Obsah

[**Kyberkriminalita a elektronické důkazy** 1](#_Toc61990540)

[**Kybernetická bezpečnost** 3](#_Toc61990541)

[**Identifikace, autentizace a datové schránky** 5](#_Toc61990542)

[**Ochrana duševního vlastnictví** 7](#_Toc61990543)

[**Ochrana osobních údajů** 9](#_Toc61990544)

[**Informace veřejného sektoru a Otevřená data** 12](#_Toc61990545)

[**Výběr z přednášek** 14](#_Toc61990546)

# **Kyberkriminalita a elektronické důkazy**

1. **Popište nároky kladené na zákonnost elektronického důkazu.**
   1. Český trestní řád nezná pojem elektronický důkaz.
      1. Podle § 89 TŘ je důkazem vše, co může přispět k objasnění věci.
   2. Prakticky všechny důkazy jsou nějakým zásahem do práva. Odposlech se dají používat při splnění podmínek subsidiarity(že jiných prostředků nelze použít) a přiměřenosti možná jen na základě soudního příkazu podle § 88 odst. 1 trestního řádu po dobu v něm stanovenou a navíc jen ohledně v § 88 odst. 1 trestního řádu uvedených trestných činů. Dále že budoucí e-mailovou komunikace nelze zjišťovat jinak, než na základě soudního příkazu podle § 88 odst. 1 trestního řádu.
   3. Uloženou komunikaci je možné získat za použití technických prostředků jen pokud nám to soudce dovolí. Z Trestního zákoníku § 158 se můžeme dočíst, že v rámci tohoto úkonu můžeme pořizovat všemožné záznamy a pokud máme souhlas soudce, může být v přiměřené míře zasaženo do práva na soukromí dotčených osob. Nicméně soud musí dostatečně jasně specifikovat okruh počítačů, na kterých jsou uložená data.
   4. Absolutní neúčinnost důkazu(neodstranitelná) je taková, kdy jsme neoprávněně získali důkaz například odposlechem – nemůžeme použít
   5. Relativní(odstranitelná) – například nám chybí podpis na lejstru – můžeme ji odstranit.
2. **Vysvětlete strukturu §230 TZ (Neoprávněný přístup k počítačovému systému a nosiči informací). Uveďte příklady k jednotlivým odstavcům.**
   1. První odstavec hovoří o překonání bezpečnostního opatření – tj. myšleno například prolomení hesla, tak bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci
   2. Druhý odstavec pojednává o zneužití, pozměnění, smazání, vložení, prakticky jakoukoliv manipulaci s daty na nosiči či v systému – toto chování bude potrestáno až na tři léta, zákazem činnosti nebo propadnutím věci. Například pokud někomu vlezu do počítače a smažu mu bakalářku, nebo mu ji ukradnu.
   3. Třetí odstavec se odkazuje na předchozí dva a zmiňuje zamýšlené úmysly:
      1. Pokud byl úmysl způsobit jinému škodu, nebo získat sobě nebo jinému neoprávněný prospěch
      2. Pokud byl úmysl omezit funkčnost systému.
   4. Čtvrtý odstavec se znova odkazuje na první a druhý s tím, že bude pachatel potrestán na 1 až 5 let, pokud splní nějakou podmínku, například pokud spáchá ten čin jako člen organizované skupiny, způsobil by značnou škodu, nebo vážnou poruchu v činnosti orgánu státní zprávy atd. Tady už můžeme mluvit o vážnějším činu, například pachatel byl členem hackerské skupiny, nebo napadl kritický systém
   5. Pátý odstavec mluví o vyšším trestu, pokud byla škoda ve velkém rozsahu, nebo získal prospěch velkého rozsahu. To už se jedná asi o nejzávažnější činy, například ransomware v nemocnici.
3. **Popište rozdíly ve fungování §88 TŘ a §8 odst. 5 TŘ ve vztahu k mobilnímu telefonu.**
   1. § 8 odst. 5 trestního řádu hovoří o vydání informací po předchozím souhlasu soudce, tj. asi se může jednat o nějakou proběhlou komunikaci, která je uložena na mobilním telefonu. Kdežto § 88 trestního řádu hovoří o možném odposlechu a záznamu telekomunikačního provozu, který je možný při splnění podmínek subsidiarity(že jiných prostředků nelze použít) a přiměřenosti jen na základě soudního příkazu podle § 88 odst. 1 trestního řádu po dobu něm stanovenou a jen v těch uvedených trestných činech
   2. Čili rozdíly jsou takové, že § 8 odst. 5 TŘ mluví o vydání uložené informace na základě souhlasu soudce a § 88 o odposlechu komunikace na základě soudního příkazu.
4. **Vysvětlete, jaké elektronické důkazy mohou hrát roli při vyšetřování trestného činu vraždy podle §140 TZ.**
   1. Může se jednat o nějaké výhružné nebo urážlivé zprávy, které by naznačovaly jistý úmysl, například urážky kvůli rase, politickému přesvědčení nebo by zprávy naznačovaly předchozí rozmysl nebo uvážení.
   2. Nebo přiznání na WoWku – „zabil jsem ženu a zakopal ji na zahradě“.
5. **Popište, co je to data retention a vysvětlete zásadní milníky v jeho legislativní historii (rozhodovací praxe SDEU a ÚS).**
   1. Data retention označuje ukládání provozních a lokalizačních údajů u poskytovatelů telekomunikačních služeb, hlavně se to využívá pro účely vyšetřování trestné činnosti. Ukládají se informace o proběhlé komunikaci, bez znalosti jejího obsahu. Data uchovávají poskytovatelé po dobu 6 měsíců, viz § 97 odst. 3 zákona 127/2005 Sb. zákonu o elektronických komunikacích.
   2. Soudní dvůr EU v roce 2020 řekl, že plošné shromažďování provozních a lokalizačních údajů na základě směrnice o data retention je neústavní – tzn. je vážným zásahem do práva na soukromí i práva na ochranu osobních údajů.
   3. Ústavní soud v ČR v roce 2019 ale zamítnul návrh na zrušení české úpravy data retention. Sice uznává, že data jsou velmi citlivá, ale na rozsudky SDEU moc nepřihlíží a konstatuje, že evropské státy mají různé reakce.

# **Kybernetická bezpečnost**

1. **Jakými předpisy je upravována oblast kybernetické bezpečnosti? Čemu se věnují?**
   1. Prvním je určitě zákon č. 181/2014 Sb. o kybernetické bezpečnosti, který především vymezuje kybernetický prostor a kybernetickou bezpečnost. Stanovuje povinnosti jednotlivým subjektům, kteří se podílejí na fungování kyberprostoru a taky upravuje dozor, který vykonává NÚKIB a taky sankce.
   2. Z mezinárodních dokumentů to jsou určitě normy skupiny ISO 27000, ten první specifikuje pojmy používané v ostatních normách. Nejhlavnější je ISO 27001, která definuje požadavky na management bezpečnosti informací a také řízení bezpečnosti důvěry informací pro zaměstnance, procesy a IT systémy.
      1. NIST – konkrétnější a techničtější normy, například pro bezpečné šifrování atd.
2. **Co je to "kritická infrastruktura", "kritická informační infrastruktura", "prvek kritické infrastruktury" a "provozovatel prvku kritické infrastruktury"? Jak spolu tyto pojmy souvisí?**
   1. **Kritická infrastruktura** dle zákona č. 240/2000 Sb. o krizovém řízení, je taková, u které by narušení její funkce mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiky státu.
   2. **Prvek KI** je např. stavba, zařízení nebo veřejná infrastruktura, která určena podle kritérii v nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury. Může to být výrobna elektřiny, tepla, pozemní komunikace atd.
   3. **Provozovatel prvku kritické infrastruktury je subjekt KI**, který odpovídá za ochranu prvku KI a za tímto účelem zpracovává plán krizové připravenosti subjektu KI. V něm jsou identifikována možná ohrožení funkce prvku KI a stanovena opatření na jeho ochranu.
   4. **Kritická informační infrastruktura** je prvek nebo systém prvků kritické infrastruktury v odvětví komunikačních a informačních technologií v oblasti kybernetické bezpečnosti. <https://img.ihned.cz/attachment.php/300/61041300/CER0yIPTNf9SMhwjnH6qz8Wm1Jd5OQAL/2schemakii-cz.pdf> - abychom se mohli stát KII, musíme splnit celkem dost „přísná“ pravidla – **průřezová a odvětvová kritéria** – např. omezení poskytování nezbytných služeb pro více než 125k lidí, více než 250 mrtvých nebo více než 25000 osob s následnou hospitalizací a pak ještě odvětvová kritéria v oblasti kyberbezpečnosti – např. jsme datové centrum, ústředna mobilní sítě, pozemní propojovací síť nebo přepravní uzel.
3. **Proč současná legislativa v oblasti kybernetické bezpečnosti nestanoví povinnosti individuálním uživatelům?**
   1. Jakože by jim nařídila povinnost mít antivirus a nepoužívat heslo 123456? Když ani nedokáže kontrolovat své instituce, kde je situace někdy úplně nepředstavitelná.
   2. Nařízení směřuje spíše proti poskytovatelům služeb – v české právní ústavě jde konkrétně o poskytovatele služeb elektronických komunikací
   3. Nařízení povinností se tak děje interně v rámci firem/podniků, kde si každý nastaví bezpečnostní politiky podle sebe.
4. **Jaký je vztah právní úpravy kybernetické bezpečnosti a právní úpravy ochrany osobních údajů?**
   1. Smysl kyberbezpečnosti – ochrana základních práv
   2. Společný mají princip ochrany informačního sebeurčení člověka – tzn. ochrana diskrétních informací, právo na soukromí, svobodný přístup k informacím
   3. [**https://science.law.muni.cz/knihy/monografie/Polcak\_Kyberneticka\_bezpecnost.pdf**](https://science.law.muni.cz/knihy/monografie/Polcak_Kyberneticka_bezpecnost.pdf) - strana 19 a 66
   4. Pokud člověk se podílí na nějakém bezpečnostním incidentu, tak předpokladem uplatnění individuální odpovědnosti uživatele, ať už o odpovědnost soukromoprávní nebo trestní, je totiž jeho ztotožnění. To přitom vyžaduje použití takových mechanismů, které mohou obecně ohrozit shora jeho anonymitu a mohou být v kontradikci s požadavky evropské ochrany soukromí a osobních údajů.
5. **Vysvětlete, co je to analýza rizik a jak do ní vstupují varování vydaná NÚKIB.**
   1. Analýza rizik je rozbor a zkoumání nežádoucích stavů, které mohou s nějakou pravděpodobností nastat a způsobit nám škody. Analýzou hledáme nejzávažnější rizika, která potřebujeme vhodnými opatřeními eliminovat, nebo zcela zamezit jejich vzniku.
   2. riziko = dopad x hrozba x zranitelnost
   3. Varování NÚKIBu jsou upozornění na existenci hrozby v oblasti kyberbezpečnosti. Subjekty, které spadají pod zákon ZKB(181/2014Sb.) jsou povinny se touto hrozbou zabývat a zohlednit ji v analýze rizik. Varování neznamená zákaz používání daných technických prostředků, ale nutnost zvážit případné bezpečnostní riziko související s jejím užíváním. Příklad NÚKIB a Huawei.

# **Identifikace, autentizace a datové schránky**

1. **Pojem elektronického podpisu a současné legislativní změny; rozdíl oproti elektronické pečeti.**
   1. **Elektronický podpis(prostý)** – základní a nejjednodušší typ elektronického podpisu – ať už napsání jména a příjmení, vložení obrázku s naskenovaným podpisem atd. Většinou mezi dvěma soukromoprávními subjekty.
   2. **Zaručený elektronický podpis** – je vytvořen na základě privátního klíče a k němu náležícímu certifikátu. Použitý certifikát nemusí splňovat žádné náležitosti a může být i self-signed.
   3. **Uznávaný elektronický podpis** – Nevychází přímo z eIDAS, ale je zaveden v zákoně č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transkace. Jedná se o zaručený elektronický podpis, k jehož vytvoření byl použit kvalifikovaný certifikát vydaný certifikační autoritou – v česku např. PostSignum
   4. **Kvalifikovaný elektronický podpis** – jedná se o nejvyšší úroveň elektronického podpisu. Nařízení eIDAS definuje tento typ jako zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů(např. čipové karty, tokeny) a který je založen na kvalifikovaném certifikátu pro elektronické podpisy. Požadavky na kvalifikované prostředky jsou uvedeny v eIDAS v příloze 2.
   5. **Elektronická pečeť** je svým způsobem „razítko“, které je zárukou původu a neměnnosti dokumentu(my, úřad, jsme v konkrétní den vytvořili nějaký dokument). Zatímco elektronický podpis je brán jako jednoznačný projev vůle konkrétní osoby(já, úředník, jsem něco rozhodl). Například pokud by nemocnice se rozhodla převést všechny lékařské zprávy do digitálního formátu, tak podepisovat každou zvlášť by nešlo. Kdežto pečeť tento problém řeší.
      1. Zase rozlišujeme prostou, zaručenou, zaručenou s certifikátem a kvalifikovanou pečeť. Kvalifikovaná pečeť je povinně uznávána v celé EU a zaručuje pravost dokumentu.
2. **Nařízení eIDAS – důvody přijetí.**
   1. **eIDAS je zkratka pro nařízení evropské unie o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na evropském trhu**. Stanovuje podmínky, za nichž členské státy uznávají prostředky pro elektronickou identifikaci fyzických a právnických osob, které spadají do oznámeného systému elektronické identifikace jiného členského státu, dále stanovuje pravidla pro služby vytvářející důvěru, zejména elektronických transakcí a taky stanoví právní rámec pro elektronické podpisy, elektronické pečetě, elektronická časová razítka, dokumenty, služby elektronického doporučeného doručování a certifikační služby pro autentizaci internetových stránek.
   2. **Důvody přijetí** byly takové, aby bylo poskytnuto občanům, společnostem a taky i státním orgánům členských států společný právní základ pro bezpečnou elektronickou komunikaci, která by zvýšila důvěryhodnost elektronických transakcí na vnitřním trhu EU a tím pádem i jejich aktivnější využívání.
3. **Charakterizujte a popište právní otázky související s elektronickou identifikací ve smyslu prokázání totožnosti.**
   1. elektronickou identifikací se rozumí postup používání osobních údajů, které jedinečně identifikují určitou osobu.
   2. Prokázání totožnosti je možné jen prostřednictvím **kvalifikovaného systému**, který spravuje kvalifikovaný správce – státní orgán nebo akreditovaná osoba(například ministerstvo vnitra), splňuje technické normy a postupy podle nařízení EU o elektronické identifikaci, umožňuje poskytnutí služby národnímu bodu(eidentita.cz – informační služby veřejné správy) ve kterém jsou údaje spojené s osobou podle nařízení EU.
4. **Datové schránky - shrňte výhody, nevýhody a mj. se zaměřte na okamžik doručení.**
   1. **Výhody**
      1. Komunikace s úřady je pomocí datové schránky zdarma
      2. Pokud DS existuje, musí být dokument do ní zaslán.
      3. Je možno s úřady komunikovat i vzdáleně – nemusíme nikam chodit.
      4. Rychlejší komunikace
      5. Možnost svěření datové schránky jiné osobě
   2. **Nevýhody**
      1. Po deseti dnech od doručení nastává fikce doručení – tj. zpráva se považuje za doručenou.
      2. Jedna firma může disponovat pouze jednou datovou schránkou, bez ohledu na počet provozoven.
5. **Judikatura k elektronické identifikaci subjektu a datovým schránkám.**
   1. Krajský soud v Českých Budějovicích pobočka v Táboře v usnesení ze dne 15. 5. 2011, sp. zn. 15 Co 337/2011, dovodil, že podání učiněné prostřednictvím datové schránky je podáním té osoby (fyzické či právnické), které byla zřízena datová schránka.
   2. Plsn 1/2015:
      1. a) žádná část datové zprávy není podepsána elektronickým podpisem žádného typu - v takovém případě se datová zpráva považuje za podanou osobou autentizovanou systémem datových schránek. Jde-li o osobu, pro kterou byla zřízena datová schránka, jde o perfektní podání v elektronické podobě (§ 18 odst. 2 zákona o elektronických úkonech)
      2. b) některá část datové zprávy (typicky např. příloha) je podepsána uznávaným elektronickým podpisem - v takovém případě se tato část datové zprávy považuje za perfektní elektronické podání učiněné tou osobou, která k němu připojila svůj uznávaný elektronický podpis (§ 6 zák. č. 297/2016 Sb.)

# **Ochrana duševního vlastnictví**

1. **Jaké technologické změny stály za tzv. “digitální revolucí” a jaký měly dopad na autorské právo?**
   1. Nástup internetu a digitálních médií měl za následek, že dílo může být používané kdekoliv a kýmkoliv. Kromě toho může být zpracované, předělané, modifikované. To byl jeden z důvodů vzniku nového autorského zákona, který byl uveden v platnost roku 2000 a nahradil předcházející z roku 1965.
2. **Za jakých podmínek lze rozmnožovat autorskoprávně chráněný obsah pro osobní potřebu?**
   1. § 30 autorského zákona – pro svou osobní potřebu můžeme zhotovit záznam, rozmnoženinu nebo napodobeninu díla – podle odst. 1 to není užití díla. Účelem tohoto užití nesmí být dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu. – Výjimkou je pořizování rozmnoženiny počítačových programů a elektronických databází pro osobní potřebu fyzické osoby či vlastní vnitřní potřebu právnické osoby nebo podnikající fyzické osoby a pořizování si rozmnoženiny audiovizuálních děl a to při jejich provozování nebo přenosu.)
      1. **Nesmíme ho ale pak nikde šířit na veřejnosti.**
   2. 5 Tdo 234/2009 - Rozmnoženina pro osobní potřebu z neoprávněného zdroje – Nejvyšší soud řekl, že lze vytvořit i rozmnoženinu díla z ilegálního zdroje. AZ neklade důraz na oprávněnost zdroje, ale pracuje s 3-stupňovým testem.
   3. SDEU řekl, že se rozmnožení nevztahuje na případ, kdy jsou soukromé rozmnoženiny pořízeny z neoprávněného zdroje – tzn. nemůžeme pořizovat rozmnoženiny
3. **Jsou právně chráněny tzv. DRM – digital rights management, tedy technické prostředky ochrany práv („elektronické zámky“)? Jak?**
   1. DRM je šifrování/kódování nebo jiná úprava díla, která má za cíl chránit dílo.
   2. Dle § 43 AZ víme, že ten, kdo obchází nebo jinak maří účinné technické prostředky, nebo vyrábí či propaguje nástroje na obcházení, tak neoprávněně zasahuje do autorského práva.
4. **Charakterizujte a stručně popište přestupky na úseku autorského práva. Uveďte příklad takového jednání.**
   1. Neoprávněně užijeme autorské dílo
   2. neoprávněně zasahuje do práva autorského způsobem uvedeným v § 43 odst. 1 nebo 2 anebo v § 44 odst. 1, nebo
      1. § 43 – Obcházení DRM a šíření prostředků k obcházení DRM
      2. § 44 – bez svolení autora umožňuji/usnadňuji porušování práva autorského
         1. Nová veřejnost - hyperlinkování
   3. Rozhodnutí, zda-li se jedná o přestupek nebo trestný čin závisí od toho, kdo neoprávněně zasáhne nikoli nepatrně(nad 10 tisíc) do zákonem chráněných práv k autorskému dílu… Tzn. vyšetřující orgán sám posoudí intenzitu neoprávněného zásahu do autorských práv.
   4. Například na netflixu si nahraju jeden film a pošlu ho pár kamarádům.
5. **Charakterizujte a stručně popište trestný čin porušení autorského práva, práv souvisejících s právem autorským a práv k databázi. Uveďte příklad takového jednání.**
   1. **§ 270 TZ**
      1. **Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi**
         1. Kdo neoprávněně zasáhne nikoli nepatrně do zákonem chráněných práv k autorskému dílu, uměleckému výkonu, zvukovému či zvukově obrazovému záznamu, rozhlasovému nebo televiznímu vysílání nebo databázi, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.
   2. Druhý odstavec mluví o tom, že pokud čin vykazuje znaky obchodní činnosti, pachatel získá značný prospěch nebo způsobí značnou škodu(1 mil. Kč), nebo se dopustí činu ve značném rozsahu, posouvá se hranice na 6 měsíců až pět let + peněžní trest nebo propadnutí věci.
   3. Příklad – mladík z Liberce (liberecký pirát) – spravoval stránku s odkazy, které přesměrovali uživatele internetu na jiný externí server, kde byly umístěny filmy – takhle tam měl asi 2500 odkazů na neoprávněné rozmnoženiny audiovizuálních děl.

# **Ochrana osobních údajů**

1. **Ochrana soukromí a ochrana osobních údajů - popište vztah mezi právní úpravou ochrany soukromí a osobních údajů**
   1. Ochrana osobních údajů je specifickým odvětvím ochrany soukromí. Je zakotvena i v čl. 10 Listiny základních práv a svobod.
   2. Osobní údaj je zákonně vymezen jako „jakákoliv informace týkající se určeného nebo určitelného subjektu údajů“. To znamená, že se jím stát může jakákoliv informace, která přímo nebo nepřímo vede k identifikaci konkrétního člověka.
   3. Účelem ochrany osobních údajů je zamezení profilování, které by mohly mít nežádoucí dopady v podobě vyzrazení informací, jež by o sobě sám nechtěl prozradit – což by byl zásah do soukromí – např. muž, který se dozvěděl o těhotenství své dcery na základě reklamních letáků, které posílal obchod na základě nakupovaných předmětů – ale mohou být i závažnější případy – diskriminační chování, krádež identity.
2. **Základní principy a zásady zpracování osobních údajů**
   1. **Zásada zákonnosti, korektnosti a transparentnosti**
      1. Zpracování musí probíhat za účelem, který je v souladu s právem.
      2. **Zpracování je zákonné, pokud je splněna alespoň jedna z určitých podmínek – právní tituly**:
         1. Subjekt údajů udělil souhlas.
         2. Zpracování je nezbytné pro splnění smlouvy/právní povinnosti/ochranu životně důležitých zájmů subjektu údajů a další.
      3. Zásada korektnosti a transparentnosti by se dala shrnout do požadavku, že správce os. údajů má údaje zpracovávat férově. Nesmí probíhat skrytě – tj. aby subjekt údajů měl vždy možnost zjistit, kdo jeho údaje zpracovává. Mimo jiné k tomu, aby mohl vykonávat kontrolu nad probíhajícím zpracováním a tím realizovat své právo na informační sebeurčení.
   2. **Zásada omezení účelem**
      1. osobní údaje musí být zpracovávány za určitým, výslovně vyjádřeným a legitimním účelem a nesmí být zpracovávány způsobem, který by byl s tímto účelem neslučitelný.
   3. **Zásada minimalizace údajů**
      1. Správce může zpracovávat jen ty údaje, které jsou striktně nezbytné pro účel, který si pro dané zpracování osobních údajů stanovil.
   4. **Zásada přesnosti**
      1. Zpracovávané osobní údaje mají být přesné, a v případě potřeby aktualizované.
   5. **Zásada omezení uložení**
      1. Osobní údaje mohou být uchovávány jen po takovou dobu, která je nezbytná vzhledem k účelu, pro který jsou zpracovávány.
   6. **Zásada integrity a důvěrnosti**
      1. Povinnost správce údajů zabezpečit proces zpracování tak, aby osobní údaje náležitě zabezpečil před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Účelem je minimalizace rizika zásahu do práv a svobod subjektu údajů.
   7. **Zásada odpovědnosti správce**
      1. Správce musí při zpracování přijmout vhodná opatření, aby splnil všechny požadavky vyplývající z předchozích zásad a zároveň musí být schopen přijetí takových opatření doložit.
3. **Osobní údaje a jejich zpracování – vymezení pojmu a zúčastněné osoby**
   1. **Osobní údaj** je uveden jako: „veškeré informace o **identifikované** nebo **identifikovatelné fyzické osobě** (subjekt údajů); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje…“
   2. **Anonymní a pseudoanonymní údaj**
   3. **Správce osobních údajů** je osoba(ať už fyzická nebo právnická), instituce, úřad nebo jiný subjekt, **který určuje účel daného zpracování** a je za ně primárně odpovědný.
   4. **Zpracovatel osobních údajů zpracovává osobní údaje pro správce.** Sám tedy účel neurčuje, ale dělá to, co mu správce řekne. Správce a zpracovatel mezi sebou musí uzavřít smlouvu, ve které se upraví detaily jejich vztahu.
   5. **Zpracování osobních údajů je jakákoliv operace s osobními údaji**, která je prováděna pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uložení, přizpůsobení, vyhledání, použití, šíření atd. atd. Definice je velice široká, obecně jde o jakoukoliv činnost, kterou správce nebo zpracovatel s osobními údaji provádí.
   6. **Citlivý údaj,** vypovídá o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě člověka a genetické údaje. Citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci člověka.
4. **Povinnosti správce osobních údajů podle nařízení 2016/679**
   1. Základní povinností je stanovit účel zpracování
   2. Určit nezbytnou dobu uložení, když zahajuje proces zpracování osobních údajů. Doba může být vyjádřena absolutně(půl roku), tak relativně(po dobu poskytování služby, nebo do odvolání souhlasu).
   3. Povinnost nést odpovědnost za zpracování.
   4. Povinnost zavést vhodná technická a organizační opatření, aby správce zajistil a byl schopen doložit, že zpracování je prováděno v souladu s GDPR.
   5. Povinnost nastavit proces zpracování osobních údajů tak, aby splňovalo požadavky záměrné a standardní ochrany osobních údajů.
   6. Povinnost vést záznamy o zpracování.
   7. Povinnost poskytnout subjektu údajů na základě žádosti vybrané údaje.
   8. **Zajistit, aby každé zpracování osobních údajů bylo podloženo právním titulem pro zpracování.**
5. **Práva subjektu údajů ve vztahu ke správci a zpracovateli podle nařízení 2016/679**
   1. **Právo na informační sebeurčení** – každý člověk má možnost určit si, jak bude nakládáno s informacemi o jeho osobě. Není to absolutní právo a existují z něj výjimky, například v podobě zpracování informací státními orgány.
   2. **Právo na přístup k osobním údajům**, dle kterého se může subjekt údajů dotázat správce, jestli zpracovává jeho osobní údaje a pokud ano, může si vyžádat jejich kopii.
   3. **Právo na opravu chybných nebo nepřesných údajů**.
   4. **Právo na výmaz** – „právo být zapomenut“ – subjekt údajů může požadovat vymazání osobních údajů, jejichž účel zpracování již pominul, u kterých není **právní titul** na zpracování, případně které jsou obecně zpracovávány protiprávně.
   5. **Právo nebýt předmětem automatizovaného rozhodování**.

# **Informace veřejného sektoru a Otevřená data**

1. **Pojem “informace veřejného sektoru”**
   1. Nejčastěji se setkáváme s pojmem informace veřejného sektoru ve spojení s právem na informace
      1. Právo na informace je právo občanů vůči orgánům veřejné moci, které mají povinnost nejen odpovídat na jednotlivé žádosti o poskytnutí informací, ale i o své činnosti
   2. Všechny dokumenty, databáze a jiné informace, které sbírá, uchovává a zpracovává veřejný sektor. Například informace o počasí, dopravě, zákonu, rozsudky Nejvyššího soudu.
2. **Povinné subjekty podle zákona č. 106/1999 Sb. – zákon o svobodném přístupu k informacím**
   1. **Jsou uvedeny v § 2**
      1. Státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce.
      2. Subjekty, které rozhodují o právech, zájmech nebo povinnostech fyzických nebo právnických osob v oblasti veřejné správy.
3. **Pojem „otevřená data“**
   1. Otevřená data jsou informace zveřejňované způsobem umožňujícím dálkový přístup v otevřeném a strojově čitelném formátu, jejichž způsob ani účel následného využití není omezen a které jsou evidovány v národním katalogu otevřených dat.
   2. Formát a struktura otevřených dat umožňuje jejich hromadné počítačové zpracování, k němuž jejich vydavatel poskytl právní svolení. Díky tomu mohou být dál volně zpracovávány, a to i v rámci softwarových aplikací.
   3. Jedná se například o jízdní řády, příjmy státu, seznam poskytovatelů sociálních služeb a další. Pocházejí z univerzit, nevládních organizací, soukromých firem nebo veřejné zprávy.
   4. Londýn – rigo pana Míška – snad všechno funguje na open data. 1 mil liber náklady na zveřejnění a návrat 58 mil. v podobě daní
4. **Obecná právní úprava otevřených dat**
   1. Zákon č. 106/1999 Sb., **Zákon o svobodném přístupu k informacím**.
      1. Umožňuje přístup k informacím na dálku, v rozumném formátu, přístup bez udání důvodů a na libovolné legální použití
      2. specifikuje povinné subjekty a jejich povinnosti
      3. Národní katalog otevřených dat (NKOD) – správcem je ministerstvo vnitra
5. **Právní překážky při poskytování informací a otevírání dat**
   1. **Anonymizace dat (ochrana osobních údajů)**
      1. Můžeme začernit
      2. Porovnáváme právo na informace a ochranu soukromí(osobních údajů)
      3. Ústavní soud ve věci seznamu soudců, kteří byli členy KSČ před listopadem 1989. Ústavní soud poměřoval právo na ochranu soukromí a osobních údajů soudců, proti kterému převážilo právo veřejnosti znát případnou komunistickou minulost toho, kdo rozhoduje o právech a povinnostech z pozice soudce.
      4. Platy státních zaměstnanců spadají do definice „veřejných prostředků“.
   2. **Licence, autorská práva**
      1. Většina open datasetů nemá vůbec licencovatelný obsah, i když se čeští poskytovatelé snaží aplikovat licence na obsah.
      2. Například mapy – jsou kartografické dílo, se může jednat o autorskoprávní obsah
      3. V případě databází autorské právo chrání její struktura, obsah samotný ne.
      4. **Velká množina dokumentů, které by jinak podléhaly autorsko právní ochraně, je z ní vyloučena působením výjimky úředního díla**.
   3. **Citlivá, tajná a nebo potenciálně zneužitelná data**
   4. **Zvláštní právo autora databáze**
      1. Pro status pořizovatele databáze je podstatné, aby daný subjekt do vzniku databáze investoval a zároveň její vznik podnítil.
      2. Pořizovatel databáze má právo na vytěžování nebo zužitkování celého obsahu databáze, nebo její kvantitativně nebo kvalitativně podstatné části.
         1. Jedná se o právo absolutní a nikdo do něj nemůže bez povolení zasáhnout tak, že by sám podstatnou část databáze vytěžil nebo zužitkoval. Poskytovatel však může udělit jiné osobě právo k výkonu tohoto práva.
         2. Vytěžování je prakticky rozmnožování nebo kopírování.
         3. Zužitkování je jakákoliv činnost, které zpřístupní obsah databáze veřejnosti.

# **Výběr z přednášek**

1. **Předmět a účel právní regulace elektronických komunikací**
   1. https://www.ctu.cz/regulace-e-komunikaci
   2. Ochrana trhu elektronických komunikací
      1. Vytvářet předpoklady pro řádné fungování hospodářské soutěže, konkurenčního prostředí a otevřeného trhu
      2. Technologická neutralita – neukládá povinnost použít konkrétní druh technologie, ani žádný druh technologie nezvýhodňuje.
   3. Ochrana uživatele
      1. Maximální výhody z hlediska možnosti volby služby, ceny a kvality
      2. Všichni koncoví uživatelé měli přístup k univerzální službě
      3. Poskytovatel musí poskytovat nepřetržitou službu, informovat spotřebitele (vyúčtování, podmínky reklamace..), ponechat lhůtu aspoň 1 týden před odpojení služby, pokud se uživatel zpozdí s platbou
      4. Zajistit vysokou úroveň ochrany osobních údajů a soukromí
   4. Modernizace a investice do infrastruktury
2. **Síťová neutralita - popis, právní úprava v EU, aktuální výzvy v USA**
   1. Síťová neutralita je princip rovnoprávnosti přenášených dat po internetu. Zabraňuje poskytovatelům internetu zvýhodňování nebo naopak zpomalování či blokování přístupu na vybrané internetové stránky nebo k vybranému obsahu.
   2. V EU zakotvena v nařízení Evropského parlamentu 2015/2120 čl. 3:
      1. Koncoví uživatelé mají právo na přístup k informacím a obsahu a jejich šíření, využívání a poskytování aplikací a služeb a využívání koncového zařízení podle svého vlastního výběru bez ohledu na polohu koncového uživatele nebo poskytovatele či polohu, původ nebo určení dané informace, obsahu, aplikace nebo služby, a to prostřednictvím své služby přístupu k internetu.
   3. V USA byla zavedena síťová neutralita v roce 2015 a v roce 2017 zrušená
      1. ISPs v Americe řekli, že nebudou blokovat nebo omezovat nějaký traffic, ale že možná budou dělat nějakou placenou prioritizaci
3. **Základní registry - popis, účel a právní úprava**
   1. 4 základní registry:
      1. **Registr obyvatel** – fyzické osoby na území ČR, jméno, místo a datum narození atd.
         1. Správcem je Ministerstvo vnitra
      2. **Registr osob** – právnické osoby, podnikající fyzické osoby, svěřenské fondy atd. Zapisují se referenční údaje, referenční vazby, IČO, IČP a další.
         1. Správcem je Český statistický úřad
      3. **Registr územní identifikace, adres a nemovitostí(RÚIAN)** – základní identifikační a lokalizační údaje, které se vztahují ke sledovaným prvkům/objektům v území(linie,plochy,body), dále adresy atd.
         1. Je zdarma veřejně přístupný(open data)
         2. Správcem je Český úřad zeměměřičský a katastrální
      4. **Registr práv a povinností** – oprávnění přístupů do jednotlivých registrů. Nejsou tam vedeny utajované informace a jsou přístupné všem orgánům veřejné moci.
         1. Správcem je Ministerstvo vnitra
4. **Hlavní překážky pro zavedení komplexní eJustice v ČR**
   1. https://www.mvcr.cz/soubor/5-zasedani-rvis-priloha-c-5-ejustice-2020-v-1-0.aspx
   2. **Problematické řízení procesů uvnitř justice, nedostatečná vzájemná kompatibilita systémů a nedostatky v komunikacích mezi informačními systémy.**
   3. Nekoncepčnost rozvoje a roztříštěnosti IT systémů a technologií
      1. Nekompatibilní systémy – problém s komunikací mezi IS
      2. Velký počet dodavatelských společností, které ne vždy dokáží reagovat dostatečně pružně na potřeby justice.
      3. Některé spisy nevedou v elektronické podobě.
   4. Uchovávání dat
      1. Chybí metodický pokyn týkající se bezpečné archivace dat – jak technického charakteru, kdy se nepřetržitě řeší problémy s malou kapacitou diskových polí
   5. Nedostatek finančních a personálních zdrojů – kvalitní pracovníci, vhodná organizace jejich práce a jejich motivací
5. **Co je to princip distinkce a jak se vztahuje ke kyberzbraním a kyber-válce?**
   1. Tallin Manual Rule 31
      1. Jediný cíl, který by měly Státy dosáhnout ve válce je oslabení armádních sil nepřítele.
   2. Ženevské úmluvy – účastníci konfliktu by měli rozlišovat mezi civilisty, kteří se neúčastní boje a vojáky
   3. Útok na civilní objekty je nezákonný, i kdyby pomohl urychlit ukončení války.
   4. Aplikace ženevské úmluvy neposkytuje dostatečnou ochranu civilistům. Důležitým faktem je, že data se standardně nepovažují za civilní objekt. Kromě toho definice útoku v kontextu kyberválky není velmi jasná. Posouzení, co se dá považovat za armádní/civilní objekt se odvozuje na základě testu proporcionality.