neautorizované průniky do soukromých sfér firem, přesměrovávání obchodních zakázek, vykrádání cizích účtů, ničení dat a databází, poškozování autorského práva atd.

Jsem přesvědčen o tom, že nelze připustit, aby se kyberprostor stal prostředím, kde by pachatelé mohli páchat de facto beztrestně jakoukoliv trestnou činnost. Existuje ale pouze jeden výchozí bod pro boj proti kriminalitě v kyberprostoru, a tím je kyberprostor sám. Je třeba pochopit, co vlastně kyberprostor představuje, na jakých principech pracuje, jaké typy kriminality se mohou v tomto virtuálním světě vyskytovat a co vše mohou orgány činné v trestním řízení, ale zejména uživatel sám, proti této protiprávní činnosti dělat.

Jak již bylo řečeno, kyberkriminalita nabývá v poslední době na stále větší intenzitě. Díky její různorodosti dochází k zásahům do široké škály základních lidských práv (např. čl. 10, 13 a 34 zákona č. 2/1993 Sb., ve znění ústavního zákona č. 162/1998 Sb., Listina základních práv a svobod.)[14] každého z nás a informační a komunikační technologie se tak stávají prostředky, jimiž dochází k páchání trestné činnosti nebo jsou samy cílem této činnosti.

Výraznou odlišností kybernetické kriminality od ostatních druhů kriminality je její vysoká latentnost, mnohdy vysoká míra tolerance společností (včetně lhostejnosti uživatelů k případným hrozbám), reálná či domnělá anonymita pachatele a jeho obtížná identifikace, jakož i celý proces dokazování. Proto je třeba řešit nejen otázky represivního působení na pachatele, ale je třeba se zabývat také otázkou prevence trestné činnosti v této oblasti, jakož i otázkou možné ochrany společnosti před touto trestnou činností.

14: Dále jen **Listina**.

**Čl. 10**

(1) Každý má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno.

(2) Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

(3) Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

**Čl. 13**

Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.

**Čl. 34**

(1) Práva k výsledkům tvůrčí duševní činnosti jsou chráněna zákonem.

Vlastní prevence zmíněných negativních jevů musí nutně začít u koncových uživatelů, neboť v kyberprostoru jsou to právě oni, kdo je typickou první obětí útočníka. Na základě svých zkušeností jsem pevně přesvědčen o tom, že výchova a vzdělávání uživatelů má být nezbytnou součástí prostupu informačních a komunikačních technologií do našich životů. Myslím si, že budování informační gramotnosti by mělo být neodmyslitelně spojeno s tvorbou, distribucí a podporou produktů či služeb, které jsou s informačními a komunikačními technologiemi spojeny. Vlastní vzdělávání v této oblasti, či spíše seznamování se s možnými hrozbami, riziky a negativy IT, by mělo být součástí výuky všech forem studia na všech úrovních školství.

Pokud se jedná o osoby, které se této problematice věnují v rámci své profese, pak jsou na tyto specialisty kladeny ještě vyšší nároky, neboť se musí neustále zdokonalovat a školit, aby byli schopni čelit stále novým a dynamicky narůstajícím útokům páchaným prostředky a v prostředí ICT.

Tato kniha shrnuje názory a zkušenosti, které jsem získal v oblasti kybernetické kriminality a kybernetické bezpečnosti. Od roku 2003 se jako vysokoškolský učitel na katedře trestního práva Policejní akademie ČR v Praze věnuji problematice kybernetické kriminality a možnosti jejího trestněprávního postihu. Od roku 2014 jsem také garantem předmětů Kybernalita/Cybernality na FIT ČVUT. Dále dlouhodobě spolupracuji se sdruženími CESNET a CZ.NIC. V rámci své činnosti přednáším zejména na vysokých školách v ČR k vybraným problémům kyberkriminality a prevence této kriminality. Díky svým zkušenostem jsem byl opakovaně přizván European Union Agency for Network and Information Security (ENISA)[15] jako člen expertního týmu při řešení problematik souvisejících s aplikací práva v souvislosti s CERT/CSIRT týmy. Ve své činnosti jsem zároveň měl možnost řídit a kompletně přebudovat infrastrukturu ICT na vysoké škole, takže se domnívám, že jsem schopen propojit jak ryze technické, tak právní a manažerské aspekty pojící se ke kybernetické kriminalitě a kybernetickým hrozbám.

Kniha, kterou právě čtete, je primárně zaměřena na problematiku kybernetické kriminality a částečně na oblast kybernetické bezpečnosti. Byť se jedná o dvě oblasti, které spolu souvisejí, je třeba tyto dvě oblasti oddělit, neboť se každá ubírá jiným směrem. Jsem si vědom toho, že toto „násilné oddělení" je v řadě případů nereálné, neboť kybernetický útok či událost, jež zasahuje do oblasti bezpečnosti, může mít zároveň znaky trestného činu, avšak pro účely této knihy se budu snažit primárně věnovat problematice kybernetické kriminality.

Cílem této monografie není detailně popsat veškeré aspekty, které mohou souviset s kyberkriminalitou (zejména technické oblasti jsou vymezeny relativně stručně), nýbrž ukázat především souvislosti a vzájemnou propojenost ICT, práva a bezpečnosti online.

Předložená publikace ideově vychází z monografie Trestně právní ochrana před kybernetickou kriminalitou, kterou jsem zpracoval společně s kolegou JUDr. Petrem Voleveckým, Ph.D., nicméně aktuální verze je podstatně přepracována a rozšířena. Cílem bylo vytvořit publikaci obsahující aktuální

15: Evropská agentura pro bezpečnost sítí a informací.

informace o kyberkriminalitě a dalších souvisejících aspektech působnosti práva v kyberprostoru, kterou by mohla použít široká veřejnost. Do knihy jsem také zapracoval, ve více či méně přepracované podobě, některé své starší texty (disertační práci, články, prezentace aj.), podobně jsem použil některé fragmenty a myšlenky z prací, které jsem dříve publikoval. Často jsem sám s odstupem času došel k tomu, že jsem své názory revidoval, či pozměnil. Mnohdy jsem k tomu potřeboval slyšet názor jiných, za což jsem jim upřímně vděčný.

Součástí knihy jsou pak i projekty, které jsem realizoval se svými studenty v rámci jejich studentských vědeckých prací, a které demonstrují nebezpečnost chování některých uživatelů v online prostředí.

Identifikační údaje osob použité v příkladech (IP adresy, e-mailové schránky apod.) byly v některých případech pozměněny, na druhou stranu monografie obsahuje celou řadu reálných případů z praxe, u nichž z důvodu objektivnosti byly zachovány informace o skutečných aktérech či detailech útoku.

Posledním, avšak o to významnějším zdrojem informací pro tuto knihu jsou postřehy a náměty studentů, s nimiž jsem měl tu čest diskutovat.

Rozhodně stojí za to, podnítit, ne jen u studentů, diskusi...

Kdykoli rád přivítám jakoukoli zpětnou vazbu od čtenářů této knihy. Vy jste totiž ti, kteří dokáží odhalit chyby a prohřešky, které jsem přehlédl, případně upozornit na témata, která Vás zajímají více. Za jakoukoli vaši zpětnou vazbu jsem vděčný. Tuto knihu jsem se rozhodl vydat pod Creative Commons licencí: CC BY ND.[16]

Závěrem bych chtěl poděkovat všem těm, kdo se o výslednou podobu této knihy zasloužili. Můj dík patří JUDr. Josefu Součkovi, CSc., Andree Kropáčové, Mgr. Juraji Kodyšovi, Bc. Janu Nejedlému, JUDr. Heleně Krejčíkové, Ph.D., mým studentům na PA ČR a FIT ČVUT, jakož i dalším odborníkům, s nimiž jsem měl tu čest spolupracovat a diskutovat. Díky jim za to, že mi otevřeli oči a umožnili mi na problematiku kybernetické bezpečnosti a kriminality nahlížet i z jiných úhlů než doposud. Děkuji všem, kdo byli ochotni číst a připomínkovat rukopis této knihy. Díky za vaše připomínky a náměty.

Poslední dík patří mé rodině, která mi umožňuje být „připojeným bláznem“.

**Jan Kolouch**
jan.kolouch@cesnet.cz

16: Blíže viz kap. 4.10 Internetové (počítačové) pirátství; konkrétně pak kap. 4.10.5 Možná řešení. Bližší informace o creative commons licencích dále naleznete např. na: http://www.creativecommons.cz/licence-cc/; https://cs.wikipedia.org/wiki/Creative_Commons
Byť to může znít šíleně, tak se jedná o následující požadavek: Uvedení autora (umožňuje ostatním rozmnožovat, rozšiřovat, vystavovat a sdělovat dílo a z něj odvozená díla pouze při uvedení autora) + Nevytváření odvozených děl (umožňuje ostatním rozšiřovat odvozená díla pouze za podmínek identické licence).

# Obsah

# Seznam zkratek

## Seznam zkratek

| | |
|---|---|
| APT | Advanced Persistent Threat |
| AZ, autorský zákon | Zákon č. 121/2000 Sb., autorský zákon ve znění pozdějších předpisů |
| BSA | Bussines Software Aliance |
| C&C | Command-and-control |
| CERT | Computer Emergency Response Team |
| CSIRT | Computer Security Incident Response Team |
| Data retention | Plošné ukládání provozních a lokalizačních údajů u poskytovatelů připojení. |
| DBE | Dluh/Banka/Exekuce. Jeden z phishingových útoků. |
| DNS | Domain Name System. Hierarchický systém doménových jmen. |
| Dodatkový protokol | Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kybernetické kriminalitě. |
| DoS, DDoS | Denial of Service. Distributed Denial of Service |
| EC3 | European Cybercrime Centre. Evropské centrum pro boj proti kybernetické kriminalitě |
| EFF | Electronic Frontier Foundation. Mezinárodní nezisková organizace zabývající se ochranou práv a svobody slova v digitálním prostředí. |
| ENISA | The European Union Agency for Network and Information Security. Evropská agentura pro bezpečnost sítí a informací. |
| EULA | End User Licence Agreement. Smlouva uzavřená mezi uživatelem a ISP |
| EXIF | EXchangeable Image File Format. Jedná se o formát metadat, která jsou vkládána do digitálních fotografií, digitálními fotoaparáty. |
| GPS | Global Positioning System |
| HTML | Hyper Text Markup Language. Jde o název značkovacího jazyka používaného pro tvorbu webových stránek. |
| HTTP | Hypertext Transfer Protocol. Internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML. |
| IAP | Internet Access Provider |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| ICT | Informační a komunikační technologie |
| IoT | Internet of Things. Internet věcí. |
| IS | Informační systém / systémy |
| ISP | Internet Service Provider. Specificky k českému právu je využíván pojem poskytovatel služeb informační společnosti. |
| IT | Informační technologie |
| Krizový zákon | Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů |
| LEA | Law Enforcement Agencies. Bezpečnostní složky státu. |
| LIR | Local Internet Registry |
| Listina | Zákon č. 2/1993 Sb., ve znění ústavního zákona č. 162/1998 Sb., Listina základních práv a svobod |
| MMORPG | Massive(ly)-Multiplayer Online Role-Playing Game – počítačová hra na hrdiny o více hráčích, umožňující zapojení hráčů z celého světa skrze Internet do hry odehrávající se ve virtuálním světě. |

| | |
|---|---|
| NAT | Network Adress Translation. Překlad síťových adres. |
| OS | Operační systém |
| OZ, občanský zákoník | Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů |
| P2P | Peer-to-peer |
| PC | Personal Computer. Osobní počítač. |
| RIR | Regional Internet Registry |
| SeznamOTP | Seznam One Time Password. Jeden z phishingových útoků. |
| TOPO, zákon o trestní odpovědnosti právnických osob | Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů |
| TŘ, trestní řád | Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů |
| TZK, trestní zákoník | Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů |
| Úmluva o kyberkriminalitě | Úmluva Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001 |
| URL | Uniform Resource Locator. Jednotná adresa zdroje. |
| Ústava | Ústava České republiky ze dne 16. 12. 1992 jako součást ústavního pořádku České republiky pod č. 1/1993 Sb., ve znění ústavních zákonů č. 347/1997 Sb., č. 300/2000 Sb., č. 395/2001 Sb., č. 448/2001 Sb. a č. 515/2002 Sb. |
| ÚZČ | Útvar zvláštních činností služby kriminální policie a vyšetřování Policie ČR. |
| VoIP | Voice over Internet Protocol |
| ZKB, zákon o kybernetické bezpečnosti | Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů |
| ZoEK, zákon o elektronických komunikacích | Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně dalších zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů |
| ZOOU, zákon o ochraně osobních údajů | Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů |
| ZoP, zákon o přestupcích | Zákon č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů, ve znění pozdějších předpisů |
| ZoZT, zákon o znalcích a tlumočnících | Zákon č. 36/1967 Sb., o znalcích a tlumočnících, ve znění pozdějších předpisů |
| ZPČR | Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů |
| ZSIS, zákon o některých službách informační společnosti | Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů |
| ZSM | Zákon č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže), ve znění pozdějších předpisů |

# 1 Pojem kybernetické trestné činnosti a pojmy související

*„K tomu, aby zlo zvítězilo, stačí jediná věc – aby dobří lidé nedělali nic.“*
Edmund Burke

# 1 Pojem kybernetické trestné činnosti a pojmy související

V této kapitole se pokusím vymezit některé základní pojmy, které jsou důležité pro pochopení problematiky kyberkriminality. Vzhledem k zaměření a rozsahu knihy není možné vysvětlit veškeré pojmosloví související s kyberkriminalitou a IT, k tomuto účelu slouží například specializované slovníky.[17]

## 1.1 Kybernetická trestná činnost (Cybercrime)

Užívání výpočetní techniky, informačních systémů a informačních technologií a jejich integrace do téměř všech odvětví lidské činnosti je jevem, který je pro dnešní dobu charakteristický. Lze konstatovat, že **v podstatě nejde nalézt takovou oblast lidské činnosti, kde by se přímo nebo zprostředkovaně nevyužívala výpočetní technika, resp. informační systém nebo informační či komunikační technologie**.

Bohužel, tak jak rostou možnosti užívání těchto vymožeností dnešní doby a vědeckotechnického pokroku, rostou i možnosti a zároveň i četnost jejich zneužívání k páchání trestné činnosti.

Různí autoři i různé právní normy používají pro označení těchto aktivit různé pojmy, mezi které patří: informační,[18] informatická,[19] elektronická kriminalita, softwarová trestná činnost, počítačová trestná činnost (Computer crime), computer-related-crime, počítačová kriminalita, kybernetická trestná činnost, kyberkriminalita aj. U této problematiky přetrvávají rozdíly nejen v označování tohoto jevu, ale rozdílně je chápán též jejich obsahový význam, což mnohdy přispívá k nesprávnému pochopení významu a škodlivosti tohoto druhu trestné činnosti.

Na tomto místě je třeba předně konstatovat terminologickou nejednotnost a různorodost v chápání výše uvedených pojmů. To je do značné míry odůvodněné interdisciplinárností přístupu k řešení dané problematiky. Proto bývají v různých odborných pracích i v právních dokumentech

17: Jedná se například o: HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* 1. Vyd. Praha: Computer Press, 1997. 456 s. či JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015. ISBN 978-80-7251-397-0. Dostupné z: http://afcea.cz/cesky-slovnik-pojmu-kyberneticke-bezpecnosti/; https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

18: **Information Crime**: jedná se o trestné činy, jejichž prostředkem jsou informace. V tomto případě nezáleží na tom, jak byly informace zpracovány, či užity k útoku.

19: **IT Crime**: cílem útoku v tomto případě nebývá pouze počítač, jeho data a programy, ale celé informační (počítačové) systémy, včetně jejich komponentů.
Blíže viz SMEJKAL, Vladimír. *Právo informačních a telekomunikačních systémů*. 2. aktualiz. a rozš. vyd. Praha: C. H. Beck, 2004, s. 693

často zaměňovány pojmy „počítačový trestný čin" s „počítačovou kriminalitou", „kybernetický trestný čin" s pojmem „kyberkriminalita" apod., resp. jsou mnohdy užívány jako synonyma.

V 90. letech 20. století se pro trestnou činnost páchanou pomocí informační techniky ustálil pojem **„počítačová kriminalita"** (Computercrime, Computerkriminalität). Smejkal ve své publikaci definuje, v polovině 90. let 20. století, počítačovou kriminalitu, jako různorodou směsici trestných činů, jejichž společným faktorem je počítač, program a data. Pod pojmem počítačová kriminalita *„…je třeba chápat páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení data nevyjímaje, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem* ***s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako movité věci, nebo jako nástroje trestné činnosti****."*[20] Z uvedené definice je patrné, že počítačová kriminalita se vztahovala pouze na počítačové systémy, jakožto na cíle útoku.

Označení „počítačová kriminalita" evokuje představu, že trestný čin musí být spáchán na počítači nebo prostřednictvím počítače, nejčastěji počítače osobního (PC - Personal Computer). Takové chápání je dnes zjednodušující, zároveň i poněkud kvantitativně redukuje množství jevů, které lze pod pojem trestná činnost páchaná prostředky informačních a komunikačních technologií zahrnout. Mnohá technická zařízení v dnešní době, díky implementaci mikroprocesorů spolu s jejich miniaturizací, již dávno převzala funkci osobních počítačů (PC), aniž by byla sama za osobní počítače označována. Jedná se o hybridy plnící rozličné funkce, které dříve plnily speciální přístroje. Soudobá technická zařízení umožňující komunikaci mezi sebou a mezi jejich uživateli a jejichž konstrukce je vedena myšlenkou *ALL-IN-ONE* (vše v jednom) dosahují mnohem větších výpočetních výkonů, než nejmodernější výpočetní jednotky z první poloviny 90. let. A i tyto prostředky,[21] přestože nejsou nazývány počítači, mohou být terčem trestné činnosti či prostředkem k jejímu spáchání. Z těchto důvodů se pojem „počítačová kriminalita" či „počítačový trestný čin" v dnešní době již v odborné literatuře téměř nepoužívá. Namísto pojmu „počítač" je v dnešní době používán spíše výraz „informační a komunikační technologie" (*Information and Communiction Technology – ICT*), resp. „trestné činy v ICT".[22]

20: SMEJKAL, Vladimír, Tomáš SOKOL a Martin VLČEK. *Počítačové právo.* Praha: C. H. Beck, 1995, s. 99

21: V současnosti se jedná o celou řadu zařízení, která jsou trestněprávní normou označována jako počítačový systém. Blíže viz kap. 1.2.3 Počítač (Počítačový systém).

22: Blíže např.:

GŘIVNA, Tomáš a Radim POLČÁK. *Kyberkriminalita a právo*. Praha: Auditorium, 2008, s. 32 a násl.

SMEJKAL, Vladimír. *Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku.* Trestněprávní revue, 2003, roč. 2, č. 6, s. 161.

POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, s. 249.

V roce 2000 vydala Rada Evropy definici počítačové kriminality pocházející ze Statutu Komise expertů pro zločin v kyberprostoru: *„Trestný čin namířený proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin v tradičním smyslu, při kterém je užito moderních informačních a komunikačních technologií.“*[23]

Rámcové rozhodnutí Rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu označuje za **„computer-related crime“** takové jednání, které směřuje proti počítači, či jednání, kde je počítač prostředkem ke spáchání trestného činu. Ze znění evropského zatýkacího rozkazu pak vychází i definice kyberkriminality.

V mezinárodních úmluvách se pro trestnou činnost páchanou prostředky informačních technologií užívá nejčastěji pojem **„kybernetická kriminalita“** a používání tohoto pojmu se z oblasti normativní přeneslo též do slovníku odborné veřejnosti. Pojem kyberkriminalita má obdobný charakter jako pojmy *„násilná kriminalita“, „kriminalita mladistvých“, „ekonomická kriminalita“ apod. Takovýmito názvy jsou označovány skupiny trestných činů mající určitý společný faktor, jako např. způsob provedení, osobu pachatele (alespoň druhově) apod. Ve své podstatě přitom může jít o velmi různorodou směsici trestných činů, spojených oním společným faktorem (počítačem, programem, daty).“*[24]

Při vymezení obsahu pojmu **kybernetická kriminalita** si je třeba uvědomit, že spolu s růstem možností využívání informačních a komunikačních prostředků roste i možnost jejich užívání (zneužívání) k páchání trestné činnosti. Proto v podstatě neexistuje jakási univerzální, obecně přijímaná definice, která by rozsah a hloubku tohoto pojmu plně postihla.

Jednu z možných definic počítačové či kybernetické kriminality je možné nalézt i ve Výkladovém slovníku kybernetické bezpečnosti:[25]

***Kybernetická kriminalita - Cyber crime***
*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 buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.*

*(Více také **Počítačová kriminalita**).*

23: MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 5

24: SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 19

25: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 57 a 73. [online]. [cit. 10.7.2016]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

***Počítačová kriminalita / Kybernetická kriminalita – Computer crime / Cyber crime***
*Zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený.*

Z těchto dvou definic je patrná snaha o vymezení všech aspektů kybernetické kriminality, avšak autoři se dopustili určitých nepřesností. Zaprvé využívají oba dva uvedené termíny jako synonymum, avšak v definici počítačová kriminalita pomíjí faktory, že počítač je zároveň cílem i prostředkem útoku. Obdobné problémy spojené s vlastním definováním pojmu kybernetická kriminalita je možné nalézt i jinde.

Vzhledem ke snaze o definování pojmu kybernetické kriminality je vhodné využít Úmluvu Rady Evropy č. 185 o kybernetické kriminalitě ze dne 23. listopadu 2001.[26] Tato úmluva však vlastní pojem kyberkriminality nevymezuje. Definuje pouze opatření, která by měla být přijata ratifikující stranou na vnitrostátní úrovni. Tato opatření v oblasti trestního práva hmotného pak vymezují hrubý rámec trestných činů, které jsou považovány za kybernetické trestné činy.[27] Toto rámcové vymezení (spolu s dalšími trestnými činy obsaženými v Dodatkovém protokolu Rady Evropy č. 189 k Úmluvě o kybernetické kriminalitě[28]) poskytuje základní prostor pro jednotnou právní unifikaci trestných činů, které je možné považovat za kybernetické, napříč jednotlivými zeměmi. Vlastní, mnohdy až velmi strohé vymezení daných trestných činů je věci spíše ku prospěchu, neboť nijak neomezuje vnitrostátní (podrobnější či rozpracovanější) implementaci těchto trestných činů, avšak zároveň zaručuje splnění minimálních požadavků (standardů) všemi ratifikujícími stranami.

I z důvodu značné nejednotnosti v názorech na to, co vše je a co není kybernetická kriminalita, v následující části této kapitoly vymezím tento pojem, a to jak z hlediska pozitivního, tak negativního.

Nejobecněji je možné kybernetickou kriminalitu definovat **jako jednání namířené proti počítači, případně počítačové síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu.** Neopomenutelnou skutečností pro to, aby bylo možné uplatnit definici kyberkriminality, je fakt, že počítačová síť, respektive kyberprostor je pak prostředím, v němž se tato činnost odehrává.

Při definici pojmu kybernetická kriminalita je nutno v prvé řadě **vymezit pojem kriminalita vůbec**. V souvislosti s provozem informačních systémů, výpočetní techniky či komunikačních prostředků dochází k celé řadě jednání, která jsou jistě nežádoucí, ale nejsou postižitelná prostředky trestního práva, přestože mohou být pro společnost značně nebezpečná (škodlivá). Taková jednání

26: Dále jen **Úmluva o kyberkriminalitě**. Blíže viz: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
27: Blíže viz kap. 5.1.1 Úmluva Rady Evropy č. 185 o kyberkriminalitě; 5.1.2 Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě; 5.2.2 Kvalifikace kybernetických útoků dle Úmluvy o kyberkriminalitě, Dodatkového protokolu a dle trestního zákoníku.
28: Dále jen **Dodatkový protokol**. ETS No. 189 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems
Blíže viz: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

a priori nemohou být kvalifikována jako počítačová, informační či jakákoliv jiná kriminalita – nejsou totiž kriminalitou vůbec. Při definování pojmu kriminalita (přičemž tuto definici je možno podat z více úhlů pohledu - sociologicky, trestněprávně atd.) se opíráme o definici kriminality jako o **souhrn všech jednání, která lze podřadit pod některou skutkovou podstatu, upravenou trestním zákonem.**[29] **Podle tohoto vymezení tedy nejsou kriminalitou taková jednání, která nenaplňují žádnou skutkovou podstatu trestného činu, tedy ani přestupku či jiného správního deliktu**. Takové vymezení pojmu kriminalita je poměrně přesné a lze s ním vystačit i v oblasti informační a komunikační techniky.

Pro páchání trestných činů v oblasti ICT je však charakteristické, že mnohdy jsou v rámci jejich spáchání používány takové postupy či prostředky, jejichž užití nenaplňuje žádnou skutkovou podstatu trestného činu, avšak jsou nedílnou součástí či předpokladem pro jednání další, které již postižitelné prostředky trestního práva je.[30] Navíc tyto netrestné postupy či prostředky představují v procesu odhalování a objasňování trestné činnosti důležité komponenty, jejichž identifikace a pochopení hraje významnou roli při odhalování pachatelů tohoto druhu trestné činnosti.[31]

Kybernetická kriminalita, resp. kybernetická trestná činnost, představuje jakousi nejširší množinu pro veškerou trestnou činnost, ke které dochází v prostředí informačních a komunikačních technologií. Delikty páchané v rámci této množiny je možno podle různých hledisek dále třídit a označovat různými pojmy. „Internetová kriminalita", „e-kriminalita", „kyberterorizmus" či např. „pirátství" pak mohou tvořit podmnožiny kybernetické trestné činnosti, přičemž tímto výčtem nedochází k vyčerpání možných podmnožin jednání, které je možné pod pojem kyberkriminalita podřadit.

Pod označením kybernetická kriminalita bývají v odborných publikacích nejčastěji označena taková kriminální **jednání, při kterých jsou prostředky informačních a komunikačních technologií**:

a) ***užity jako nástroj pro spáchání trestného činu,***
b) ***cílem útoku pachatele***, přičemž tento útok je trestným činem.

29: Blíže srov. GŘIVNA, Tomáš, Miroslav SHEINOST, Ivana ZOUBKOVÁ a kol. *Kriminologie.* 4. vyd. Praha: Wolters Kluwer, 2014, s. 21–22.

30: Např. zasílání nevyžádané pošty (SPAM). Spam někdy může být pouze reklamním (obchodním) sdělením. Takovéto jednání pak není postižitelné prostředky trestního práva. Může však nastoupit postih správněprávní (na základě zákona č. 480/2004 Sb., o některých službách informační společnosti). Avšak ani tento zákon nepostihuje zasílání SPAMu, který není nevyžádaným obchodním sdělením. Lze si tak představit například zasílání SPAMu politicky, nábožensky, či jinak motivovaného. Jindy může SPAM obsahovat malware umožňující získat přístupové jméno a heslo k bankovnímu účtu klienta (což je za určitých okolností možné kvalifikovat např. jako přípravu k trestnému činu podle § 20 TZK).

31: Např. díky komunikaci pachatele s okolím je možno vystopovat IP adresu jeho PC a následně lokalizovat místo připojení pachatele k síti Internet.

**Takové vymezení kybernetické kriminality však v dnešní době již neobstojí.** Zahrnovalo by totiž i takové trestné činy, při kterých sice dojde k použití informačních technologií, avšak nikoliv v kontextu jejich běžného užívání či určení (např. jde o případy, kdy pachatel ublíží poškozenému na zdraví úderem monitoru či jinou součástí počítače do temene hlavy v úmyslu způsobit ublížení na zdraví; nebo půjde o krádež nákladního automobilu převážejícího počítačové komponenty apod.). Jde o trestné činy, kde je ICT využito mimo svůj rámec určení – např. jako zbraň, jako věc, která má určitou hodnotu vyjádřitelnou penězi, bez ohledu na to, za jakým účelem slouží nebo má sloužit. Při odhalování a objasňování těchto činů se uplatní jiné metodiky vyšetřování (např. metodika vyšetřování krádeží apod.), nikoliv metodika vyšetřování kybernetické kriminality.

Aby bylo možno hovořit o kybernetické kriminalitě, musí být informační a komunikační technologie, které byly ke spáchání trestného činu užity nebo které byly cílem takového činu, zasazeny do určitého kontextu. V tomto duchu je tedy ke dvěma výše uvedeným bodům nutno přiřadit ještě jeden bod, obsahující tuto podmínku. Kybernetická kriminalita pak tedy představuje takovou kriminalitu, kde jsou prostředky informačních a komunikačních technologií:

*a)* ***užity jako nástroj pro spáchání trestného činu*****,**
*b)* ***jsou cílem útoku pachatele,*** **přičemž tento útok je trestným činem,** ***za podmínky, že jsou tyto prostředky užity či zneužity v informačním, systémovém, programovém či komunikačním prostředí (tedy v kyberprostoru).***

Takové vymezení kybernetické kriminality je však stále ještě nedostatečné. Za použití takto stanovených kritérií pro určení, zda je či není konkrétní jednání možno považovat za kybernetickou kriminalitu, dojdeme k závěru, že např. hlediska vymezení účastenství ve smyslu § 24 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů,[32] je možné spáchat každý úmyslný trestný čin pomocí informačních prostředků (např. osoba přiměje pomocí e-mailových zpráv jiného ke spáchání úmyslného trestného činu vraždy). Obdobně tomu bude i u jiných forem trestné součinnosti (např. podněcování, schvalování trestného činu). Ty lze též spáchat prostřednictvím informačních technologií. **Takováto jednání však za kybernetickou kriminalitu označit nelze. Ve svém důsledku by akceptace opačného názoru vedla k jedinému možnému závěru - každý trestný čin, při jehož spáchání pachatel použil jakýmkoliv způsobem informační a komunikační technologie, je kybernetickou kriminalitou.** Z tohoto hlediska by se pak těžko hledaly trestné činy, které za kyberkriminalitu považovat nelze.

**Z uvedeného vyplývá, že kybernetickou kriminalitu nepostačí vymezit pouze pozitivně, ale je nutno ji vymezit i výčtem jednání, která zásadně za kybernetickou kriminalitu považovat nelze.**

Určitý pokus o takové vymezení je možno nalézt v jednom z dokumentů Odboru bezpečnostní politiky Ministerstva vnitra z roku 2006, který vymezuje trestnou činnost na úseku informačních

32: Dále jen **trestní zákoník** či **TZK.**

technologií jako *„…páchání trestné činnosti, 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 buď jako předmět této trestné činnosti,* ***ovšem s výjimkou majetkové trestné činnosti, nebo jako nástroj trestné činnosti.*** "[33]

S tímto negativním vymezením je možno souhlasit jen částečně. Mezi trestné činy hlavy V. trestního zákoníku, tedy mezi majetkové trestné činy, jsou totiž zařazeny i skutkové podstaty trestných činů, které slouží přímo k ochraně informačních a komunikačních technologií (respektive počítačových systémů), jejich součástí, dat na nich uložených, což jsou typické příklady kybernetické trestné činnosti.

V tomto duchu pak bude možno pod pojem kybernetická kriminalita zařadit trestné činy tří různých kategorií:

1) trestné činy, jejichž individuálním objektem charakterizujícím skutkovou podstatu je přímo ochrana počítačového systému, jeho vybavení a součástí před specifickými druhy útoku resp. oprávněné zájmy osob na nerušené užívání těchto technických prostředků,

2) trestné činy, kde je způsob spáchání prostřednictvím informační a komunikační techniky jedním ze znaků skutkové podstaty,

3) ostatní v úvahu připadající trestné činy, které nespadají do první ani druhé kategorie, avšak které mohou být v konkrétním případě též spáchány prostřednictvím informačních technologií a které odpovídají výše uvedené definici, neboť v rámci jejich odhalování a objasňování se mohou uplatnit obdobné postupy jako při vyšetřování trestných činů z 1. a 2. kategorie (např. obdobně zaměřené znalecké posudky).

## Klasifikace forem kyberkriminality

Domnívám se, že pokud se chceme zabývat problematikou kyberkriminality, bylo by vhodné alespoň rámcově vymezit, co vše je možné pod tuto trestnou činnost zahrnout. Na závěr této subkapitoly chci proto čtenáři předložit některé klasifikace kybernetické (či počítačové) kriminality tak, jak je vnímají různé právní normy, různí autoři, či organizace, které se věnují boji s kybernetickou kriminalitou. Na těchto členěních chci demonstrovat i genezi pohledu na problematiku kybernetické kriminality.

33: *Analýza současného stavu a trendů vývoje trestné činnosti na úseku informačních technologií a internetu včetně návrhu řešení.* [online]. [cit. 2.10.2008]. Dostupné z: http://www.mvcr.cz/dokument/2006/informacni.doc

### 1. Klasifikace dle Úmluvy o kyberkriminalitě a dle dodatkového protokolu.

Úmluva o kyberkriminalitě dělí kybernetické trestné činy do čtyř kategorií:

1) **trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů** (Offences against the confidentiality, integrity and availability of computer data and systems),

2) **trestné činy související s počítači** (Computer-related offences),

3) **trestné činy související s obsahem** (Content-related offences),

4) **trestné činy související s porušováním autorských práv a práv souvisejících** (Offences related to infringements of copyright and related rights).

Dodatkový protokol pak definuje další kybernetické trestné činy:

1) **šíření rasistických a xenofobních materiálů pomocí počítačových systémů** (Dissemination of racist and xenophobic material through computer systems),

2) **rasisticky a xenofobně motivované vyhrožování** (Racist and xenophobic motivated threat),

3) **rasisticky a xenofobně motivované útoky** (Racist and xenophobic motivated insult),

4) **popírání, snižování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti** (Denial, gross minimisation, approval or justification of genocide or crimes against humanity).

### 2. Klasifikace Commitee of Experts on Crime in Cyberspace

Dle Statutu Komise expertů Rady Evropy pro zločin v kyberprostoru (Commitee of Experts on Crime in Cyberspace) z roku 2000 lze kyberzločin rozdělit:

1) **Dle pozice počítače při páchání trestné činnosti:**
   - *cíl (terč) útoku;*
   - *prostředek (nástroj) útoku.*

2) **Podle typu činu:**
   - *protiprávní jednání tradiční* (např. padělání bankovek aj.)
   - *protiprávní jednání nová* (např. phishing, DDoS aj.)[34]

34: [online]. [cit. 11.3.2010]. Dostupné z: http://assembly.coe.int/documents/WorkingDocs/doc01/edoc9263.htm
Srov. MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 49

### 3. Klasifikace dle eEurope+

Tento dokument členil počítačové zločiny na:

1) **Zločiny porušující soukromí**
   - Nelegální sběr, uchovávání, modifikace, zveřejňování a šíření osobních dat.

2) **Zločiny se vztahem k obsahu počítače**
   - Dětská pornografie, rasizmus, vyzývání k násilí aj.

3) **Ekonomické**
   - Neautorizovaný přístup, sabotáž, hackerství, šíření virů, počítačová špionáž, počítačové padělání a podvody.

4) **Zločiny se vztahem k duševnímu vlastnictví**[35]

### 4. Klasifikace počítačové trestné činnosti dle kriminalistiky

Porada a Konrád[36] dělí počítačovou kriminalitu do pěti základních skupin.

1) **Neoprávněné zásahy do vstupních dat**
   - změna vstupního dokladu pro zpracování počítačem,
   - vytvoření dokladu obsahujícího nepravdivé údaje pro následné zpracování dat počítačem,

2) **Neoprávněné změny v uložených datech**
   - manipulace s daty, neoprávněný zásah do nich a následný návrat k normálu,

3) **Neoprávněné pokyny k počítačovým operacím**
   - přímý pokyn k provedení operace, či instalace softwaru provádějícího operace automaticky,

4) **Neoprávněné pronikání do počítačů, počítačového systému a jeho databází**
   - informativní vstup do databáze, bez využití informací,
   - neoprávněné užívání informací pro vlastní potřeby,
   - změny, ničení, či nahrazování informací jinými,
   - nelegální „odposlech“ a záznam provozu elektronické komunikace,

5) **Napadení cizího počítače, programového vybavení a souborů a dat v databázích**
   - vytváření programů sloužících k napadení,
   - zavedení viru do programového vybavení počítače,
   - vlastní napadení viry, či jinými programy.[37]

35: Blíže: JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007, s. 92

36: Blíže: STRAUS, Jiří a kol. *Kriminalistická metodika.* Plzeň: Aleš Čeněk, 2006, s. 272–274

37: Tamtéž

## 5. Zaměření Europolu na některé druhy kyberkriminality dle závažnosti

Europol respektuje Úmluvu o kyberkriminalitě a vychází z členění trestných činů v ní obsažených. Pro podporu boje s kyberkriminalitou a pomoc členským státům došlo, v rámci Europolu ke vzniku The European Cyber Crime Centre (EC3).[38] Tento tým jasně deklaroval svoje pole působnosti v rámci boje s kybernetickou trestnou činností a vymezil následující tři oblasti (FP – focal point), kterým se věnuje:

1) **FP TERMINAL – Payment fraud**. Skupina, která se věnuje a poskytuje podporu při řešení online podvodů.

2) **FP Cyborg – High-Tech Crimes**. Skupina, která se věnuje a poskytuje podporu při různých kybernetických útocích, jež ovlivňují kritickou infrastrukturu[39] a informační systémy. Zejména se jedná o útoky typu: Malware, Ransomware, Hacking, Phishing, Identity Theft aj.

---

38: *Combating Cybercrime in a Digital Age.* [online]. [cit. 7.5.2016]. Dostupné z: https://www.europol.europa.eu/ec3

39: Pokud jde o vymezení pojmu kritická infrastruktura, pak je v ČR (v případě kyberprostoru) třeba vycházet ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dále jen **zákon o kybernetické bezpečnosti** nebo **ZKB**. Tento zákon v § 2 písm. b) vymezuje pojem kritická informační infrastruktura a prvek nebo systém prvků kritické infrastruktury.

Definice pojmu kritická informační infrastruktura vychází z právních předpisů upravujících oblast krizového řízení. Kritická informační infrastruktura je součástí kritické infrastruktury, která je vymezena zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) ve znění pozdějších předpisů („dále jen krizový zákon"). Aby mohl být určitý informační systém nebo služba a síť elektronických komunikací zařazena do kritické informační infrastruktury, musí splnit definiční kritéria kritické infrastruktury, jakož i prvku kritické infrastruktury, vymezené krizovým zákonem a dále pak i průřezová a odvětvová kritéria stanovená nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

V odvětvových kritériích pro určení prvku kritické infrastruktury je od účinnosti zákona a kybernetické bezpečnosti vložen bod VI. *„Komunikační a informační systémy"*, písm G.: *oblast kybernetické bezpečnosti*. Zde jsou stanovena odvětvová kritéria pro určení daného informačního systému, služby nebo sítě elektronických komunikací kritickou informační infrastrukturou.

Nicméně toto vymezení se vztahuje pouze na oblast kybernetické bezpečnosti. Obecně **je možné vymezit kritickou infrastrukturu následovně**:

1. Kritickou infrastrukturou se rozumí prvek kritické infrastruktury nebo systém prvků kritické infrastruktury narušení, jehož funkce by měla závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.
2. Prvkem kritické infrastruktury se rozumí stavba, zařízení, prostředek nebo veřejná infrastruktura určená podle průřezových a odvětvích kritérií, která jsou stanovena nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.
3. Průřezovým kritériem pro určení prvku kritické infrastruktury je hledisko:
   a) obětí s mezní hodnotou více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací po dobu delší než 24 hodin,
   b) ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo
   c) dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.

3) **FP Twins – Child Sexual Exploitation**. Skupina, která se věnuje a poskytuje podporu při vyšetřování trestné činnosti, při níž dochází k sexuálnímu zneužívání dětí.

### Další možné klasifikace kyberkriminality

Existuje i mnoho jiných způsobů klasifikace, pro ilustraci uvádím další možné dělení kyberkriminality.[40]

Na tomto místě si dovolím uvést i klasifikaci, kterou jsem vytvořil na základě vlastních poznatků získaných zejména při interpretaci problematiky kyberkriminality na různých seminářích či konferencích.

Je možné konstatovat, že velmi zjednodušeně lze kyberkriminalitu dělit ze tří hledisek:

1) **Dle četnosti (povahy) útoků:**

   a) **porušování práv autorských** (viz kap. 4.10 Internetové (počítačové) pirátství. Jde o jednání, které je v rámci kyberprostoru dominantní a při kterém dochází k porušování intelektuálního vlastnictví. Snaha o potírání tohoto jevu je zjevná zejména za strany soukromých organizací hájících práva autorů.);

   b) **ostatní kybernetické útoky** (viz kap. 4 Projevy kyberkriminality. Vyjma kap. 4.10 Internetové (počítačové) pirátství.).

2) **Dle postižitelnosti trestním právem:**

   a) **trestním právem řešené jednání** (viz kap. 5.2.2 Kvalifikace kybernetických útoků dle Úmluvy o kyberkriminalitě, Dodatkového protokolu a dle trestního zákoníku – některé z uvedených jednání subsumovatelných pod skutkovou podstatu trestného činu);

   b) **trestním právem neřešené (nepostižitelné) jednání** (některé z uvedených jednání není možné, ani za použití přípustné analogie,[41] subsumovat pod zákonné znaky skutkové podstaty trestného činu. Jedná se například o jednání popsaná v kap. 4.5 Spam a kap. 4.12 DoS, DDoS, DRDoS útoky).

---

40: Srov. PROSISE, Chris a Kevin MANDIVA. *Incident response & computer forensic, second edition.* Emeryville: McGraw-Hill, 2003, s. 22 a násl.
Dále pak např. *Cybercrime*. [online]. [cit. 1.2.2015]. Dostupné z:
http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime; aj.

41: **Analogií se rozumí subsumpce případu v trestním zákoně výslovně neuvedeného, pod zákonné ustanovení podobné, v zákoně uvedené.** Oproti extenzivnímu výkladu je v rámci analogie využíváno ustanovení, které se na subsumovaný případ podle svého smyslu nevztahuje. Extenzivní výklad se realizuje v souladu s účelem trestního zákona a v jeho mezích, kdežto analogie tyto pomyslné hranice překračuje. Užitím analogie dochází k **vyplňování mezer v zákonech**. Jsou jí řešeny případy, které zákonodárce opomněl upravit právní normou. **Nelze ji** však **využít v neprospěch (k tíži) pachatele** (in malam partem).
Blíže viz NOVOTNÝ, František, Josef SOUČEK a kol. *Trestní právo hmotné*. 3. rozš. vyd. Plzeň: Aleš Čeněk, 2010, s. 83

3) **Dle míry tolerance většinovou společností:**

   a) **společností tolerované jednání** (nejvíce je tolerováno již zmiňované Internetové (počítačové) pirátství);

   b) **společností neakceptované jednání** (např. dětská pornografie - viz kap. 4.13 Šíření závadového obsahu aj.).

## 1.2 Pojmy související s kybernetickou trestnou činností

### 1.2.1 Kyberprostor (Cyberspace)

*„Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky… Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v neprostoru mysli, shluky a souhvězdí dat. Jako světla města, …"*
William Gibson: Neuromancer (1984)

Kyberprostor představuje ono pomyslné pískoviště, na kterém se pohybujeme, ale zároveň se jedná o klíčový prvek v definici kybernetické kriminality. Aby bylo možné definovat kyberprostor, je nezbytně nutné vymezit pojem Internet, který právě s kyberprostorem bezprostředně souvisí.[42]

Světové počátky Internetu, který je nezbytnou materiální podstatou kyberprostoru, se datují do 50. let 20. století.[43] V té době došlo k budování a testování sítí propojených počítačů především pro vědeckovýzkumné a vojenské účely. Ačkoli byl Internet vybudován na základech sítí ARPANET a NSFNET,[44] v současné době není nikdo vlastníkem Internetu a neexistuje ani centrální autorita či instituce, která by jej řídila. *„Přesto existují instituce podílející se významnou měrou na fungování a dalším rozvoji Internetu. Jako první jmenujme Internet Society (ISOC), jenž sdružuje internetové uživatele. ISOC má dvě hlavní složky, Internet Activities Board (IAB) a Internet Engeneering Task Force (IETF). Obě tyto složky spolupracují s nejvýznamnějšími počítačovými firmami na tvorbě standardů potřebných pro další rozvoj Internetu."*[45]

---

42: Specifikace připojení koncového uživatele k Internetu je vysvětlena v kap. 1.3 Počítačové sítě a jejich fungování a 1.4 ISP (Internet Service Provider). Vymezení této specifikace je mimo jiní nezbytné i pro postup orgánů činných v trestním řízení, avšak je nadbytečné ji vysvětlovat vrámci pojmu kyberprostor.

43: **Československá republika se k internetu poprvé připojila v roce 1992** prostřednictvím univerzity: České vysoké učení technické.

44: Srov. *Internet History of 1980s*. [online]. [cit. 7.6.2016]. Dostupné z: http://www.computerhistory.org/internethistory/1980s/

45: *Internet, připojení k němu a možný rozvoj (Část 2 – Historie a vývoj Internetu)*. [online]. [cit. 10.2.2008]. Dostupné z: http://www.internetprovsechny.cz/clanek.php?cid=163

Osobně se však domnívám, že výsostné postavení v rámci sítě Internet má sdružení ICANN[46] (Internet Corporation for Assigned Names and Numbers). Do náplně činnosti tohoto sdružení totiž spadá stanovení pravidel pro provoz systému doménových jmen. V současné době se však do popředí stále více dostávají, a větší úlohu hrají ISP.[47]

**Materiální (hmotnou) podstatou** Internetu je jeho páteřní síť, která vede signál (data) vzduchem, kabely, či jinými přenosovými médii. **Technicky se jedná o celosvětovou distribuovanou počítačovou síť složenou z jednotlivých menších sítí, které jsou navzájem spojeny pomocí protokolů IP a tím je umožněna komunikace, přenos dat, informací a poskytování služeb mezi subjekty navzájem.** Tím je vlastně vytvořen dynamický, neustále se měnící a vyvíjející systém vázaný na hardware, avšak zároveň vytvářející těžko definovatelný a prakticky neomezený **kyberprostor**. Lze říci, že kyberprostor je virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném. Vzniká tak zajímavý paradox, který sice umožňuje existenci nehmotného média (kyberprostoru), schopného se, díky distribuovanosti hmotného média (prvků sítě, jednotlivých počítačových systémů, cloudových úložišť, propojených služeb, atd.), adaptovat a měnit v případě poškození materiálního média, avšak v případě úplného kolapsu materiálního média (respektive všech jeho součástí) dojde k nevratnému poškození, či zániku kyberprostoru jako takového.

Kyberprostor je také možné definovat jako prostor kybernetických aktivit či jako prostor vytvořený informačními a komunikačními technologiemi, který vytváří virtuální svět (či prostor) jako paralelu k prostoru reálnému.

Pokud jde o legální definici kyberprostoru, je možné využít například znění § 2 písm. a) ZKB, kde je uvedeno, že *„**kybernetickým prostorem je digitální prostředí** umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“*

Do obecného povědomí se pojem kyberprostor začíná dostávat po vydání deklarace Johna Barlowa (zakladatele Electronic Frontier Foundation): „A Declaration of the Independence of Cyberspace“:

*„Vlády Průmyslového světa, vy znavení obři z masa a oceli, přicházím z Kyberprostoru, nového domova Mysli. Jménem budoucnosti vás žádám, abyste nás vy, lidé minulosti, nechali na pokoji. Nejste mezi námi vítáni. Vaše svrchovanost nesahá do míst, kde se scházíme.*

*Nemáme žádnou volenou vládu a nejspíše ani žádnou mít nebudeme, proto k vám promlouvám s autoritou o nic větší než tou, se kterou vždy mluví sama svoboda. Prohlašuji námi budovaný globální společenský prostor za přirozeně nezávislý na tyraniích, do kterých se nás snažíte uvrhnout. Nemáte žádné*

46: Blíže viz https://www.icann.org/

47: ISP – Internet Service Provider. Blíže viz kap. 1.4 ISP (Internet Service Provider) a 2.5 Odpovědnost poskytovatele služeb informační společnosti

*morální právo nám vládnout a nemáte ani žádné donucovací prostředky, kterých bychom se skutečně museli obávat.*

*Vlády odvozují svou spravedlivou moc od souhlasu podřízeného lidu. O náš souhlas jste nežádali a ani jste žádný nedostali. Nezvali jsme vás. Neznáte nás a neznáte ani náš svět. Kyberprostor neleží uvnitř vašich hranic. Nemyslete si, že ho můžete budovat, jako by to byl nějaký veřejný stavební projekt. Nemůžete. Je to přírodní jev, který roste prostřednictvím našich společných činů.*

*Nezapojili jste se do našeho velkého podmanivého dialogu a nevytvořili jste ani bohatství našich trhů. Neznáte naši kulturu, naše mravy, ani nepsané zákony, které naší společnosti již teď dodávají větší řád, než by mohlo přinést kterékoliv vaše nařízení.*

*Tvrdíte, že mezi námi jsou problémy, které vy musíte vyřešit. Tohle tvrzení využíváte jako záminku, abyste mohli vtrhnout do našeho výsostného prostoru. Spousta těch problémů vůbec neexistuje. Pokud vzniknou skutečné spory, pokud nastanou křivdy, sami je odhalíme a vyřešíme vlastními prostředky. Vytváříme svou vlastní Společenskou smlouvu. Tohle zřízení vznikne podle podmínek našeho světa, ne toho vašeho. Náš svět je jiný.*

*Kyberprostor sestává z transakcí, vztahů a myšlenek vůbec, uspořádaných jako stojatá vlna v síti našich komunikací. Náš svět je zároveň všude a nikde, ale není tam, kde žijí tělesné schránky.*

*Vytváříme svět, kam mohou všichni vstoupit bez výsad a předsudků spjatých s rasou, ekonomickou mocí, vojenskou silou nebo místem narození.*

*Vytváříme svět, ve kterém může kdokoliv a kdekoliv vyjádřit své přesvědčení, jakkoliv ojedinělé, aniž by se musel bát, že bude násilím umlčen nebo donucen se přizpůsobit.*

*Vaše právní koncepty majetku, projevu, totožnosti, pohybu a kontextu se na nás nevztahují. Všechny jsou založené na hmotě, a tady žádná hmota není.*

*Naše identity nemají tělesné schránky, takže na rozdíl od vás nemůžeme zjednat pořádek pomocí fyzického násilí. Věříme, že naše zřízení se vyvine z mravů, osvíceného osobního zájmu a veřejného prospěchu. Naše identity mohou být rozeseté do spousty vašich právních řádů. Všechny naše dílčí kultury budou obecně uznávat jen jediný zákon, Zlaté pravidlo. Doufáme, že naše vlastní řešení problémů budeme moci vybudovat na jeho základě. Jenže nemůžeme přijmout řešení, která se nám snažíte vnutit.*

*Ve Spojených státech jste dnes vytvořili Zákon o reformě telekomunikací, který popírá vaši vlastní Ústavu a uráží ideály Jeffersona, Washingtona, Milla, Madisona, DeToquevilla a Brandeise. Tyto ideály se teď musejí znovu zrodit v nás.*

*Děsíte se svých vlastních dětí, protože jsou domorodci ve světě, kde vy budete vždy jen přistěhovalci.*

*Protože se jich bojíte, svěřujete svým byrokratickým aparátům rodičovské povinnosti, ke kterým nemáte odvahu postavit se čelem. V našem světě jsou všechny postoje a projevy lidstva, od těch nejpokleslejších až po ty nejvznešenější, součástí jediného nedělitelného celku, globálního dialogu bitů. Není možné oddělit dusivý vzduch od vzduchu, o který se opírají křídla.*

*V Číně, Německu, Francii, Rusku, Singapuru, Itálii a Spojených státech se snažíte zahnat virus svobody budováním strážných věží na hranicích Kyberprostoru. Ty sice nákazu mohou na krátkou chvíli zadržet, jenže budou k ničemu ve světě, který brzy zaplaví bitonosná média.*

*Váš zastarávající informační průmysl se bude snažit upevnit svou pozici navrhováním zákonů, v Americe i jinde, podle kterých by každé slovo na celém světě bylo jejich majetkem. Tyto zákony prohlásí všechny myšlenky jen za další průmyslový výrobek, o nic ušlechtilejší než surové železo. V našem světě se veškeré výtvory lidské mysli dají neomezeně reprodukovat a šířit s nulovými náklady. Globální výměna myšlenek se teď obejde bez vašich továren.*

*Čím dál více nepřátelské a koloniální praktiky nás staví do stejné pozice, v jaké byli i ti předchozí milovníci svobody a sebeurčení, kteří museli odmítnout autoritu vzdálené neinformované mocnosti. Musíme svá virtuální já prohlásit za nedotknutelná vaší svrchovaností, přestože nadále přijímáme vaši nadvládu nad našimi tělesnými schránkami. Rozprostřeme se po celé Planetě, aby nikdo nemohl uvěznit naše myšlenky.*

*V Kyberprostoru vytvoříme civilizaci Mysli. Nechť je lidštější a spravedlivější než svět, který v minulosti vytvořily vaše vlády.*

*Davos, Švýcarsko*
*8. února 1996"* [48]

Osobně jsem přesvědčen o tom, že i po dvaceti letech od vydání této deklarace je její text více než aktuální. Současná společnost se snaží reagovat na obrovský rozmach informačních a komunikačních technologií, jejich vzájemné prolínání a propojování, vznik nových trendů aj. Tato reakce je však mnohdy primárně postavena na vynucování a restrikci, než na pochopení a výchově uživatelů.

Kyberprostor, oproti světu reálnému, je značně specifický a rozhodně je mylné se domnívat, že v něm budou fungovat stejná pravidla, jako ve světě reálném. Obecně je sice možné konstatovat, že na kyberprostor lze aplikovat standardní kritéria,[49] která jsou uplatňována v návaznosti na

48: BARLOW, Perry John. *A Declaration of the Independence of Cyberspace.* [online]. [cit. 23.9.2014].
Dostupné z: https://www.eff.org/cyberspace-independence.
Český zdroj: http://www.piratskelisty.cz/clanek-1476-deklarace-nezavislosti-kyberprostoru

49: Viz kap. 2 Působnost práva v kyberprostoru a specificky 2.2 Prostředky trestního práva.

skutečnou fyzickou lokalizaci dat či informací. Druhou možností je vytvoření nových kritérií, pro aplikaci principu místní působnosti (jedná se o virtuální lokalizaci právních vztahů).[50]

Pro kyberprostor je příznačné, že se do něj propojila značná část společnosti (odhaduje se zapojení přibližně 3,6 miliard obyvatel, přičemž celosvětová populace činí přibližně 7,4 miliard obyvatel).[51] Zároveň je třeba konstatovat, že k masovému zapojení společnosti začalo docházet teprve před cca 15–20 lety.

Mezi znaky kyberprostoru je možné zařadit jeho decentralizovanost, globálnost, otevřenost, bohatost na informace (a to včetně informací v podobě „informačního smogu", naprostých nesmyslů, polopravd a lží), interaktivnost a možnost ovlivňování mínění skrze uživatele (avatary[52]). Podstatným charakterem kyberprostoru je, že primární roli v něm zaujímají technologie a na ně navázané služby. V poslední době se čím dál víc ukazuje, že projev světa virtuálního může a má dopady ve světě reálném.[53]

Rychlost a zejména dostupnost přenášených dat se stává klíčovým elementem dnešní doby. Uživatel zpravidla nechce a ani nemá snahu zjišťovat, kudy a jakým způsobem dochází k přenosu dat jím do informačních sítí vložených. Nezajímá ho ani, kde se nachází adresát přenášených dat, či kde jsou data uchovávána, tím dochází k odhmotnění obsahu od fyzické struktury informačních sítí.

Na jednu stranu je možné sledovat situaci, kdy jsou **společenské vztahy v kyberprostoru delokalizovány**,[54] což s sebou přináší problémy z hlediska aplikace práva, avšak na stranu druhou tato delokalizace umožňuje uživatelům volně („svobodně" a bez omezení v podobě hranic) komunikovat, zasílat, uchovávat a měnit data.

Kyberprostor je možné si představit jako pomyslný ledovec, kde viditelná část představuje prostor, v němž se běžný uživatel pohybuje při své rutinní práci s ICT.

---

50: Blíže viz REED, Chris. *Internet Law*. Cambridge: Cambridge University Press, 2004, s. 218

51: Viz např. *World Internet Users and 2015 Population Stats.* [online]. [cit. 9.8.2015]. Dostupné z: http://www.internetworldstats.com/stats.htm

52: Pojem avatar zde užívám záměrně, neboť jde o vyjádření virtuální identity, která je vytvořena jedincem reálným. Pojem avatár původně vychází z Hinduismu, kde tento pojem označoval zhmotnění boha, či osvobozené duše v tělesné formě na zemi (pozemské vtělení duchovní bytosti).
V současnosti je tento pojem používán jako vizuální reprezentace (ikona či postava) uživatele ve světě virtuálním (ve hře, blogu, fóru, Internetu aj.), tedy v kyberprostoru.

53: Viz jednotlivé útoky uvedené v kap. 4 Projevy kyberkriminality, nebo i například rozmach augmentované reality a služeb na ni navázaných (např. Ingress, Pokemon Go aj.).

54: *Delokalizace právních vztahů na internetu* [online]. [cit. 15.4.2012]. Dostupné z: http://is.muni.cz/do/1499/el/estud/praf/js09/kolize/web/index.html


Obrázek 1: Zobrazení kyberprostoru

Tento ledovec[55] lze rozdělit na následující tři části:
1) **Surface Web,**
2) **Deep Web,**
3) **Dark Web.**

Deep a Dark Weby jsou také často souhrnně označovány jako **D4rkN3ts – Darknets**. Všechny tyto součásti pak společně vytváří skutečný kyberprostor.[56]

Surface Web (také označován jako **Visible Web, Clearnet, Indexed Web aj.**) je ta součást kyberprostoru, která je dostupná většinové společnosti a lze se v ní „pohybovat" za použití standardních

55: *The „Deep Web" is Not All Dark*. [online]. [cit. 12.5.2016]. Dostupné z: http://www.deepwebtech.com/deepweb-not-darkweb/
56: Srov. Např. *The dark Web explained*. [online]. [cit. 20.7.2016]. Dostupné z:
https://www.yahoo.com/katiecouric/now-i-get-it-the-dark-web-explained-214431034.html
či *Surface Web, Deep Web, Dark Web – What's the Difference*. [online]. [cit. 20.7.2016]. Dostupné z:
https://www.cambiaresearch.com/articles/85/surface-web-deep-web-dark-web----whats-the-difference

prostředků (např. webových prohlížečů aj.). Tato část kyberprostoru v sobě obsahuje služby (stránky), jako jsou např. Google, Facebook, YouTube, Seznam aj. Surface web pak spadá do správy ICANN a má jasně danou strukturu.[57]

Na tomto místě je vhodné zmínit se i o intranetu, respektive o privátních či poloprivátních částech kyberprostoru. Intranet je typicky využíván jako firemní či podniková, počítačová síť (tj. umožňující komunikaci mezi subjekty navzájem, jakož i umožňující přenos dat a informací), avšak tato síť, či její prvek není veřejně dostupný. Tím částečně dochází k vytváření Deep Webu, jakožto jedné ze součástí kyberprostoru. Je třeba si uvědomit, že **Darknets nejsou separátní fyzickou sítí, ale že se jedná o aplikační vrstvu v rámci existujících sítí a služeb**. Rozdíl spočívá především v indexaci obsahu. Surface web představuje onu indexovanou část kyberprostoru, avšak tato indexace činí přibližně pouhé 4 % z celkového objemu kyberprostoru. Oněch 96 % obsahu pak připadá právě na Darknets.

Jsem přesvědčen o tom, že je třeba vymýtit tvrzení, která přirovnávají Darknet k prostředí, v němž se nemáte pohybovat. Stejně jako budete ve světě reálném vykázáni z určité oblasti, protože tam například probíhá demolice, tak je vhodné respektovat určitá doporučení a omezení i ve světě virtuálním. Pro pohyb v kyberprostoru je třeba pochopit základní principy, na nichž funguje připojení vašeho počítačového systému do tohoto prostředí[58] a stejně tak je třeba znát podstatu a pravidla poskytovaných či nabízených služeb. Například vytvořením své soukromé VPN[59] mezi dvěma specifickými počítačovými systémy již vstupujete do prostředí Darknetu. Avšak bez tohoto připojení se v mnoha společnostech nejste schopni připojit k pracovnímu počítači, nebo nemůžete navštívit své oblíbené sociální sítě například z území Čínské lidové republiky.

Vždy pak vyvstane otázka: Je to hrozba? Pro řadu uživatelů budou Darknets vždy představovat hrozbu a nelze u nich změnit názor na to, že jde pouze o prostředí, kde se prodávají drogy, zbraně a dětská pornografie. Pro druhou skupinu lidí pak Darknets představují **„…internet pod Internetem, jehož základní ideou je neregulované a necenzurované prostředí…"**[60] a nástroj Tor Browser, běžný nástroj umožňující nesvobodným svobodnou komunikaci. Než něco odsoudíme, je vhodné se seznámit s podstatou fungování konkrétní věci.

Při plném respektování minimálních základních pravidel Darknets nepředstavují takovou hrozbu, jak mnohá média prezentují.[61] Řadu nástrojů a prostředků, pomocí nichž můžu páchat

57: Viz RIR a LIR v kap. 3.1.1 Digitální stopa neovlivnitelná.

58: Blíže viz kap. 1.3 Počítačové sítě a jejich fungování.

59: Virtual private network – virtuální privátní síť.

60: NUTIL, Petr. *Darknet, aneb cesta do hlubin internetu* [online]. [cit. 10.5.2016]. Dostupné z: http://www.kurzy.cz/zpravy/382630-darknet-aneb-cesta-do-hlubin-internetu/

61: Např.: LOUDA, Pavel. *Darknet: Tak vypadá horší stránka internetu.* [online]. [cit. 15.7.2016]. Dostupné z: http://computerworld.cz/internet-a-komunikace/darknet-temna-strana-internetu-52610

kybernetickou či jinou trestnou činnost, mohu zcela legálně získat i v rámci Surface Webu například na stránkách www.alibaba.com. Jen pro zajímavost si zkuste zadat do vyhledávače na této stránce výraz *card skimmer*. Nemíním nikoho navádět k páchání trestné činnosti, jen se snažím poukázat na to, že pokud se někdo rozhodne spáchat trestný čin, pak si prostředek k jeho spáchání může obstarat kdekoliv.

Na druhou stranu je třeba objektivně přiznat, že v oblasti Dark Webu je možné snadněji narazit na všechny výše zmiňované negativní jevy, jako je prodej drog, dětská pornografie aj.

Princip fungování Darknetu je zpravidla postaven na připojení se na bázi Friend-to-friend (F2F) / Peer-to-peer (P2P). Mezi nejznámější „anonymní sítě", či anonymizéry patří: Freenet[62] a TOR project.[63]

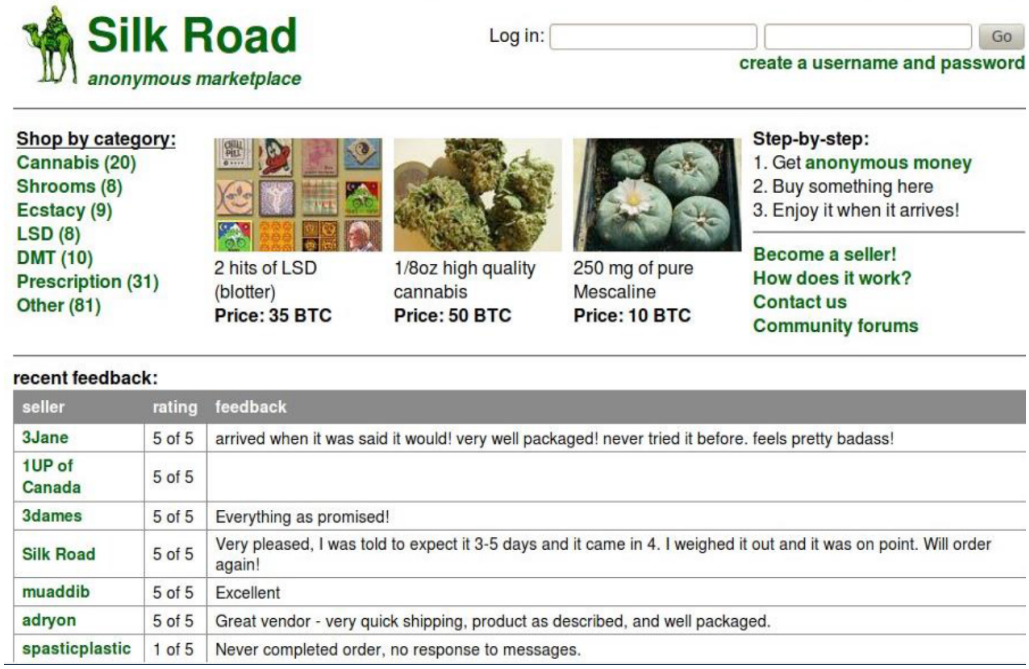
Asi nejznámějším příkladem tržiště v rámci Darknetu, byl Silk Road (http://silkroad6ownowfk.onion, zakladatel: Ross Ulbricht, screen stránky Silk Road je uveden na obrázku č. 2 - Tržiště Silk Road), který zahájil svoji činnost v roce 2011 a uzavřen byl v říjnu 2013 v rámci akce FBI. Podstatou Silk Roadu byla snaha o zachování anonymity jak prodávajícího, tak kupujícího. Transakce byly hrazeny prostřednictvím virtuální měny (v tomto případě Bitcoin[64]) a účty, jež si jednotliví uživatelé zakládali, byly fiktivní. Rozmach Silk Roadu byl spojen především s prodejem drog a s teritoriálním umístěním většiny uživatelů (USA – distribuce zakoupených drog pak zpravidla nenarážela na problémy teritoriality a s nimi spojené procedury, jako je celní kontrola zboží převáženého mezi jednotlivými suverénními státy). Nicméně kromě drog bylo možné na tomto tržišti získat například kradený software; ukradené přihlašovací údaje k e-mailovým adresám, sociálním účtům; falešné či kradené občanské a řidičské průkazy, pasy; kreditní karty; zbraně; padělané zboží všeho druhu aj. Různé zdroje uvádí,[65] že obrat stránky (po dobu jejího fungování) činil okolo **9 519 664** Bitcoinů a bylo zde **957 079** registrovaných uživatelů.

62: https://freenetproject.org/

63: Tor byl původně vytvořen v roce 1995 v U.S. Naval Research Lab, jako prostředek zabezpečeného předávání informací v rámci vládních složek online, přičemž odesílatel a příjemce měli zůstat utajeni. V roce 2003 byl Tor „uvolněn" i pro veřejnost. Bližší informace naleznete na: https://www.torproject.org.

64: Bližší informace naleznete např. na: https://www.bitcoin.com/; http://www.bitcoin-bitcoiny.cz/; http://www.kurzy.cz/bitcoin/ aj.

65: Srov. např.: FRANCESCHI-BICCHIERAI, Lorenzo. *The Silk Road Online Drug Marketplace by the Numbers.* [online]. [cit. 16.6.2016]. Dostupné z: http://mashable.com/2013/10/04/silk-road-by-the-numbers/#9USbF1JntiqU. Zkratka pro bitcoin – BTC.




Obrázek 2: Tržiště Silk Road

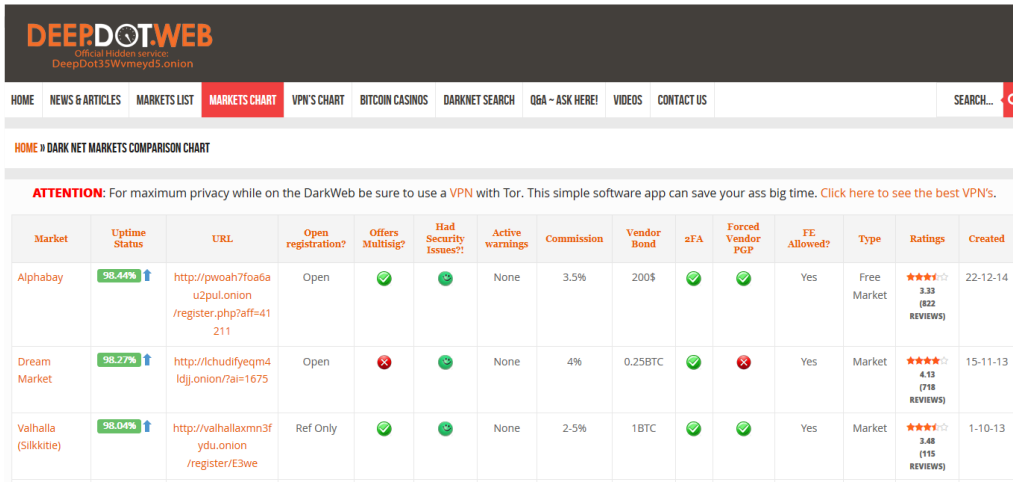
V rámci služby Silk Road byl vždy určitý poplatek z každé transakce připsán na účet Rosse Ulbrichta. Ulbricht byl obviněn z praní špinavých peněz, obchodování s drogami, protivládní konspiraci a hackerství. FBI zajistilo Bitcoiny (26 000 BTC) v hodnotě přibližně 4 milionů dolarů a byly zajištěny finanční prostředky Rosse Ulbrichta pocházející z této trestné činnosti.

Po uzavření Silk Road založili stejní administrátoři, ještě v roce 2013, tržiště Silk Road 2.0. Toto tržiště bylo uzavřeno v rámci společné akce Europolu a FBI dne 17. 10. 2014 (viz Obrázek 3). Dle vyjádření vyšetřovatelů[66] docházelo v rámci tržiště Silk Road 2.0 k transakcím s měsíčním obratem přibližně 8 milionů dolarů, přičemž drogy činily až 70 % prodávaného zboží.

66: U. S. Attorney's Office. *Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court.* [online]. [cit. 18.6.2016]. Dostupné z: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court

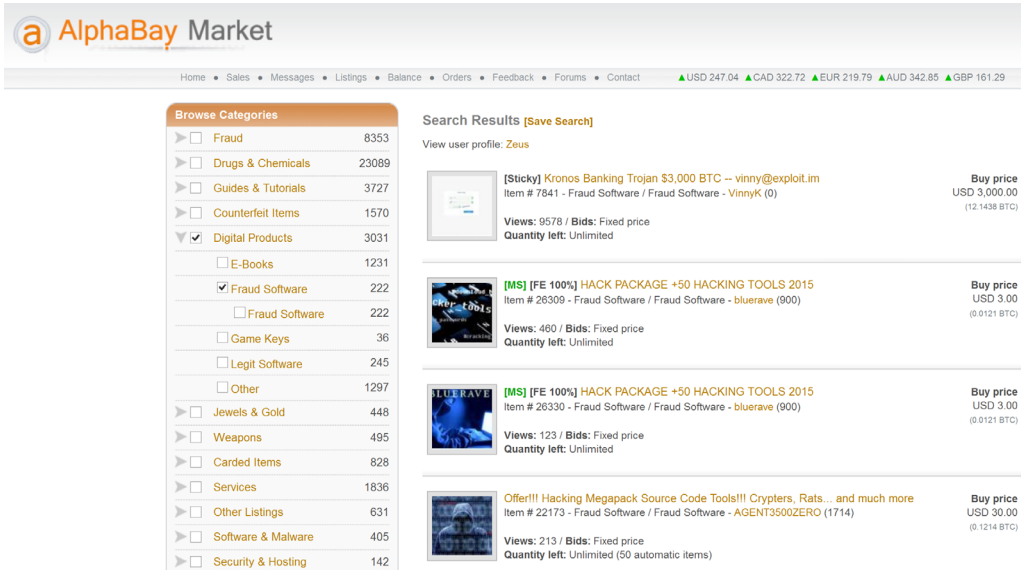

Obrázek 3: Printscreen zobrazující uzavření tržiště Silk Road 2.0

Praxe však ukazuje, že pokud ve virtuálním prostředí jednu službu zakáži nebo jinak znepřístupním, pak na její místo téměř okamžitě nastoupí služby nové, obdobné, mnohdy lépe zabezpečené. Jako příklad je možné uvést seznam tržišť, které fungují v Darknetu, a který naleznete na https://www.deepdotweb.com/dark-net-market-comparison-chart/.



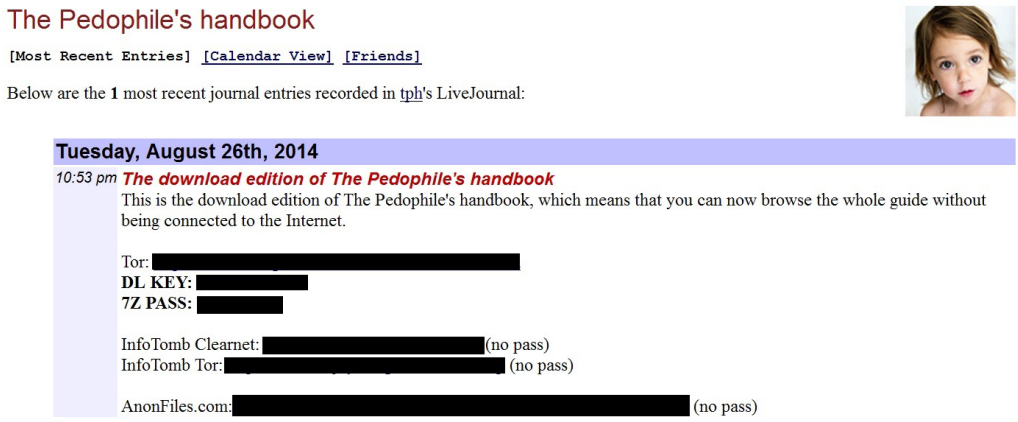

Obrázek 4: Seznam tržišť, které fungují v Darknetu

V současnosti je jedním z oblíbených tržišť tržiště Alphabay. V porovnání se Silk Road 1.0 a 2.0 je třeba konstatovat, že zde dochází k nabízení téměř identického zboží.

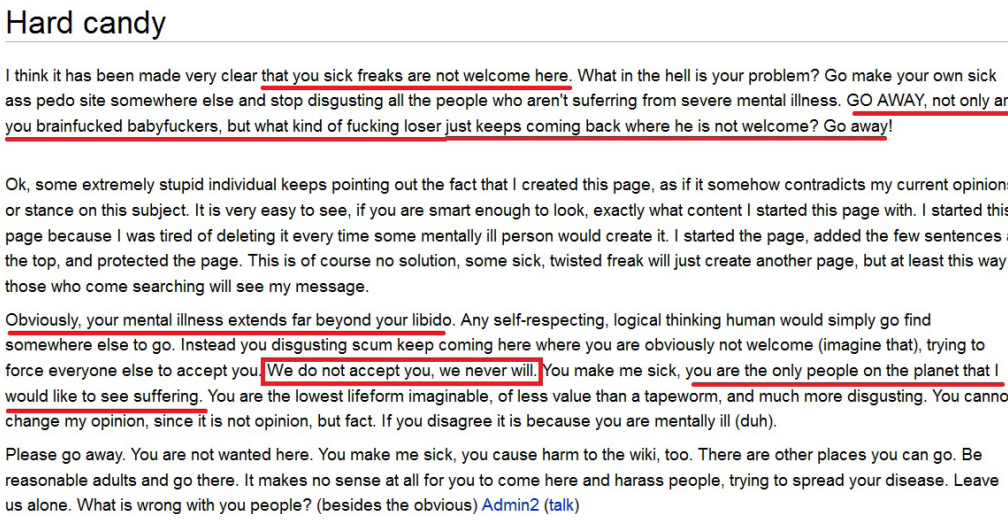



Obrázek 5: Nabídka malware na tržišti AlphaBay Market

Nicméně i v oblasti Dark Webu a aktivit zde prováděných je možné pozorovat určitý posun. Například v roce 2015 bylo možné na Hidden Wiki (http://kpvz7ki2v5agwt35.onion) nalézt návod i stránky na stažení *The Pedophile's handbook* (viz Obrázek 6). Nicméně správce Hidden Wiki se v současnosti jasně a velmi striktně distancuje od podobných aktivit (viz Obrázek 7 - Vyjádření správce The Hidden Wiki k vyhledávání dětské pornografie). Netvrdím, že tímto činem vymizí tisíce pedofilů či jiných osob, které se chtějí dopouštět trestné činnosti, z Dark Webu, avšak je možné pozorovat snahu uživatelů a správců o regulaci obsahu i v prostředí, kde de facto žádná regulace fungovat nemusí. Je mi jasné, že pod Dark Webem může vzniknout Dark Dark Web, či Pitch Black Web, ale i v tomto prostředí záleží na uživateli, správci a dalších osobách, jaké aktivity připustí (budou tolerovat) a jaké už ne.




Obrázek 6: The Pedophile's handbook



## Hard candy

I think it has been made very clear that you sick freaks are not welcome here. What in the hell is your problem? Go make your own sick ass pedo site somewhere else and stop disgusting all the people who aren't suferring from severe mental illness. GO AWAY, not only are you brainfucked babyfuckers, but what kind of fucking loser just keeps coming back where he is not welcome? Go away!

Ok, some extremely stupid individual keeps pointing out the fact that I created this page, as if it somehow contradicts my current opinions or stance on this subject. It is very easy to see, if you are smart enough to look, exactly what content I started this page with. I started this page because I was tired of deleting it every time some mentally ill person would create it. I started the page, added the few sentences at the top, and protected the page. This is of course no solution, some sick, twisted freak will just create another page, but at least this way those who come searching will see my message.

Obviously, your mental illness extends far beyond your libido. Any self-respecting, logical thinking human would simply go find somewhere else to go. Instead you disgusting scum keep coming here where you are obviously not welcome (imagine that), trying to force everyone else to accept you. We do not accept you, we never will. You make me sick, you are the only people on the planet that I would like to see suffering. You are the lowest lifeform imaginable, of less value than a tapeworm, and much more disgusting. You cannot change my opinion, since it is not opinion, but fact. If you disagree it is because you are mentally ill (duh).

Please go away. You are not wanted here. You make me sick, you cause harm to the wiki, too. There are other places you can go. Be reasonable adults and go there. It makes no sense at all for you to come here and harass people, trying to spread your disease. Leave us alone. What is wrong with you people? (besides the obvious) Admin2 (talk)

Obrázek 7: Vyjádření správce The Hidden Wiki k vyhledávání dětské pornografie

Na závěr chci říci, že je možné být anonymní, ovšem pouze za podmínky, že máte dostatečné znalosti ICT, Internetu, jste důslední a máte dostatek času a často i zdrojů. Avšak jako lidé často chybujeme a neuvědomujeme si, že anonymizace jednoho připojení není synonymem pro anonymizaci sítě. Je možné anonymizovat například připojení počítačového systému do počítačové sítě, avšak například využívané služby uchovávají a předávají informace o aktivitách uživatele a počítačovém systému jako takovém.[67]

Domnívám se, že je mnohem lepší pochopit, poznat a porozumět, než pouze zakazovat či nepovolovat. Veškeré tyto aktivity pouze zákonitě vzbudí touhu po zakázaném a neznámém. Cestou k poznání je podle mě pochopení alespoň základních principů, na nichž funguje svět ICT.[68]

### 1.2.2 Kybernetický útok (Cyber attack)

Prosise a Mandiva charakterizují tzv. **„počítačovou bezpečnostní událost"** (kterou lze chápat jako počítačový útok či počítačový trestný čin), jako nezákonnou, nepovolenou, neautorizovanou, nepřijatelnou akci, která zahrnuje počítačový systém či počítačovou síť. Tato akce může být zaměřena například na

67: Blíže např viz kap. 3 Anonymita uživatele, konkrétně pak 3.1.1 Digitální stopa neovlivnitelná a 3.2 Smluvní podmínky (EULA).

68: Blíže viz kap. 1.3 Počítačové sítě a jejich fungování.

krádež osobních údajů, spam či jiné obtěžování, zpronevěru, šíření či držení dětské pornografie aj.[69]

Jirásek a kol. definují kybernetický útok, jako: *„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“*[70]

Takovéto vymezení kybernetického útoku by bylo značně zužující a nepostihující všechny negativní aktivity uživatelů kyberprostoru,[71] zejména z toho důvodu, že kumulativně slučuje podmínky poškození IT a získání informací. Kybernetickým útokem přitom může být i jednání v podobě sociálního inženýrství,[72] kde je jediným cílem získat informace, či naopak útok DoS, či DDoS,[73] kde může být jediným cílem potlačení (tedy nikoliv poškození) funkčnosti jednoho či více počítačových systémů, případně poskytovaných služeb.

Na základě výše uvedeného je tedy možné **kybernetický útok**[74] definovat jako **jakékoli protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby**.[75] Tato jednání nemusí mít vždy podobu trestného činu, podstatné je, že narušují běžný způsob života poškozeného. Kybernetický útok může být dokonán, stejně jako může být ve stádiu přípravy či pokusu.[76]

Kybernetický trestný čin musí být zároveň kybernetickým útokem, avšak ne každý kybernetický útok musí být trestným činem. Řadu kybernetických útoků je, i díky absenci trestněprávní normy, možné subsumovat pod jednání, které bude mít povahu správněprávního, či občanskoprávního deliktu, případně se nemusí jednat o jednání, které je postižitelné jakoukoli právní normou (může jít např. pouze o nemorální či nechtěné jednání).

---

69: PROSISE, Chris a Kevin MANDIVA. *Incident response & computer forensic, second edition.* Emeryville: McGraw-Hill, 2003, s. 13

Srov. dále CASEY, Eoghan. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Second Edition.* London: Academic Press, 2004, s. 9 a násl.

70: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 59. Dostupný online: http://afcea.cz/cesky-slovnik-pojmu-kyberneticke-bezpecnosti/

71: V uvedené definici chybí zejména vymezení jakékoliv jiné motivace útočníka, než té, která spočívá ve *„...způsobení poškození či zisku strategicky důležitých informací.“* Jako příklad, který tato definice nepostihuje, lze uvést ekonomicky motivované útoky, jejichž počet v současnosti dramaticky roste.

72: Viz kap. 4.1 Sociální inženýrství (Sociotechnika).

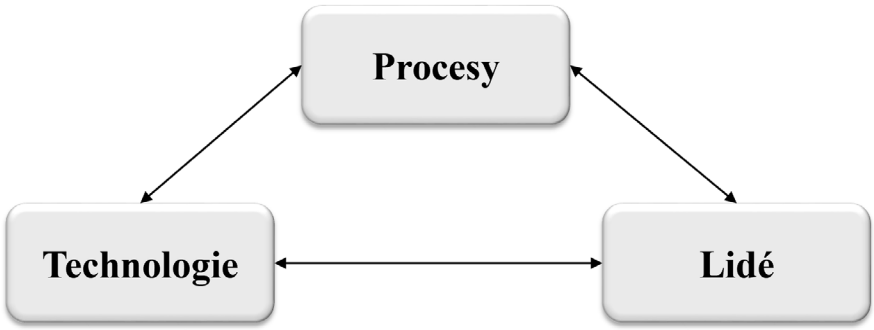
73: Viz kap. 4.12 DoS, DDoS, DRDoS útoky.

74: Od pojmu kybernetický útok je třeba odlišit pojem **bezpečnostní incident**, který představuje narušení bezpečnosti IS/IT a pravidel definovaných k jeho ochraně (bezpečnostní politika).

75: Může jít o jednání uvedená v kap. 4 Projevy kyberkriminality, ale stejně tak může jít o další aktivity v této publikaci neuvedené.

76: Např. útok virem Conficker, který vytvořil Botnet (viz kapitola 4.2 Botnet). Tím byl útok dokonán. Otázkou však zůstává, k jakým účelům bude tato síť případně využita (může se jednat o přípravu daleko vážnějšího kybernetického útoku).

Úspěšnost kybernetického útoku typicky spočívá v porušení některého z prvků, které tvoří kybernetickou bezpečnost (**lidé, procesy a technologie**). **Tyto prvky je třeba uplatňovat, případně modifikovat v průběhu celého jejich životního cyklu. Zejména jde o prevenci, detekci a rekci na útok.**[77] Bezpečnost IT, informací a dat je také přímo závislá na repektování principů „C" „I" „A".[78]




Obrázek 8: Prvky kybernetické bezpečnosti

Pokud chceme definovat pojem kybernetický útok, je vhodné využít i definice, které vyplývají ze zákona o kybernetické bezpečnosti. Tento zákon totiž definuje v § 7 pojmy kybernetická bezpečnostní událost a kybernetický bezpečnostní incident. **Kybernetickou bezpečnostní událostí** je *„událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací."* De facto jde o událost bez zatím reálného negativního následku pro daný komunikační nebo informační systém, ve své podstatě se jedná pouze o hrozbu, která však musí být reálná.

**Kybernetickým bezpečnostním incidentem** je *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události."* Kybernetický bezpečnostní incident tak představuje samotné narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací, tj. narušení informačního nebo komunikačního systému s negativním dopadem.

77: Blíže viz SVOBODA, Ivan. *Řešení kybernetické bezpečnosti.* Přednáška v rámci CRIF Academy. (23. 9. 2014)

78: **C** – Confidentiality/důvěrnost; **I** - Integrity/celistvost; **A** – Availability/dostupnost. Systémy, data a informace je nutné chránit před narušením důvěrnosti (Confidentality), dostupnosti (Availability) a integrity (Integrity) a to v průběhu celého jejich životního cyklu.

### 1.2.3 Počítač (Počítačový systém)

Pojmy počítač a počítačový systém jsou na tomto místě uváděny a vysvětlovány záměrně, neboť i když může být na první pohled patrné, že se jedná o notoriety, trestní zákoník tyto pojmy užívá[79] a jejich vymezení z pohledu práva nemusí být vždy jednoznačné.

Existuje celá řada definic pojmu **počítač**.

1) Za počítač je možné označit zařízení, které se vyznačuje následujícími rysy: zařízení obsahuje centrální procesorovou jednotku, schopnou řídit se programovým kódem a schopnou ovládat přidružené periferie a další části počítače; dále zařízení obsahuje médium pro ukládání dat (paměť, disk aj.). Mezi nepovinné prvky počítače se pak řadí zařízení pro vstup dat (klávesnice, myš aj.), zobrazovací zařízení (nejčastěji se jedná o monitor, ale může se jednat i o projektor či jiné zobrazovací zařízení) a jiné periferie.[80]

2) Počítačem je funkční jednotka schopná provádět rozsáhlé výpočty, včetně mnoha aritmetických a logických operací, bez zásahu člověka.[81]

3) Počítačem je každá funkční jednotka schopná provádět výpočty a operace bez lidského zásahu a podle určitého programu, zařízení na zpracování, uchovávání a využívání dat, která převádí na číselné kódy.[82]

4) Jde o soubor technického vybavení (hardware) schopného vyplňovat posloupnost předem stanovených příkazů. Tyto příkazy jsou ve formě programu nebo sady programů (software).

5) *„V nejobecnějším smyslu lze za počítač považovat přístroj, který může být naprogramován za účelem samostatné realizace aritmetických a logických operací.“*[83]

6) *„Elektronické zařízení, které je schopné přijímat informace (data) v určité formě a provádět sekvenci operací v souladu s předem nastavenou, ale variabilní sadou procesních instrukcí (program) za účelem vytvoření výsledku ve formě informací nebo signálů.“*[84]

79: Viz např. § 120, 230, 231 TZK.

80: Srov. HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* Praha: Computer Press, 1997, s. 85

81: Viz Norma ČSN ISO/IEC 2382-1. Informační technologie – Slovník, Část 1: Základní termíny - s. 20.

82: Viz KUCHTA, Josef a kol. *Kurs trestního práva. Trestní právo hmotné. Zvláštní část.* Praha: C. H. Beck, 2009. s. 224

83: POLČÁK, Radim, František PÚRY, Jakub HARAŠTA a kolektiv. *Elektronické důkazy v trestním řízení.* Brno: Masarykova univerzita, Právnická fakulta, 2015, s. 84

84: Viz Oxford Dictionaries. *Computer* [online]. [cit. 7.5.2016]. Dostupné z: http://www.oxforddictionaries.com/definition/english/computer

Veškerá činnost počítače musí být předem naprogramována. Počítač je prostřednictvím paměťových médií schopen uchovávat informace, které do něj mohou být vkládány, zpracovávány a transformovány, nebo je počítač může zpětně poskytovat ve vnímatelné podobě (na zobrazovacím zařízení, jako zvukové signály, případně jako určité činnosti při řízení výrobních procesů).

Pojem počítačový systém je pojmem, který je využíván trestním zákoníkem a který byl do našeho právního řádu včleněn na základě ratifikace Úmluvy o kyberkriminalitě. V čl. 1 písm. a) této Úmluvy je definován počítačový systém jako *„jakékoli zařízení nebo skupina propojených nebo přidružených zařízení, z nichž jedno nebo více provádí automatické zpracování dat podle programu.“*

**Počítačový systém** je tedy funkční jednotkou, která **je složena z jednoho nebo více počítačů a přidruženého software**, využívající paměťové médium pro všechny, nebo část programů a dat nezbytných pro vykonání programů.

**Počítačový systém může být samostatnou funkční jednotkou** (pracující samostatně - např. osobní počítač, notebook, smartphone aj.), **nebo může jít o soubor několika vzájemně propojených počítačových systémů** (např. počítačová síť).[85]

Příkladem počítačového systému je osobní počítač (včetně připojených periferií), bankomat (ATM), mobilní telefon, PDA, tablet, herní konzole (např. Sony Playstation, PSP, Wii, Xbox 360) aj. Mezi počítačové systémy je však možné například zařadit i televize či jiné domácí spotřebiče umožňující spouštění aplikací, včetně připojení na Internet, či systémy v automobilech, poskytující obdobné funkce. V současné době, zjednodušeně řečeno, je za počítačový systém možné považovat téměř každé zařízení, které splňuje podmínky **Internet of Things (IoT)**.[86] Relativně komplexním počítačovým systémem je Internet jako takový.

---

85: *Computer system.* Překlad autora. [online]. [cit. 16.2.2010]. Dostupné z: http://www.its.bldrdoc.gov/fs-1037/dir-008/_1198.htm

86: Dále jen IoT, či Internet věcí. **Typicky se jedná o zařízení (počítačové systémy), které sbírají a vyměňují si data s jinými počítačovými systémy. Předpokladem je, že jsou tato zařízení připojena do počítače, či jiné počítačové sítě.** Příkladem může být:

- komunikace mezi televizí a žárovkou, pokud bude televize se žárovkou schopna navázat kontakt, bude možné zajistit optimální nastavení světla, kterou žárovka svítí ve vztahu k aktuálnímu nastavení jasu televize;
- předávání informací z osobní váhy do telefonu či přímo lékaři;
- předání informací z wearables („nositelná“ elektronika, čidla aj.) umístěného v oblečení, botách do počítačového systému pro výpočet ušlých kroků, spálených kalorií aj.
- sledování pozice GPS a předávání této informace;
- sledování množství potravin v lednici a případný automatický nákup chybějících potravin aj.

Bližší informace naleznete např. na: *What is Internet of Things.* [online]. [cit. 15.7.2016]. Dostupné z: https://www.microsoft.com/en-us/cloud-platform/internet-of-things

*Internet of Things (IoT).* [online]. [cit. 15.7.2016]. Dostupné z: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Lze konstatovat, že počítačový systém je souhrnem technických a programových prostředků, jejichž variabilita je značná a uvedený výčet je pouze orientační a zdaleka nepostihující všechny možnosti. Vývojem techniky se tak i rozsah zařízení, které spadají do definice počítačového systému, značně posouvá.[87]

### 1.2.3.1 Hardware

**Hardware** (z angl. významu: „technické vybavení"). Pojem hardware vyjadřuje souhrn hmotných technických prostředků umožňujících nebo rozšiřujících provozování počítačového systému.[88] Jde o veškeré fyzické zařízení, které je třeba pro funkci systémů zpracování informací. Je to v podstatě počítač sám. Negativním vyjádřením lze uvést, že hardware je vše, co není programovým vybavením (software). Hardware je možné rozčlenit na dvě skupiny:

1) **Vnitřní vybavení počítače.** Jedná se o součásti hardwaru, bez kterých by nebyla možná vlastní činnost počítače. Těmito nezbytnými komponentami jsou: základní deska s obvody, paměť, procesor, napájecí zdroj. Mezi současné standardní vnitřní vybavení počítače však dále patří harddisk, grafická karta (umožňující vizualizaci činnosti počítače), mechaniky paměťových médií (FDD, CD, DVD, CD-RW, DVD-RW, Blu-Ray, čtečky karet), porty/řadiče (ATA-PATA/SATA, PCI, USB, FireWire, E-SATA aj.), síťové komponenty (umožňující komunikaci v rámci sítí), zvukové a televizní karty aj.

2) **Periferie** (peripheral, či **peripheral device**).[89] Jedná se o zařízení, která ve své podstatě nejsou nezbytně nutná k samotnému provozu počítače (pouze rozšiřuje možnosti jeho využití). *„**V širším slova smyslu** se za periferii považuje cokoli kromě základní desky počítače s jeho procesorem (periferií tedy je: paměť, disk, disketová mechanika, porty, klávesnice, monitor), **v užším slova smyslu** pak až zařízení připojovaná k počítači externě a skutečně nepotřebná k obvyklému provozu i ovládání počítače."*[90] Nejběžněji je periferie chápána právě v užším slova smyslu, tak jak je zde uvedeno. V tomto pojetí se jedná o zařízení, které se různými metodami (kabely, infračervený přenos, technologie Bluetooth, WiFi aj.) připojuje k počítači. Periferií je například klávesnice, myš, monitor, tablet, externí paměťová zařízení, tiskárna, datový projektor, optické senzory, scanner, plotr, externí modem, joystick aj.

Za **předmět sloužící k ovládání počítačového systému** je možné považovat některé z výše uvedených periferií (např. klávesnice, myš, tablet aj.).

87: Srov. SVETLÍK, Marian. Počítače a kriminalita. In: *Sborník odborných sdělení ze semináře uskutečněného na Policejní akademii dne 26. 1. 1999*. Praha: Policení akademie 1999, s. 93 a 97

88: Viz HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* Praha: Computer Press, 1997, s. 182

89: Periferní zařízení - Norma ČSN ISO/IEC 2382-1. Informační technologie - Slovník. Část 1: Základní termíny, s. 9

90: Viz HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* Praha: Computer Press, 1997, s. 309

**Procesor (Central Processing Unit – CPU)** je nezbytnou součástí každého počítače. Tato základní elektronická součást počítače je schopna provádět strojové instrukce. Dochází v ní ke kontrole a provedení všech zadaných operací.[91]

Hlavními součástmi procesoru jsou: aritmeticko-logická jednotka (ALU - tato jednotka provádí vlastní výpočetní operace), registry (lze rozlišovat registry obecné a řídící) a řadič. Řadič řídí činnost procesoru, neboť zprostředkovává načítání strojových instrukcí z paměti, jejich dekódování, provedení a následné uložení výsledků. Pokud má obvod v sobě více procesorových jednotek, pak je označován jako vícejádrový procesor (přičemž uváděn je počet fyzických a virtuálních jader).

Současné počítače v sobě kromě hlavní procesorové jednotky mají zabudovány zpravidla další „podpůrné" procesorové jednotky, které s hlavní procesorovou jednotkou spolupracují. Tyto jednotky slouží např. pro provádění výpočtů pro grafické výstupy (GPU), zajištění WiFi, Bluetooth komunikace, příjem GPS aj.

**Paměťové** nebo **záznamové médium** (případně datový nosič či nosič informací) je externí nebo interní prostředek k zápisu a uchovávání dat. Kromě popsaných pevných disků jsou to nejčastěji diskety, kompaktní disky s různou hustotou zápisu (CD, DVD, Blu-Ray), paměťové karty (SD, MMC, CF karty, SDHC aj.), elektronické paměti typu USB (flashdisky) apod. Paměťovým médiem jsou však i operační paměti.

**Operační paměť** (**vnitřní** či **hlavní paměť**. Anglicky: main memory, internal memory, primary storage) je nezbytnou součástí počítače, neboť umožňuje čtení i zápis dat, nad nimiž programy vykonávají operace. Operační paměť je s procesorem spojena pomocí rychlé sběrnice a procesor má okamžitý, či přímý přístup k této paměti,[92] respektive k přímo požadované buňce operační paměti. Operační paměť je rozdělena do paměťových míst (buněk), které mají definovanou velikost (typicky 1, 2, 4 či 8 bytů). Toto rozdělení se nazývá **fyzický adresový prostor (FAP)** a slouží k:

- přidělování paměťových regionů na požádání procesů,
- uvolňování paměťových regionů na požádání procesů,
- udržování informací o obsazení adresového prostoru,
- zabezpečení ochrany paměti (zabránění přístupu procesu k paměti mimo jeho přidělený region).

V současných počítačích je operační paměť v podobě RAM (Random Access Memory). Jedná se o polovodičovou paměť, která je typicky volatilní (dochází ke ztrátě uložených dat v případě odpojení od zdroje napájení) a dynamická. Mimo paměti RAM se v počítači nachází i paměť

91: Překlad autora. Viz Oxford Dictionaries. *Central processing unit* [online]. [cit. 4.4.2016].
Dostupné z: https://www.oxforddictionaries.com/definition/english/central-processing-unit

92: Překlad autora. Viz Oxford Dictionaries. *Main memory* [online]. [cit. 4.4.2016].
Dostupné z: https://www.oxforddictionaries.com/definition/english/main-memory?q=main+memory

ROM (Read Only Memory), která umožňuje pouze čtení, nikoliv však zápis dat. Tato paměť typicky slouží pro uchování základního řídícího software počítače (BIOS: Basic Input Output System. Tato paměť je součástí polovodičové desky – základní desky), či pro uchování firmware aj. Paměť ROM je energeticky nezávislá.

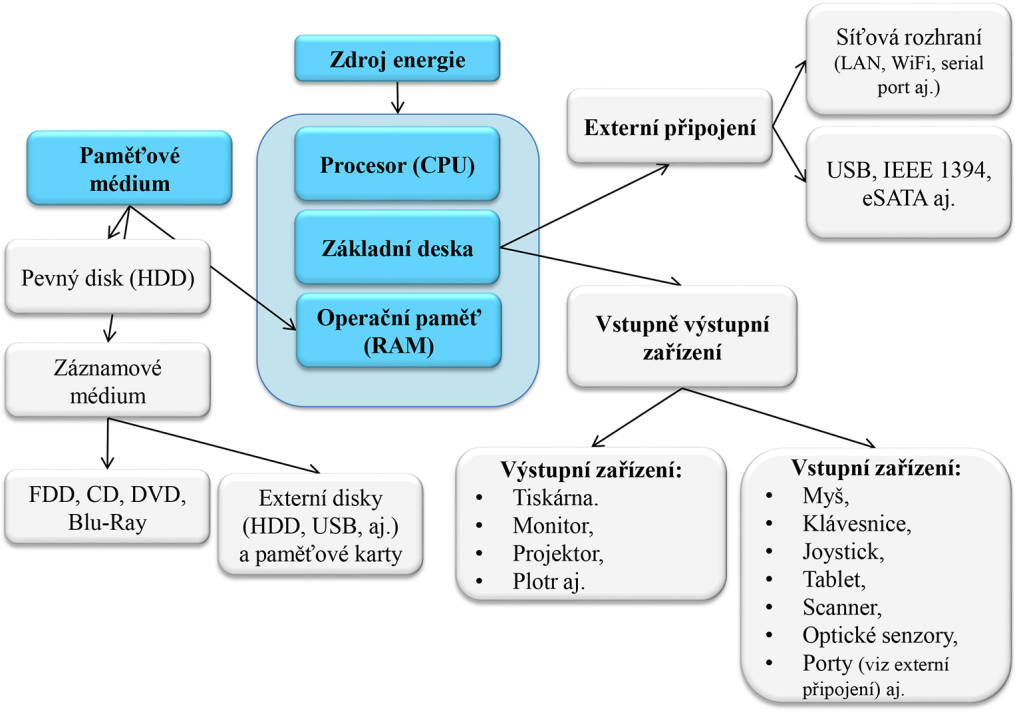
**Základní deska (mainboard, motherboard)** propojuje jednotlivé součásti počítače do fungujícího celku. Přes základní desku dochází k napájení jednotlivých komponent. Základní deska obsahuje integrované obvody zabudované v čipové sadě (chipset). Fyzicky se může jednat o jeden či dva čipy, přičemž čipová sada rozhoduje o tom, jaký procesor a operační paměť lze k základní desce připojit.

**Harddisk (pevný disk)** je paměťové médium zabudované v počítači sloužící k ukládání a uchování dat a programů, instalaci a načtení systému. Povrch disku je rozdělen do sektorů, které mají přesně definované umístění a obsahují příslušná data. Alokační tabulka disku (jedná se nejčastěji o tabulku FAT či NTSF, která je na pevně daném místě disku) určuje, v jakém sektoru disku se data nacházejí. Toto určení má význam zejména z hlediska znaleckého zkoumání paměťových médií. V současnosti se kapacita jednotlivých pevných disků pohybuje v rozmezí několika desítek či stovek MB až po několik TB. Pevné disky mohou být propojeny i v tzv. diskovém poli nejčastěji prostřednictvím SCSI (Small Computers System Interface), či SATA, PATA aj.

**Server** je výkonný počítačový systém, užívaný nejčastěji v počítačové síti jako zdroj dat a programů pro koncové počítače, tzv. klienty nebo pracovní stanice. Pracovní stanice mohou všechny současně pracovat s daty na serveru, přičemž využívají jeho diskové kapacity a programy uložené na jeho discích. Serverů může být zapojeno v síti i několik a každý z nich může plnit specifickou funkci (např. tiskový server, databázový server, terminal server, firewall aj.).

Pokud bychom chtěli graficky znázornit současný počítačový systém, pak by jedním z vhodných zobrazení mohlo být to následující (Modré[93] bloky jsou povinné a bez nich nemůže počítačový systém fungovat. Šedé bloky pak představují periferii v užším či širším slova smyslu. **Zároveň je třeba konstatovat, že počítačový systém musí využívat přidružený software pro to, aby mohl fungovat.**):

93: Poznámka vydavatele: V černobílé verzi knihy nahrazuje modrou barvu tmavě šedá.




Obrázek 9: Grafické zobrazení počítačového systému a jeho částí

### 1.2.3.2 Software

Mezi pojmy **programové vybavení, počítačový program a software** je rozdíl. Nejširším pojmem je software (softwarový produkt), který v sobě zahrnuje nejen počítačový program, ale i databáze a multimédia apod.

Z hlediska přehlednosti budou vymezeny všechny výše uvedené pojmy, nicméně je třeba uvést, že české i mezinárodní právní normy pracují jak s pojmem počítačový program, tak pojmem programové vybavení či software.[94] Mnohdy jsou tyto pojmy využívány jako synonyma, avšak nelze než zopakovat, že mezi vlastními pojmy existují určité odlišnosti.

94: Například trestní zákoník využívá jak pojem **počítačový program** (konkrétně v ustanoveních § 103, 231, 236, 348 TZK), tak **programové vybavení** (v ustanoveních § 120, 230, 232, 264, 267 TZK).

**Programové vybavení** (někdy nepřesně označované jako software) je součást výpočetní techniky. Jsou to programy a přidružená dokumentace, jimiž je doplněno technické vybavení počítače, aby bylo umožněno jeho využití.[95]

Programové vybavení v sobě zahrnuje programy počítačů, počítačové programy včetně software. Jedná se o programy, procedury, pravidla a příslušnou dokumentaci systému zpracování informací nebo jejich část.[96]

**Software** je anglický výraz označující veškeré programové či netechnické vybavení, nutné k provozu počítačů. Software zahrnuje programy od základních vstupně/výstupních systémů (BIOS) a jednoduchých utilit přes operační systémy [nejčastěji MS Windows v různých verzích a OS Linux], grafická rozhraní a veškeré aplikace, od jednoduchých až po komplexní programové systémy.[97] *„Software jsou instrukce, které způsobí, že počítač může být využit. Označuje tedy „logickou" část počítače, kterou nelze vnímat přímo lidskými smysly, tj. „vidět ji nebo si na ni sáhnout". V širším slova smyslu to jsou veškeré informace, které jsou v počítači nějakým způsobem uloženy a dále se dělí podle způsobu použití do dvou základních skupin. Jsou to PROGRAMY a DATA."*[98]

**Počítačový program** je charakterizován jako zápis algoritmu v takovém tvaru, ve kterém jej systém na zpracování údajů dokáže zpracovat. Lze jej charakterizovat jako ucelený souhrn instrukcí (příkazů), pomocí nichž provádí počítač určitou činnost. Program je tvořen souborem nebo více soubory, které jsou v úhrnu dostatečně schopné provádět předepsanou činnost. Příbuznými termíny, mezi kterými lze těžko vymezit ostrou hranici, jsou:

- *aplikace, čímž se označuje obvykle komplexnější souhrn často i několika programů, které plní úkoly dané oblasti;*

- *software, čímž se označuje jakékoli programové vybavení počítače, které je ucelené spíše svým vnějším zjevem.*[99]

Dle Šámala je počítačový program souborem instrukcí, které mohou být počítačovým systémem provedeny pro dosažení zamýšleného účinku. *„Lze ho definovat i tak, že jde o množinu příkazů, instrukcí, deklarací a popř. jiných prvků programovacího jazyka, vyjadřující algoritmus řešení nějakého problému."*[100]

95: Blíže viz ČSN 36 90 01 – dnes již nezávazná.

96: Blíže viz ČSN ISO/IEC 2382 – s. 9

97: Jako jsou například hry, textové a tabulkové programy, grafické programy aj. - srov. HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* Praha: Computer Press, 1997, s. 379

98: Viz PORADA, Viktor a Zdeněk KONRÁD. *Metodika vyšetřování softwarového pirátství.* Praha: Policejní akademie, 1999, s. 43

99: Srov. HAVELKA, Jiří a kol. *Výkladový slovník výpočetní techniky a komunikací.* Praha: Computer Press, 1997, s. 328

100: ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. vyd. Praha: C. H. Beck, 2012, s. 2306

**Počítačový program** je chráněn jako dílo literární,[101] bez ohledu na formu jeho vyjádření, a to včetně přípravných koncepčních materiálů. Chráněny však nejsou myšlenky a principy, na nichž je založen jakýkoliv prvek počítačového programu.

Program je zapsán ve **strojovém (binárním) kódu** či **zdrojovém kódu**.

**Strojový kód** je souhrn operací či příkazů vyjádřených v řetězci přirozených číslic v binárním tvaru. Jedná se o základní podobu povelů, které je stroj schopen přečíst.

**Zdrojový kód** je (v informatice) označení zápisu textu počítačového programu v některém programovacím jazyce, který je uložen v jednom nebo více textových souborech. *„Zdrojový text a jeho převod do binárního kódu tvoří celek jako dílo (pokud splňují další znaky autorského díla).*[102]

Zdrojový kód je nadřazen kódu strojovému.

### Příklady některého software

**Public domain** jsou programy, které jsou volně šiřitelné a lze je jakýmkoli způsobem dále upravovat a používat, aniž by se osoba vystavovala případné trestní odpovědnosti. Public domain programy jsou chráněny jako autorská díla. Jde o program určený pro volné užití (jedná se např. o 7-Zip, SQLite, CERN httpd aj.)

**Firmware** je základním programovým vybavením počítače (BIOS) uloženým v paměti ROM. Firmware v sobě obsahuje programy a funkce, které jsou relativně neměnné a nevyjímatelné (jedná se např. MB BIOS, GPU BIOS aj.).

**Freeware** jsou programy, které jsou volně šiřitelné, autor však nedovoluje jejich úpravu a modifikaci. Freeware zcela podléhá ochraně prostředky autorského a trestního zákona (jedná se např. Audacity, Imgburn, Itunes, CCleaner, Recuva, Google Chrome, Opera aj.).

**Shareware** jsou programy, které jsou určeny k vyzkoušení a které lze volně šířit. Po definovaném čase, případně počtu spuštění, může program přestat fungovat a uživatel je vyzýván k zaregistrování (další legální používání je pak možné pouze po zakoupení licence). Shareware je obvykle distribuován ve verzi, která je oproti registrované verzi nějakým způsobem omezená (funkčně nebo časově) a zpravidla slouží k tomu, aby se uživatel seznámil s programem před jeho zakoupením. Shareware programy jsou chráněny jako autorská díla (jedná se např. CommView, File Scavenger, MP3 Speed Changer, WinRAR aj.).

**Komerční software** lze získat pouze jeho zakoupením nebo jiným legálním převodem vlastnických práv (dar, dědictví). Jeho volné šíření není dovoleno. Zpravidla si uživatel zakupuje

101: viz § 65 zákona č. 121/2000 Sb., autorský zákon. Dále jen **autorský zákon** či **AZ**.

102: Viz PORADA, Viktor a Zdeněk KONRÁD. *Metodika vyšetřování softwarového pirátství*. Praha: Policejní akademie, 1999, s. 43

pouze licenci umožňující (za přesně stanovených podmínek) užívání softwaru (jedná se např. o Adobe Acrobat Pro, Final Cut Pro aj.).

**Licenční smlouvou** (srov. § 46 AZ) poskytuje autor nabyvateli oprávnění k výkonu práva dílo užít (**licence**) k jednotlivým způsobům nebo ke všem způsobům užití v předem stanoveném rozsahu. Koncový uživatel počítače se zakoupením operačního systému či kancelářského aplikačního programu nestává majitelem tohoto programu, jak se mnozí mylně domnívají, ale je mu poskytnuta pouze licence k užití díla.

### 1.2.3.3 Data a informace

Dle Úmluvy o kyberkriminalitě[103] se **počítačovými daty** rozumí *„jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.*"

**Data** *„jsou fakta, čísla, události, grafy, mapy, transakce atd., které byly zaznamenány. Jsou základním materiálem, surovinou pro informace.*"[104] Data jsou jakékoli prvky s informační hodnotou, které jsou zpracovávány počítačem. Data jsou uchovávána v ucelených souborech, které mohou být různého typu (např. textové, obrazové, binární aj.). Data jsou zpracovávána tak, aby následně utvořila informaci.

Definici dat, respektive počítačových dat, uvádí i Úmluva o kyberkriminalitě v čl. 1, kde je stanoveno, že *„počítačová data znamenají jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.*"[105]

Data jsou z hlediska trestního práva uchovávána na nosičích informací (viz např. § 230 a násl. TZK). Pojem nosič informací je opět pouze synonymem pro nosič dat či paměťové médium (viz kap. 1.2.3.1 Hardware). Podstatné je, že vzhledem ke kontextu uvedeného v trestním zákoníku je třeba za nosič informací považovat takové médium, které je schopno uchovat data v digitální podobě.[106]

Pokud jde o definici **informace**, pak je možné využít teoreticko právní definici od Knappa, který uvádí, že informace je něčím, co snižuje entropii znalostí příjemce, a to tím, že rozmnožuje jeho znalosti, znalosti ověřuje nebo je zdokonaluje.[107]

103: Čl. 1 písm. b) Úmluvy o kyberkriminalitě.

104: Blíže viz POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005. s. 24

105: *Úmluva o kyberkriminalitě.* [online]. [cit. 20.8.2016]. Dostupné z: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0

106: Nosičem informací dle ustanovení § 230 a násl. TZK tedy nebude např. listina, či jiné médium, které je schopno nést informace v „nedigitální" podobě.

107: Srov. KNAPP, Viktor. *Teorie práva.* Praha: C. H. Beck, 1995, s. 222.

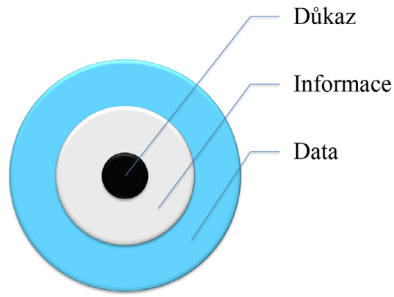
Smejkal uvádí, že za informaci je možné považovat *„každé energetické sdělení, které může mít smysl buď pro toho, kdo je činí, nebo pro toho, kdo je přijímá.“*[108]

**Informace** *„jsou údaje, které byly zpracovány do podoby užitečné pro příjemce. Každá informace je tedy údajem, datem, ale jakákoli uložená data se nemusejí nutně stát informací.“*[109] **Vymezení vztahu mezi informacemi a daty je nutné zejména pro dokazování v trestním řízení.**

Informace jsou vnímány jako něco „kvalifikovanějšího“, nežli data. Data jsou fakta, která se stávají informacemi tehdy, pokud jsou vnímána či vyjádřena v kontextu a nesou význam, který je pochopitelný pro lidi.[110]

Pro úplnost a názornost uvádím i pojem **důkaz** a jeho vztah k pojmům data a informace. Důkazem je informace vyplývající z určitého úkonu trestního řízení, kterým se orgán činný v trestním řízení přesvědčuje o skutečnosti důležité buď pro rozhodnutí ve věci samé, nebo pro následný postup v trestním řízení.[111] Důkaz je přímým poznatkem o předmětu dokazování (což je skutečnost, která má být zjištěna) získaný důkazním prostředkem (postupem dle trestního řádu) z nositele důkazu (jedná se o zdroj informace; tímto zdrojem může být osoba nebo věc).[112] Ne každá informace může být důkazem, ale každý důkaz musí být nutně informací.

Vztah dat, informací a důkazu demonstruje následující graf :[113]




108: SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 36

109: POŽÁR, Josef. *Informační bezpečnost.* Plzeň: Aleš Čeněk, 2005, s. 25

110: ŠÁMAL, Pavel a kol. *Trestní zákoník II. § 140 až 421. Komentář.* 2. Vyd. Praha: C. H. Beck, 2012, s. 2308

111: Srov. FENYK, Jaroslav, Dagmar CÍSAŘOVÁ, Tomáš GŘIVNA a kol. *Trestní právo procesní*. 6 vyd. Praha: Wolters Kluwer, 2015, s. 330

Srov. NOVOTNÝ, František, Josef SOUČEK et al. *Trestní právo procesní*. Plzeň: Aleš Čeněk, 2009, s. 227

Důkaz je přímým poznatkem o předmětu dokazování získaný v procesu dokazování pomocí důkazního prostředku.

112: Blíže viz kap. 6.3 Specifika dokazování kyberkriminality.

113: Graf vychází ze zobrazení vztahu data a informace, uvedeného Požárem (viz: POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, s. 25) avšak je doplněn vztah důkazu.

## 1.3 Počítačové sítě a jejich fungování

Tato subkapitola definuje pojem počítačové sítě a další základní pojmy a některá technická specifika související s počítačovými sítěmi a Internetem. Uvedená minimální charakteristika je zcela nezbytná pro pochopení fungování počítačových systémů v rámci počítačových sítí.

Alespoň obecná znalost v této subkapitole uvedeného schématu připojení k počítačové síti a jeho jednotlivých komponent je důležitá pro úspěšné pochopení fungování IT světa, možnosti vytvoření a nastavení si vlastních pravidel, jakož i odhalování kybernetických útoků a trestné činnosti páchané prostřednictvím ICT.

### 1.3.1 Počítačová síť (Computer network)

Existuje celá řada definic pojmu počítačová síť, pro představu čtenáře některé z nich uvádím.

Jednu z možných definic počítačové sítě je možné nalézt ve Výkladovém slovníku kybernetické bezpečnosti, kde autoři uvádějí, že se jedná o *„soubor počítačů spolu s komunikační infrastrukturou (komunikační linky, technické vybavení, programové vybavení a konfigurační údaje), jejímž prostřednictvím si (počítače) mohou vzájemně posílat a sdílet data.*“[114]

Další definici je možné nalézt v dnes již neplatné normě ČSN ISO/IEC 2382-1 která definovala počítačovou síť jako *„síť uzlů, které se při datové komunikaci propojují.*“[115]

*„Jedná se o množství vzájemně propojených počítačů, strojů, nebo operací.*“[116]

Počítačovou síť si je možné asi nejjednodušeji představit jakožto **soubor (množinu) počítačových systémů, které jsou navzájem propojeny a mezi nimiž dochází k výměně dat či informací**.

Počítačové sítě je možné dělit z celé řady hledisek. Uvedu tři možná dělení, která mají význam pro tuto publikaci:

114: JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, 2015, s. 73. Dostupný online: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/

115: Viz Norma ČSN ISO/IEC 2382-1. Informační technologie – Slovník, Část 1: Základní termíny - s. 15.

116: Viz Oxford Dictionaries. *Network.* [online]. [cit. 4.5.2016]. Dostupné z: https://www.oxforddictionaries.com/definition/english/network

1) **Dělení dle rozlehlosti sítí.** Podle rozlehlosti, respektive rozsahu sítí se sítě rozdělují na čtyři základní skupiny, přičemž v současnosti jsou nejvýznamnější sítě uvedené pod písmeny b) a d):

   a) **PAN** (**Personal Area Network** – Osobní síť). Jedná se o malou privátní síť, která zpravidla slouží pro potřeby jednotlivce či domácnosti. V rámci této sítě dochází typicky k propojení jednotlivých počítačových systémů (mobilní telefon, PDA, laptop aj.) typicky za pomoci Bluetooth, IrDA, WiFi, ZigBee.[117]

      PAN sítě se v současnosti značně rozšiřují a zapojují do své struktury čím dál více zařízení. Příkladem fungování PAN sítě je komunikace jednotlivých technologií v domácnosti například s mobilním telefonem či počítačem, a to v rámci propojení těchto systémů do Internetu věcí (IoT) či Internetu všeho (IoE).[118]

   b) **LAN** (**Local Area Network** – Lokální počítačová síť). Typicky je tento pojem využíván pro označení lokální, či místní sítě, což je síť, v rámci které dochází k propojení uzlů[119] v rámci jedné či více budov. Nezáleží na způsobu propojení jednotlivých uzlů. Toto propojení může být realizováno metalickými, optickými či bezdrátovými sítěmi. Tato síť mívá typicky vyšší přenosovou rychlost a menší vzdálenost mezi jednotlivými uzly. Lokální sítí může být např. kompletní síť (subsítě) univerzity, organizace, ale zároveň se může jednat o malou síť, která je vybudována v rámci domácnosti (například jde o propojení více počítačových systémů: počítače, tiskárny, Smart TV, datové úložiště aj. přes switch či router).

   c) **MAN** (**Metropolitan Area Network** – Metropolitní síť). Jedná se o síť, která propojuje LAN sítě v městské zástavbě. Síť MAN spojuje jednotlivé uzly v řádech jednotek až desítek kilometrů. Někteří autoři řadí tuto síť do sítí WAN.

   d) **WAN** (**Wide Area Network** – Vzdálená počítačová síť). Pojem WAN označuje počítačovou síť propojující geograficky vzdálené oblasti. Typicky jsou do sítě WAN propojovány jednotlivé LAN a MAN sítě. Z geografického hlediska je možné definovat WAN sítě, jako sítě s rozsahem například v teritoriu státu, kontinentu i jako sítě celosvětové.

117: Jedná se o bezdrátovou komunikaci realizovanou na standardu IEEE 802.15.4.

118: Blíže viz kap. 3 Anonymita uživatele.

119: Pojem síťový uzel (node) označuje **zařízení v rámci počítačové sítě, které slouží k jejich vzájemnému propojování, nebo jako koncový bod**, kterým může být jakýkoli počítačový systém. **Každý uzel musí mít svoji MAC adresu** (blíže viz kap. 1.3.3 MAC Adresa).

2) **Dělení dle postavení síťových uzlů.**

a) **Peer-to-peer** (**P2P** – „rovný s rovným", či klient-klient) je počítačovou sítí, kde mezi sebou přímo komunikují jednotliví uživatelé, respektive jednotlivé počítačové systémy. Tento typ sítě nelze centrálně spravovat. Tyto sítě jsou například používány pro sdílení souborů, systémových prostředků aj.

b) **Klient-server** je typem sítě, kde je jeden či více počítačových systémů (server) nadřazen počítačovému systému či systémům (klient/klienti). Klient-server označuje vztah „nadřízenosti a podřízenosti" mezi dvěma počítačovými programy. Klient typicky žádá o služby server. Na modelu klient-server jsou založeny služby typu e-mail, web, přístup k databázi aj.

3) **Dělení dle vlastnictví sítí.**

a) **Privátní síť** je počítačovou sítí, která využívá privátní IP[120] adresy. Privátní adresy jsou používány v rámci sítě LAN (domácí, podnikové aj.). Pokud privátní síť potřebuje připojení k Internetu (přes přidělené veřejné IP adresy), musí používat překlad síťových adres (NAT), nebo proxy server. Privátní sítě se využívají zejména z důvodu nedostatečného množství veřejných IP adres ve verzi IPv4.

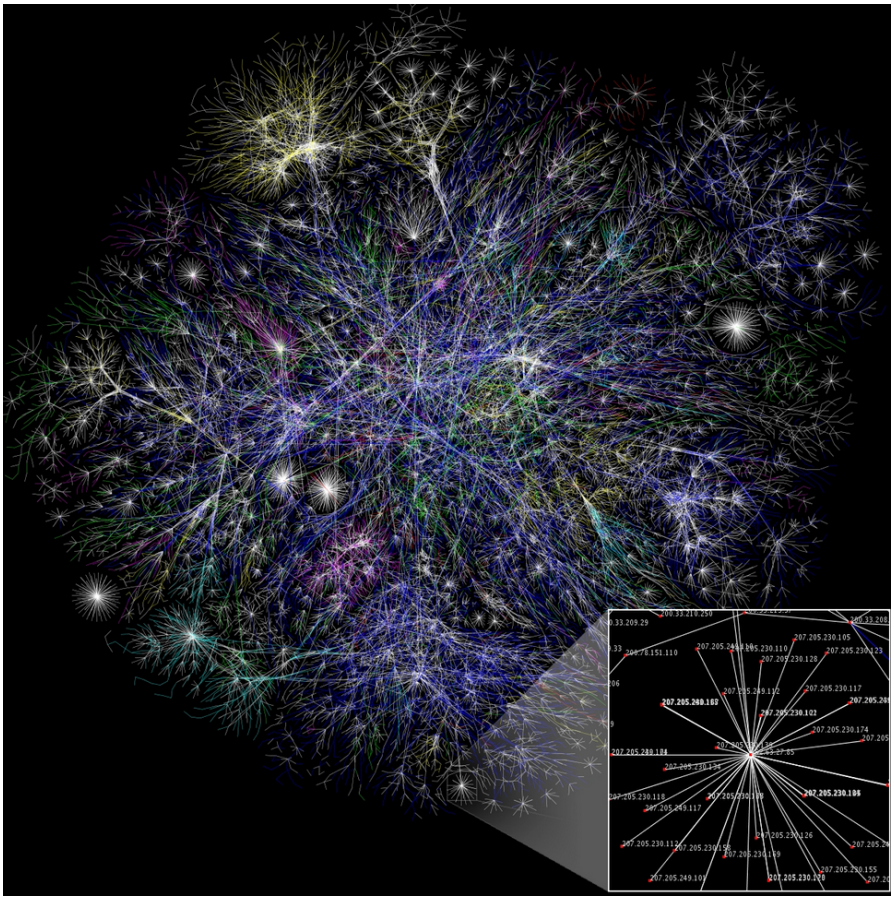
b) **Veřejná síť** je otevřena *„nejširší veřejnosti, které nabízí své služby spočívající v přenosu dat. Uživatelem takovéto sítě se skutečně může stát kdokoli, kdo o to má zájem a je ochoten za to zaplatit, resp. přistoupit na podmínky toho, kdo takovouto síť provozuje. Provozovatelem přitom bývá takový subjekt, který svou datovou sám nepoužívá – vlastní ji a provozuje především proto, aby její služby mohl poskytovat na komerční bázi jiným subjektům."*[121]

c) **Virtuální privátní síť** (**VPN** – Virtual Private Network). VPN je mechanismus (nebo metoda) umožňující propojení počítačových systémů prostřednictvím nedůvěryhodné (např. veřejné) počítačové sítě tak, že propojené počítačové systémy mezi sebou budou moci komunikovat, jako by byly propojeny v rámci důvěryhodné (uzavřené privátní) sítě. Tyto počítačové systémy ověřují svoji totožnost (např. pomocí certifikátů, hesla aj.) a po vzájemné autentizaci je komunikace mezi těmito privátně propojenými počítači šifrována.

Komplexní a globální počítačovou sítí pak je **Internet**, který je také označován jako **„Síť sítí". Technicky se jedná o decentralizovanou, celosvětovou distribuovanou počítačovou síť** složenou z jednotlivých menších sítí navzájem spojených pomocí protokolů TCP/IP.

120: Viz kap. 1.3.2 Internet Protocol a IP adresa.

121: PETERKA, Jiří. *Terminologie datových sítí.* [online]. [cit. 10.11.2015].
Dostupné z: http://www.earchiv.cz/b00/b0003002.php3



Obrázek 10: Jedno z možných grafických zobrazení Internetu[122]

## Protokoly počítačových sítí a Internetu podle modelu ISO/OSI

K tomu, aby bylo možno přenášet data mezi jednotlivými počítačovými systémy, byl definován model ISO/OSI jako referenční komunikační model. Tento model rozděluje komunikaci do sedmi vzájemně propojených vrstev. Tento model je zařazen do ISO/IEC 7498-1:1994 [v ČR: ČSN EN ISO/IEC 7498-1 (369614). Informační technologie – Propojení otevřených systémů – Základní referenční model – Základní model (ISO 7498-1:1994).].

122: Viz Wikipedia. *Internet map* [online]. [cit. 4.7.2016].
Dostupné z: https://upload.wikimedia.org/wikipedia/commons/d/d2/Internet_map_1024.jpg

Graficky je možné těchto sedm vrstev znázornit následovně:[123]

OSI (Open Source Interconnection) 7 Layer Model

| Layer | Application/Example | | Central Device/ Protocols | | DOD4 Model |
|---|---|---|---|---|---|
| **Application (7)** Serves as the window for users and application processes to access the network services. | **End User layer** Program that opens what was sent or creates what is to be sent<br>Resource sharing • Remote file access • Remote printer access • Directory services • Network management | | **User Applications**<br>SMTP | GATEWAY | Process |
| **Presentation (6)** Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network. | **Syntax layer** encrypt & decrypt (if needed)<br>Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation** | | JPEG/ASCII EBDIC/TIFF/GIF PICT | | |
| **Session (5)** Allows session establishment between processes running on different stations. | **Synch & send to ports** (logical ports)<br>Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc. | | **Logical Ports**<br>RPC/SQL/NFS NetBIOS names | | |
| **Transport (4)** Ensures that messages are delivered error-free, in sequence, and with no losses or duplications. | **TCP** Host to Host, Flow Control<br>Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing | PACKET FILTERING | TCP/SPX/UDP | | Host to Host |
| **Network (3)** Controls the operations of the subnet, deciding which physical path the data takes. | **Packets** ("letter", contains IP address)<br>Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting | | **Routers**<br>IP/IPX/ICMP | | Internet |
| **Data Link (2)** Provides error-free transfer of data frames from one node to another over the Physical layer. | **Frames** ("envelopes", contains MAC address)<br>[NIC card — Switch — NIC card] (end to end)<br>Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control | | **Switch Bridge WAP**<br>PPP/SLIP | Land Based Layers | Network |
| **Physical (1)** Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium. | **Physical structure** Cables, hubs, etc.<br>Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts | | **Hub** | | |

Can be used on all layers

123: Rozložení vrstev a funkcí je částečně převzato z *The OSI Model's Seven Layers Defined and Functions Explained*. [online]. [cit. 8.7.2016]. Dostupné z: https://sarvesict.blogspot.cz/2015/11/the-osi-models-seven-layers-defined-and.html. Původní tabulka je však doplněna o definice jednotlivých vrstev, které je možné nalézt na: http://site.the.cz/index.php?id=4. Další možná znázornění OSI modelu je možné nalézt např. na: *Network Layers*. [online]. [cit. 8.7.2016]. Dostupné z: http://www.comptechdoc.org/independent/networking/protocol/protlayers.html
*Network vulnerabilities and the OSI model*. [online]. [cit. 8.7.2016]. Dostupné z: http://cybersecuritynews.co.uk/network-vulnerabilities-and-the-osi-model/

Další možné grafické znázornění v sobě zahrnuje i příklady aktivit v rámci jednotlivých vrstev, či využívané protokoly:[124]

| **OSI Model** | | | | |
|---|---|---|---|---|
| Data Unit (protokolová datová jednotka) | | Layer (Vrstva) | | Function (Funkce) |
| Host Layers | Data | 7 | Aplikační | Definuje způsob, jakým komunikují se sítí aplikace, například databázové systémy, elektronická pošta nebo programy pro emulaci terminálů. Používá služby nižších vrstev, a díky tomu je izolována od problémů síťových technických prostředků. Je softwarová. |
| | Data | 6 | Prezentační | Specifikuje způsob, jakým jsou data formátována, prezentována, transformována a kódována. Řeší například háčky a čárky, CRC, kompresi a dekompresi, šifrování dat. Je softwarová. |
| | Data | 5 | Relační | Koordinuje komunikace a udržuje relaci tak dlouho, dokud je potřebná. Dále zajišťuje zabezpečovací, přihlašovací a správní funkce. Je softwarová. |
| | Segments (Segmenty) | 4 | Transportní | Vlastní přenos dat. Definuje protokoly pro strukturované zprávy a zabezpečuje bezchybnost přenosu (provádí některé chybové kontroly). Řeší například rozdělení souboru na pakety a potvrzování. Je softwarová. |
| Network Layers | Packets (pakety) | 3 | Síťová | Definice protokolů pro směrování dat. Adresování a směrování dat v síti od zdroje k cíli. Definuje protokoly pro směrování dat, jejichž prostřednictvím je zajištěn přenos dat do požadovaného cílového uzlu. Je hardwarová, ale když směrování řeší PC s dvěma síťovými kartami je softwarová. |
| | Frames (rámce) | 2 | Linková | Zajišťuje integritu toku dat z jednoho uzlu sítě na druhý. V rámci této činnosti je prováděna synchronizace bloků dat a řízení jejich toku. Je hardwarová. |
| | Bits (bity) | 1 | Fyzická | Definuje prostředky pro komunikaci s přenosovým médiem a s technickými prostředky rozhraní. Dále definuje fyzické, elektrické, mechanické a funkční parametry týkající se fyzického propojení jednotlivých zařízení. Je hardwarová. |

124: *What is the OSI Model* [online]. [cit. 8.7.2016]. Dostupné z: http://blog.buildingautomationmonthly.com/what-is-the-osi-model/

Dalším síťovým modelem vytvořeným pro sítě internetového typu je **TCP/IP.**[125] Graficky by bylo možné TCP/IP model znázornit následovně:[126]

| TCP/IP | OSI |
|---|---|
| Aplikační | Aplikační |
| | Prezentační |
| | Relační |
| Transportní | Transportní |
| Síťová | Síťová |
| Vrstva síťového rozhraní | Linková |
| | Fyzická |

Technické vymezení sítě tak, jak bylo uvedeno výše, však právem běžně používáno není. Z hlediska práva, zejména trestního, je třeba na závěr kapitoly o počítačových sítích vymezit i pojem ***„veřejně přístupná počítačová síť"*** [viz § 117 písm. a) TZK].

Trestní zákoník v tomto ustanovení uvádí, že trestný čin je spáchán veřejně, pokud je spáchán *„obsahem tiskoviny nebo rozšiřovaného spisu, filmem, rozhlasem, televizí,* ***veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.***"

Šámal k tomuto pojmu uvádí, že se jedná o *„funkční propojení počítačů do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především internet a jiné podobné informační systémy (např. francouzský Minitel apod.). Z technického hlediska je veřejně přístupná počítačová síť soustavou serverů, datových komunikací a k nim připojených počítačů. Z organizačního hlediska jde o provozovatele jednotlivých sítí a podsítí, zprostředkovatele připojení i uživatele a další subjekty."*[127]

K pojmu spáchání činu veřejně přístupnou počítačovou sítí se dále blíže vyjadřuje **Tpjn 300/2012** (stanovisko trestního kolegia Nejvyššího soudu České republiky z 30. 1. 2013) – Rt 20/2013:[128]

Toto kolegium *„obecně uznává, že za veřejně přístupnou počítačovou síť se v obecných rysech považuje funkční propojení do sítí s cílem vytvořit informační systém pracující s tzv. dálkovým přístupem, jakým je především Internet a jiné podobné komunikační systémy. Internet je informační a komunikační systém, který má kromě jiného i povahu prostředku, jehož prostřednictvím lze veřejně šířit informace.*

125: Transmission Control Protocol/Internet Protocol

126: BOUŠKA, Petr. *OSI model.* [online]. [cit. 8.7.2016]. Dostupné z: http://www.samuraj-cz.com/clanek/osi-model/

127: ŠÁMAL, Pavel a kol. *Trestní zákoník I. § 1 až 139. Komentář.* 2. vydání. Praha: C. H. Beck, 2012, s. 1300–1301

128: Rozhodnutí Nejvyššího soudu Tpjn 300/2012, ze dne 30.1.2013. [online]. [cit. 8. 7. 2016]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/510D3BBA2FD98693C1257B2B0054DA9B?openDocument&Highlight=0

*Je tedy patrné, že internet je počítačovou sítí, která figuruje jako přenosové médium umožňující využívání určitých služeb, z nichž nejvýznamnější je přenos informací.*

*K tomu je možno dodat, že na základě výše uvedených skutečností je internet veřejně přístupnou sítí, neboť zaregistrovat se na něm a využívat jeho služby může obecně každý. Podmínka veřejně přístupné sítě je splněna bez dalšího v případě, pokud by komunikace byla vedena formou veřejně přístupných webových stránek, na kterých by např. byly závadné materiály vyvěšeny. K takovým stránkám, pokud nejsou zakódovány či opatřeny heslem, má přístup každý či může se stát uživatelem při splnění určitých podmínek. Webové stránky jsou tedy obecně přístupné blíže neurčenému a neomezenému okruhu uživatelů.“*

### 1.3.2 Internet Protocol a IP adresa

Internet Protocol (**IP**) zajišťuje vysílání **datagramů** na základě síťových IP adres uvedených v jejich hlavičce. Datagram je samostatná datová jednotka, která obsahuje všechny potřebné údaje o adresátovi i odesílateli a pořadové číslo datagramu ve zprávě. Jednotlivé datagramy jedné zprávy putují sítí nezávisle na sobě, mohou putovat jinou cestou a pořadí jejich doručení nemusí odpovídat pořadí ve zprávě. Vlastní doručení datagramu není zaručeno, spolehlivost přenosu datagramu musí zajistit vyšší vrstvy (TCP, aplikace aj.).

Podstatnou informací je, že pokud chce počítačový systém komunikovat v rámci jakékoli sítě, musí mít přidělenou **IP adresu**,[129] která je v rámci dané koncové sítě jedinečná. IP adresy mohou být přidělovány staticky (počítačovému systému je „napevno“ manuálně přidělena IP adresa) či dynamicky, kdy mu je (při každém připojení nového počítačového systému k počítačové síti) na základě MAC adresy přidělena automaticky IP adresa nová. IP adresa není standardně anonymní a počítačový systém ji využívá při komunikaci s jinými počítačovými systémy jakožto jeden z identifikátorů.

V současnosti existují dvě verze Internetového protokolu:

1) **Internet Protocol version 4 (IPv4)**. Jedná se o první, masově rozšířenou a v současnosti stále nejrozšířenější verzi Internet protokolu. IPv4 používá 32bitové adresy, které jsou zapsány dekadicky po jednotlivých oktetech (osmicích bitů). Veřejná adresa[130] v rámci IPv4 je tvořena čtveřicí čísel, vždy od sebe oddělených tečkou, přičemž hodnota každého z nich nepřesahuje **255**. IP adresa tedy může mít podobu například takovéhoto číselného řetězce:

129: Pro doručení jakéhokoliv objektu v libovolném systému musí být splněna podmínka možnosti jednoznačné adresace. Základním komunikačním protokolem Internetu je protokol **TCP/IP**. Základem adresovací struktury sady protokolů TCP/IP je **jedinečná adresa (číslo)**, která určuje jak konkrétní síť na Internetu, tak každý konkrétní počítačový systém v Internetu.

130: Blíže viz rozdělení IP adres v rámci působnosti RIR. Kap. 3.1.1 Digitální stopa neovlivnitelná.

195.113.149.160, či 64.233.168.99 apod. Číselný řetězec IP adresy: 302.233.8.158, či 64.233.168.299 v tomto provedení je nesmyslný a není se možné jeho prostřednictvím přihlásit do sítě Internet.

Protokol IPv4 poskytuje teoretický adresní prostor v rozsahu 232 (což je 4 294 967 296 adres). Prakticky je však využitelnost menší, protože kvůli přidělování adresových bloků je část adres nevyužitých.

Internet Engineering Task Force[131] rozhodla o zachování následujících rozsahů IPv4 adres pro privátní sítě:

| **Označení RFC 1918** | **Rozsah IPv4 adres** | **Počet adres** | **Největší CIDR blok (maska podsítě)** | **Pro síťové rozhraní** |
|---|---|---|---|---|
| 24bitový blok | 10.0.0.0–10.255.255.255 | 16 777 216 | 10.0.0.0/8 (255.0.0.0) | 24 bitů |
| 20bitový blok | 172.16.0.0–<br>172.31.255.255 | 1 048 576 | 172.16.0.0/12<br>(255.240.0.0) | 20 bitů |
| 16bitový blok | 192.168.0.0–<br>192.168.255.255 | 65 536 | 192.168.0.0/16<br>(255.255.0.0) | 16 bitů |

Z důvodu nedostatku veřejných IP adres ve verzi IPv4 došlo k zavedení protokolu IPv6. Tyto dva protokoly v této době fungují současně, avšak je předpokládáno postupné nahrazení protokolu IPv4.

2) **Internet Protocol version 6 (IPv6).** IPv6 je novým protokolem, který by měl vyřešit problémy související s nedostatkem veřejných IP adres. IP adresa verze 6 má délku 128 bitů, které jsou zapsány hexadecimálně (např. 2001:0:5ef5:79fd:386a:e7:4dee:fb51). U IPv6 je odstraněna potřeba použití překladu síťových adres. IPv6 obsahuje celkem 2 128 adres.

Adresní architekturu IPv6 definuje RFC4291. Adresní prostor je rozdělen následovně:

| **prefix** | **význam** |
|---|---|
| ::/128 | neurčená |
| ::1/128 | smyčka (loopback) |
| ff00::/8 | skupinové |
| fe80::/10 | individuální lokální linkové |
| ostatní | individuální globální |

131: https://www.ietf.org/

Protokol IPv6 zavádí tři typy adres:

- **Individuální (unicast)**, která identifikují právě jedno síťové rozhraní.
- **Skupinové (multicast)**, která označuje skupinu síťových rozhraní, jejímž členům se mají data dopravit. Skupinově adresovaný datagram se doručuje všem členům skupiny.
- **Výběrové (anycast)**, která označují také skupinu síťových rozhraní, data se však doručují jen jejímu nejbližšímu členovi.

Z pohledu práva je třeba uvést, že IP adresa je schopna více méně (viz užití NAT,[132] TOR aj.) jednoznačně identifikovat síťové rozhraní v počítačové síti, nikoliv ale přímo konkrétní osobu. IP adresa je schopna identifikovat počítačový systém „po celou dobu" jeho připojení k počítačové síti (skrze všechna jednotlivá připojení). *„V tomto ohledu lze hovořit o tom, že IP adresa sama o sobě představuje neperfektní identifikátor směřující pouze k místu připojení, případně k síti více počítačů či jednomu konkrétnímu počítači. Samotná IP adresa tak z principu neslouží k identifikaci konkrétní osoby, ale směřuje toliko k místu, kde je realizována nějaká činnost, přičemž není samo o sobě známo, zda jde o činnost strojovou (tj. počítače), nebo činnost konkrétní osoby."*[133] U předmětného počítačového systému mohla sedět osoba provádějící konkrétní aktivity, avšak mohla tam sedět i osoba jiná, nebo se mohlo jednat o vlastní (či naprogramovanou) činnost počítačového systému. Prokázání skutečnosti, kdo byl v daný okamžik uživatelem počítačového systému, je významné zejména pro trestní řízení.

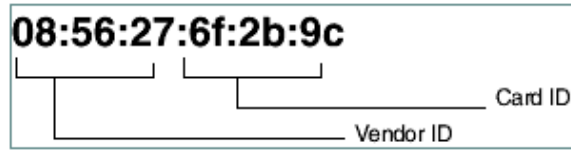
K otázce, zda je IP adresa osobním údajem, se vyjádřil i Nejvyšší správní soud, který v jednom ze svých rozsudků[134] (mimo jiné i s odvoláním na Soudní dvůr EU) uvedl: *„Při posuzování povahy IP adresy je možno podpůrně odkázat rovněž na judikaturu Soudního dvora EU. Ten ve svém rozhodnutí ze dne 29. 1. 2008, sp. zn. C-275/06, Productores de Música de Espana (Promusicae) vs. Telefónica de Espana SAU (rozhodnutí je dostupné z http://curia.europa.eu), považoval IP adresu v kontextu daného případu (Promusicae požadovala po Telefonice odhalení identit osob, kterým poskytovala připojení*

132: **Network Adress Translation** (překlad síťových adres). Dále jen NAT.
Blíže viz např. *NAT.* [online]. [cit. 16.6.2016]. Dostupné z: https://www.abclinuxu.cz/slovnik/nat
**NAT** *se používá k úspoře IP adres v současném Internetu. Většinou je realizován například na routeru připojujícím lokální síť k síti poskytovatele připojení. V lokální síti mohou pak být použity libovolné adresy (nejčastěji se jedná o adresy z neveřejného rozsahu).*
*Když počítač z lokální sítě odesílá paket do vnější sítě (např. Internetu), odešle jej se svou zdrojovou IP adresou a portem. Při průchodu NATem jsou však zdrojové IP adresy v paketech přepsány na veřejnou IP adresu NATu. Také je přepsáno číslo zdrojového portu na port, který NAT odesílajícímu počítači přidělil. NAT si zároveň uloží toto přidělení do své převodní tabulky (ve které jsou uloženy veškeré informace o vzájemném mapování jednotlivých adres).*
*Když pak následně dorazí odpověď od vzdáleného počítače, hlavičky paketů jsou znovu přepsány – tentokrát je cílová adresa a port přepsána příslušnými informacemi z převodní tabulky (lokální IP adresou a portem příslušného počítače) a paket je předán dál k doručení do lokální sítě.*
133: Blíže viz MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, 2013, s. 90
134: Rozhodnutí Nejvyššího správního soudu 1 As 90/2008, ze dne 4. 2. 2009. [online]. [cit. 8.7.2016]. Dostupné z: http://nssoud.cz/files/SOUDNI_VYKON/2008/0090_1As__0800189A_prevedeno.pdf

*k Internetu a u nichž byla známá jejich IP adresa a datum a čas připojení) za osobní údaj ve smyslu předpisů na ochranu osobních údajů. Pro účely nyní posuzované věci lze z uvedeného závěru vyvodit, že jestliže může IP adresa za určitých okolností představovat osobní údaj, tedy údaj, na jehož základě lze identifikovat (přímo či nepřímo) nějakou konkrétní osobu, pak může sloužit také jako důkaz v přestupkovém řízení, byť jako důkaz nepřímého charakteru.* "[135]

### 1.3.3 MAC Adresa

MAC adresa (Media Access Control) je jedinečný identifikátor síťového zařízení, který používají různé protokoly druhé (spojové) vrstvy OSI. MAC adresa je přiřazována síťové kartě bezprostředně při její výrobě, proto je také někdy označována za fyzickou adresu. Přidělená MAC adresa je vždy celosvětově jedinečná (unikátní), avšak je ji možné podvrhnout.[136] MAC adresa je rozdělena na dvě poloviny, přičemž první z nich definuje výrobce síťové karty a druhá polovina je pak jedinečným identifikátorem karty, který jí přidělil výrobce (viz Obrázek 11[137]).




Obrázek 11: MAC adresa a její součásti

Ethernetová MAC adresa se skládá ze 48 bitů a podle standardu by se měla zapisovat jako tři skupiny čtyř hexadecimálních čísel (např. 08:56:27:6f:2b:9c). Mnohem častěji se ale píše jako šestice dvojciferných hexadecimálních čísel oddělených pomlčkami nebo dvojtečkami (např. 00-B0-D0-86-BB-F7).

MAC adresa se zobrazuje pouze k nejbližšímu síťovému zařízení (např. router u poskytovatele připojení k Internetu) a slouží tedy k identifikaci počítačových systémů pouze v jedné, značně omezené části počítačové sítě.

135: Blíže viz MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí*. Praha: CZ.NIC, 2013, s. 91

136: Blíže viz např.: https://cs.wikipedia.org/wiki/MAC_spoofing;
http://www.howtogeek.com/192173/how-and-why-to-change-your-mac-address-on-windows-linux-and-mac/;
http://www.gohacking.com/spoof-mac-address-on-android-phones/ aj.

137: *Addresses and Names* [online]. [cit. 9.7.2016]. Dostupné z:
http://www.wildpackets.com/resources/compendium/wireless_lan/wlan_addresses

## 1.4 ISP (Internet Service Provider)

Na závěr kapitoly, která se věnuje vymezení některých pojmů bezprostředně se vztahujícím ke kyberkriminalitě, IT/ICT, kyberprostoru a aktivitám v něm uskutečňovaným, považuji za nezbytné vydefinovat pojem Internet Service Provider (ISP).[138] Internet Service Provider je nezbytnou součástí fungování světa informačních a komunikačních technologií, zejména pak Internetu a s ním spojenými službami. Internet Service Provider se svou vlastní činností bezprostředně podílí na jeho budování, obměně.

Internet Service Provideři poskytují jednotlivé služby v rámci Internetu. V nedávné minulosti se primárně jednalo o služby, které byly spojeny s poskytnutím internetového připojení, a zkratka ISP označovala pouze subjekty, které zajišťovaly koncovým uživatelům (fyzickým či právnickým osobám) „konektivitu".[139] V minulosti byla většina ISP zároveň telefonními společnostmi nebo si od nich fyzickou infrastrukturu pronajímali. **V současnosti však pojem ISP nezahrnuje pouze ty subjekty, které zajišťují fyzickou konektivitu, ale i subjekty, které poskytují další služby v prostředí Internetu.** V současnosti je možné konstatovat, že začínají převažovat ISP poskytující jiné služby než konektivitu (cloudová úložiště, e-mail, sociální sítě aj.) nad ISP, kteří poskytují konektivitu, byť ti první jsou na druhých závislí. **V České republice není v legislativě používán pojem ISP, ale pojem poskytovatel služby informační společnosti.**[140]

### Poskytovatel služby informační společnosti

Jedná se o subjekty, jejichž prostřednictvím mohou koncoví uživatelé vstupovat do počítačových sítí a využívat zde nabízené služby. ***Směrnice*** Evropského parlamentu a Rady č. ***98/34/ES*** o postupu při poskytování informací v oblasti norem a technických předpisů ve znění směrnice ***č. 98/48/ES*** **nedefinuje pojem poskytovatele** služeb informační společnosti, **ale pouze pojem** samotné **informační společnosti**.[141]

Pojem **služba informační společnosti** je vymezen v čl. 1 odst. 2 směrnice č. 98/34/ES následovně:

*„**službou**" je jakákoliv služba informační společnosti, to je každá služba zpravidla poskytovaná za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb.*

138: Pro označení tohoto subjektu jsou užívány i jiné pojmy. Dle práva ČR půjde zejména o pojem: **poskytovatel služeb informační společnosti**, dále pak **ISP – Internet Service Provider**, někdy také **Information service provider**. V této knize budu pro obecné označení těchto subjektů používat pojem **ISP** či **Internet Service Provider**, případně pak specificky k českému právu pojem poskytovatel služeb informační společnosti.

139: Někdy je pro tyto poskytovatele využíván pojem **IAP – Internet Access Provider.**

140: Někdy také označován jako: „**information intermediary**" (což lze přeložit jako: informační zprostředkovatel).

141: POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 46

**Pro účely této definice se rozumí:**

- ***„službou poskytovanou na dálku"*** *služba poskytovaná bez současné přítomnosti stran,*

- ***„službou poskytovanou elektronicky"*** *služba odeslaná z výchozího místa a přijatá v místě jejího určení pomocí elektronického zařízení pro zpracování a uchovávání dat (včetně digitální komprese) a jako celek odeslaná, přenesená nebo přijatá drátově, rádiově, opticky nebo jinými elektromagnetickými prostředky;*

- ***„službou na individuální žádost příjemce služeb"*** *služba poskytovaná přenosem dat na individuální žádost.*

Příklady služeb, které nejsou zahrnuty do této definice, jsou uvedeny v příloze V. směrnice č. 98/34/ES.

Pojem ***„poskytovatel služeb"*** pak vymezila teprve ***směrnice č. 2000/31/ES*** o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu").

Tato směrnice definuje poskytovatele v čl. 1 odst. 2 takto:

- ***„poskytovatelem"*** *je každá fyzická nebo právnická osoba, která poskytuje určitou službu informační společnosti;*

- ***„usazeným poskytovatelem"*** *je poskytovatel, který účinně vykonává prostřednictvím stálého zařízení po neurčitou dobu hospodářskou činnost; existence a používání technických prostředků a technologií nezbytných k poskytování služby nevytváří samy o sobě usazení poskytovatele;*

- ***„příjemcem služby"*** *je každá fyzická nebo právnická osoba, která k profesním či jiným účelům využívá služeb informační společnosti, zejména pro vyhledávání či zpřístupňování informací;*

- ***„spotřebitelem"*** *je každá fyzická osoba, která jedná za účelem nespadajícím do její profesní či obchodní činnosti.*

Do českého práva byly tyto normy implementovány zákonem č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů.[142]

142: Dále jen **zákon o některých službách informační společnosti** či **ZSIS**.

Ustanovení § 2 tohoto zákona uvádí, že:

a) ***službou informační společnosti*** *je jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu; služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat,*

b) ***elektronickou poštou*** *je textová, hlasová, zvuková nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne,*

c) ***elektronickými prostředky*** *jsou zejména síť elektronických komunikací, elektronická komunikační zařízení, koncová telekomunikační zařízení a elektronická pošta,*

d) ***poskytovatelem služby*** *je každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti,*

e) ***uživatelem*** *je každá fyzická nebo právnická osoba, která využívá službu informační společnosti, zejména za účelem vyhledávání či zpřístupňování informací.*

Zákon o některých službách informační společnosti je, z pohledu českého práva, lex generali ve vztahu k některým jiným právním normám.[143] Tento zákon definuje tři základní skupiny poskytovatelů služeb informační společnosti (ISP). Autor českého zákona následoval **klasifikaci poskytovatelů služeb informační společnosti** tak, jak je provedena směrnicí č. 2000/31/ES. Dle této klasifikace se poskytovatelé dělí na:[144]

1) **Poskytovatele služeb spočívající v přenosu informací poskytnutých uživatelem (angl. Mere Conduit nebo Access Provider).** De facto se jedná o osobu (fyzickou, či právnickou), která je schopna poskytovat jiným osobám, či subjektům přístup k Internetu. Jde tedy **o ISP, kterého je možné označit jako „poskytovatele připojení"**. Jedná se o:

    - *Operátory elektronických komunikací,*
    - *ostatní operátory fyzických linek a*
    - *operátory logických linek.*

143: Zejména k zákonu č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Dále jen **zákon o elektronických komunikacích** či **ZoEK**.
Na druhou stranu je třeba konstatovat, že tento zákon je v některých ustanoveních i *lex specialis* (např. ve vztahu § 6 ZSIS a § 2901 OZ).
Srov. HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014, s. 141
144: Blíže: POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 55

2) **Poskytovatele služeb spočívajících v automatickém mezi ukládání informací poskytnutých uživatelem (tzv. caching).**

3) **Poskytovatele služeb spočívajících v ukládání informací poskytnutých uživatelem (tzv. storage nebo hosting).**

Poskytovatele uvedené pod body č. 2 a 3 je vzhledem, k povaze jimi poskytovaných služeb, možné označit jako **„poskytovatele služeb"**. V současnosti, zejména při poskytování komplexních služeb, je možné se setkat s poskytovatelem, který bude spadat do více skupin, či jej není mnohdy možné striktně podřadit pod určitou skupinu vymezenou tuzemskými i mezinárodními právními předpisy, neboť činnost ISP mnohdy přesahuje rámec té které skupiny. Pokud ISP spadá do více kategorií, je třeba vždy individuálně posuzovat každý konkrétní případ.

Uvedené členění do tří základních skupin je významné zejména z hlediska případné právní odpovědnosti. Podrobnější definice práv a povinností jednotlivých poskytovatelů služeb informační společnosti je uvedena v kap. 2.5 Odpovědnost poskytovatele služeb informační společnosti.

Pro názornost lze uvést i jiné členění poskytovatelů služeb informační společnosti, které uvádí ve své monografii Polčák (jeho výčet není úplný a ani autor sám si tento cíl nekladl). Autor dělí poskytovatele na:

- *provozovatele síťové komunikační infrastruktury (fyzické, logické);*
- *provozovatele síťové asistenční infrastruktury;*
- *provozovatele hostingových služeb, služeb pro bloggery apod;*
- *provozovatele e-mailových služeb;*
- *vyhledávače, portály;*
- *diskusní servery, diskusní služby;*
- *zpravodajské servery;*
- *doménové autority.*[145]

Na závěr se pokusím o velmi zjednodušené grafické znázornění připojení koncového uživatele, za použití ICT, skrze jednotlivé ISP k službám poskytovaným v Internetu. Je třeba si uvědomit, že technické provedení částečně znázorněné na obrázku [privátní síť[146] (či podsítě), různé řídící prvky (switch, router), prvky zabezpečení sítě a jednotlivých počítačových systémů aj.] je možné nalézt jak na straně poskytovatele připojení, tak na straně poskytovatele služeb.

145: Blíže: POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 49

146: Privátní síť je u ISP poskytujícího připojení znázorněna záměrně. V našem regionu (viz **RIR** kap. 3.1.1 Digitální stopa neovlivnitelná) jsou veřejné IPv4 adresy de facto vyčerpány. ISS jsou tedy nuceni vytvářet podsítě (subnets) v rámci přidělených veřejných IP adres. Subnet je možné vytvořit de facto v celém rozsahu IP adres přidělených pro privátní sítě (viz kap. 1.3.2 Internet Protocol a IP adresa). V rámci každé jedné privátní adresy je pak možné vytvořit další podsíť. Jednotlivé podsítě je pak možné hierarchicky spravovat.

Z pohledu práva je problematické, pouze za použití technických informací získaných z protokolu TCP/IP, jednoznačné a nezpochybnitelné určení koncového uživatele. K tomuto určení je však možné použít i jiné identifikátory uvedené například v kapitole 3 Anonymita uživatele.