**Užívání IT a právní odpovědnost**

**IT use and legal liability**

Projekt 2

Studijní program: Informatika a kybernetika ve zdravotnictví

Autor práce: Šimon Kochánek

Vedoucí práce: RNDr. Dagmar Brechlerová, Ph.D.

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství

Katedra informačních a komunikačních technologií v lékařství Akademický rok: 2021/2022

**Z a d á n í P r o j e k t II**

Student: **Simon Kochánek**

Obor: Informatika a kybernetika ve zdravotnictví

Téma: **Užívání IT a právní odpovědnost**

Téma anglicky: **IT use and legal liability**

Z á s a d y p r o v y p r a c o v á n í :

Seznamte se s příslušnými paragrafy Trestního zákoníku, které se týkají použití výpočetní techniky a pohybu na Internetu. Dále se seznamte se Zákonem o kybernetické bezpečnosti a jeho dopadem na běžného uživatele. Seznamte se s tím, jaké povinnosti má běžný uživatel zařízení (počítač, mobil) s internetovým připojením. Shrňte právní odpovědnost uživatele do základního velmi jednoduchého a přehledného materiálu, který bude možno použít pro vzdělávání laiků v této oblasti. Cílem tohoto projektu je jednak pro studenta zvýšení znalosti toho, co je legální a kdy už porušuje zákon v kyber prostředí, a dále vypracování materiálu.

Seznam odborné literatury:

1. <https://www.zakonyprolidi.cz/cs/2009-40> aktuální znění
2. Jan Kolouch a kolektiv, "CYBERSECURITY", https://knihy.nic.cz/
3. <https://www.nukib.cz/cs/>, vzdělávací materiály
4. <https://www.zakonyprolidi.cz/cs/2014-181> aktuální znění

Vedoucí: RNDr. Dagmar Brechlerová, Ph.D.

Konzultanti:

V Praze dne 28.2.2022

....................................................

studentka / student

....................................................

vedoucí práce

....................................................

vedoucí / zástupce ved. katedr

**PROHLÁŠENÍ**

Prohlašuji, že jsem práci s názvem „Užívání IT a právní odpovědnost“vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k práci.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu §60 Zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Kladně 23.5.2022 …...….………...………………...

Šimon Kochánek

**PODĚKOVÁNÍ**

Rád bych poděkoval paní doktorce Brechlerové za možnost práce pod jejím vedením na tomto projektu.

**ABSTRAKT**

**Užívání IT a právní odpovědnost**

Hlavními cíli je rešerše na téma práva v IT. Dále vzdělání se v zákonu o kybernetické bezpečnosti a zjištění si práv a povinností s internetovým připojením. Mnoho informací bylo čerpáno z přednášek doc. Jana Koloucha a od Národního Úřad pro Kybernetickou a Informační Bezpečnost.

**Klíčová slova**

Právo v IT, zákon o kybernetické bezpečnosti, kybernetická bezpečnost

**ABSTRACT**

**IT use and legal liability**

Main goal is to make a research about law in IT.Next to learn about cyber security law and understand your obligations with internet connection.Information was mainly gathered from lectures by doc. Jan Kolouch and from websites and information manuals by Národní Úřad pro Kybernetickou a Informační Bezpečnost.

**Keywords**

Cybersecurity law, cybersecurity, IT legal liability

Obsah

[Seznam symbolů a zkratek 8](#_Toc476327912)

[1 Úvod 9](#_Toc476327913)

[1.1 Přehled současného stavu 9](#_Toc476327914)

[1.2 Cíle práce 9](#_Toc476327915)

[2 Metody 10](#_Toc476327917)

[2.1 Trestní zákoník 10](#_Toc476327914)

[2.2 Zákon o kybernetické bezpečnosti 11](#_Toc476327915)

[2.3 Právní odpovědnost s připojením k internetu 12](#_Toc476327915)

[3 Výsledky 13](#_Toc476327918)

[4 Diskuse 14](#_Toc476327919)

[5 Závěr 15](#_Toc476327920)

[Seznam použité literatury 16](#_Toc476327921)

# Seznam symbolů a zkratek

#### Seznam zkratek

|  |  |
| --- | --- |
| Zkratka | Význam |
| KB  NÚKIB | Kybernetická Bezpečnost  Národní Úřad pro Kybernetickou a Informační Bezpečnost (správní orgán pro KB, včetně ochrany utajovaných informací atd.) |
| CERT  ZoKB  CSIRT | Computer Emergency Response Team  Zákon o Kybernetické bezpečnosti  Computer Security Incident Response Team |

# Úvod

Naprostá většina z nás se denně setkává s počítači, mobilními telefony, informačními systémy atd.. Měli bychom si proto uvědomit, že našim konáním můžeme způsobit trestný čin a ani o tom nevědět. Nicméně se právo často mění, a minimálně já si nemůžu být jist, že svým konáním v kyber prostoru nekonám něco nezákonného. S příchodem zákona o kybernetické bezpečnosti, o kterém panují velké debaty je také velmi důležité vědět jak se bude chovat informační infrastruktura spadající pod něj. Dále také tvoří důležitou základnu pro ePrivacy, ochranu osobních údajů a další ochranu informací a bezpečnosti, které s aktuálním rozvojem informačních technologií zasahují do života každého z nás. Proto vznikl i tento projekt, ve kterém se na tyto věci zaměřím.

## Přehled současného stavu

Na úvod je nutno říct, že tato práce je čistě rešeršní za použití mnoha zdrojů. Pro danou problematiku je jedním z mých hlavních zdrojů kniha CyberSecurity od doktora Jana Koloucha a spol., která k datu psaní této práce dává všechny platné informace. Dále jsem také čerpal z prezentací a webových návodů a dokumentů od Národního Úřadu pro Kybernetickou a Informační Bezpečnost zkráceně NÚKIB.

Zřetelný problém je v nepřehlednosti pro laické a zákona neznalé uživatele výpočetních technologií. NÚKIB jako instituce se snaží laiky vzdělávat, nicméně pro laiky je stále těžké pochopit, kdy se mohou např. s internetovým připojením dostat k přestupku nebo i k trestnému činu.

## Cíle práce

Jako prvním mým cílem se stalo prostudování trestního zákoníku zákonu č. 40/2009 Sb. a nalezení paragrafů týkajících se výpočetních technologií. Zákony odkazují na dřívější zákony, ale zákony tykající se výpočetní techniky jsou primárně 230,231,232. Dále jsem si měl prostudovat zákon o kybernetické bezpečnosti zákon č. 181/2014 Sb.. K tomu se vázal jeho dopad na běžného uživatele a jak by se podle něj měl řídit. Dalším cílem bylo si prostudovat zásady použití internetového připojení a jaké právní povinnosti z něj vyplývají. Z těchto témat právních odpovědností bylo dále nutné vytvořit vzdělávací materiál pro laiky v tomto tématu. Hlavním cílem byla rešerše na dané téma, a hlavně mé možnost se sám dovzdělat v tomto oboru a zvýšit vlastní, ale i laické povědomí o tématu kybernetické bezpečnosti a práva v IT.

1. **Metody**
   1. **Trestní zákoník**

Hlavní paragrafy jsou 230, 231, 232 Trestního zákoníku č. 40/2009 Sb..

**§ 230** Neoprávněný přístup k počítačovému systému a nosiči informací: [1]

Překonání bezpečnostního opatření k neoprávněnému přístupu k počítačovému systému Tzn. že i když mám heslo na papírku vedle počítače, nemohu ho použít, protože bych porušil zákon. Podle odstavce 2 je zakázáno jakkoli modifikovat či smazat data z počítačového systému nebo je neoprávněně použít, padělat atd. Podle odstavce 3 nesmí uživatel způsobit jinému škodu nebo omezit funkčnost počítačového systému.

**§ 231** Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat: [2]

Zakazuje podle trestného činu porušení tajemství či neoprávněného přístupu k nosiči informací. S použitím nástroje, postupu, programu a dalších věcí k získání přístupu. Dále také zakazuje jakkoli distribuovat jakoukoliv možnost na neoprávněný přístup do sítě, informaci atd.. Daný trestný čin dále eskaluje jedná-li v rámci organizované skupiny nebo se jedná o značný prospěch pro někoho.

**§ 232** Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti: [3]

Jestliže z nedbalosti poruším povinnosti vyplívající z nějakého závazku nebo podle zákona či smlouva a tím zničím, poškodím, pozměním data v počítačovém systému nebo učiním zásah do fyzického nebo software vybavení počítače a tím způsobím škodu na cizím majetku budu potrestán.

Podle těchto paragrafů se určují trestné činy s výpočetní technikou, ale vždy se jedná tento trestný čin spolu s nějakým, jako např. urážkou na cti, vydíráním atd.

* 1. **Zákon o kybernetické bezpečnosti**

Zákon o kybernetické bezpečnosti (Dále jako ZoKB) neukládá trestní ani právní trestní odpovědnost pachatelům kybernetických útoků (o to se stará trestní zákoník), ale vytváří systém a právní základ pro bezpečností opatření, které mají výskytu a existenci předcházet. Mají zajistit, že případný kybernetické bezpečností incident neohrozí celkové fungování informačních a komunikačních systémů nebo fungování kritické společenské informační infrastruktury. [5]

Jak už bylo řečeno ZoKB stanovuje, jak provádět opatření proti kyber útoku a stanovuje úřad, který bude sloužit v zájmu kybernetické bezpečnosti. Národní Úřad Kybernetické a Informační Bezpečnosti (dále jako NÚKIB). Jedná se o správní úřad pro: KB, ochranu utajovaných informací, kryptografickou ochranu atd.

NÚKIB připravuje zákony a podzákonné normy v oblasti KB. NÚKIB se také soustředí na přípravu a varování před kybernetickými útoky a hrozbami. NÚKIB také vydá varování, dle kterého se subjekty uvedené v paragrafu 12 musí řídit. Subjekty, kterých se týká dané varování musí vzít ve své analýze rizik tuto hrozbu, zhodnotit ji a vyvodit výsledky při praktikování kybernetické bezpečnosti.

NÚKIB také spolupracuje s vládním CERT a týmy typu CSIRT [6]. Jejich hlavním úkolem je ochrana kritické informační infrastruktury a významných informačních systémů podle ZoKB. Také jsou zdroj bezpečnostních informací a pomoci pro orgány státu, organizace i občany.

ZoKB dále také ustanovuje jakých infrastruktur se týká. Existují tři:

Základní: služba závislá na sítích elektronických komunikací nebo informačních systémech a narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví: energetika, doprava, zdravotnictví banky atd.

Významná: služba, jenž zajišťuje přenosové systémy atd.. které pokud zajišťuje přímé zahraniční připojení do veřejné komunikační sítě nebo zajištující přímé připojení ke kritické informační infrastruktuře.

Kritická: Pokud by kyber hrozba výrazně ovlivnila hospodářské ztráty, nebo měla za následek 250 mrtvých nebo 2500 zraněných s hospitalizací delší než 24h případně omezení nezbytných služeb nebo jiný závažný zásah do každodenního života více než 125 000 lidí, pak se jedná o kritickou informační infrastrukturu [7].

**2.3 Právní odpovědnost s připojením k internetu**

Právo na přístup k internetu bez omezování patří jako základní lidské právo na informace a svobodu projevu a přístup k informacím. Pro používání připojení k internetu si každý operátor klade své podmínky a u mého providera internetového připojení nemám žádné právní odpovědnosti.

U mnoha poskytovatelů jsem nenašel smluvní podmínky připojení k internetu a pohybu na internetu. Tykající se většinou koncového bodu, který nesmíte přemisťovat, má mít určité specifikace a technologie, které mají zaručit rychlost a kvalitu podle smlouvy. Poskytovatelé rádi za malý poplatek zapůjčí techniku k připojení potřebnou. Dále se týkají omezení a toho, jak bude připojení k internetu vypadat atd.

# Výsledky

Z mých skoro nulových znalostí práva okolo výpočetní techniky se díky tomuto projektu podařilo mé povědomí o právu zvýšit a mohl jsem trochu prohloubit své základy práva.

K danému úkolu vytvoření materiálu pro laiky v této oblasti. Právní odpovědnosti běžného uživatele při používaní výpočetní techniky jsou vždy uloženy vlastníkem této techniky s přístupem na internet. Dle trestního zákoníku uživatel nesmí neoprávněně využívat výpočetní techniku. Nesmí překonat jakékoliv bezpečností opatření, které bylo nastaveno, aby se zabránilo přístupu. Ani zmačknutí klávesy při přihlášení bez dovolení. Také nesmíme přechovávat, distribuovat kódy, nástroje atd. na neoprávněný přístup do počítačového systému.

V paragrafu 232 se nám uvádí, že nesmíme zničit či jinak poškodit záznam v počítačovém nosiči z nedbalosti či v něčí prospěch.

Zákon o kybernetické bezpečnosti ovlivňuje jen orgány, osoby a společnosti, jenž spadají do kritické, významné či základní infrastruktury. Subjekt i běžný laik, který by mohl být správcem takového to subjektu, jenž by mohl spadat pod ZoKB by se měl poradit s právním expertem, či se obrátit na NÚKIB a tam nalézt požadované informace.

Z těchto informací tedy víme, že běžný laik se nemusí strachovat dodržováním ZoKB a může brát informace a varování z NÚKIB jen jako informace.

Běžný uživatel si tedy musí přečíst smluvní podmínky s poskytovatelem, ale ve většině případů se každý trestný čin řeší s ním individuálně a není stíhán poskytovatel, jelikož ten předá policii všechny záznamy a informace o pachateli. Pokud by někdo použil uživatelovo připojení pro spáchání trestného činu pak by mohl být uživatel stíhán na napomáhání, ale uživatel nemusí být schopen zabránit kyber útoku.

Dané informace zmíněné v metodách a výsledcích by měli uživateli dát základ v právu, aby mohl s lepším chápáním projít zákoníky a hledat další informace.

# Diskuse

S ohledem na cíle práce jsem se seznámil s trestním zákoníkem a vybral uvedené paragrafy. Relativně důkladně jsem prostudoval ZoKB a přednášky jednoho z autorů doc. Jana Koloucha, a i jeho knihu CyberSecurity, kterou jsem si po delší době čtení zakoupil fyzicky. Zákon o kybernetické bezpečnosti jsem zpracoval tak aby uživatel mohl prostudovat, jak ho ovlivňuje. Také jsem prostudoval nabídky poskytovatelů internetových připojení včetně mého poskytovatele. Mým hlavním cílem bylo sebe vzdělání, abych měl lepší přehled kdy bych mohl spáchat trestný čin a jak funguje ZoKB, který byl v mém povědomí, ale nikdy nebylo dostatek času ho prostudovat.

# Závěr

V rámci tohoto projektu jsem měl šanci nahlédnou do aktuálního stavu práva v IT, u kterého je bohužel možné, že se každou chvíli právně změní ale i přesto jsem zvýšil své povědomí. Při hledání zdrojů a informací jsem měl šanci se dostat k NÚKIBU a u něj zjistit i nabídku stáží na kterou bych se rád díky této práci a získaným znalostem přihlásil. V budoucnu bych se chtěl více věnovat právu a směřovat svůj profesní život k takovéto kariéře a možná se i dostat do CERT nebo CSIRT.

# Seznam použité literatury

[1] *Úplné znění zákona č. 40/2009 Sb., trestní zákoník: Citace trestního zákoníku paragrafu 230*. Vydání: desáté. Praha: Armex Publishing, 2019. Edice kapesních zákonů. ISBN 978-80-87451-64-9.

[2] *Úplné znění zákona č. 40/2009 Sb., trestní zákoník: Citace trestního zákoníku paragrafu 231*. Vydání: desáté. Praha: Armex Publishing, 2019. Edice kapesních zákonů. ISBN 978-80-87451-64-9.

[3] *Úplné znění zákona č. 40/2009 Sb., trestní zákoník: Citace trestního zákoníku paragrafu 232*. Vydání: desáté. Praha: Armex Publishing, 2019. Edice kapesních zákonů. ISBN 978-80-87451-64-9.

[4] *Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. Česko: Ze dne 23. července 2014 [cit. 2022-06-16]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2014-181>

[5] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity* [online]. Praha: CZ.NIC, z.s.p.o., 2019 [cit. 2022-06-16]. CZ.NIC. ISBN 978-80-88168-31-7. Dostupné z: <https://knihy.nic.cz/files/edice/cybersecurity.pdf>

[6] *Vládní CERT: NÚKIB* [online]. Brno: NÚKIB, 2014 [cit. 2022-06-19]. Dostupné z: <https://www.nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/>

[7] *Kritická informační infrastruktura* [online]. Brno: NÚKIB, 2018 [cit. 2022-06 19]. <https://www.nukib.cz/download/publikace/podpurne_materialy/Schema_KII.pdf>