

## 06 Právo ICT

tags: řsss-řk

> kybernetická kriminalita a kybernetická bezpečnost. Odpovědnost poskytovatelů internetového připojení (směrnice o elektronickém obchodu), internetová jurisdikce, ochrana autorských práv k softwaru, patentová ochrana softwaru, licencování softwaru (včetně open source), ochrana osobních údajů, ochrana soukromí, zákon o kybernetické bezpečnosti (směrnice NIS, zákon o kybernetické bezpečnosti), počítačové zločiny (Budapešťská smlouva)

**Proč ICT chránit?** - Bezpečné a spolehlivé fungování ICT je jedním ze základních předpokladů prosperity - Rozvoj ICT představuje bezpečnostní výzvu pro celou společnost - Rostoucí závislost společnosti na ICT zvyšuje zranitelnost státu vůči kybernetickým útokům

### Základní pojmy

- **Kyberkriminalita** - trestní činnost, orgány činné v trestním řízení
  - cyber-enabled: klasická kriminalita páchaná prostřednictvím ICT
    - šíření protiprávního obsahu, porušení autorského práva, nebezpečné pronásledování, podvod (phishing)
  - cyber-dependent: kriminálním chování jehož cílem je ICT
    - proti CIA triádě systémů (důvěrnost, integrita a dostupnost), Hacking, MITM, DoS, etc.
  - cyber-supported: kriminalita, při níž došlo neúmyslného využití ICT
- **Kyberbezpečnost** - Ochrana infrastruktury, správní orgány s působností v kyberbezpečnosti (NÚKIB)
- **Kyberobrana** - Obrana kybernetické suverenity státu, armáda a bezpečnostní složky, využití bezpečnostních nástrojů k předcházení, zastavení nebo odvrácení kybernetického útoku ohrožujícího zajišťování obrany státu

**Kybernetický prostor** – digitální prostředí umožňující zpracování informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací.

**Kritická informační infrastruktura** – prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti. zdroj ##  
Směrnice o elektronickém obchodu \* ISP: Poskytovatel služeb informační společnosti \* Mere conduit – prostý přenos \* Caching – ukládání do vyrovnávací paměti za účelem posílení dostupnosti dat \* Hosting – shromažďování dat \* V případě ISP nás zajímá především odpovědnost za uživatelský obsah (tedy sekundární odpovědnost) \* Právní úprava se snaží hledat rovnováhu mezi efektivní ochranou práva a nelimitováním rozvoje informační společnosti \* Poskytovatelé jsou odpovědní za obsah pouze pokud: \* **Mere conduit**: sám přenos iniciuje nebo zvolí nebo změní obsah přenášené informace \* **Caching**: vyloučení odpovědnosti podobné jako u MereConduit \* **Hosting**: nejčastěji vzniklá odpovědnost \* mohl vědět, že obsah informací nebo jednání uživatele je protiprávní \* dozvěděl-li se prokazatelně o protiprávní povaze ukládaných informací nebo jednání uživatele a neučinil kroky k odstranění \* Poskytovatelé nejsou povinni: \* Dohlížet na obsah přenášených nebo ukládaných informací \* Aktivně vyhledávat skutečnosti poukazující na protiprávnost \* Poskytovatelé mají **povinnost součinnosti při trestním vyšetřování** (jen neutajované informace) \* **Data Retention**: Právnícká nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat **po dobu 6 měsíců provozní a lokalizační údaje** - tj. údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace a dále údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace - Zároveň nesmí být uchováván obsah zpráv a takto uchovávaný dále předáván

## Internetová jurisdikce

- Snaha o regulaci společenských vztahů vznikajících v souvislosti s kontaktem lidské společnosti a internetu
- Působnost práva je obecně podmíněna existencí státní moci schopné právo vymáhat, ale ICT systémy nejsou díky technickým vlastnostem teritoriálně omezené (fyzická poloha komunikujících stran není podstatná)
- Kybernetická kriminalita zpravidla zahrnuje přeshraniční prvek - určení jurisdikce pak stanovují mezinárodní úmluvy, nebo právo příslušného státu (zpravidla vazba na: lokace pachatele, oběti či důsledků kyberkriminality)
- Co je zločin stanovují státy v rámci své suverenity (snaha o harmonizaci - nejlépejší zatím Úmluva o kyberkriminalitě viz dále)
  - úpravu elektronického obchodování (ochrana spotřebitelů)
  - právo duševního vlastnictví se zaměřením na vztahy a díla souvisejícími s internetem (autorskoprávní ochrana software, doménové právo)
  - e-government
  - internetová kriminalita
  - pomáhá určit, který právní orgán může projednávat případ mezi žalobcem a žalovaným, kterým byl potenciální trestný čin spáchán na internetu (např. provozovatele webových stránek definují v rámci podmínky použití webových stránek u jakého soudu a jaké zemi budou případné spory řešeny)

zdroj ## Ochrana autorských práv k softwaru \* Autorská práva jsou souborem automatických oprávnění, které náleží tvůrcům autorských děl \* práva osobnosti: právo rozhodnout o zveřejnění díla, právo osobovat si autorství a právo na nedotknutelnost díla \* práva majetková: právo dílo užít (rozmnožovat, rozšiřovat, půjčovat, pronajímat, vystavovat a sdělovat veřejnosti) \* Nositel autorských práv je vždy **pouze fyzická osoba**, která dílo vytvořila a těchto práv se nedá vzdát. \* Český autorský zákon stanovuje, že za autorské dílo se považuje také počítačový program (nedefinuje přesně) \* Nemohou být ale chráněny takové programy, které jsou vytvářeny automaticky, aniž by šlo skutečně o autorovu vlastní duševní tvorbu \* Autorská práva k software se např. nevztahují na pouhé myšlenky a principy \* Pokud chce autor povolit nakládání s dílem jiné konkrétní osobě, musí s ní uzavřít **licenční smlouvu** \* **Licenční smlouva:** \* o jaký software se jedná \* jakým způsobem může nabyvatel licence užívat \* může/nemůže autor SW sdílet s ostatními - výhradní/nevýhradní \* časový rozsah licence \* **Smlouva o postoupení práv k počítačovému programu:** \* většina SW je tzv. zaměstnanecké dílo, k němuž vykonává majetková práva ze zákona zaměstnavatel \* zaměstnanec v rámci smlouvy, pak poskytuje svolení se zveřejněním díla či jeho úpravami \* přechází majetková práva na postupníka (toho kdo si SW objednal) \* narození od licence získá postupník mnohem výhodnější postavení, protože postupitel, ztrácí oprávnění k dílu. Na rozdíl od licence se tak nemusí precizně formulovat, jakým způsobem se dílo užívá

zdroj

## Patentová ochrana softwaru

- narození od autorské ochrany, **není automatická** - patent musí být registrován a udržován
- patentován není program, ale řešení (chrání vynálezce) - mnohdy patenty pokrývají obecně formulované jednoduché až triviální myšlenky
- ten kdo vlastní patent na software nebo jeho část, může vymáhat práva z patentu nejen proti tomu, kdo neoprávněně kopíruje tentýž program, ale i proti tomu, kdo **uvádí na trh program s podobnou funkcí nebo ovládáním**
- v EU je patentů výrazně méně než v USA (vysoká cena a časová náročnost patentových přihlášek)
- problémy patentové ochrany:
  - je velmi těžké žádný patent neporušit
  - je těžké zjistit zda SW patenty porušuje
  - mimo EU patentová ochrana SW vede v praxi k výraznému posílení velkých nadnárodních softwarových společností na úkor menších hráčů, neschopných vynaložit dostatečné finance a úsilí k získání patentové ochrany svých řešení

zdroj ## Licencování softwaru - Licence je právní nástroj, definován v rámci autorského

zákonu, který umožňuje používat nebo redistribuovat software - licence je definována v rámci **licenční smlouvy** - **Proprietární SW licence**: \* EULA (End User License Agreement) pak obvykle velmi striktně vymezuje, co uživatel může - **Open Source licence**: \* BSD, MIT: minimální nároky na distribuci a modifikaci SW \* GPL: copyleftová licence, dovoluje modifikaci i distribuci ale pod stejnou licencí \* public domain: autor zcela vzdává nárok na ochranu svého díla a bez jakýchkoliv dalších podmínek ho veřejně nabízí k dispozici

- CC: Creative commons, set licencí, které lze použít na dokumentaci, game art, hudbu atd.
- Copyleftované licence: vlastnost licence, která udává že programy, které vznikly modifikací, musí být povinně šířeny pod stejnou licencí jako původní program (GPL a CC)

[zdroj](#)

## Ochrana osobních údajů

**Osobní údaje** jsou jakékoliv informace, které by mohli vést k identifikaci subjektu. Osobní údaje jsou jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Mezi obecné osobní údaje řadíme jméno, pohlaví, věk a datum narození, osobní stav, ale také IP adresu a fotografický záznam. Vzhledem k tomu, že se GDPR vztahuje i na podnikající fyzické osoby, řadíme mezi osobní údaje i tzv. organizační údaje, kterými jsou například e-mailová adresa, telefonní číslo či různé identifikační údaje vydané státem.

### GDPR

- General Data Protection Regulation, 2016
- nařízení EU, která se týká všech firem a institucí, ale i jednotlivců a online služeb, které zpracovávají data residentů EU
- ukládá **povinnosti firmám a organizacím** a definuje práva občanů
- definuje:
  - **Datový subject**: ten jehož data jsou zpracována
  - **Správce osobních údajů**: každé zpracování má stanovenou osobu, která je odpovědná za jeho průběh - správce
    - je odpovědný za zákonné zpracování údajů
  - **Zpracovatel osobních údajů**: zpracovává osobní údaje jménem správce.
    - má povinnost uchovat data a oznámit porušení zabezpečení
- definuje **základní principy zpracování dat**:
  - transparentnost: zpracování dat má být transparentní
  - limitace účelem: účely zpracování dat musí být předem definované uživateli
  - minimalizace: pouze data zcela potřebná pro účel mohou být zpracována
  - přesnost: uložená data musí být přesná
  - integrita a důvěrnost: při zpracování dat musí být zachována integrita a důvěrnost dat

✓ Označení správce

🖨️ Účely zpracování

👤 Kategorie subjektů a údajů, příjemců

🕒 Lhůty pro výmaz

📄 Dokumentace bezpečnostních opatření

specifikuje povinnosti, postupy a deadlines po úniku dat - 72 hodin - uděleje **práva uživatelům**: - právo být informován - právo být zapomenut - právo opravy - pokud jsou

data zastaralá nebo nepřesná - právo přístupu - každá společnost, která data zpracovává musí na vyžádání vydat data, které o jedinci má \* ukládá sankce v maximální výši 20.000.000 eur nebo 4 % z celkového ročního obrátu společnosti (vyšší z obou možností)

## Zákon o kybernetické bezpečnosti

- cílem je zvýšit **bezpečnost kybernetického prostoru a kritické infrastruktury**
- specifikuje **bezpečnostní opatření** a ukládá povinnost a rozsah bezpečnostních opatření správcům systémů kritické infrastruktury a významných informačních systémů
  - **organizační opatření:** řízení rizik, bezpečnostní politika, organizační bezpečnost...
  - **technické opatření:** fyzická bezpečnost, nástroje pro ověřování identity uživatele, nástroj pro ochranu před škodlivým kódem, nástroj pro zaznamenání činnosti administrátora, uživatelů v kritické informační infrastruktuře
- Specifikuje kybernetickou **bezpečnostní událost a incident**
  - ukládá povinnost detekce a bezodkladného hlášení incidentu
- Specifikuje **varování**
  - Vládní CERT vydá varování, dozví-li se zejména z vlastní činnosti nebo z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o hrozbě v oblasti kybernetické bezpečnosti
  - informace o hrozbě zobrazí na svých stránkách
  - na varování není vyžadována konkrétní akce ale je povinnost hrozby zohlednit
- specifikuje opatření:
  - reaktivní: v důsledku na incident
  - ochranná
- Povinné osoby:
  - **Významná síť:** Významnou sítí se rozumí síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo přímé připojení ke kritické informační infrastruktuře. **Jde především o provozovatele významných páteřních komunikačních infrastruktur.**
  - **Významný informační systém:** Významným informačním systémem se rozumí informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.
  - **Kritická informační infrastruktura:** Je to informační infrastruktura kritické infrastruktury, která je určena průřezovými kritérii.
  - **Digitální služba:** Služba informační společnosti podle zákona upravujícího některé služby informační společnosti, která spočívá v provozování online tržiště, internetového vyhledávače a cloud computingu.

Povinné osoby	Bezpečnostní opatření	Detekce a hlášení KBI	Reaktivní opatření	Ochranné opatření	Kontaktní údaje
Poskytovatel/zajišťující služby a sítě el. komunikací	NE	NE	NE/ANO*	NE	ANO – národní CERT
Orgán/osoba zajišťující významné sítě	NE	ANO – národní CERT	NE/ANO*	NE	ANO – národní CERT
Správce informačního systému KII	ANO	ANO – NÚKIB	ANO	ANO	ANO – NÚKIB
Správce komunikačního systému KII	ANO	ANO – NÚKIB	ANO	ANO	ANO – NÚKIB
Správce významného informačního systému	ANO	ANO – NÚKIB	ANO	ANO	ANO – NÚKIB
Správce informačního systému základní služby	ANO	ANO – NÚKIB	NE	NE	ANO – NÚKIB
Poskytovatel digitální služby	ANO	ANO- národní CERT	NE	NE	ANO – národní CERT

- Definuje činnost dohledových pracovišť (**národní a vládní CERT**) - **Národní CSIRT/CERT:** Provozován nevládním subjektem (CZ.NIC), který je k činnosti oprávněn

The diagram illustrates the role of the ZKB (Cybersecurity Center) in the Czech Republic's cybersecurity framework. The ZKB is central, coordinating various entities and systems. It defines and manages critical information infrastructure (KII) and critical information systems (KIS). It also oversees the implementation of cybersecurity measures by ISMS (Information Security Management System) and regulates the activities of regulated persons (Regulovaná osoba). The ZKB is responsible for the security of digital services (DS) and basic services (ZS). It also manages the information system for critical information services (ISZ) and the information system for critical information systems (VIS). The ZKB is defined by the Act on Cybernetic Security (Zákon č. 316/2014 Sb.) and the Act on the Security of Information Systems (Zákon č. 317/2014 Sb.). It is also defined by the Act on the Security of Information Systems (Zákon č. 317/2014 Sb.) and the Act on the Security of Information Systems (Zákon č. 317/2014 Sb.).

## Budapešťská úmluva – úmluva o počítačové kriminalitě

- v platnost vstoupila 1. července 2004, podepsána 65 státní k 2020
- např. Indie, Brazílie a Rusko ji odmítají
- první **mezinárodní smlouva**, která se snaží řešit internetovou a počítačovou kriminalitu
- zaměřuje se na zlepšení **vyšetřovacích technik** a **zvýšení spolupráce** mezi národy
  - Urychlené uchování a vydání provozních dat
  - Prohledání a zajištění dat
  - Sběr dat v reálném čase
  - Odposlech obsahových dat
- sjednocuje definici kyberzločinů ale nepokrývají zdaleka všechno
  - Zločiny proti důvěrnosti, integritě a dosažitelnosti systémů
  - Zločiny se vztahem k počítači a k přenášenému obsahu
  - Zločiny se vztahem k autorským právům
- Ukládá vládcům EU přímou povinnost ISP vyhovět dožádání podle práva MS
- spolupráce je i tak zdoluhavým procesem:

