ZÁKONY A PŘEDPISY UPRAVUJÍCÍ KYBERNETICKOU BEZPEČNOST

Co-funded by the Erasmus+ Programme of the European Union

Obsah knihy

1. Úvod do předmětu, systém práva, právní norma, právo a internet

Právo představuje jeden z nejvýznamnějších prostředků stabilizace sociálních vztahů a regulace společnosti.

Právo je nezbytné a v současné době nezapstupitelné, neboť kde je společnost, je i právo. Společnost není schopna dlouhodbě existovat bez řádu a pravidel. Právo jako takové výrazně snižuje míru chaosu (entropie) ve společnosti a stabilizuje poměry.

Vše výše uvedené je pravdivé, avšak pouze za předpokladu, že je právo dodržováno a také za podmínky, že právo samo o sobě je stabilní (alespoň relativně).

Právo, stejně jako společnost se vyvýjí a mění.

Právo představuje soubor obecně závazných pravidel chování pžijatých společností, definovaný státem, respektive orgány k tomu státem pověřenými. Aby bylo právo udržitelné je nezbytné, aby bylo vynutitelné. Právo bez podmínky vynutitelnosti je sice stále právem, ale reálně spíš představuje soubor doporučení u nichž záleží na každém, zda je bude respektovat.

K tomu, aby občan či subjekt, na který se bude právo vztahovat, mohl využít svých práv či je účinným způsobem chránit a aby si byl také vědom svých povinností, které správy úzce souvisejí, potřebuje vykazovat alespoň minimální znalost základních ustanovení právního řádu.

V současné společnosti je právo možné charakterizovat jako relativně přesně vymezený systém právních norem, zajištěný státní mocí a zabezpečený státním donucením. K tomu, aby fyzická či právnická osoba mohla využít svých práv či je účinným způsobem chránit, stejně tak aby si tato osoba byla vědoma svých povinností, které z práva přímo vyplývají, je nezbytné, aby se tato osoba projevila alespoň minimální znalost základních ustanovení právního řádu.

Vlastní pojem právo je relativně obtížné vymezit, neboť se jedná se o multimediální fenomén a nelze jej vymezit pouze jednou definicí:

- **právo přirozené** (*ius naturale*). Existuje nezávisle na státě, vzniká a vyvíjí se ve společnosti. Obecně se jedná o souhrn principů, které jsou adekvátní dosaženému stupni vývoje společnosti.

- **právo pozitivní** (*ius pozitivum*). Toto právo je dané státem, respektive mocenským zřízením. Pozitivní právo je tedy předem dáno, jsou to předvídatelná pravidla, která se vynucují, tzn., že protiprávní jednání je postihováno.

- **právo objektivní** – (odpovídá anglickému výrazu „*law*"). V případě práva objektivního rozumíme právem souhrn právních norem jako obecně závazných pravidel chování stanovených nebo uznaných státem a státem vynucovaných

- **právo subjektivní** – (odpovídá anglickému výrazu „*right*"). V tomto případě právem rozumíme právní normou zaručenou možnost chování právních subjektů, jíž obvykle odpovídá právní povinnost jiného právního subjektu. Právu v tomto významu odpovídá například vyjádření subjektu, že „má na něco právo".

1.1. Právní norma

Právní norma je základním prvkem právního státu.

Právní norma představuje je obecně závazné pravidlo chování, které upravuje práva a povinnosti subjektů. Toto pravidlo chování je vyjádřeno ve zvláštní státem (resp. Unií) uznané právní formě a jeho dodržování je zabezpečováno státním donucením.

Z uvedené definice právní normy vyplývají dva obligatorní znaky, které jsou dále konkretizovány. Jedná se o znak:

1. Formální

Z hlediska naplnění formálního znaku právní normy je třeba, aby právní normu vydal oprávněný subjekt a byl současně splněn zákonem předepsaný způsob publikace.

2. Materiální

Do materiálního znaku právní normy je možné zařadit:

- regulativnost – reguluje společenské vztahy,
- právní závaznost – pravidlo chování závazně reguluje společenské vztahy,
- obecnost – co do předmětu právní úpravy, tak i do objektu právní normy,
- vynutitelnost státní mocí – „státním donucením" v případě, že právo není respektováno.

Standardní **struktura právní normy je složena ze tří částí** jimiž jsou **hypotéza, dispozice a sankce**.

Hypotéza stanoví podmínky, za kterých se právní norma realizuje. Hypotéza zýejména vymezuje právní skutečnosti, subjekty a objekty normy, kterých se oprávnění a povinnosti týkají.

Dispozice představuje vlastní pravidlo chování, neboť stanoví a konkretizuje komu a jaká vznikají práva a povinnosti v případě, že nastanou podmínky uvedené v hypotéze.

Sankce představuje vyjádření důsledků porušení právní povinnosti vyplývající z dispozice právní normy.

Dělení právních norem

Právní normy je možné členit dle různých kritérií. Jedná se zejména o:

1. *Povahu pravidel stanovených právní normou.* Dle povahy pravidel se právní normy člení na:
   - Dispozitivní. Právní norma dispozitivní nestanoví vůbec zásadní pravidlo chování, nebo ho stanoví pouze alternativně. Je ponecháno na adresátech, aby si sami stanovili pravidla. Jestliže tak adresáti neučiní, slouží ustanovení v normě jako vodítko pro soudce, aby věděl, jak rozhodnout. Dispozitivní normy se nejvíce aplikují v občanském právu resp. v občankoprávních vztazích, které umožňují větší variabilitu řešení různých situací (seberegulace).
   - Kogentní (kategorické). Právní norma kogentní závazně stanoví pravidlo chování, neponechávají prostor pro vůli adresáta.
2. *Znění slovního vyjádření.* Dle znění slovního vyjádření se právní normy člení na:
   - Opravňující. Tyto právní normy výslovně formulují pouze oprávnění.
   - Zavazující. Tyto právní normy výslovně formulují povinnost, ať už formou příkazu nebo zákazu.
3. *Postavení subjektů.* Dle postavení subjektů se právní normy člení na:
   - Veřejné. Tyto právní normy se uplatňují tam, kde je realizována veřejná moc. Veřejnou moc vykonává stát prostřednictvím orgánů moci zákonodárné, výkonné a soudní. Za právo veřejné považujeme tu oblast práva, v níž jsou vztahy založeny na nerovnosti zúčastněných subjektů, kdy jeden představuje veřejnou moc, která vystupuje vůči soukromým osobám s příkazy, zákazy a donucení.
   - Soukromé. Tyto právní normy se uplatňují v oblasti práva soukromého, tedy tam kde subjekty vystupují v rovném postavení a žádný z nich nemůže autoritativně rozhodnout o právech a povinnostech toho druhého. Subjekty si vzájemná práva a povinnosti upravují smlouvami a dohodami.
4. *Předmět regulace.* Dle předmětu regulace se právní normy člení na:
   - Mezinárodní. Tyto právní normy regulují vztahy mezi státy nebo jejich obyvateli, případně na úrovni Unie.
   - Národní. Národní právní normy upravují vztahy mezi subjekty v rámci jurisdikce konkrétního státu, respektive zpravidla na jeho územní.
5. *Metodu právní úpravy*. Dle metody právní úpravy se právní normy člení na:
   - Hmotněprávní. Tyto právní normy vymezují právní vztahy obecně, stanovují práva a povinnosti subjektů.
   - Procesněprávní. Tyto právní normy upravují postup orgánů veřejné moci při aplikaci norem hmotného práva, jehož výsledkem může být vydání veřejnoprávního aktu.
6. *Rozsahu právní úpravy.* Dle rozsahu právní úpravy se právní normy člení na:

- Obecné. Tyto právní normy dopadají na celé území státu resp. Unie, přičemž se vztahují na všechny subjekty a není předem omezena jejich časová působnost.

- Zvláštní. Tyto právní normy působí jen na určitém území, nebo se vztahují jen na určitou kategorii subjektů nebo na určité časové období.

Účinnost právních norem

Účinnost právní normy znamená, že z ní jejím adresátům vznikají práva a povinnosti. Předpokladem účinnosti právní normy je její platnost. To znamená, že právní norma může nabýt účinnosti nejdříve dnem její platnosti. Právní norma však může nabýt účinnosti později. Mezi dnem, kdy se právní předpis stal platným a mezi dnem, kdy nabyl účinnosti, může tedy uplynout určitá doba (tzv. *Legisvakační lhůta*). Tato lhůta má adresátům právní normy umožnit se s právní normou náležitě seznámit a adaptovat se na ni. Datum nabytí účinnosti je zpravidla uvedeno v posledním ustanovení dané právní normy.

Příklady práva kolem nás:

- Kupní smlouva
- Smlouva o dílo
- Smlouva o úvěru
- Pracovní smlouva/smlouva o dílo/dohoda o provedení práce
- Smlouva o poskytování poradenských služeb
- Licenční smlouva
- Manažerská smlouva
- Dohoda o důvěrnosti
- Smlouva o prodeji obchodního podílu
- Civilněprávní delikty (pomluva, porušení smlouvy)
- Trestné činy (např. krádež, podvod, porušování autorských práv aj.)

1.2. Vztah práva a kyberprostoru

O vztahu práva a nových technologií, zejména pak Internetu, včetně jeho změn a transformací, toho bylo publikováno mnoho, řada klíčových otázek však zůstává neřešena, řada dalších problémů se nachází pouze ve fázi jejich identifikace, případně analýzy, nicméně hledání rozumných řešení je v lepším případě na dobré cestě, v horším pak v nedohlednu. Internet je bezesporu fenomén *sui generis*, jako takový nestojí samostatně a je regulován zejména prostřednictvím regulace chování jeho uživatelů.

Právo je jedním z jeho možných regulativů v podobě nedokonalých normativních konstrukcí, kde platí více než jinde, že mezi realitou, tedy tím, co je v prostředí Internetu skutečně realizováno, a normativitou, tedy tím, co má být (z vůle regulátora i naší), není shoda. Realita Internetu a jeho normativní regulace jsou tedy dvě relativně samostatné kategorie. Tento předpoklad nebude popírán ani v této publikaci, právě naopak, bude jedním z jejích nosných pilířů.

Většinu právních problémů týkajících se Internetu je nutné posuzovat v celkovém právním i technologickém kontextu, nikoliv pouze optikou zažitých vzorců či optikou jednotlivých právních oborů *per se*.[1]

[1] MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, 2013. ISBN 978-80-904248-7-6 s. 25

2. Zodpovědnost v kyberprostoru

2.1. Kyberprostor

„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 bezpečnosti. Aby bylo možné definovat kyberprostor, je nezbytně nutné vymezit pojem Internet, který právě s kyberprostorem bezprostředně souvisí.

Světové počátky Internetu, který je nezbytnou materiální podstatou kyberprostoru, se datují do 50. let 20. století. 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[1], 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.“* [2]

Výsostné postavení v rámci sítě Internet má sdružení ICANN[3] (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.[4]

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.

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

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth.

We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.

Our identities have no bodies, so, unlike you, we cannot obtain order by physical coercion. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis. But we cannot accept the solutions you are attempting to impose.

In the United States, you have today created a law, the Telecommunications Reform Act, which repudiates your own Constitution and insults the dreams of Jefferson, Washington, Mill, Madison, DeToqueville, and Brandeis. These dreams must now be born anew in us.

You are terrified of your own children, since they are natives in a world where you will always be immigrants. Because you fear them, you entrust your bureaucracies with the parental responsibilities you are too cowardly to confront yourselves. In our world, all the sentiments and expressions of humanity,

from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits. We cannot separate the air that chokes from the air upon which wings beat.

In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media.

Your increasingly obsolete information industries would perpetuate themselves by proposing laws, in America and elsewhere, that claim to own speech itself throughout the world. These laws would declare ideas to be another industrial product, no more noble than pig iron. In our world, whatever the human mind may create can be reproduced and distributed infinitely at no cost. The global conveyance of thought no longer requires your factories to accomplish.

These increasingly hostile and colonial measures place us in the same position as those previous lovers of freedom and self-determination who had to reject the authorities of distant, uninformed powers. We must declare our virtual selves immune to your sovereignty, even as we continue to consent to your rule over our bodies. We will spread ourselves across the Planet so that no one can arrest our thoughts.

We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.

Davos, Switzerland
*February 8, 1996**[5]***

I téměř 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, která jsou uplatňována v návaznosti na skutečnou fyzickou lokalizaci dat či informací. Druhou možností je vytvoření nových kritérií, pro aplikaci principu místní působnosti (jedná se o virtuální lokalizaci právních vztahů).[6]

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).[7] 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[8]). 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.

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**[9], 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, měnit data.

Mezi **znaky kyberprostoru** je možné zařadit jeho **decentralizovanost**, **globálnost**, **otevřenost**, **bohatost na informace**, **interaktivnost** a možnost ovlivňování mínění skrze uživatele. Podstatným rysem 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 mít a má dopady ve světě reálném.

Pokud jede o legální definici kyberprostoru, je možné využít například znění § 2 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti[10] , kde je uvedeno, že *„kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací."*

Dle našeho názoru jednu z velmi zdařilých definic kyberprostoru přináší dokument Cyberspace Operations: Concept Capability Plan 2016-2028, který definuje **kyberprostor jako prostor složený ze tří vrstev:**[11]

1. **fyzické**,
2. **logické** a
3. **sociální**.

Tyto vrstvy se pak skládají z celkem pěti komponent.

Ad 1) Fyzická vrstva

Tato vrstva zahrnuje pojem „**geographic component**" a pojem **fyzické síťové komponenty**. Pojem „geographic component" nemá v našem jazyce přesný ekvivalent, nicméně je jím myšleno přesné umístění síťových prvků ve fyzickém světě. Pojem fyzické síťové komponenty pak zahrnuje infrastrukturu v podobě kabelů, řídících prvků sítě (switch, router) a dalšího zařízení.

Toto rozdělení fyzické vrstvy má svou logiku. Zatímco geopolitické hranice mezi státy mohou být v kyberprostoru snadno překročeny, v reálném světě zde stále existují omezení, která vyplývají z podstaty našeho fyzického světa.

Pokud tuto myšlenku převedeme do světa kyberútoků a incidentů, znamená to, že mohu jako útočník poškodit prvek fyzické vrstvy buď vzdáleně, například tím, že znám jeho konkrétní zranitelnost, kterou lze vzdáleně napadnout, nebo jej mohu poškodit přímo v reálném světě, pokud se mi k němu podaří fyzicky dostat a zaútočit na něj například s použitím fyzické síly. Dopad v kyberprostoru bude stejný, ale provedení samotného útoku je značně odlišné.

Ad 2) Logická vrstva

Tato vrstva obsahuje **logické síťové komponenty**, čímž jsou myšlena logická propojení mezi síťovými uzly. Ta jsou realizována prostřednictvím síťových komunikačních protokolů. Uzly mohou být počítače, telefony a další síťová zařízení.

Ad 3) Sociální vrstva

Tato vrstva se skládá z komponent nazvaných „**kyberosobnost**" a **osobnost**.

Komponenta „kyberosobnost" zahrnuje identifikaci osoby na síti, jako je e-mailová adresa, IP adresa, číslo telefonu a další. Komponenta osobnost se skládá ze skutečných osob připojených k síti. Jedna individualita pak může mít více „kyberosobností", například různé e-maily na různých zařízeních, a jedna „kyberosobnost" může být ve skutečnosti více různých skutečných osob, využívajících například jeden společný sdílený účet.

Kyberprostor je také možné definovat podle dostupnosti a dohledatelnosti dat pro běžného uživatele. Podle tohoto dělení lze kyberprostor rozdělit na služby a data dostupná pomocí Internetu, na služby a data dostupná pouze v rámci konkrétních sítí a zařízení a na služby a data záměrně skrytá a dostupná s využitím speciálních nástrojů.

Obvykle se pro tyto kategorie používají názvy:

1. **Surface Web**,
2. **Deep Web** a
3. **Dark Web**.

Deep a Dark Weby jsou také souhrnně označovány jako **D4rkN3ts** – **Darknets**. Všechny tyto součásti pak společně vytváří skutečný kyberprostor.[12]

Na terminologii, která používá k rozdělení kyberprostoru pojem *web,* se bohužel podepsal fakt, že pro většinu laické veřejnosti platí jednoduchá rovnice:

KYBERPROSTOR = INTERNET = **WEB**

Nicméně kyberprostor se netýká pouze webových stránek, ale všech počítačových systémů, služeb, uživatelů a dat, jež se v tomto prostoru pohybují.

---

[1] Srov. *Internet History of 1980s.* [online]. [cit. 7. 6. 2016]. Dostupné z:

http://www.computerhistory.org/internethistory/1980s/

[2] *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

[3] Blíže viz https://www.icann.org/

[4] ISP – Internet Service Provider.

[5] BARLOW, Perry John. *A Declaration of the Independence of Cyberspace.* [online]. [cit.23.9.2014]. Dostupné z: https://www.eff.org/cyberspace-independence.

[6] Blíže viz REED, Chris. *Internet Law*. Cambridge: Cambridge University Press, 2004, str. 218

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

[8] 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.

[9] *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

[10] Dále jen ZKB

[11] TRADOC. Cyberspace Operations: Concept Capability Plan 2016-2028. [online]. [cit. 18. 2. 2018], s. 8-9 Dostupné z: www.fas.org/irp/doddir/army/pam525-7-8.pdf?

[12] 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

2.2. Působnost práva v Kyberprostoru

Kyberprostor, je otevřený a snadno přístupný všem, ***„...neplatí zde žádné zvláštní zákony a je třeba se řídit obecně závaznými normami.“***[1]

Neoddiskutovatelnou skutečností je, že se do prostředí informačních sítí přesouvá realizace stále většího množství společenských, ale i ekonomických vztahů, a tím pádem vyvstává potřeba určité právní regulace takového jednání. Díky delokalizaci subjektů práva v různých zemích na celém světě je otázkou, jaký právní systém (jestli vůbec nějaký) se bude vztahovat na případné úkony (či protiprávní jednání) učiněné v Internetu.

Je tedy třeba primárně řešit dvě otázky. Za prvé, zda platí právo na Internetu, a pokud ano, jaké právní normy se užijí. Za druhé, jakým způsobem je možné toto právo aplikovat, a to včetně případných sankcí či jiných opatření. Jako příklad, na němž lze demonstrovat obtížnou aplikaci práva, může sloužit případ, kdy v roce 2005 v Číně jeden hráč online hry *„The Legend of Mir 3“* **zabil druhého hráče kvůli krádeži virtuální zbraně**. Mezi hráči této hry funguje nejen prodej virtuálních komodit, ale i systém půjček. Zejména se tak děje u hráčů, kteří se znají důvěrně, není však podmínkou, aby se znali z reálného světa. Právě půjčka byla příčinou uvedené vraždy. Hráč Qui Chengwei půjčil virtuální šavli - *„Dragon sabre“*, svému virtuálnímu příteli Zhu Caoyuanovi. Zhu ale podlehl vidině lehce vydělaných peněz a zbraň prodal za 7 200 junů (což je v přepočtu asi 19.000 - 20.000,- Kč) na internetové aukci. Poté, co se Qui o prodeji dozvěděl, obrátil se na policii a nahlásil krádež virtuální šavle. Policie odmítla skutek řešit s tím, že na virtuální vlastnictví (de facto neexistující věci) se zákony nevztahují. Qui ztratil trpělivost a napadl Zhua u něj doma a ubodal ho k smrti.[2]

Je zřejmé, že se jedná o velmi extrémní případ, ale je na něm vhodně demonstrováno, že virtuální svět není od reálného světa odtržený, a proto je třeba řešit i otázku právní odpovědnosti v něm.[3] De facto od počátku rozvoje Internetu docházelo ke konfrontaci světa technického a právního. Technicky je Internet řešen logicky s jasnou hierarchií a strukturou. Právo, a zejména pak právo lokální, však často do této logičnosti vnášelo a vnáší „chaos“. Pojem „chaos“ asi nejvýstižněji vystihuje snahu legislativy o regulaci tohoto ryze technického světa, neboť v kyberprostoru má uživatel širokou řadu možností, jak určitý zákaz či restrikci „obejít“. Na následujících příkladech se pokusím demonstrovat ovlivňování světa reálného a virtuálního.

LICRA vs. Yahoo

Jeden z prvních případů vztahujících se k aplikovatelnosti práva v Internetu se stal v roce 2000 ve Francii. V únoru 2000 navštívil Marc Knobel (francouzský žid, který svůj život zasvětil boji s nacismem), aukční server www.yahoo.com a zjistil, že tento server nabízí na svých webových stránkách řadu předmětů s tematikou nacismu nebo předmětů vztahujících se k německým válečným silám z druhé světové války. Po tomto zjištění se Marc Knobel obrátil na Yahoo! Inc. s požadavkem na blokaci těchto stránek. Společnost Yahoo! Inc. však jeho požadavku nevyhověla. Marc Knobel prostřednictvím L.I.C.R.A. (Ligue Internationale Contre Le Racisme et l´Antisémitisme) podal, dne 11. dubna 2000, žalobu na Yahoo! Inc. u francouzského soudu za porušování francouzských zákonů, neboť ve Francii je zakázána propagace a podpora nacismu v televizi, v rozhlase i v psané podobě. Společnost Yahoo! Inc. se bránila tvrzením, že servery, na nichž je provozován aukční portál, jsou fyzicky umístěny v USA, a tak nelze připustit, aby se francouzské zákony uplatnily na hardware a weby provozované v Americe. Obhajoba dále namítala, že obsah webů je primárně určen pro americké rezidenty, jimž první dodatek Ústavy USA zaručuje svobodu projevu. Jakékoli snahy o odstranění těchto stránek by pak bylo v rozporu s tímto dodatkem.

LICRA však poukázala na skutečnost, že pokud firma Yahoo! Inc. podniká ve Francii, je nucena respektovat zákony Francie, přičemž Internet není výjimkou. Yahoo! Inc. na tento argument reagovalo tak, že není schopno určit, odkud se jejich zákazníci k aukčnímu portálu přihlašují. Pokud by tedy odstranili předmětné stránky, nejen že by nerespektovaly První dodatek Ústavy USA, ale znemožnili by přístup všem uživatelům, nehledě na hranice. Tím by se francouzské zákony staly de facto zákony celosvětovými. Dne 22. května 2000 byl soudcem Jean–Jacques Gomez vynesen rozsudek, který nařídil společnosti zablokovat pro francouzské uživatele přístup na americké aukční stránky s nacistickými pamětními předměty. Své rozhodnutí odůvodnil mimo jiné i tím, že Yahoo! Inc. dokáže identifikovat francouzské uživatele natolik dobře, že na jimi navštěvované stránky umí umístit reklamu ve francouzštině. Soudce dal společnosti Yahoo! Inc. 90 dní na to, aby nainstalovali na francouzské stránky Yahoo! Inc. filtrovací systém na bázi klíčových slov. *„Soudce Gomez v odůvodnění uvedl, že je možné zablokovat až devadesáti procentům francouzských uživatelů přístup na inkriminované internetové stránky. Technické řešení, s nímž má Yahoo! na základě rozsudku přijít, posoudí tříčlenný mezinárodní panel. Jeho dřívější nález uvádí, že je možné až sedmdesát procent uživatelů odblokovat podle označení jejich poskytovatele internetového připojení (ISP), dalších dvacet procent pak podle sledování klíčových slov zadávaných do hledače na stránkách Yahoo!.“*[4]

Právní zástupce Yahoo! Inc. Greg Wrenn uvedl: *„Kdykoli bude na stránce připomínající oběti holocaustu zmíněno slovo Hitler, bude stránka automaticky zavřena. Není možné vůbec mluvit o efektivním rozsudku, protože fakticky není možné jej naplnit.“*

Technické problémy v té době spočívaly, a částečně spočívají i dodnes, v tom, že filtrovat lze to, co se dá jasně definovat (např. slova jako Nazi, Heil Hitler aj.). Ale filtr není schopen odhalit všechny možné verze nežádoucího materiálu (např. N_A_Z_I, H3Il HiT_L3R aj.). Tyto rozdíly mohou poznat osoby fyzické (např. zaměstnanci konkrétního ISP), které pak stránku odstraní, nicméně provozovatel závadového fóra nebo aukce si může jednoduše změnit adresu a pokračovat ve své činnosti dál.

Společnost Yahoo! Inc. se vzdala odvolání proti rozsudku francouzského soudu a zahájila blokaci francouzských uživatelů na stránkách nabízejících závadný obsah. Společnost Yahoo! Inc. se však zároveň obrátila na místně příslušný okresní soud[5] v USA se žádostí o vynesení deklaratorního rozsudku, jež by působnost francouzského soudu nad americkou firmou vyloučil. Tento soud společnosti Yahoo! Inc. vyhověl v tom smyslu, že výkon francouzského rozhodnutí na území USA je protiústavní. LICRA proti tomuto rozsudku podala odvolání. Odvolací soud v USA reagoval odmítnutím své jurisdikce nad organizacemi LICRA. V roce 2006 se případ dostal před Nejvyšší soud v USA[6], který se v závěru věcí odmítl zabývat. Rozsudky soudů v USA tak spíše vyzněly v prospěch společnosti Yahoo! Inc., ta se však nakonec sama dobrovolně rozhodla, že zcela odstraní stránky nabízejících předměty s nacistickou tématikou ze svých serverů, a to nejen ve Francii.

Gutnick vs. Dow Jones

Joseph Gutnick (australský podnikatel s diamanty), si o sobě v roce 2000 přečetl v internetovém vydání novin Barron's[7] článek, který považoval za pomluvný. Gutnick podal žalobu pro pomluvu na vydavatelství Dow Jones u australského soudu. Dow Jones využilo obdobné argumenty, jako Yahoo! Inc. ve sporu s LICRA. Argumentace se primárně opírala o skutečnost, že tištěná verze novin je primárně určena pro trh v USA, tudíž se na případ nemohou australské zákony vztahovat.

Navzdory této argumentaci rozhodl australský soud[8] v roce 2002[9] následujícím způsobem: *„jelikož je materiál (článek) dostupný také v Austrálii, tedy v místě, kde je podnikatel Gutnick nejznámější, může jej pomluva nejvíce poškodit. Dow Jones je povinno zaplatit Gutnickovi odškodnění.“* Soud konstatoval, že se nebude zabývat tím, zda má či nemá Internet hranice a vzal v potaz především to, kde byl obsah dostupný, nikoli, kde byl zveřejněn. Soud také konstatoval, že každý má právo na právní ochranu před obdobným jednáním či dalšími útoky. Australský soud ve svém rozsudku také konstatoval realitu přeshraničního charakteru Internetu, kterému odpovídá extenzívní uplatňování jurisdikce.

GoDaddy

GoDaddy[10] je americký majoritní registrátor internetových domén. V roce 2016 spravuje více než 61 milionů internetových domén, což z GoDaddy činí největšího registrátora domén. Registrace domény u tohoto ISP je velmi jednoduchá a cenově dostupná. Zároveň je, díky lokaci společnosti (USA), uživatelům poskytována právní ochrana jejich osobních údajů a dat uvedených na doméně zaregistrované právě v rámci GoDaddy, pokud však uživatelé neporušují právo USA. Z tohoto důvodu jsou domény registrované u GoDaddy velmi často využívány například extremistickými, rasistickými a jinými skupinami či uživateli. Tito uživatelé pak spoléhají na ústavní právo USA a První dodatek Ústavy USA:

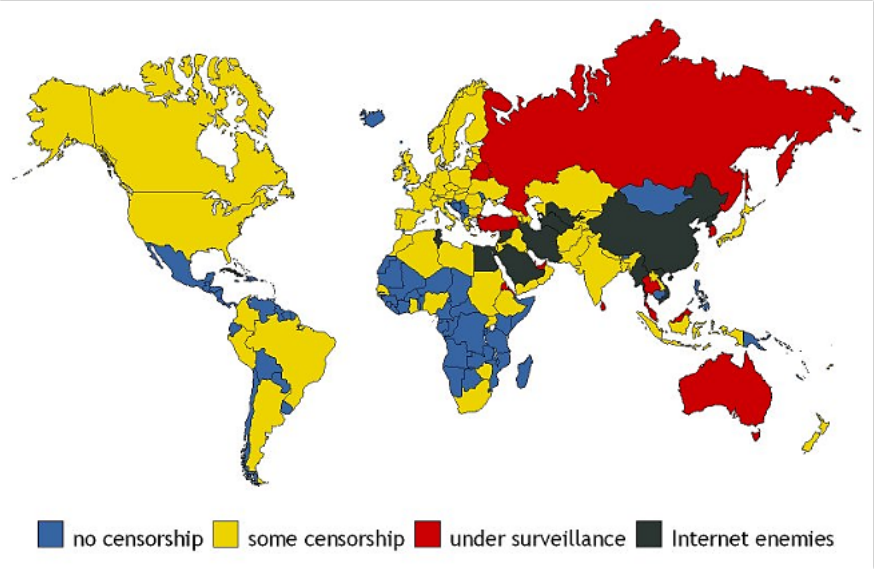
„Kongres nevydá žádný zákon, který by nerespektoval svobodu vyznání, nebo by obsahoval zákaz volného výkonu (bohoslužebných úkonů), nebo oklešťující svobodu slova nebo tisku nebo právo lidu pokojně se shromažďovat, a podávat petici vládě s cílem nápravy křivd.“[11]

Problémem při řešení kybernetické trestné činnosti s výše uvedeným obsahem je pak prokázání reálnosti hrozby, či trestného činu tak, aby zároveň nešlo o porušení prvního dodatku Ústavy.

Second Life (a „dětské“ porno).

Second Life představuje 3D virtuální prostředí vyvíjené společností Linden Lab. Toto prostředí umožňuje vytváření vlastních avatarů, jejich vzájemné interakce, včetně možnosti generování zisku. Second Life je rozdělen do dvou virtuálních světů podle věku uživatele.[12] Uživatelé jsou schopni si měnit svoji totožnost a modifikovat si vzhled avatara dle svých představ. V roce 2007 upozornila německá stanice ARD a následně CNN na existenci „pedofilního ostrova.“ [13]

V této reportáži je poukazováno na skutečnost, že někteří uživatelé MainGrid (tedy uživatelé starší 18 let) si vytvořili avatary v podobě dítěte a jiní se vydávali za dospělé. V rámci vzájemné interakce pak docházelo ke zneužívání dětských avatarů avatary dospělými. Orgány činné v trestním řízení v SRN zahájily vyšetřování, neboť podle německého trestního práva je držení virtuální dětské pornografie trestné.[14] Společnost Linden Lab poskytla německým orgánům součinnost při zjišťování identity uživatelů a majitelů virtuálních pozemků, na kterých se virtuální dětská pornografie uskutečňovala. Ve Spolkové republice Německo a Velké Británii bylo předmětné jednání možné postihnout prostředky trestního práva, ale v USA bylo takové jednání nepostižitelné.



Obrázek 1 - Rozdělení států dle cenzury Internetu

V současnosti na světě neexistuje stát, který by se vzdal práva na potrestání protiprávního jednání, které zasahuje zájmy, jež chrání.

Mimo výše uvedené případy existuje celá řada dalších příkladů regulace Internetu a služeb na Internetu poskytovaných ze strany organizací nebo států. Tato regulace pak nutně přináší problémy s aplikovatelností a vynutitelností práva.

Ze zobrazené mapy (viz Obrázek 1)[15] vyplývá ta skutečnost, že většina zemí světa přijala právní nástroje, které ovlivňují Internet či poskytované služby.

Z hlediska uživatele je třeba konstatovat, že princip teritoriality v souvislosti s Internetem ztrácí smysl, protože se lze v kterémkoli okamžiku nacházet kdekoli na světě, aniž by uživatel musel vědět, kde je umístěn server, s nímž právě komunikuje. Z tohoto pohledu je Internet globální a nezná hranice.

„Je sice pravda, že lze v každý konkrétní okamžik vystopovat fyzické umístění určité informace – příslušná lokace je však mnohdy nahodilá, velmi krátkodobá a pro informaci jako takovou a její právní efekt zpravidla naprosto irelevantní.“[16]

Právo by mělo s virtuálním světem držet krok, bohužel ne vždy se to daří, neboť státy (uzavřené v pevných teritoriích) mnohdy postrádají prostředky, jak efektivně vynucovat právo v rámci kyberprostoru.[17] V podstatě existují dvě možnosti řešení totoho problému. Jednou z možností je respektovat principy teritoriality států tak, jak jsou nastaveny dnes. Tento přístup by pak de facto znamenal to, že pokud by někdo zasáhl do práv, jež se stát garantoval chránit, muselo by se počkat, než se útočník ocitne ve fyzické jurisdikci státu[18], či by musel využít cesty mezinárodní právní pomoci.

Druhou možností pak je vytvoření speciální právní úpravy, tzv. internetové jurisdikce, která by se vztahovala na online svět. Otázkou je, jak by bylo toto nové právo přijato jednotlivými zeměmi. Osobně se domnívám, že za současných podmínek není možné celosvětově sjednotit všechna právní odvětví (občanské, obchodní, trestní, správní aj.), do nichž nějakým způsobem intervenuje Internet. Svoje tvrzení opírám mimo jiné i o skutečnost, že v roce 2001 byla přijata Úmluva o kyberkriminalitě, která definuje základní skupiny trestných činů, které by měly být v kyberprostoru stíhány, avšak k 1. 8. 2016 ji ratifikovalo pouze 49 zemí.

Jako problematické se, vzhledem ke globálnosti Internetu, dále jeví **určení**:

1. **rozhodného práva** (podle práva kterého státu se bude případný soudní spor rozhodovat),

2. **orgánu, který je oprávněn vydat rozhodnutí**,

3. **orgánu, který může rozhodnutí vymoci či přímo vykonat.**[19]

Vedle klasických právních norem se na tvorbě práva, respektive pravidel na Internetu, podílejí *definiční autority* tvorbou *definičních norem*.

---

[1] SMEJKAL, Vladimír. *Internet a §§§*. 2. aktualiz. a rozš. vyd. Praha: Grada, 2001, s. 32

[2]Srov. HAINES, Lester. *Online gamer stabbed over „stolen" cybersword.* [online]. [cit.3.10.2006]. Dostupné z: http://www.theregister.co.uk/2005/03/30/online_gaming_death/

[3] Srov. Rozhodnutí Nejvyššího soudu 4 Tz 265/2000, ze dne 16.1.2001. [online]. [cit.13.3.2008]. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/B82A96F8E1B60D3AC1257A4E00694707?openDocument&Highlight=0

[4] ŠTOČEK, Milan. *V Hitlerově duchu proti Hitlerovi.* [online]. [cit.10.7.2016]. Dostupné z: http://www.euro.cz/byznys/v-hitlerove-duchu-proti-hitlerovi-814325

[5] United States District Court for the Northern District of California in San Jose

[6] United States Supreme Court

[7] http://online.barrons.com

[8] High Court of Australia

[9] Rozsudek [2002] HCA 56 z 10. prosince roku 2002, [online]. [cit.24.3.2014]. Dostupné z:

http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html

[10] https://uk.godaddy.com/

[11] *First Amendment.* [online]. [cit.10.7.2016]. Dostupné z: https://www.law.cornell.edu/constitution/first_amendment. Překlad autora

[12] **MainGrid** - určený pro uživatele od dosažení věku 18 let; **TeenGrid** - určený pro věkovou skupinu v rozmezí od 13 do 18 let.

[13] Blíže k uvedenému viz: *CNN on pedophile sex in Second Life.* [online]. [cit.18.6.2009]. Dostupné z:

[14] *Second Life 'child abuse' claim.* [online]. [cit. 16. 6. 2009]. Dostupné z:

http://news.bbc.co.uk/2/hi/technology/6638331.stm

[15] *Internet censorship.* [online]. [cit.10.8.2016]. Dostupné z: http://www.deliveringdata.com/2010_10_01_archive.html

[16] POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 7

[17] Srov. vyjádření v rámci **Deklarace nezávislosti kyberprostoru** („A Declaration of the Independence of Cyberspace").

Srov. THOMAS, Douglas. *Criminality on the Electronic Frontier.* In Cybercrime. London: Routledge, 2003, s. 17 a násl.

Srov. JOHNSON, David R. a David POST. *The Rise of Law in Cyberspace.* [online]. [cit.10.7.2016]. Dostupné z: http://poseidon01.ssrn.com/delivery.php?ID=797101088103069021099122095084084095061040041017050027018013071117008115007025117112101013061121056036119084118089028085067043

[18] Příkladem tohoto přístupu může být případ, kdy uživatel např. z ČR bude v Internetu veřejně a opakovaně napadat ten který stát (např. pro nedodržování lidských práv v této zemi aj.), případně bude vyvíjet další činnost, která je v tomto státě protiprávní (avšak není protiprávní v ČR). Pokud se tento uživatel někdy v budoucnu rozhodne navštívit onu zemi, proti které takto vystupoval, může na něj být při překročení hranic tohoto státu uplatněho jeho teritoriální právo.

[19] POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 7

2.3. SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

ℹ️

- Pro pochopení problematiky **Zákony a předpisy upravující kybernetickou bezpečnost** je třeba alespoň základní principy fungování práva, jeho dělení a implementace. První dvě kapitoly prezentují právě obecný rámce aplikovatelnosti práva v kyberprostoru.
- Právní norma představuje je obecně závazné pravidlo chování, které upravuje práva a povinnosti subjektů. Toto pravidlo chování je vyjádřeno ve zvláštní státem (resp. Unií) uznané právní formě a jeho dodržování je zabezpečováno státním donucením.
- Právo je jedním z jeho možných regulativů v podobě nedokonalých normativních konstrukcí, kde platí více než jinde, že mezi realitou, tedy tím, co je v prostředí Internetu skutečně realizováno, a normativitou, tedy tím, co má být (z vůle regulátora i naší), není shoda. Realita Internetu a jeho normativní regulace jsou tedy dvě relativně samostatné kategorie. Tento předpoklad nebude popírán ani v této publikaci, právě naopak, bude jedním z jejích nosných pilířů.
- Kybernetickým prostorem je:
  - prostor kybernetických aktivit, či jako prostor vytvořený informačními a komunikačními technologiemi, který vytváří virtuální svět (či prostor) jako paralelu k prostoru reálnému.
  - digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.
  - prostor jako prostor složený ze tří vrstev: fyzické, logické a sociální.
- Na jednotlivých kazuistikách byly prezentovány příklady aplikace práva v kyberprostoru.

🗝️

KLÍČOVÁ SLOVA K ZAPAMATOVÁNÍ

- právo
- právní norma
- kyberprostor

❓

KONTROLNÍ OTÁZKY

- Co je to právo?
- Co je to právní norma a jak se dělí?
- Co je to kyberprostor?
- Z jakých vrstev se kyberprostor sestává?
- Platí právo v kyberprostoru, a pokud ano, jaké právní normy se užijí?
- Jakým způsobem je možné právo v kyberprostoru aplikovat, a to včetně případných sankcí či jiných opatření?
- Uveďte některý z příkladů aplikace práva v kyberprostoru.

3. Právní základ činnosti ISP (internet service provider - poskytovatel internetových služeb).

Na tvorbě práva na Internetu, na omezování či rozšiřování jeho aktivit, se podílejí *definiční autority* tvorbou *definičních norem*. Aby bylo možné pochopit otázku případné odpovědnosti poskytovatelů služeb informační společnosti, musím nejdříve charakterizovat právě definiční normu a definiční autoritu.

Definiční normy jsou vytvářeny a implementovány subjekty, které jsou oprávněny definovat prostředí informační sítě. Jde de facto o normy *sui generis*, které vymezují informační sítě jako takové. Vyskytují se ve vrstvách, které jsou na sobě závislé. *„Definiční normy jsou vytvářeny telekomunikačními operátory, producenty kancelářského softwaru, ale i například tvůrci, či provozovateli online her, nebo každý, kdo si otevře blog, nebo kdo má emailovou schránku (definiční norma vytvořená uživatelem této schránky je například filtr, který automaticky provádí nastavenou operaci s doručenou poštou).“* [1]

Definiční autority jsou původci definičních norem, jde o subjekt, který svým fungováním vytváří pravidla fungování logického systému, ve kterém autorita působí. Jak již bylo uvedeno dříve, má mezi těmito autoritami výsostné postavení ICANN, neboť této organizaci přísluší přidělování, správa a stanovení pravidel pro systém doménových jmen.[2] Další definiční autoritou je například IETF.[3] Byť se definiční autority mohou jevit jako neomezení správci kyberprostoru, stále jsou subjektem práva některého státu.[4]

Specifikem **Internet**u je, že **existuje** právě **jen díky definičním autoritám**. **Je z nich složen. Žádná operace se neuskuteční bez účasti** (provedení či zprostředkování operace) **definiční autority.**

Lawrence Lessig ve své knize Code and Other Laws of Cyberspace (Code v. 2) uvádí: *„Můžeme postavit, navrhnout nebo nakódovat*[5] *(naprogramovat) kyberprostor k ochraně hodnot, které pokládáme za základní. Můžeme jej ale také navrhnout nebo naprogramovat tak, že tyto hodnoty necháme vymizet. Žádná prostřední možnost tu není, vše v kyberprostoru je nějakým způsobem postaveno. Kód nikdy neobjevujeme, ten vždy utváříme.“*[6]

Po výše uvedeném vyjádření a svých zkušenostech s kyberprostorem si dovolím tvrdit, že největší **definiční autoritou**, byť se nejedná o subjekt, který vytváří pravidla fungování logického systému, **je uživatel jako takový**. Jeho definiční role působí zprostředkovaně. Uživatel služeb, jež poskytují jednotliví ISP, přímo či zprostředkovaně ovlivňuje to, co bude v kyberprostoru úspěšné, a co ne. Pokud se dostatečně velká skupina uživatelů rozhodne, že aktivně přestane využívat některou ze služeb, poskytovaných ISP, bude tato služba nucena změnit své „chování“ na základě poptávky uživatele, nebo v horším případě zanikne. Je otázkou, jak velká skupina lidí by musela přestat využívat např. služby Google, Microsoft, Facebook aj., aby to pro tyto společnosti nebylo marginální, nicméně právě v kyberprostoru mají uživatelé možnost přímo svým aktivním konáním či zdržením se konání ovlivnit fungování či nefungování jednotlivých služeb.

Lze tedy vyslovit tyto závěry:

§ **Kyberprostor je tvořen vůlí definičních autorit.**

§ **Všichni poskytovatelé služeb informační společnosti jsou definičními autoritami.**

§ **Každý poskytovatel služeb, jako jakýkoli jiný subjekt práva, je právně odpovědný za své jednání.**

Problematika odpovědnosti poskytovatelů služeb informační společnosti (ISP) dle zákona o některých službách informační společnosti je zde uváděna záměrně, neboť má přímý vztah k problematice kybernetické kriminality, odpovědnosti uživatelů a zjišťování a zajišťování informací podstatných pro trestní řízení. *„Obecně platí zásada, že je-li informace protiprávní a ISP neměl ani povědomosti o jejím vytvoření či komunikaci, je ISP zbaven odpovědnosti ze zákona.“*[7]

Pojem poskytovatel služby je mimo výše uvedeného zákona definován například i v Úmluvě o kyberkriminalitě, konkrétně v čl. 1 písm. c), kde je uvedeno, že poskytovatelem služby je:

§ jakýkoli veřejný nebo soukromý subjekt, **který uživatelům své služby umožňuje komunikovat prostřednictvím počítačového systému**, a

§ jakýkoli jiný subjekt, **který zpracovává nebo uchovává počítačová data pro takovou komunikační službu nebo pro uživatele takové služby.**

---

[1] Srov. POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 42 a násl., s. 88 a násl.

Do definičních norem je možné podřadit i **RFC** (*Request For Comments*). Byť se jedná o dokumenty mající spíše povahu doporučení než norem, tak jsou uživateli respektovány, jako by normami byly. RFC lze volně získat na adrese http://www.ietf.org/rfc.html.

[2] Doménové jméno slouží k označení „třídy“ počítačových systémů připojených k Internetu, které se vyznačují určitou geografickou a organizační jednotou: např. všechny počítače v doméně **.cz** se nalézají na území České republiky, všechny počítače v doméně (subdoméně) **nic.cz** jsou počítače pod správou sdružení CZ.NIC. Jména hlavních domén (vycházející z geografie) jsou pevně rozdělena.

Polčák k doménovým jménům mimo jiné uvádí, že: „Formou **virtuální reality** může být doménové jméno. To je záznamem v databázích DNS. **Pokud se doménová autorita rozhodne vymazat doménové jméno, přestane tato virtuální realita existovat.** Je jedno, jestli jde o doménové jméno např.: www.tondovy_stranky.cz, či o www.google.com.

[3] IETF - The Internet Engineering Task Force. Blíže viz: https://www.ietf.org/

[4] Vždy jde o fyzickou nebo právnickou osobu, která má sídlo či trvalé bydliště. Tudíž se na ně vztahuje právo jako na jakýkoli jiný subjekt. V některých zemích (např. **Čína**) je definiční autoritou sám stát.

[5] **Definiční normu** označuje Lessig jako **kód (code).**

[6] Srov. LESSIG, Lawrence. *Code v. 2. str.* 6 Dostupný v plném znění (Angl.) [online]. [cit.13.3.2008]. Dostupné z: http://pdf.codev2.cc/Lessig-Codev2.pdf

[7] POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 55

3.1. Regulace činnosti ISP v České republice

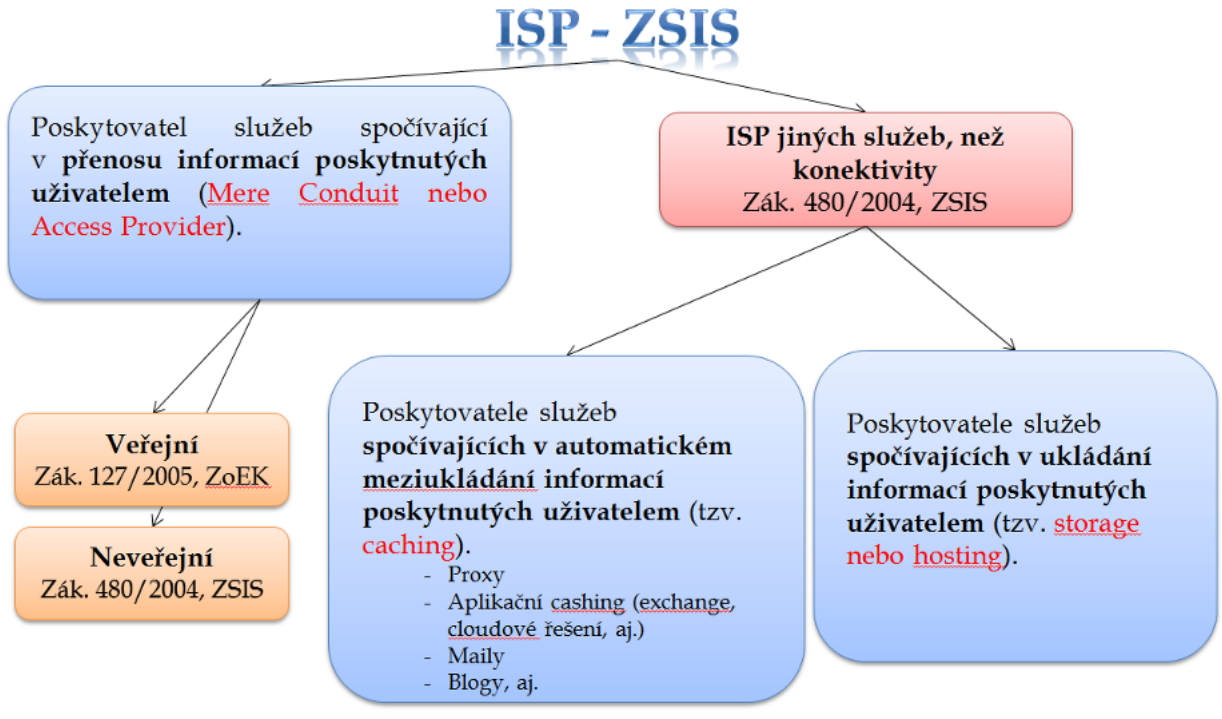
Základní právní normou charakterizující činnost ISP v České republice je zákon č. 480/2004 Sb., o některých službách informační společnosti[1]. Tento zákon je implementací Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.[2]

Český zákon o některých službách informační společnosti rozeznává následující tři poskytovatele služeb, přičemž stanoví, že poskytovatelem služby je každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti:[3]

1. **Poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem** (angl. Mere Conduit nebo Access Provider).
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).

Z výše uvedené definice není vyloučena žádná osoba (nemusí se jednat např. o osobu podnikající podle jiného právního předpisu), nicméně platí, že pokud se na poskytovatele vztahují další speciální předpisy (viz např. některý z poskytovatelů připojení), musí se jimi také řídit.

Graficky je možné uvedené poskytovatele (a vázanost jednotlivými právními předpisy znázornit následovně:



Příjemcem služby informační společnosti je pak uživatel, kterým může být každá fyzická nebo právnická osoba, která využívá službu informační společnosti, zejména za účelem vyhledání či zpřístupnění informací.[4]

Službou informační společnosti se dle zákona o některých službách informační společnosti rozumí *„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.“* ***[5]***

Definice uvedená v České právní úpravě pak přímo vychází ze Směrnice Evropského parlamentu a Rady (EU) 2015/1535 [čl. 1 písm. b)], která uvádí, že službou je *„jakákoli služba informační společnosti, tj. každá služba poskytovaná* ***zpravidla za úplatu, na dálku, electronicky*** *a* ***na individuální žádost příjemce služeb.“***

Z této definice vyplývají čtyři základní znaky služby:

- je poskytovaná elektronickými prostředky,
- je poskytována na individuální žádost uživatele,
- je běžně poskytována za odměnu,
- je poskytována distančně (na dálku).

Pojem poskytování pomocí **elektronických prostředků** je uveden ve Směrnici Evropského parlamentu a Rady (EU) 2015/1535 v čl. 1 písm. b) ii), kde je definováno, že se jedná o službu, která je odeslána z výchozího místa a je přijata v místě jejího určení prostřednictvím elektronického zařízení pro zpracování (včetně digitální komprese) a uchovávání dat. Tato služba je jako celek odeslána, přenesena nebo přijata drátově, rádiově, opticky nebo jinými elektromagnetickými prostředky. Česká úprava využívá demonstrativního výčtu, kde je uvedeno, že se jedná zejména o síť elektronických komunikací, elektronická komunikační zařízení, automatické volací a komunikační systémy, telekomunikační koncová zařízení a elektronickou poštu.[6]

Individuální žádost uživatele znamená, že se musí jednat o aktivní činnost ze strany uživatele. Husovec uvádí, že jde o případy, kdy například uživatel sám vpíše adresu do políčka prohlížeče (IE, Firefox, Chrome aj.), čímž formuluje žádost na otevření příslušné stránky, nebo napíše SMS zprávu. Typickým příkladem služby, která je poskytována bez individuální žádosti, pak podle Husovce je např. televizní vysílání.[7]

Nejproblematičtějším kritériem definice služby informační společnosti je, že tato **služba je poskytována za odměnu**. Česká úprava kopíruje i v tomto bodě úpravu mezinárodní a obsahuje ustanovení *„zpravidla za úplatu"*. V prostředí Internetu či jiných počítačových sítí existuje celá řada služeb, které jsou poskytovány „zdarma". Husovec zcela správně argumentuje tím, že pod pojmem odměna si je možné představit celou řadu skutečností odlišných od ryze peněžitého plnění.[8] Může se jednat o plnění, které bude mít podobu nepeněžitého charakteru, kdy ISP získá o uživatelích informace v podobě osobních, technických a jiných údajů, času stráveného užíváním dané služby, nabídne uživateli reklamu na jiné produkty atd. Nicméně i tato podmínka by měla dle Husovce být interpretována extenzivněji, a to tak, že je vyvíjena činnost *potenciálně ekonomická*.[9]

Díky tomu, že si pod pojmem úplata lze představit skutečně rozlišné možnosti (např. poděkování, návštěva stránky či odkazu, finanční či jiné plnění), a díky znění zákona o některých službách informační společnosti (viz *„zpravidla za úplatu"*) lze vyvodit závěr, že činnost poskytovatele služeb informační společnosti může být poskytována i zdarma.

Pojem **na dálku** definuje Směrnice Evropského parlamentu a Rady (EU) 2015/1535 jako službu, která je poskytována bez současné přítomnosti stran.[10]

Husovec ve své monografii dále uvádí příklady, které demonstrují, co vše lze považovat za službu informační společnosti. Pod tento pojem je třeba dle Směrnice 2000/31/ES Evropského parlamentu a Rady zařadit celou řadu činností, ke kterým dochází v online světě. Může se jednat o online prodej zboží, služby, které poskytují online informace, komerční komunikaci, či služby poskytující nástroje pro vyhledávání, přístup a získávání údajů, služby poskytující přenos informací prostřednictvím komunikační sítě aj.

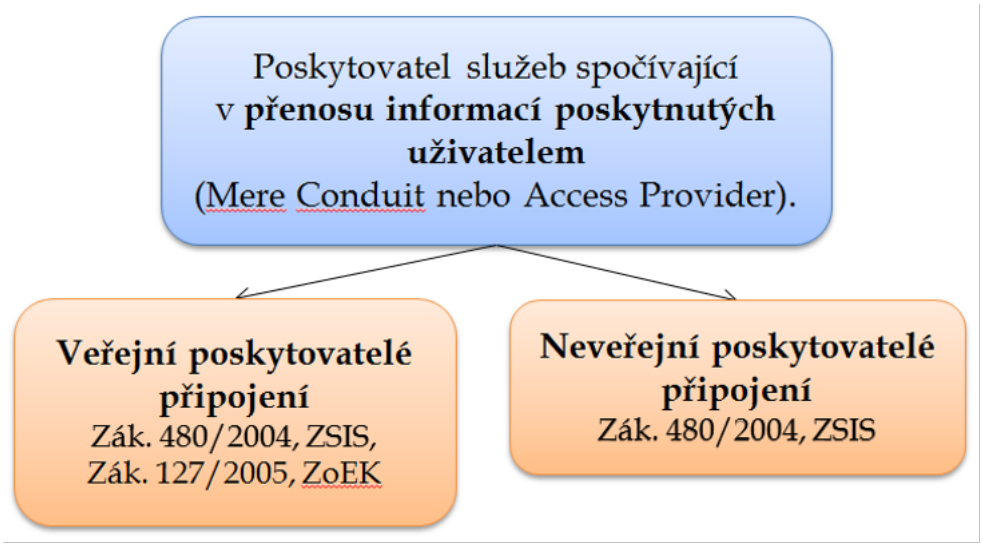
„Judikatura Soudního dvora EU již přímo či nepřímo uznala například službu AdWords (inzertní služba ve vyhledávači Google)[11]*, službu pojištění motorových vozidel přes Internet****[12]****, on-line prodej kontaktních čoček*[13]*, připojení se k Internetu*[14]*, rezervaci hotelu skrze email****[15]****, rezervaci služeb cestovní kanceláře skrze email*[16]*, aukční server eBay*[17]*a klasické vyhledávání od společnosti Google."* [18]

3.1.1 Poskytovatelé služeb spočívajících v přenosu informací poskytnutých uživatelem (Mere Conduit či Access Provider)

Z hlediska zákona o některých službách informační společnosti může být tímto poskytovatelem jakákoli fyzická či právnická osoba, která je schopna poskytovat jiným subjektům (fyzickým či právnickým osobám) službu přenosu informací (poskytnutých uživatelem) prostřednictvím sítí elektronických komunikací nebo ve zprostředkování přístupu k sítím elektronických komunikací za účelem přenosu informací.

Takovýmto poskytovatelem pak nebudou pouze osoby podnikající v oblasti připojování jiných k počítačovým sítím či do Internetu (typicky se bude jednat o osoby zapsané v *Evidenci podnikatelů v elektronických komunikacích podle všeobecného oprávnění*)[19], ale půjde o jakoukoli osobu poskytující či zprostředkovávající přenos informací prostřednictvím sítí elektronických komunikací. Lze si tedy představit situaci, kdy bude poskytovatelem připojení podle tohoto zákona i osoba, která zřídí a jiným zpřístupní například WiFi připojení v rámci restaurace, bytového domu, domácnosti aj. Stejně tak do této kategorie budou spadat například i školy (typicky vysoké školy poskytující svým studentům a učitelům konektivitu v rámci své sítě či do Internetu.). Službou spočívající v přenosu informací však je i např. aplikace Skype, ICQ aj. Velmi zjednodušeně můžeme označit tyto poskytovatele za **poskytovatele připojení.**

Z hlediska vymezení jednotlivých práv a povinností poskytovatelů připojení je nicméně třeba tyto poskytovatele rozdělit do dvou skupin, a to na poskytovatele **veřejné a neveřejné.** Na obě dvě skupiny poskytovatelů připojení se vztahuje zákon o některých službách informační společnosti, avšak na veřejné poskytovatele připojení se dále vztahuje zákon o elektronických komunikacích, který těmto poskytovatelům stanoví další práva a povinnosti.
K určení, zda je poskytovatel zařazen do té které skupiny pomůže výše uvedená *Evidence podnikatelů v elektronických komunikacích podle všeobecného oprávnění* spravovaná Českým telekomunikačním úřadem.



3.1.1.1 Práva a povinnosti poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem dle ZSIS

Zákon o některých službách informační společnosti v případě poskytovatele připojení v co možná největší míře omezuje odpovědnost tohoto subjektu za přenášené informace. Zvláštní požadavky a podmínky jsou však stanoveny vůči operátorům služeb elektronických komunikací. Tyto podmínky stanoví zákon o elektronických komunikacích. Ustanovení čl. 12 směrnice č. 2000/31/ES umožňuje členským státům nařídit Poskytovateli, aby přerušil poskytování služeb,

skrze něž dochází k přenosu informací, jež neoprávněně zasahují do práv jiného. Tato možnost je jedním z prostředků, jak zabránit protiprávnímu jednání. Příkaz k přerušení poskytování služeb zpravidla vydává soud.

Poskytovatele **připojení lze činit odpovědného za obsah informace** jen pokud:

§ přenos sám iniciuje,

§ zvolí uživatele přenášené informace, **nebo**

§ zvolí nebo změní obsah přenášené informace.[20]

Podle § 6 ZSIS **není poskytovatel připojení povinen** dohlížet na obsah přenášených informací, či aktivně zjišťovat protiprávnost přenášené informace. Poskytovatele nelze činit odpovědného za kvalitu informace (kterou mu nelze přičíst), a to i v případě, že si je vědom protiprávnosti přenášené informace.[21]

3.1.1.2 Práva a povinnosti poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem dle zák. č. 127/2005 Sb.

Veřejní poskytovatelé připojení se dále řídí zákonem č. 127/2005 Sb., o elektronických komunikacích[22]. Tento zákon definuje některé pojmy, které dále používá. Pro účely této monografie se jedná zejména o:

- **Službu elektronických komunikací** [§ 2 písm. n) ZoEK[23]]. Tímto pojmem se dle § 2 písm. n) ZoEK rozumí služba, která je obvykle poskytována za úplatu a spočívá (zcela nebo převážně) v přenosu signálů po sítích elektronických komunikací. Touto službou pak nejsou služby nabízející obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaný službami elektronických komunikací. Dále touto službou nejsou služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací.
- **Veřejně dostupnou službou elektronických komunikací** [§ 2 písm. o) ZoEK]. Touto službou je taková služba elektronických komunikací, z jejíhož využívání není nikdo předem vyloučen.

Nevyloučením se rozumí možnost uzavřít smlouvu s podnikatelem, jenž poskytuje veřejně dostupnou službu elektronických komunikací. Podstatné je, že tato služba je otevřena širokému okruhu lidí, z nichž není nikdo předem vyloučen. Opakem takovéto služby může být například členství v různých spolcích, komorách, či například status studenta školy.

- **Podnikatel**, který zajišťuje nebo je oprávněn zajišťovat veřejnou komunikační síť nebo přiřazené prostředky, je tímto zákonem označován za **operátor**a [§ 2 písm. e) ZoEK].
- **Účastníkem** [§ 2 písm. a) ZoEK] je každý, kdo uzavřel s podnikatelem poskytujícím veřejně dostupné služby elektronických komunikací smlouvu na poskytování těchto služeb. **Uživatelem** [§ 2 písm. n) ZoEK] je každý, kdo využívá nebo žádá veřejně dostupnou službu elektronických komunikací.

Zákon o elektronických komunikacích zavedl, na základě Směrnice Evropského parlamentu a Rady 2006/24/ES, ze dne 15. března 2006, *o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES* [24], povinnost preventivně uchovávat **provozní a lokalizační údaje**[25] o uskutečněné elektronické komunikaci. Tato povinnost se vztahuje pouze na podnikatele, který zajišťuje nebo je oprávněn zajišťovat veřejnou komunikační síť nebo přiřazené prostředky.

Účelem směrnice o Data Retention bylo **harmonizovat předpisy členských států týkající se povinnosti poskytovatelů veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí**, pokud jde o uchovávání provozních a lokalizačních údajů tak, aby se daly poskytovat příslušným orgánům členských států pro účely **prevence, vyšetřování, odhalování a stíhání závažné trestné činnosti, jako jsou terorismus a organizovaný zločin**

Rozsah směrnice byl stanoven na oblast provozních a lokalizačních údajů o právnických i fyzických osobách a na související údaje, které jsou nezbytné k identifikaci účastníka nebo registrovaného uživatele.

Tato směrnice se nevztahovala na obsah elektronických sdělení ani na informace vyžadované při použití sítě elektronických komunikací.

Členské státy byly dle Směrnice **povinny zajistit, aby se telekomunikační údaje uchovávaly po dobu nejméně šesti měsíců a nejvýše dvou let ode dne komunikace.** Uvedená směrnice byla v různých podobách transponována do právních řádů členských zemí EU. Nicméně už od jejího vzniku docházelo k názorovým střetům na směrnici jako takovou. Odpůrci namítali, že směrnice nepřiměřeným způsobem zasahuje do základních lidských práv a svobod, zejména tím, že de facto přikazuje plošné sbírání informací o jednotlivých uživatelích. Dále bylo argumentováno, že směrnice (v takto obecné podobě) by nebyla schopna projít testem proporcionality.

Test proporcionality je standardním právním nástrojem jak soudů mezinárodních, tak soudů ústavních (národních) v případě, že se posuzuje konflikt ustanovení právního řádu, sledující ochranu ústavně zaručeného práva či veřejného zájmu, s jiným základním právem či svobodou. Test proporcionality zahrnuje tři kritéria posuzování přípustnosti zásahu:

1. **Princip vhodnosti** (způsobilosti naplnění účelu), dle něhož **musí být příslušné opatření vůbec schopno dosáhnout zamýšleného cíle**, jímž je ochrana jiného základního práva nebo veřejného statku.
2. **Princip potřebnosti**, dle něhož **je povoleno použití pouze prostředku nejšetrnějšího k dosažení požadovaného účelu** (zásahu do základních práv a svobod), **z více možných prostředků.**
3. **Princip přiměřenosti** (v užším smyslu), dle kterého **újma na základním právu nesmí být nepřiměřená ve vztahu k zamýšlenému cíli**, tj. opatření omezující základní lidská práva a svobody nesmějí, jde-li o kolizi základního práva či svobody s veřejným zájmem, svými negativními důsledky přesahovat pozitiva, která představuje veřejný zájem na těchto opatřeních.

Směrnice o Data Retention, respektive její národní transpozice se staly předmětem ústavních žalob v některých zemích EU. Z těch nejvýznamnějších je třeba zmínit rozhodnutí ústavních soudů Rumunska (2009), Německa (2010) a České republiky (2011). Zaměřím se na rozhodnutí soudů v SRN a ČR.

Spolkový ústavní soud SRN, který řešil konflikt mezi svobodou a bezpečností (na základě směrnice o Data Retention) a vyslovil se ve prospěch svobody jednotlivce. Dne 2. března 2010 soud rozhodl, že hromadné uchovávání údajů o telefonických a datových přenosech je v Německu neústavní.

Soud tak reagoval na hromadnou stížnost 35 000 občanů, kteří žádali zrušení zákona z roku 2008, jenž telekomunikačním společnostem nařizoval archivovat záznamy o telefonických hovorech a e-mailové komunikaci po dobu šesti měsíců pro potřeby vyšetřovacích orgánů. Spolkový ústavní soud napadené předpisy jako neústavní zrušil. Dále uvedl, že povinnost uchovávat údaje ve stanoveném rozsahu sice není od samého počátku zcela protiústavní, chybí však zákonná úprava odpovídající zásadě přiměřenosti. Dle vyjádření soudu nebyly napadené předpisy v souladu s ústavněprávními požadavky na bezpečnost dat, nedošlo k jasnému vymezení účelu použití údajů (a transparentnosti použití údajů) a nebyla dostatečně zajištěna právní ochrana.

Soud uvedl, že *„využívání základních práv a svobod občanů (zde tajemství zpráv podávaných elektronickými komunikačními prostředky) nesmí být ze strany státu kompletně sledováno, dokumentováno a registrováno; to patří k ústavně právní identitě Spolkové republiky Německo, o jejíž zachování se republika musí zasazovat v evropských i mezinárodních souvislostech“.*[26]

V České republice došlo k implementaci směrnice o Data Retention ještě před její účinností v rámci EU (V EU byla implementována 15. března 2007, s požadavkem na transpozici do 15. září 2007. V ČR byla implementována do § 97/3 ZoEK, s účinností od 1. 5. 2005). I v ČR došlo k podání ústavní stížnosti, konkrétně sdružením Iuricum Remedium, kterou podpořila skupina 51 poslanců . Tato stížnost byla podána k Ústavnímu soudu v březnu 2010. V roce 2011 pak Ústavní soud rozhodl a zcela vyhověl návrhu na úplné zrušení příslušných pasáží zákona o elektronických komunikacích (konkrétně se jednalo o § 97 odst. 3 a 4) a prováděcí vyhlášky č. 485/2005 Sb., o rozsahu provozních a lokalizačních údajů a zrušení ustanovení trestního řádu.[27] Soud se vyjádřil následovně: *„Ústavní soud seznal, že napadená právní úprava porušuje ústavněprávní limity, neboť nesplňuje požadavky plynoucí z principu právního státu a je v kolizi s požadavky na omezení základního práva na soukromí v podobě práva na informační sebeurčení ve smyslu čl. 10 odst. 3 a čl. 13 Listiny, které plynou z principu proporcionality.“*

Legislativci v ČR reagovali na námitky Ústavního soudu ČR a byla přijata **nová právní úprava**, která v ČR nadále umožňuje plošné uchovávání provozních a lokalizačních údajů, neboť **respektuje** již dříve zmíněný **test proporcionality** zejména tím, že jasně deklaruje okruh subjektů (oprávněných provozní a lokalizační údaje vyžadovat) a účel pro který je možné údaje vyžadovat.

Zároveň byla přijata opatření, jež přikazují podnikatelům dle zákona o elektronických komunikacích přijmout taková pravidla, aby měly provozní a lokalizační údaje zajištěny stejnou kvalitu a podléhaly stejnému zabezpečení a ochraně před neoprávněným přístupem, změnou, zničením, ztrátou anebo odcizením nebo jiným neoprávněným zpracováním nebo využitím, jako údaje podle § 88 ZoEK.[28]

Byla také **stanovena maximální délka, po kterou je možné tyto údaje uchovávat, ta v současnosti činí 6 měsíců.** Po uplynutí této doby je právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, povinna je zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným k jejich využívání podle zvláštního právního předpisu nebo pokud zákon nestanoví jinak (§ 90 ZoEK). Dále byla stanovena **povinnost zajistit, aby při uchovávání provozních a lokalizačních údajů nebyl uchováván obsah zpráv a takto uchovávaný dále předáván** (§ 97 odst. 3 ZoEK).

Zároveň byla v trestním řádu zdůrazněna **zásada subsidiarity** (zejm. § 88 a 88a zák č. 141/1961 Sb., o trestním řízení soudním: *„nelze-li sledovaného účelu dosáhnout jinak, nebo bylo-li by jinak jeho dosažení podstatně ztížené“*). Garance minimální ingerence do základních lidských práv je v těchto případech dána mimo jiné i tím, že příkaz k vydání provozních a lokalizačních údajů vydává soudce na návrh státního zástupce.

Kdo a za jakých podmínek je tedy v ČR oprávněn žádat vydání provozních a lokalizačních údajů? Dle § 97 odst. 3 ZoEK je právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, na požádání povinna je bezodkladně poskytnout:

a) **orgánům činným v trestním řízení** pro účely a při splnění podmínek stanovených zvláštním právním předpisem[29],

b) **Policii České republiky** pro účely zahájeného **pátrání po konkrétní hledané nebo pohřešované osobě**, **zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby** a při splnění podmínek stanovených zvláštním právním předpisem[30],

c) **Bezpečnostní informační službě** pro účely a při splnění podmínek stanovených zvláštním právním předpisem[31],

d) **Vojenskému zpravodajství** pro účely a při splnění podmínek stanovených zvláštním právním předpisem[32],

e) **České národní bance** pro účely a při splnění podmínek stanovených zvláštním právním předpisem[61)] [33].

V rámci Evropské unie pak soudní dvůr EU (dne 8. 4. 2014) po předchozím stanovisku[34] svého generálního advokáta Pedra Cruze Villalóna vynesl verdikt[35], v jehož rámci **zneplatnil příslušnou směrnici o data retention (2006/24/ES).**

„Dnešním rozsudkem prohlašuje Soudní dvůr směrnici za neplatnou.“

„Vzhledem k tomu, že Soudní dvůr neomezil časové účinky rozsudku, je prohlášení neplatnosti účinné ode dne, kdy směrnice vstoupila v platnost“.

Soudní dvůr EU zejména vytýkal tu skutečnost, že *„unijní zákonodárce překročil přijetím směrnice o uchovávání provozních údajů hranice vymezené požadavkem na dodržování zásady proporcionality.“*

Rozhodnutí spočívající v ponechání či zrušení platných legislativ, které řeší uchovávání provozních a lokalizačních údajů v členských státech EU, je plně na příslušných národních orgánech a samotná Unie jim nehodlá ani doporučovat či dávat nějaké vodítko ohledně toho, jak se mají zachovat.[36]

Jak se postavit k plošnému uchovávání provozních a lokalizačních údajů? Osobně se domnívám, že v kyberprostoru není možné jiným způsobem zrekonstruovat události, které se odehrály v minulosti, než tak, že budou uchovávány provozní a lokalizační údaje. Kyberprostor a ICT, které umožňují velmi rychlou změnu topologie sítě, služeb aj. technologie, které umožňují získání několika různých identit v rámci jednotek sekund vlastně ani jinou možnost nepřipouští.

Uvědomuji si, že plošné uchovávání provozních a lokalizačních údajů zasahuje do mých základních práv a svobod, nicméně tím, že jsem přijal koncepci společenské smlouvy a vzdal jsem se části svých práv a svobod ve prospěch autority (v našem případě státu), která má zajistit ochranu moji a mých práv, vlastně ani jinou možnost nemám. Domnívám se, že pokud chceme efektivně prověřovat a vyšetřovat kybernetickou trestnou činnost, kybernetické útoky a jiné negativní jevy, jež se odehrávají v kyberprostoru, tak se bez tohoto nástroje neobejdeme. Otázka, kterou bychom měli řešit, by neměla znít: *„Jak omezit sbírání údajů a dat o osobách v kyberprostoru (neboť toto se na zcela jiných úrovních děje), a tím omezit možnosti státu řešit negativní jevy v kyberprostoru?“* Otázky, které jsou zcela legitimní a které by měly být řešeny, jsou: *„Jak nastavit pravidla, komu a za jakých podmínek povolit přístup k těmto údajům, co se s těmito údaji děje, pro jaké účely mohou být využívány, atd.“*

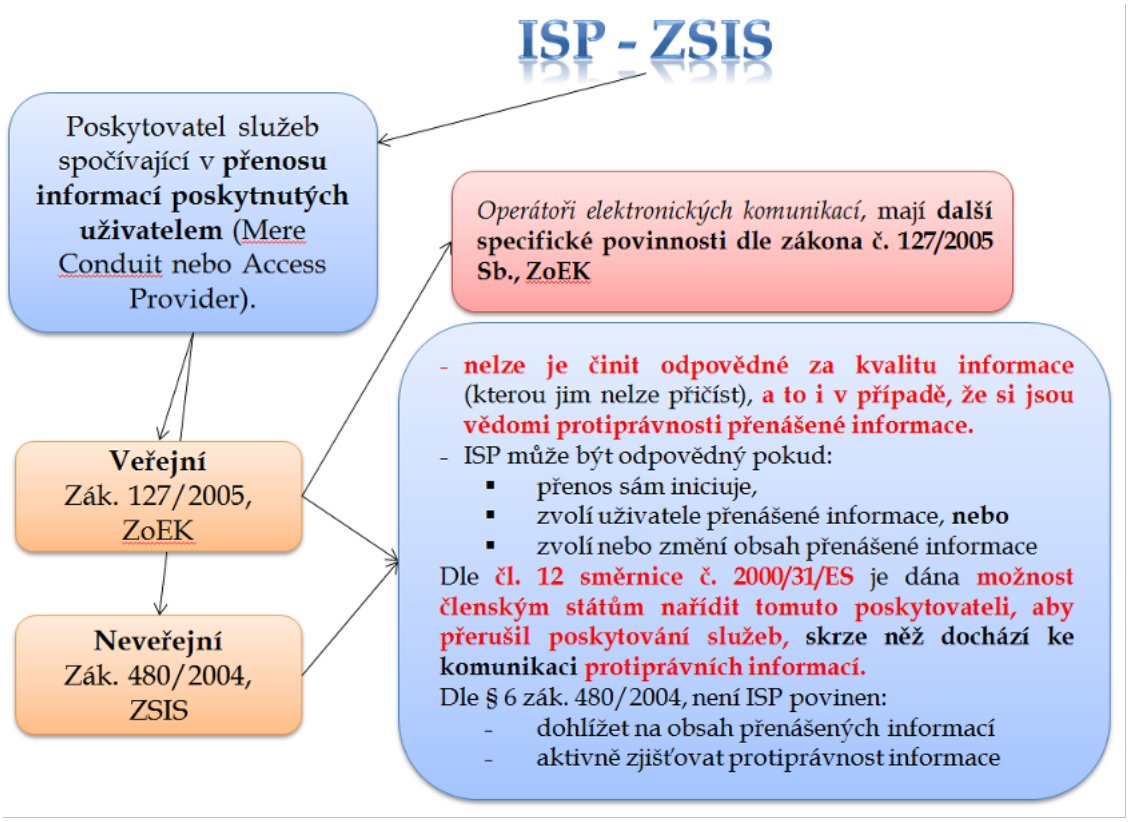
Osobně jsem přesvědčen o tom, že podobné údaje by neměli uchovávat pouze veřejní poskytovatelé připojení, ale všichni ISP, kteří poskytují nějakou službu. Důvodů pro toto tvrzení mám několik.

Za prvé se domnívám, že ostatní služby, než ty, jež spočívají v poskytnutí připojení, jsou a do budoucna budou majoritními službami v kyberprostoru. Uživatel tak přestává řešit otázku, kdo a jakým způsobem ho připojuje, a primárně se věnuje službám, které mohou mít například i podobu virtuálního propojení do různých virtuálních prostředí. Významné tedy nebude samo fyzické propojení, jako propojování mezi jednotlivými službami.

Druhým důvodem je ta skutečnost, že v současnosti již ze strany poskytovatelů těchto služeb dochází v drtivé většině k uchovávání ne jen provozních a lokalizačních údajů, ale celé řady dalších údajů, které jim uživatelé dovolí uchovávat na základě smluvních podmínek uzavřených mezi ISP a koncovým uživatelem.

Posledním důvodem je vlastní ochrana ISP před uživateli. Poskytovatel služby musí respektovat právo a je v jeho nejlepším zájmu uchovávat údaje, které by ho mohly případně zprostit odpovědnosti například za škodu, či jinou újmu.

K uchovávání provozních a lokalizačních údajů se nedávno vyjádřil i generální advokát[37], který konstatoval, že data retention představuje v mnoha případech jediný účinný nástroj k řešení bezpečnostních rizik a závažné trestné činnosti. Současně formuloval požadavky na jeho proporcionální implementaci v právních řádech členských států.



Grafické znázornění rozdělení poskytovatelů připojení a některých jejich práv a povinností

3.1.2 Poskytovatelé služeb spočívajících v automatickém meziukládání informací poskytnutých uživatelem (tzv. caching)

Caching spočívá v přenosu informací, při němž dochází automaticky dočasně k jejich meziuložení. Následně je tato informace přenesena příjemci služby na jejich žádost.

„Caching je v podstate špecialnou upravou služby mere conduit, keďže aj ten zahŕňa prenos s prechodnym medzi-uložením informacii. Jediny rozdiel, v ktorom by služba caching mohla vybočovať z ramca široko koncipovanej mere conduit je to, že ukladanie pri prenose je vykonane na „dobu dlhšiu, ako je primerane nutne na prenos".[38]

Husovec dále velmi výstižně popisuje služby cachingu na příkladu proxy serveru či browseru cachingu, které urychlují načítání webových stránek. Příjemcem služby je majitel webové stránky deníku (tzv. primární příjemce), jehož obrázky si poskytovatel cachingu uloží na geograficky bližším počítači (např. v Evropě), aby nemusel neustále přistupovat na počítač, kde je v originále webová stránka uložena (např. Afrika), čímž se urychlí celkové načítání stránky (v Evropě). Uživatel, který jde webovou stránku navštívit a je dalším příjemcem služby (tzv. sekundární příjemce), tak na základě individuální žádosti adresované poskytovateli služby cachingu získá obrázek z jeho počítače a není nucen „cestovat" na počítač originální.[39]

Poskytovatelé cachingu nejsou zbaveni odpovědnosti za kvalitu informací, pokud dojde z jejich strany k porušení standardních či smluvených technických podmínek cachingu.[40]

Poskytovatel cachingu je dle § 4 ZSIS odpovědný v případě, že:

a) změní obsah informace,

b) nevyhoví podmínkám přístupu k informaci,

c) nedodržuje pravidla o aktualizaci informace, která jsou obecně uznávána a používána v příslušném odvětví,

d) překročí povolené používání technologie obecně uznávané a používané v příslušném odvětví s cílem získat údaje o užívání informace, nebo

e) ihned nepřijme opatření vedoucí k odstranění jím uložené informace nebo ke znemožnění přístupu k ní, jakmile zjistí, že informace byla na výchozím místě přenosu ze sítě odstraněna nebo k ní byl znemožněn přístup nebo soud nařídil stažení či znemožnění přístupu k této informaci.

Poskytovatel cachingu nemá povinnost aktivně vyhledávat skutečnosti a okolnosti poukazující na protiprávní obsah informace či dohlížet na obsah jimi přenášených nebo ukládaných informací.

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

Poskytováním storage nebo hostingu se rozumí zpřístupnění úložiště (prostoru) uživateli, aby si tam mohl umístit data. Ukládání informací, resp. dat, na rozdíl od mere confuit či cachingu, není pouze dočasné. Mezi služby hostingu je možné zařadit:

a) Webhosting (Active 24, Ignum, Zoner aj.)

b) Cloudová úložiště umožňující ukládání jakýchkoli souborů a dat (Dropbox, iCloud, Microsoft OneDrive, ownCloud aj.)

c) Úložiště souborů (Rapidshare, DropBox aj.)

d) Úložiště videí (YouTube aj.)

e) Úložiště zvukových souborů (iTunes aj.)

f) Služby internetových aukcí (eBay aj.)

g) Blogy, fóra, diskusní chaty aj.

h) Sociální sítě (Facebook, Twitter aj.).

Uvedený výčet není konečný, v rámci hostingu může být poskytována celá řada dalších služeb.

U poskytovatelů hostingu je situace s jejich případnou právní odpovědností nejsložitější.[41] Opět se vychází z ustanovení směrnice č. 2000/31/ES, jejíž doporučení přejal český zákonodárce do § 5 ZSIS. V tomto ustanovení je dána podmínka alespoň nevědomé nedbalosti[42] poskytovatele ve vztahu k protiprávnímu obsahu informace u něj uložené. **Zákonodárce** však **neukládá poskytovatelům povinnost aktivně vyhledávat protiprávní informace uživatelů**[43] (neboť by v mnohých případech šlo de facto o zásah do základních práv a svobod zaručených Listinou - např. čl. 13) či dohlížet na obsah přenášených nebo ukládaných informací.

Poskytovatel hostingu je dle § 5 odst. 1 ZSIS odpovědný v případě, že:

a) ***mohl vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní****, nebo*

b) ***dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele*** *a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.*

Poskytovatel hostingu je vždy odpovědný za obsah uložených informací v případě, že vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele.[44]

Pro účely této monografie byly vybrány pouze určité aspekty, které se vztahují k poskytovatelům služeb informační společnosti, zejména s ohledem na využitelnost informací v rámci odhalování a vyšetřování kybernetické kriminality a kybernetických útoků.

---

[1] Dále jen zákon o některých službách informační společnosti či ZSIS

[2] Dostupný online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L1535&qid=1624364501265

[3] Viz § 2 písm. d) ZSIS

[4] Viz § 2 písm e) ZSIS

[5] § 2 písm. a) ZSIS

[6] Viz § 2 písm. c) ZSIS

[7] Blíže viz HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014, s. 100

[8] Tamtéž viz s. 98

[9] Tamtéž s. 99

[10] Viz čl. čl. 1 písm. b) i) této směrnice.

[11] Rozhodnutie *Google France* C-236/08 až C-238/08.

[12] Rozhodnutie *Bundesverband* C-298/07.

[13] Rozhodnutie *Ker-Optika* C-108/09.

[14] Rozhodnutie *Promusicae* C-275/06 a *Tele 2*. C-557/07

[15] Rozhodnutie *Alpenhof* C-144/09.

[16] Rozhodnutie *Pammer* C-585/08.

[17] Rozhodnutie *L'Oreal v. Ebay* 324/09.

[18] HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014. ISBN: 978-80-904248-8-3, s. 101-102.

[19] Databáze podnikatelů v elektronických komunikacích podle všeobecného oprávnění je dostupná online: https://www.ctu.cz/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni

[20] Tyto tři možnosti činí poskytovatele připojení odpovědného de facto pouze v případě, že je sám subjektem, který aktivně odesílá, či jinak manipuluje s přenášenými informacemi.

[21] Srov. čl. 12 směrnice č. 2000/31/ES a ust. § 3 odst. 1, 2 zák. č. 480/2004 Sb.

[22] Dále jen ZoEK

[23] Dále jen ZoEK

[24] Dále jen směrnice o **Data Retention.** Pojem data retention znamená plošné ukládání provozních a lokalizačních údajů u poskytovatelů připojení (v ČR u poskytovatelů dle zákona o elektronických komunikacích).

[25] Viz § 97 odst. 4 ZoEK.

Provozními a lokalizačními údaji jsou zejména **údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace** a dále **údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace.**

Rozsah provozních a lokalizačních údajů, forma a způsob jejich předávání orgánům oprávněným k využívání podle zvláštního právního předpisu (viz § 97 odst. 3 ZoEK) a způsob jejich likvidace stanoví prováděcí právní předpis. Prováděcím předpisem je **vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.**

[26] *German Federal Constitutional Court rejects data retention law.* [online]. [cit.16.7.2016]. Dostupné z: https://edri.org/edrigramnumber8-5german-decision-data-retention-unconstitutional/

Srov dále např.:

National legal challenges to the Data Retention Directive. [online]. [cit.16.7.2016]. Dostupné z: https://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html

Data retention unconstitutional in its present form. [online]. [cit.16.7.2016]. Dostupné z: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html?nn=5404690

German Bundestag Passes New Data Retention Law. [online]. [cit.16.7.2016]. Dostupné z: http://www.gppi.net/publications/global-internet-politics/article/german-bundestag-passes-new-data-retention-law/

[27] Viz Nález Ústavního soudu Pl. ÚS ÚS 41/11, ze dne 22. 3. 2011. *Shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu.* [online]. [cit. 24. 8. 2016]. Dostupné z: http://nalus.usoud.cz/Search/ResultDetail.aspx?id=69635&pos=1&cnt=4&typ=result

[28] Blíže viz § 88a ZoEK

[29] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů.

[30] Zákon č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů.

Zákon č. 137/2001 Sb., o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů.

[31] § 6 až 8 zákona č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů.

[32] § 9 a 10 zákona č. 289/2005 Sb., o Vojenském zpravodajství.

[33] Zákon č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů.

[34] Stanovisko Generálního advokáta Pedra Cruz Villalóna. Věc C-293/12 a C-594/12. [online]. [cit.15.7.2016]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=727954

[35] Soudní dvůr Evropské unie. Tisková zpráva č. 54/14, ze dne 8. 4. 2014. **Rozsudek ve spojených věcech C-293/12 a C-594/12.** [online]. [cit.15.7.2016]. Dostupné z: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054cs.pdf

[36] PETERKA, Jiří. *Uchovávat provozní a lokalizační údaje nám už EU nenařizuje. My to v tom ale pokračujeme.* [online]. [cit. 10. 11. 2015]. Dostupné z: http://www.earchiv.cz/b14/b0428001.php3

[37] Stanovisko Generálního advokáta SAUGMANDSGAARD ØE, ze dne 19. 7. 2016. Ve spojených věcech C-203/15 a C-698/15. [online]. [cit.10.8.2016]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=111650

[38] viz HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014, s. 133

[39] Tamtéž s. 133

[40] Srov. čl. 13 směrnice č. 2000/31/ES a ust. § 4 ZSIS

Srov. POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 58

[41] Srov. čl. 14 směrnice č. 2000/31/ES a ust. § 5 ZSIS

[42] Srov. ust. § 16 odst. 1 písm. b) TZK.

[43] Srov. čl. 15 směrnice č. 2000/31/ES a ust. § 6 ZSIS

[44] § 5 odst. 2 ZSIS

3.2. Možnosti právní odpovědnosti uživatele za jednání v kyberprostoru

Řada uživatelů informačních a komunikačních systémů si neuvědomuje svoji případnou odpovědnost za zneužití těchto technologií.[1] Informační a komunikační systémy jsou věcí a ten, kdo s nimi disponuje, je povinen si **počínat při svém konání tak, aby nedošlo k nedůvodné újmě na svobodě, životě, zdraví nebo na vlastnictví jiného.**[2]

Pokud **škůdce způsobí poškozenému újmu, úmyslným porušením dobrých mravů, je povinen ji nahradit;** vykonává-li však své právo, je škůdce povinen škodu nahradit, jen sledoval-li jako hlavní účel poškození jiného.[3]

Z této dikce občanského zákoníku tak jednoznačně vyplývá jednak povinnost řádně spravovat informační a komunikační systémy, stejně jako povinnost předcházet škodám, které by z jeho činnosti (tedy i užívání ICT v prostředí Internetu) mohla vzniknout.

Řada běžných uživatelů podceňuje ochranu a zabezpečení prostředků ICT, jimiž disponují, ať již z nedbalosti či úmyslně.

Určení formy zavinění u jednání koncového uživatele má rozhodující význam pro možnou občansko, či trestněprávní odpovědnost. Toto tvrzení je možné demonstrovat na třech ilustrativních případech z praxe.

> *Uživatel osobního počítače využíval nelegální kopii operačního systému Windows 7, přičemž tento systém úmyslně neaktualizoval. Uživatel úmyslně nainstaloval do počítače programy, které umožňovaly manipulaci s tímto počítačem třetím osobám, bez jeho další součinnosti.*

Smyslem činnosti výše popsaného uživatele bylo zprostit se případné trestněprávní odpovědnosti za útok provedený prostřednictvím takto připraveného počítače jinou osobou (např. počítač je úmyslně součástí sítě botnet).

V praxi je možné se setkat právě s útočníky, kteří svoji obhajobu staví na faktu, že oni nebyli tou osobou, která provedla prostřednictvím daného počítače konkrétní útok.

Vyvinění se tvrzením, že daná osoba není přímým útočníkem a svým jednáním konkrétní útok nezpůsobila, není dle mého názoru možné, respektive není možné toto tvrzení přijmout absolutně.

Z hlediska trestního práva by v úvahu mohlo přicházet minimálně uplatnění institutu účastenství a zásady akcesority účastenství[4], neboť jednání osoby, která umožnila nebo usnadnila jinému spáchání trestného činu (zejména **opatřením prostředků**, **odstraněním překážek**, vylákáním poškozeného na místo činu, hlídáním při činu, radou, utvrzováním v předsevzetí nebo slibem přispět po trestném činu) je možné subsumovat pod ustanovení o pomocníkovi.[5] Opatřením prostředků by se v tomto případě rozumělo i zpřístupnění počítačového systému, či jeho části ke spáchání úmyslného trestného činu.

Pokud by byla prokázána vyšší míra přímé účasti uživatele na protiprávním jednání jiné osoby, bylo by možné takovéhoto uživatele považovat případně i za spolupachatele[6] trestného činu. Rozhodující by byla míra informovanosti o využívání daného počítače k protiprávnímu činu a dále pak srozumění s tím, že touto činností může dojít k porušení nebo ohrožení zájmů chráněného trestním zákonem.[7]

Z hlediska občanského práva by pak jednání takového uživatele bylo jednak možné subsumovat pod § 2909 OZ, případně by bylo možné využít i § 2915 OZ, který upravuje případ, kdy je škoda způsobena několika osobami. Toto ustanovení stanoví, že: *„je-li k náhradě zavázáno několik škůdců, nahradí škodu společně a nerozdílně; je-li některý ze škůdců povinen podle jiného zákona k náhradě jen do určité výše, je zavázán s ostatními škůdci společně a nerozdílně v tomto rozsahu.* ***To platí i v případě, že se více osob dopustí samostatných protiprávních činů, z nichž mohl každý způsobit škodlivý následek s pravděpodobností blížící se jistotě, a nelze-li určit, která osoba škodu způsobila.***“ Právě větu druhou § 2915 odst. 1) OZ lze, dle mého názoru, velmi dobře aplikovat na výše popsaný případ.

> *Uživatel osobního počítače využíval nelegální kopii operačního systému Windows 7, přičemž tento systém úmyslně neaktualizoval. V počítači měl nainstalovánu řadu her a jiných aplikací, u nichž došlo k porušení práv autorských zejména tím, že byly obcházeny či potlačovány prvky jejich ochrany a k instalaci bylo využito keygenů či cracků[8], které však v sobě obsahovaly malware jiných útočníků. Uživatel si nebyl vědom té skutečnosti, že jeho počítač je využíván jinými uživateli.*

V praxi se jedná o nejčastější případ, při němž dochází ke zneužití počítače bez vědomí jeho oprávněného uživatele, i když tento svým protiprávním jednáním (zejména porušování práva autorského) či z prosté neznalosti výpočetní techniky zapříčinil stav, že jeho počítač je zneužit k útoku na třetí osoby.

Z hlediska trestního práva není v tomto případě možné využít institutu účastenství a zásady akcesority účastenství, neboť jednání osoby, která umožnila nebo usnadnila jinému spáchání trestného činu, nebylo úmyslné, tudíž nesměřovalo k pomoci hlavnímu pachateli trestného činu.

Z hlediska zavinění by bylo na uživatele takto napadeného počítače možné aplikovat ustanovení týkající se nedbalosti nevědomé, neboť pachatel nevěděl, že svým jednáním může způsobit porušení nebo ohrožení zájmu chráněného trestním zákonem, ač o tom vzhledem k okolnostem a k svým osobním poměrům vědět měl a mohl.[9]

Vzhledem k tomu, že v trestním zákoníku neexistuje nedbalostní skutková podstata trestného činu dle § 230 TZK: *Neoprávněný přístup k počítačovému systému a nosiči informací*, nebude možné využít v tomto konkrétním případu institutů trestního práva.

Z hlediska občanského práva by pak jednání takového uživatele, bylo možné subsumovat pod § 2912 odst. 1 OZ: *„Nejedná-li škůdce, jak lze od osoby průměrných vlastností v soukromém styku důvodně očekávat, má se za to, že jedná nedbale.“* V této souvislosti je třeba připomenout, že ten, kdo škodu způsobil (škůdce), je povinen škodu nahradit, a to bez ohledu na své zavinění v případech stanovených zvlášť zákonem.[10]

> *Uživatel o svůj počítač adekvátně „pečuje“ (má legální software, aktualizuje jej aj.) a rozumně jej zabezpečil (používá antivirovou, antispamovou a antimalware ochranu a kontrolu), a přesto byl tento počítač napaden zvenčí, (např. zapojen do botnetu) a následně využit k útoku proti jinému.*

Domnívám se, že z hlediska zavinění by v tomto případě nebylo možné na uživatele takto napadeného počítače aplikovat ani ustanovení týkající se nedbalosti nevědomé. Vzhledem k proaktivní činnosti uživatele pak nepřichází v úvahu ani aplikace § 232 TZK: *Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti*, neboť v tomto ustanovení je vyžadována hrubá nedbalost.[11]

Z hlediska občanského práva by pak jednání takového uživatele dle mého názoru nebylo možné subsumovat pod dříve uvedený § 2912 odst. 1 OZ, neboť v tomto případě jednal uživatel tak, jak od něj lze spravedlivě požadovat. Toto je však třeba chápat šířeji, neboť pokud se uživatel dozví, že jeho prostředky ICT jsou zneužity k protiprávnímu útoku na jiného, je povinen toto bez zbytečného odkladu oznámit osobě, které z toho může újma vzniknout[12], a upozornit ji na možné následky. Splní-li oznamovací povinnost, nemá poškozený právo na náhradu té újmy, které mohl po oznámení zabránit.[13]

V konkrétním případu vždy bude záležet na všech okolnostech případu a povinnost náhrady škody je oprávněn stanovit pouze soud.

Na druhou stranu, pokud se uživatel o počítač „nestará" (tj. nezabezpečí jej, neprovádí údržbu aj.) a ten bude následně zneužit, je reálné, že soud v řízení o náhradě škody určí takovémuto uživateli povinnost částečně či zcela (např. dojde k využití výpočetního výkonu jednoho datového centra) saturovat poškozenému škodu, která mu byla prostřednictvím počítače uživatele způsobena.

---

[1] Pro tuto část textu byly použity teze, jež byly částečně uveřejněny v článku: KOLOUCH, Jan a Andrea KROPÁČOVÁ. Liability for Own Device and Data and Applications Stored therein. In: *Advances in Information Science and Applications Volume I: Proceedings of the 18th International Conference on Computers (part of CSCC '14)*. [B.m.], c2014, s. 321 – 324. Recent Advances in Computer Engineering Series, 22. ISBN 978-1-61804-236-1 ISSN 1790-5109.

[2] § 2900 OZ

[3] § 2909 a násl. OZ

[4] Jedná se o zásadu závislosti trestní odopovědnosti a trestnosti účastníka (viz § 24 TZK) na trestní odpovědnosti a trestnosti hlavního pachatele (viz § 22 TZK), za podmínky, že se hlavní pachatel dospustil alespoň pokusu trestného činu, na němž se účastník podílel.

[5] Za podmínky domluvy (dohody) účastníka a hlavního pachatele. Viz § 24 odst. 1 písm. c) TZK

[6] Viz § 23 TZK

[7] Viz § 15 odst. 1 písm. b) TZK

[8] Jde o zásahy do programů jinými osobami za účelem modifikace směřující ke snadnějšímu spuštění (keygenů), ochromení ochrany programu, která zabraňuje jeho kopírování či spuštění za předem daných podmínek (cracky) a další přepracovávání těchto programů směřující k následnému užívání, případně distribuci dalším osobám.

[9] Viz § 16 odst. 1 písm. b) TZK

[10] Viz § 2895 OZ

[11] Viz § 16 odst. 2 TZK: *„Trestný čin je spáchán z hrubé nedbalosti, jestliže přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem."*

[12] Je otázkou, zda je možné takovouto osobu v daný okamžik (okamžik útoku) reálně určit.

[13] Viz § 2092 OZ

3.3. SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

ℹ️

SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

- Na tvorbě práva na Internetu, na omezování či rozšiřování jeho aktivit, se podílejí definiční autority tvorbou definičních norem.
- Definiční normy jsou vytvářeny a implementovány subjekty, které jsou oprávněny definovat prostředí informační sítě. Jde de facto o normy *sui generis*, které vymezují informační sítě jako takové. Vyskytují se ve vrstvách, které jsou na sobě závislé. *„Definiční normy jsou vytvářeny telekomunikačními operátory, producenty kancelářského softwaru, ale i například tvůrci, či provozovateli online her, nebo každý, kdo si otevře blog, nebo kdo má emailovou schránku (definiční norma vytvořená uživatelem této schránky je například filtr, který automaticky provádí nastavenou operaci s doručenou poštou).“*
- Definiční autority jsou původci definičních norem, jde o subjekt, který svým fungováním vytváří pravidla fungování logického systému, ve kterém autorita působí. Jak již bylo uvedeno dříve, má mezi těmito autoritami výsostné postavení ICANN, neboť této organizaci přísluší přidělování, správa a stanovení pravidel pro systém doménových jmen. Další definiční autoritou je například IETF. Byť se definiční autority mohou jevit jako neomezení správci kyberprostoru, stále jsou subjektem práva některého státu.
- Internet existuje právě jen díky definičním autoritám. Je z nich složen. Žádná operace se neuskuteční bez účasti (provedení či zprostředkování operace) definiční autority.
- Kyberprostor je tvořen vůlí definičních autorit.
- Všichni poskytovatelé služeb informační společnosti jsou definičními autoritami.
- Každý poskytovatel služeb, jako jakýkoli jiný subjekt práva, je právně odpovědný za své jednání.
- Pojem ISP je definován i v Úmluvě o kyberkriminalitě, konkrétně v čl. 1 písm. c), kde je uvedeno, že poskytovatelem služby je:
  - jakýkoli veřejný nebo soukromý subjekt, který uživatelům své služby umožňuje komunikovat prostřednictvím počítačového systému, a
  - jakýkoli jiný subjekt, který zpracovává nebo uchovává počítačová data pro takovou komunikační službu nebo pro uživatele takové služby.
- Český zákon o některých službách informační společnosti rozeznává následující tři poskytovatele služeb, přičemž stanoví, že poskytovatelem služby je každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti:[1]
  - Poskytovatele služeb spočívajících v přenosu informací poskytnutých uživatelem (angl. Mere Conduit nebo Access Provider).
  - Poskytovatele služeb spočívajících v automatickém mezi ukládání informací poskytnutých uživatelem (tzv. caching).
  - Poskytovatele služeb spočívajících v ukládání informací poskytnutých uživatelem (tzv. storage nebo hosting).

---

[1] Viz § 2 písm. d) ZSIS

🗝️

KLÍČOVÁ SLOVA K ZAPAMATOVÁNÍ

- ISP
- Definiční autorita
- Definiční norma
- Mere Conduit nebo Access Provider
- Cashing provider
- Hosting provider
- Data retention

❓

KONTROLNÍ OTÁZKY

- Definujte pojem ISP.
- Jak se dělí ISP? Dle jakých kritérií.
- Jaké povinnosti mají ISP?
- Co je to definiční norma?
- Kdo je definiční autoritou a jakou má roli?
- Co to je data retention?

4. Kybernetická bezpečnost a její právní úprava

Snahy o řešení problematiky kybernetické bezpečnosti je možné vypozorovat de facto již od počátku využívání informačních a komunikačních technologií. Postupně v této oblasti docházelo k přijímání doporučení, standardů, či technických norem, které zpravidla definovaly minimální požadavky zaručující určitou úroveň bezpečnosti.

Důvodů pro zavádění a implementaci kybernetické bezpečnosti existuje celá řada. Mezi ty nejběžnější je možné zařadit například negativní ekonomický dopad v případě úspěšného kybernetického útoku, při kterém jsou zcizena citlivá data. Úspěšný kybernetický útok také může ohrozit vlastní chod a fungování organizace, neboť může dojít například k omezení přístupu k počítačovým systémům nebo datům pomocí ransomware. Dalším z důvodů pro zavedení kybernetické bezpečnosti také může být i ztráta kredibility dané napadené organizace aj.

Posledním, avšak o nic méně významným důvodem pro implementaci kybernetické bezpečnosti je respektování právních předpisů a práv a povinností z těchto předpisů vyplývajících. Tento legislativní důvod pro mnoho subjektů vyplývá ze zákona o kybernetické bezpečnosti, je však mylné se domnívat, že se jedná o jedinou právní normu, která souvisí s problematikou kybernetické bezpečnosti.

Zejména v posledních letech dochází k masivnímu nárůstu primárně mezinárodní právní úpravy, která se specificky zaměřuje na činnost subjektů (fyzických, právnických osob či států a dalších organizací) v kyberprostoru.

Oblast kybernetické bezpečnosti se značně liší od jiných oblastí, na které jsou aplikovány standardní principy bezpečnosti ve světě reálném. Ona odlišnost spočívá především v možnosti dynamického vývoje a okamžité změny kybernetických útoků a hrozeb (většina hrozeb ve světě reálném zůstává relativně neměnná), což ve vztahu k legislativě může přinášet určité problémy. Právní regulace této oblasti musí být na jednu stranu dostatečně obecná, aby umožňovala efektivně reagovat na dílčí negativní kybernetické jevy bez nutnosti jejich detailní specifikace, na druhou stranu však nesmí být příliš vágní, aby nezasáhla do práv a oprávněných zájmů osob ve větší míře, než je nezbytně nutné.

Před vlastní analýzou stávající platné a účinné legislativy v oblasti kybernetické bezpečnosti je třeba podotknout, že nejen v rámci Evropské unie je zřetelná snaha po implementaci účinnějších právních nástrojů, které by zvyšovaly kvalitu kybernetické bezpečnosti a umožnily adekvátně reagovat na kybernetické hrozby a útoky. V současnosti dochází k postupnému odstraňování rozporů a nedostatků v právních normách členských států EU a dalších států, které se rozhodly aktivně zapojit do vytváření kybernetické bezpečnosti.

*„**Způsoby ochrany dat a informačních systémů jsou dnes předmětem nejednoho vědního výzkumu, ovšem toliko technická ochrana těchto systémů a dat bez právního podkladu může být neefektivní v důsledku nejasného vymezení, kam až je možno při takové ochraně zajít.** V tomto kontextu se naplno projevuje nesoulad právních úprav jednotlivých států s právními úpravami států ostatních. Díky rozvoji počítačových a informačních technologií, které udávají mezinárodní charakter kybernetických trestných činů, je efektivní ochrana počítačových systémů a dat nemyslitelná bez existence mezinárodního resp. nadnárodního právního rámce, a to nejen mezi členskými státy EU, ale v celosvětovém měřítku.“* [1]

Tato kapitola se bude věnovat legislativnímu rámci kybernetické bezpečnosti v EU a zemích partnerů participujících na projektu Erasmus+.

---

[1] KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013, s. 65

4.1. Dokumenty EU/ES sloužící k harmonizaci právních úprav při řešení problematiky kybernetické bezpečnosti

Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market.

The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union.

Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people. Owing to that transnational nature, substantial disruptions of those systems, whether intentional or unintentional and regardless of where they occur, can affect individual Member States and the Union as a whole. The security of network and information systems is therefore essential for the smooth functioning of the internal marke.

Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security ('ENISA'), should be established to support and facilitate strategic cooperation between the Member States regarding the security of network and information systems. For that group to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of security of network and information systems in their territory. In addition, security and notification requirements should apply to operators of essential services and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported.[1]

Zejména díky specifičnosti spočívající v neohraničenosti kyberprostoru a potřebě účinné mezinárodní spolupráce se EU snaží sblížit právní úpravu jednotlivých členských států tak, aby bylo možné efektivně řešit problematiku kybernetické bezpečnosti.

Prostředkem pro sbližování práva jednotlivých zemí EU jsou především nařízení, směrnice, rámcová rozhodnutí a další dokumenty EU/ES. Z pohledu kybernetické bezpečnosti jsou nejvýznamnějšími následující dokumenty:

Primární právo EU

- Listina základních práv Evropské unie

Směrnice Evropského parlamentu a Rady

- 91/250/EHS o právní ochraně počítačových programů
- 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů, ve znění směrnice 98/48/ES
- 1999/5/ES o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody
- 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)
- 2002/19/EC o přístupu k sítím elektronických komunikací a přidruženým zařízením a o jejich propojení (přístupová směrnice)
- 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice), ve znění směrnice 2009/140/ES
- 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice), ve znění směrnice 2009/140/ES
- 2002/22/EC o universální službě a uživatelských právech týkajících se sítí a služeb elektronických komunikací (směrnice o universální službě)
- 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací
- 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí
- 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu
- 2011/93/EU o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV
- 2013/11/EU o alternativním řešení spotřebitelských sporů a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES (směrnice o alternativním řešení spotřebitelských sporů)
- 2013/40/EU o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV
- 2015/1535 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti
- 2015/2366 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES („revidovaná směrnice o platebních službách")
- 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV
- **2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (NIS)**

Nařízení Evropského parlamentu a Rady

- 460/2004/ES o zřízení Evropské agentury pro bezpečnost sítí a informací ve znění nařízení č. 1007/2008
- 1077/2011/ES kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva
- 526/2013 o Agentuře Evropské unie pro bezpečnost sítí a informací (**ENISA**) a o zrušení nařízení (ES) č. 460/2004 Text s významem pro EHP
- 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (**eIDAS**[2])679/2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů - **GDPR**)

Rozhodnutí Rady

- 92/242/EHS o bezpečnosti informačních systémů
- **2005/222/SVV o útocích proti informačním systémům**
- 2011/292/EU o bezpečnostních pravidlech na ochranu utajovaných informací EU

Další dokumenty

- Úmluva Rady Evropy č. 185 o kybernetické kriminalitě
- Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě
- Úmluva Rady Evropy č. 196 o prevenci terorismu
- Prováděcí nařízení Komise (EU) 2018/151, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný

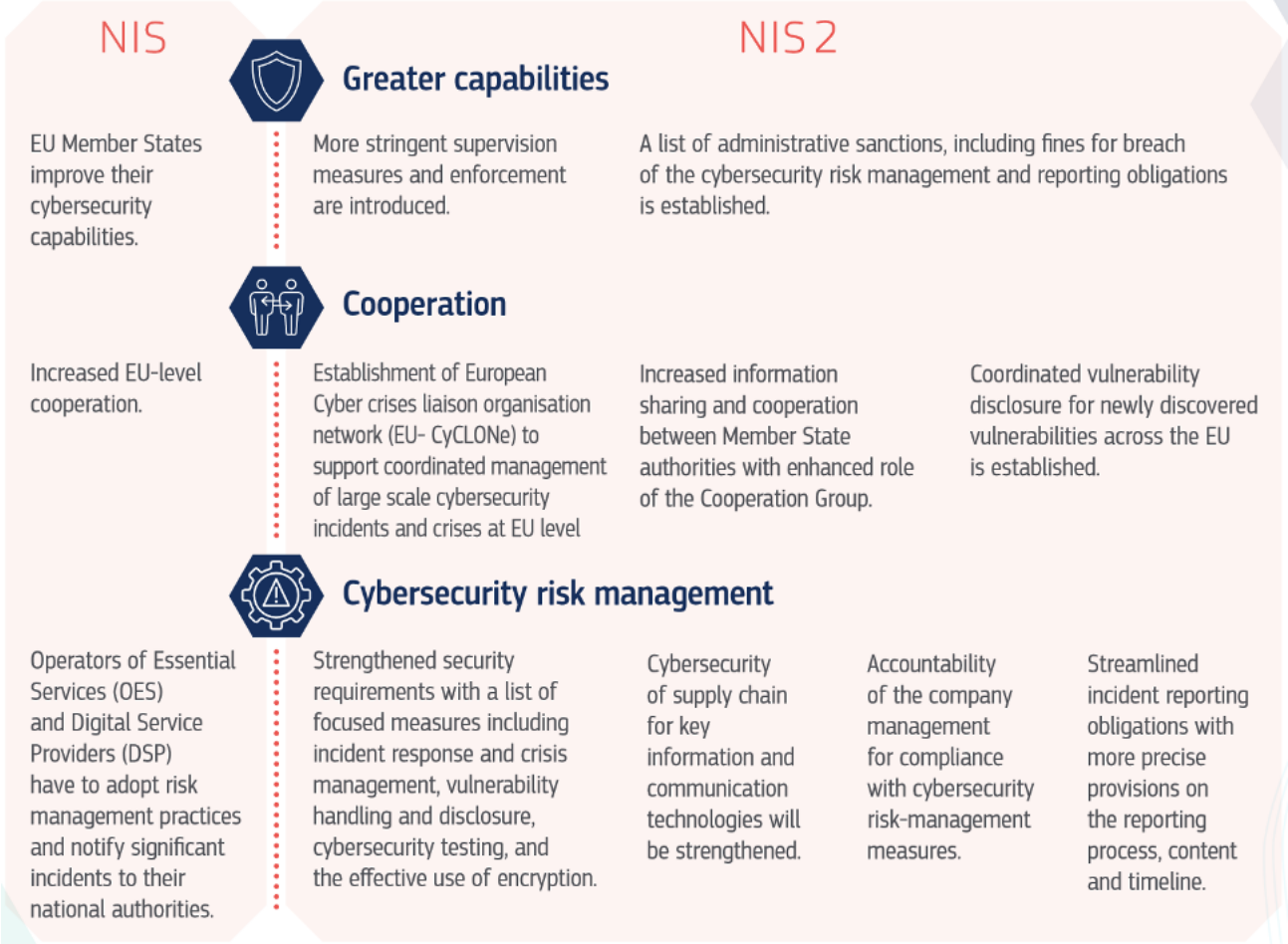
Mezinárodní normy

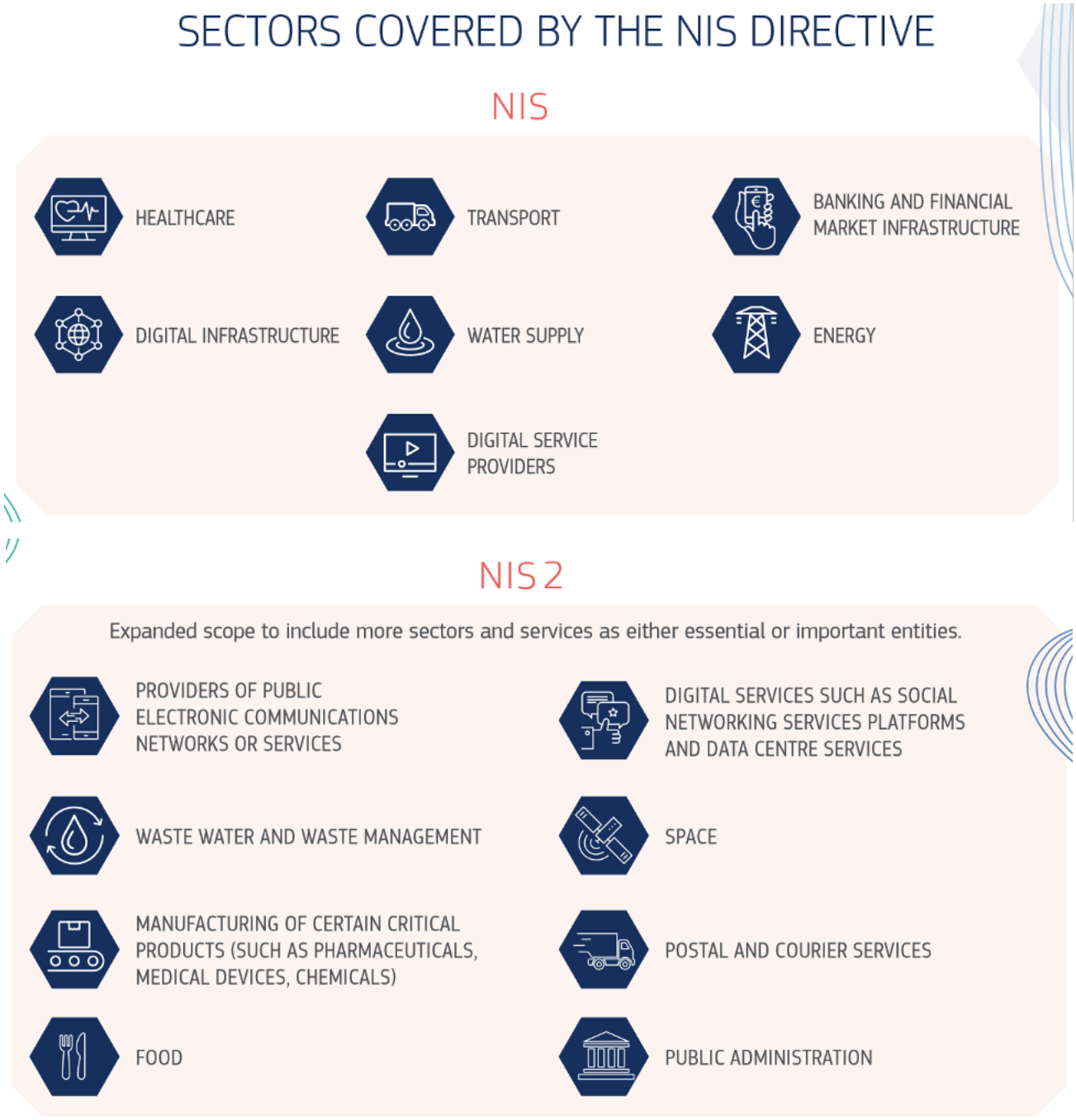
- ISMS řady ISO/IEC 27000
- v ČR ČSN ISO/IEC 27001:2014

V současné době je nejvýznamějším dokumentem Evropské unie, vztahujícím se k problematice kybernetické bezpečnosti, DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union.[3]

Tato směrnice prochází v současné době revizí a je připravována směrnice NIS2. The first EU-wide law on cybersecurity, the NIS Directive, came into force in 2016 and helped achieve a higher and more even level of security of network and information systems across the EU. In view of the unprecedented digitalisation in the last years, the time has come to refresh it.

Změny revidované směrnice jsou vhodně prezentovány v dokumentu Evropské komise[4]:





[1] https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

[2] Dále jen **eIDAS**

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=CS

[4] https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72155

4.2. Legislativa kybernetické bezpečnosti v ČR

Problematika kybernetické bezpečnosti začala být poprvé systémově státem řešena v roce **2000**.

V roce 2010 bylo přijato usnesení vlády č. 205, které se věnuje **Řešení problematiky kybernetické bezpečnosti České republiky.**[1] Toto usnesení ustanovilo MVČR gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Ministru vnitra bylo dále uloženo:

1. koordinovat činnost ostatních státních institucí v oblasti zajišťování kybernetické bezpečnosti,

2. koordinovat zastupování České republiky v otázkách kybernetické bezpečnosti na mezinárodních fórech, včetně účasti státních orgánů na činnosti příslušných mezinárodních organizací,

3. do 30. dubna 2010 předložit vládě ke schválení statut meziresortní koordinační rady pro kybernetickou bezpečnost,

4. do 15. prosince 2010 předložit vládě strategii pro oblast kybernetické bezpečnosti,

5. nejpozději k 31. prosinci 2010 zahájit zajišťování provozu vládního pracoviště CSIRT (Computer Security Incident Response Team).

Dne **19. října 2011** přijala vláda České republiky usnesení č. 781 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.[2] Současně tímto usnesením Vláda ČR zřídila **Radu pro kybernetickou bezpečnost**[3] a schválila vznik **Národního centra kybernetické bezpečnosti** (jakožto součásti NBÚ).

V roce **2011** byla přijata **Strategie pro oblast kybernetické bezpečnosti České republiky na období let 2011 až 2015**[4] a **akční plán k této strategii.** Nicméně díky převodu gesce z MVČR na NBÚ je tato strategie častěji označována jako: **Strategie pro oblast kybernetické bezpečnosti České republiky na období let 2012 až 2015.**[5]

V předložené strategii byly vytýčeny následující strategické cíle a opatření:

- vytvoření legislativního rámce,
- vybudování Národního centra kybernetické bezpečnosti a vládního pracoviště CERT,
- ochrana kritických informačních infrastruktur,
- posilování kybernetické bezpečnosti informačních a komunikačních systémů veřejné správy,
- zefektivnění potírání kriminality v kybernetickém prostoru,
- koordinace aktivit k zajištění kybernetické bezpečnosti v Evropě,
- používání spolehlivých a důvěryhodných informačních technologií,
- zvyšování povědomí o kybernetické bezpečnosti,
- odezva na kybernetické útoky.

Dne 28. června 2013 předložil NBÚ návrh zákona o kybernetické bezpečnosti Vládě České republiky. Následný legislativní proces proběhl bez významnějších připomínek a **zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů** (zákon o kybernetické bezpečnosti) vstoupil v platnost dne 29. srpna 2014 s účinností od **1. ledna 2015.**

Současně se zákonem byly vypracovávány i prováděcí právní předpisy, konkrétně:

- vyhláška č. 316/2014, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (**vyhláška o kybernetické bezpečnosti**);
- vyhláška č. 317/2014, **kterou se stanoví významné informační systémy a jejich určující kritéria**;
- vyhláška č. 315/2014, novela nařízení vlády č. 432/2010 Sb., **o kritériích pro určení prvku kritické infrastruktury**.

Veškeré prováděcí předpisy nabyly účinnosti současně se zákonem o kybernetické bezpečnosti.

V srpnu 2015 byl na základě požadavků stanovených v ZoKB vybrán provozovatel Národního CERT týmu. Tímto provozovatelem se stalo sdružení CZ.NIC.[6] Dne 18. prosince 2015 pak došlo k podpisu Veřejnoprávní smlouvy o zajištění činnosti Národního CERT a o spolupráci v oblasti kybernetické bezpečnosti.[7] Tato smlouva byla uzavřena na dobu neurčitou.

Zákon o kybernetické bezpečnosti od roku 2015, kdy nabyl účinnosti, prošel dvěma obsahově významnými novelizacemi.

První novelizace byla provedena zákonem č. 104/2017 Sb.,[8] s účinností od 1. července 2017 a zákona č. 205/2017 Sb. s účinností od 1. srpna 2017. Tato novela rozšířila okruh povinných osob spadajících pod ZoKB o provozovatele informačních systémů a dále upravila některé sankce.

Druhá obsahově významnější novelizace byla provedena zákonem č. 205/2017 Sb.,[9] s účinností od 1. srpna 2017. Touto novelou byla do ZoKB implementována **Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (NIS)** a zároveň byl zřízen **Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)**, který po NBÚ převzal práva a povinnosti v oblasti kybernetické bezpečnosti včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. NÚKIB je ve výše uvedených oblastech ústředním správním orgánem.

V současné době je problematika kybernetické bezpečnosti specificky řešena zákonem o kybernetické bezpečnosti, nicméně dílčí aspekty ochrany České republiky před kybernetickými útoky je možné nalézt i v jiných právních předpisech. Z pohledu kybernetické bezpečnosti jsou nejvýznamnějšími následující dokumenty:

Ústavní zákony

- Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů
- Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů[10]

- Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky

Zákony

- zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů[11]
- zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů
- zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon), ve znění pozdějších předpisů
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů
- zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů[12]
- zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů[13]
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů[14]
- zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů[15]
- zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů
- zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
- zákon č. 89/2012 Sb., občanský zákoník
- **zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)**
- zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce

Prováděcí předpisy

- nařízení vlády č. 522/2005 Sb., kterým se stanoví seznamy utajovaných informací, ve znění pozdějších předpisů
- vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění pozdějších předpisů
- vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)
- **nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury**
- vyhláška 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů
- **vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích**
- **vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby**
- **vyhláška č. 82/2018 Sb.**, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (**vyhláška o kybernetické bezpečnosti**)

---

[1] *USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 15. března 2010 č. 205 o řešení problematiky kybernetické bezpečnosti České republiky.* [online]. Dostupné z: https://apps.odok.cz/attachment/-/down/KORN97BQ9ASZ

[2] *USNESENÍ VLÁDY ČESKÉ REPUBLIKY ze dne 19. října 2011 č. 781 o ustanovení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.* [online]. Dostupné z: https://apps.odok.cz/attachment/-/down/KORN97BUKZ3E

[3] Tato rada je poradním orgánem předsedy vlády pro oblast kybernetické bezpečnosti.

[4] *Strategie pro oblast kybernetické bezpečnosti České republiky na období let 2011 až 2015.* [online]. Dostupné z: https://www.databaze-strategie.cz/cz/cr/strategie/strategie-pro-oblast-kyberneticke-bezpecnosti-cr-2011-2015?typ=struktura

[5] *Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 - 2015.* [online]. Dostupné z: https://www.govcert.cz/download/legislativa/container-nodeid-719/20120209strategieprooblastkbnbu.pdf

[6] Viz https://www.nic.cz/page/351/

[7] Blíže viz [online]. Dostupné z: https://www.nic.cz/files/nic/doc/NBU-Smlouva-narodni-cert-201512.pdf

[8] Zákon č. 104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., **o informačních systémech veřejné správy** a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony. [online]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-104

[9] Zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony. [online]. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-205

[10] Dále jen Listina základních práv a svobod či **Listina**.

[11] Dále jen zákon o ochraně osobních údajů či **ZoOU**. V souvislosti s účinností GDPR dojde k rekodifikaci tohoto zákona a předpokládá se, že bude nahrazen zákonem o zpracování osobních údajů. Blíže viz např. [online]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5

[12] Dále jen zákon o některých službách informační společnosti či **ZSIS**.

[13] Dále jen **ZoEK**

[14] Dále jen **ZoOUI**

[15] Dále jen trestní zákoník, či **TZK**.

5. Systém řízení bezpečnosti informací

ISMS - Information Security Management System

5.1. Rámec ISMS

Systém řízení bezpečnosti informací (angl. **I**nformation **S**ecurity **M**anagement **S**ystem[1] - **ISMS**) **představuje soubor pravidel**, jejichž cílem je zachovat důvěrnost, integritu a dostupnost informací aplikováním procesu řízení rizik a dát jistotu zainteresovaným stranám, že jsou rizika přiměřeně řízena.[2]

V rámci ISMS jsou chráněna aktiva, řízena rizika bezpečnosti informací a již zavedená opatření jsou kontrolována.

Systémem řízení bezpečnosti informací se rozumí ta část systému řízení, která je založená na přístupu k rizikům informačního a komunikačního systému. Tato část systému řízení definuje způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat.

I z výše uvedené definice je zřejmé, že **ISMS je součástí procesů a celkového systému řízení organizace a je do těchto systémů integrován**.

ISMS lze aplikovat na organizaci jako celek, jakož i na organizační složku v rámci organizace, či na specificky určený informační a komunikační systém, případně jeho část.

„ISMS lze zavést a používat v organizaci s deseti pracovníky, a stejně tak i ve velkém holdingu, který může čítat tisíce zaměstnanců. Zjednodušeně lze říci, že ISMS je jen jeden, a to ten, který je popsán v normě ISO/IEC 27001. Interpretace a implementace jednotlivých doporučení se však může výrazně lišit podle rozsahu systému, počtu uživatelů, způsobu zpracování dat, jejich hodnoty a především podle reálných bezpečnostních rizik apod. Strategie ISMS nebývá v malých a středních firmách popsána tak detailně, jako je tomu zvykem ve velkých, zejména nadnárodních organizacích.

ISMS se netýká jen průmyslových podniků a privátních organizací, ISMS se týká všech organizací včetně veřejně právních institucí a orgánů státu. Toho důkazem je i existence mnoha národních vládních a resortních usnesení doporučujících anebo vyžadujících implementaci ISMS v organizacích řízených a zřízených státem.“[3]

Řada norem ISMS má pomoci organizacím všech typů a velikostí zavést a provozovat ISMS. Sestává z následujících mezinárodních norem se společným názvem *Informační technologie – Bezpečnostní techniky****[4]*** (uvedených dále v číselném pořadí):

- ISO/IEC 27000 — *Systémy řízení bezpečnosti informací – Přehled a slovník*
- **ISO/IEC 27001** — ***Systémy řízení bezpečnosti informací – Požadavky***
- ISO/IEC 27002 — *Soubor postupů pro opatření bezpečnosti informací*
- ISO/IEC 27003 — *Směrnice pro implementaci systému řízení bezpečnosti informací*
- ISO/IEC 27004 — *Řízení bezpečnosti informací – Měření*
- ISO/IEC 27005 — *Řízení rizik bezpečnosti informací*
- ISO/IEC 27006 — *Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací*
- ISO/IEC 27007 — *Směrnice pro audit systémů řízení bezpečnosti informací*
- ISO/IEC TR 27008 — *Směrnice pro auditory opatření bezpečnosti informací*
- ISO/IEC 27009 — *Oborově specifická aplikace ISO/IEC 27001 – Požadavky*
- ISO/IEC 27010 — *Řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi*
- ISO/IEC 27011 — *Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002*
- ISO/IEC 27013 — *Pokyn pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1*
- ISO/IEC 27014 — *Správa a řízení bezpečnosti informací*
- ISO/IEC TR 27015 — *Směrnice pro řízení bezpečnosti informací pro finanční služby*
- ISO/IEC TR 27016 — *Řízení bezpečnosti informací – Organizační ekonomika*
- ISO/IEC 27017 — *Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002*

- ISO/IEC 27018 — *Soubor postupů pro ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII*
- ISO/IEC 27019 — *Směrnice pro řízení bezpečnosti informací na základě ISO/IEC 27002 pro systémy řízení procesů specifické pro odvětví energetiky*

Mezinárodní normy, které nejsou uvedeny pod tímto společným názvem, ale jsou také součástí řady norem ISMS, jsou uvedeny dále:

- ISO 27799 — *Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002*[5]

Řešení ISMS vyžaduje systémový a komplexní přístup, respektující principy a prvky v rámci celého životního cyklu kybernetické bezpečnosti. Systém řízení ISMS je založen na Demingově cyklu, neboli též na **PDCA cyklu** (**P**lan-**D**o-**C**heck-**A**ct; **P**lánuj-**D**ělej-**K**ontroluj-**J**ednej).

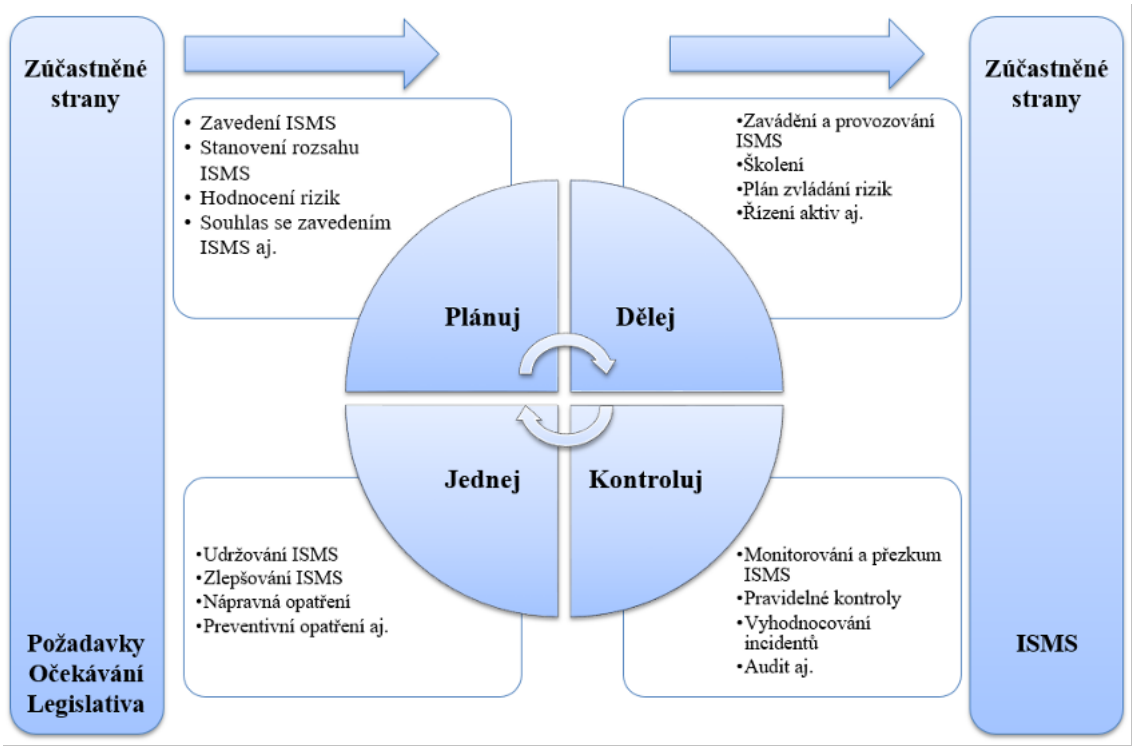
PDCA cyklus je jedním ze základních manažerských principů spočívající v postupném zlepšování kvality procesů, služeb, dat, výrobků aj. díky neustálému opakování jeho čtyř základních činností: Plan-Do-Check-Act.

V současné době existuje celá řada variant PDCA cyklu[6], přičemž jednou z vhodných modifikací tohoto cyklu, jež je využitelná i v oblasti kybernetické bezpečnosti, je varianta **OPDCA**, která původní model rozšiřuje o fázi **Observe** (**Pozoruj**/Poznamenej) **předcházející** fázi plánování.

PDCA cyklus, či některé jeho modifikace je možné aplikovat na všechny procesy ISMS. Nejjednodušeji je možné tento model zobrazit jako nikdy nekončící kruh:

Obrázek: Model PDCA[7]

Model PDCA byl vyjádřen i v normě ISO/IEC 27001:2005 a znázorňoval, jak ISMS přijímá požadavky bezpečnosti informací a očekávání zainteresovaných stran jako vstup, a jak pomocí nezbytných činností a procesů vytváří výstupy bezpečnosti informací, které splňují tyto požadavky a očekávání.



Obrázek: PDCA model aplikovaný na procesy ISMS[8]

Plánuj (ustavení ISMS)	

	Ustavení politiky ISMS, cílů, procesů a postupů souvisejících s managementem rizik a zlepšováním bezpečnosti informací tak, aby poskytovaly výsledky v souladu s celkovou politikou a cíli organizace.
Dělej (zavádění a provozování ISMS)	Zavedení a využívání politiky ISMS, opatření, procesů a postupů.
Kontroluj (monitorování a přezkoumání ISMS)	Posouzení, kde je to možné, i měření výkonu procesu vůči politice ISMS, cílům a praktickým zkušenostem a hlášení výsledků vedení organizace k přezkoumání.
Jednej (udržování a zlepšování ISMS)	Přijetí opatření k nápravě a přijetí preventivních opatření, založených na výsledcích interního auditu ISMS a přezkoumání systému řízení ze strany vedení organizace tak, aby bylo dosaženo neustálého zlepšování ISMS.

Norma ISO/IEC 27001 prosazuje přijetí procesního přístupu pro **ustavení**, **zavádění, provozování**, **monitorování**, **udržování** a **zlepšování ISMS** v organizaci. Důraz je kladen zejména na:

- pochopení požadavků na bezpečnost informací organizace a potřebu stanovení politiky a cílů bezpečnosti informací,
- zavedení a provozování opatření pro management bezpečnosti informací v kontextu s řízením celkových rizik činností organizace,
- monitorování a přezkoumání výkonnosti a účinnosti ISMS,
- neustálé zlepšování založené na objektivním měření.

„Pro ISMS v rámci organizace musí být jednoznačně popsána organizace řízení, odpovědnost za informační bezpečnost řídících pracovníků všech stupňů, odborných orgánů a rolí v systému bezpečnosti informací.

V organizační struktuře organizace musí být informační bezpečnost zohledněna tak, aby pokrývala činnosti a spolupráci vedení, osob odpovědných za aplikační systémy, provozní služby, koncové uživatele a osoby odpovědné za jednotlivé činnosti. Informační bezpečnost předpokládá úzkou spolupráci všech uvedených skupin pracovníků a poskytování školení v oblasti informační bezpečnosti, tak aby kromě osob, které v organizaci odpovídají za informační a další bezpečnost, měli základní znalosti o informační bezpečnosti i pracovníci pracující ve správě informací a všichni uživatelé informační techniky."[9]

S ohledem na výše uvedené si je možné vydefinovat standardní cíle ISMS v rámci organizace:

- zajištění bezpečnosti informačních a komunikačních systémů a služeb,
- zajištění kontinuity provozu informačních a komunikačních systémů a služeb,
- ochrana dat a informací,
- ochrana dalších aktiv,
- řešení hrozeb, událostí a incidentů včetně prevence,
- zvyšování bezpečnosti informačních a komunikačních systémů a služeb,
- zvyšování obecného podvědomí uživatelů o bezpečnosti a bezpečnostních hrozbách (edukace),
- sdílení zkušeností s dalšími subjekty.

Zavedení ISMS v organizaci však **nemůže zajistit naprostou bezpečnost aktiv** organizace. Implementace ISMS však může výrazně snížit rizika zásahu do aktiv na přijatelnou úroveň. Celý systém je tak silný, jak silný je jeho nejslabší článek. V tomto případě je oním nejslabším článkem, a největším nebezpečím pro zabezpečení informací, člověk.

---

[1] Dále jen **ISMS**

[2] Srov. úvod ČSN ISO/IEC 27001

[3] POŽÁR, Josef a Luděk NOVÁK. *Pracovní příručka bezpečnostního manažera.* Praha: AFCEA, 2011. ISBN 978-80-7251-364-2, s. 5 případně: POŽÁR, Josef a Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.cybersecurity.cz/data/srib.pdf s. 1

[4] Společný název „*Informační technologie – Bezpečnostní techniky*" označuje, že tyto mezinárodní normy byly vypracovány společnou technickou komisí ISO/IEC JTC 1 *Informační technologie,* subkomisí SC 27 *IT Bezpečnostní techniky*

[5] Přehled norem viz: ČSN EN ISO/IEC 27000 (369790) - Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník

[6] ROSER, Christoph. *The Many Flavors of the PDCA.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.allaboutlean.com/pdca-variants/

[7] *PDCA cycle.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.creativesafetysupply.com/glossary/pdca-cycle/

[8] Upravený a doplněný model PDCA. Původní model byl představen v ISO/IEC 27001:2005 s. 7

[9] POŽÁR, Josef a Luděk NOVÁK. *Pracovní příručka bezpečnostního manažera.* Praha: AFCEA, 2011. ISBN 978-80-7251-364-2, s. 7-8 případně: POŽÁR, Josef a Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.cybersecurity.cz/data/srib.pdf s. 2

5.2. Řízení rizik

Dle čl. 7 NIS má každý členský stát přijmout národní strategii pro bezpečnost sítí a informačních systémů, ve které vymezí strategické cíle a příslušná politická a regulační opatření s cílem dosáhnout vysoké úrovně bezpečnosti sítí a informačních systémů a udržovat ji. Předmětem národní strategie pro bezpečnost sítí a informačních systémů jsou především následující cíle a opatření:

a) cíle a priority národní strategie pro bezpečnost sítí a informačních systémů;

b) správní rámec pro naplnění cílů a priorit vnitrostátní strategie pro bezpečnost sítí a informačních systémů, včetně úlohy a povinností vládních orgánů a dalších relevantních subjektů;

c) stanovení opatření týkajících se připravenosti, reakce a obnovy, včetně spolupráce veřejného a soukromého sektoru;

d) vymezení vzdělávacích, informačních a školicích programů souvisejících s vnitrostátní strategií pro bezpečnost sítí a informačních systémů;

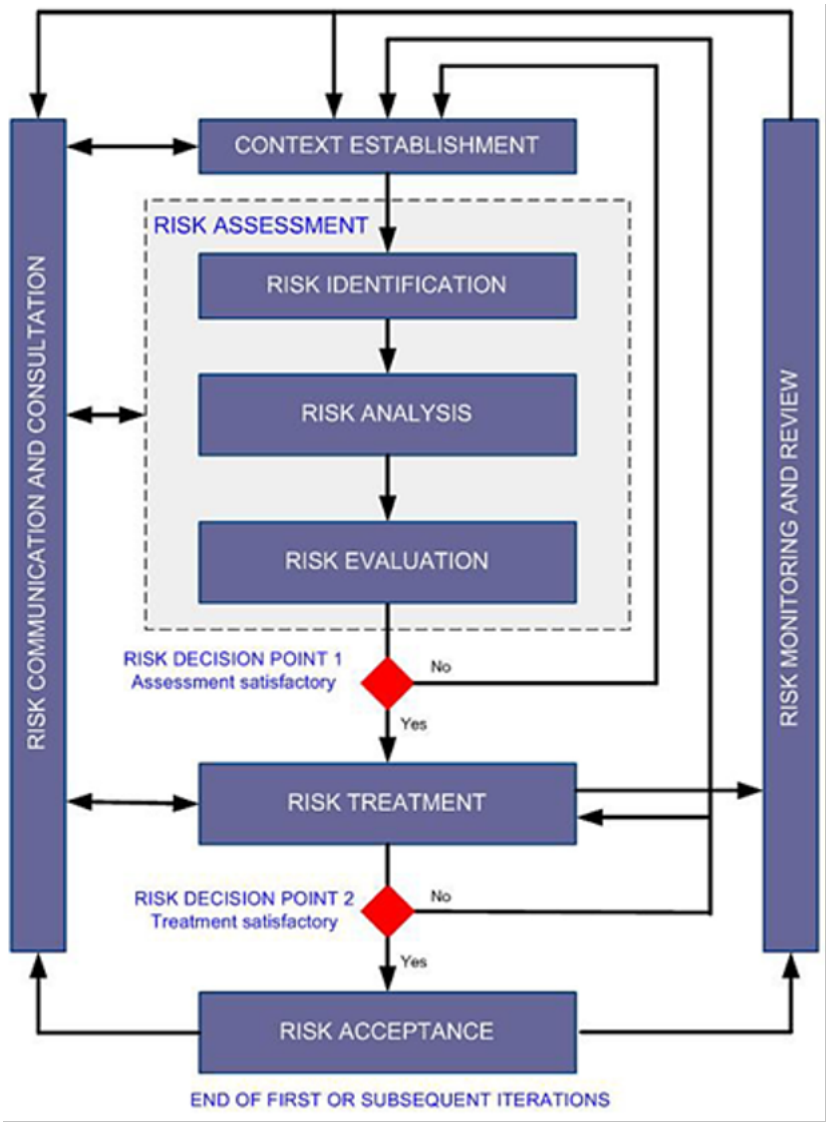
e) vymezení výzkumných a rozvojových plánů souvisejících s národní strategií pro bezpečnost sítí a informačních systémů;

f) plán posouzení rizik pro určení rizik;

g) seznam různých subjektů zapojených do provádění národní strategie pro bezpečnost sítí a informačních systémů.

Dle české legislativy se **hodnocením rizik** rozumí **celkový proces identifikace, analýzy a vyhodnocení rizik.**

Procesu hodnocení rizik se věnuje např. ISO/IEC 27005, kde je tento proces demonstrován.



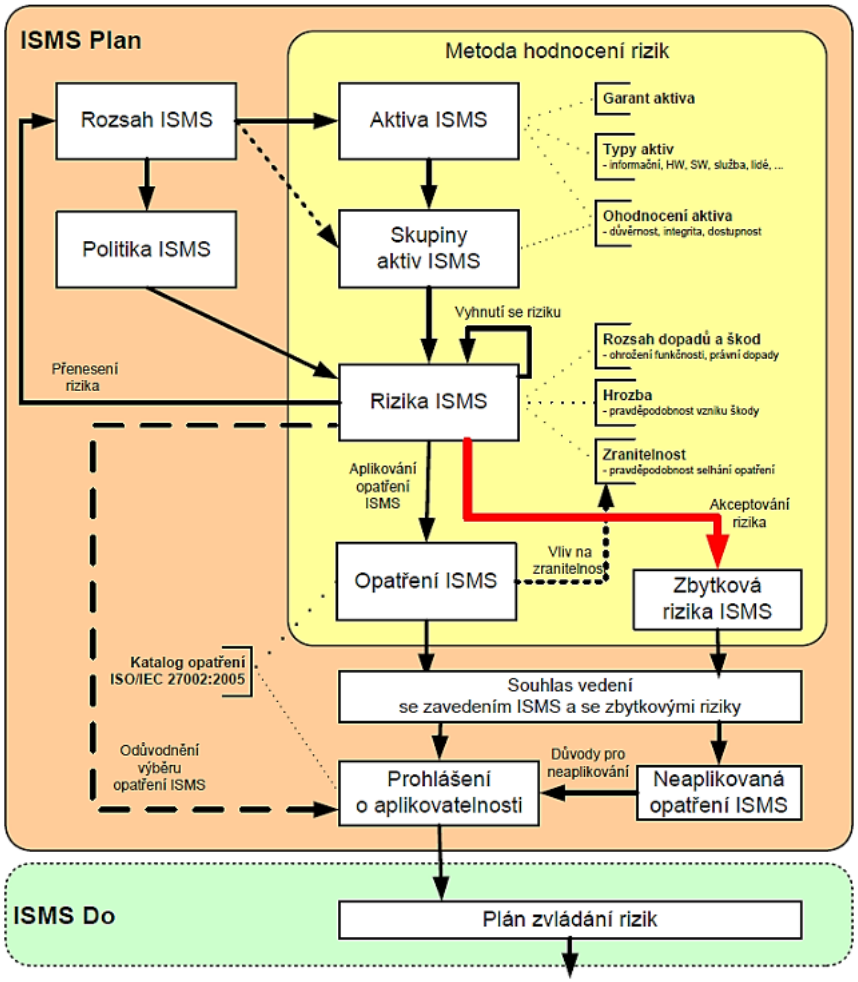
Obrázek: Demonstrace hodnocení rizik v ISMS[1]

I v rámci procesu hodnocení rizik je třeba respektovat model PDCA, který je však přizpůsoben pro hodnocení rizik.[2]

ISMS proces	Proces hodnocení rizik v ISMS
Plan	Vytvoření kontextu

	Odhad rizika Vypracování plánu zvládání rizika Přijetí rizika
Do	Implementace plánu zvládání rizika
Check	Nepřetržité sledování a revize rizik
Act	Udržování a zlepšování procesu hodnocení a řízení rizik Řídící proces

Pokud jde o vlastní řízení rizik, pak je možné tento proces graficky znázornit následovně:



Obrázek: Řízení rizik v procesu ISMS[3]

Hodnota rizika je nejčastěji vyjádřena jako funkce, kterou ovlivňuje dopad, hrozba a zranitelnost. Pro vlastní hodnocení rizika lze využít například následující funkci:

Riziko = dopad * hrozba * zranitelnost

V případě, že povinná osoba využívá metodu pro hodnocení rizik, která nerozlišuje hodnocení hrozby a zranitelnosti, je možné stupnice pro hodnocení hrozeb a zranitelností sloučit. Sloučení stupnic by nemělo vést ke ztrátě schopnosti rozlišení úrovně hrozby a zranitelnosti. Za tímto účelem lze použít například komentář, který zřetelně vyjádří jak úroveň hrozby, tak i úroveň zranitelnosti. Obdobně se postupuje i v případech, kdy povinná osoba používá jiný počet úrovní pro hodnocení dopadů, hrozeb, zranitelností a rizik.[4]

Příloha č. 3 VoKB dále uvádí používané stupnice pro hodnocení hrozeb, zranitelností a rizik.

Úroveň	**Popis**
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby **není častější než jednou za 5 let.**
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí **od 1 roku do 5 let**.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od **1 měsíce do 1 roku**.

Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby **je častější než jednou za měsíc**.

Obrázek: Stupnice pro hodnocení hrozeb

Úroveň	Popis
Nízká	**Zranitelnost neexistuje nebo je** zneužití zranitelnosti **málo pravděpodobné**. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
Střední	**Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné**. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	**Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné**. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	**Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté**. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Obrázek: Stupnice hodnocení zranitelností

Úroveň	Popis
Nízké	**Riziko je** považováno za **akceptovatelné**.
Střední	**Riziko může být sníženo méně náročnými opatřeními** nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.
Vysoké	**Riziko je dlouhodobě nepřípustné** a musí být zahájeny systematické kroky k jeho odstranění.
Kritické	**Riziko je nepřípustné** a musí být neprodleně zahájeny kroky k jeho odstranění.

Obrázek: Stupnice pro hodnocení rizik

---

[1] ISO/IEC 27005 s. 8

[2] ISO/IEC 27005 s. 9

[3] POŽÁR, Josef a Luděk NOVÁK. *Pracovní příručka bezpečnostního manažera.* Praha: AFCEA, 2011. ISBN 978-80-7251-364-2, s. 12 případně: POŽÁR, Josef a Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.cybersecurity.cz/data/srib.pdf s. 5

[4] Viz příloha č. 3 odst. 5 k VoKB

5.3. Bezpečnostní politika

Bezpečnostní politikou rozumí **soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv.**

Bezpečnostní politiky standardně spočívá v tom, že určené subjekty s ohledem na systém řízení bezpečnosti informací jsou povinny:

a) **stanovit bezpečnostní politiku** a **vést bezpečnostní dokumentaci** zahrnující oblasti následující politiky:[1]

- systému řízení bezpečnosti informací,
- řízení aktiv,
- organizační bezpečnosti,
- řízení dodavatelů,
- bezpečnosti lidských zdrojů,
- řízení provozu a komunikací,
- řízení přístupu,
- bezpečného chování uživatelů,
- zálohování a obnovy a dlouhodobého ukládání,
- bezpečného předávání a výměny informací,
- řízení technických zranitelností,
- bezpečného používání mobilních zařízení,
- akvizice, vývoje a údržby,
- ochrany osobních údajů,
- fyzické bezpečnosti,
- bezpečnosti komunikační sítě,
- ochrany před škodlivým kódem,
- nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí,
- bezpečného používání kryptografické ochrany,
- řízení změn,
- zvládání kybernetických bezpečnostních incidentů,
- řízení kontinuity činností.

Dále je stanoven **obsah bezpečnostní dokumentace**, jež musí zahrnovat:

- zprávu z auditu kybernetické bezpečnosti,
- zprávu z přezkoumání systému řízení bezpečnosti informací,
- metodiku pro identifikaci a hodnocení aktiv a pro hodnocení rizik,
- zprávu o hodnocení aktiv a rizik,
- prohlášení o aplikovatelnosti,
- plán zvládání rizik,
- plán rozvoje bezpečnostního povědomí,
- evidenci změn,
- hlášené kontaktní údaje,
- přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků,
- další doporučenou dokumentaci (např. topologii infrastruktury, přehled síťových zařízení).

b) **pravidelně přezkoumávat bezpečnostní politiku** a **bezpečnostní dokumentaci,**

c) zajistit, aby byla bezpečnostní politika a bezpečnostní dokumentace aktuální.

Bezpečnostní politika a bezpečnostní dokumentace musí být:

- dostupná v listinné nebo elektronické podobě,
- komunikována v rámci povinné osoby,
- přiměřeně dostupná dotčeným stranám,
- řízena,
- chráněna z pohledu důvěrnosti, integrity a dostupnosti,
- vedena tak, aby informace v nich obsažené byly úplné, čitelné, snadno identifikovatelné a snadno vyhledatelné.

---

[1] Blíže viz příloha č. 5 VoKB

5.4. Organizační bezpečnost

Vymezení organizační bezpečnosti a zejména ukotvení kybernetické či ICT bezpečnosti v rámci již fungujících struktur organizace je velmi zásadní pro případné zvládání kybernetických hrozeb či útoků.

Problematika bezpečnosti by měla být v rámci organizaci řešena na operativní, taktické, ale i strategické úrovni z pohledu managementu organizace.

Z pohledu bezpečnosti je významné, aby byl útvar (odbor) kybernetické bezpečnosti oddělen od útvaru (odboru), který zajišťuje provoz ICT.[1]

> **Příklad:** Autor se setkal se správcem sítě, po kterém jeho zaměstnavatel požadoval, aby se stal současně manažerem bezpečnosti. V praxi by to znamenalo, že by si tento správce sám navrhoval směrnice, kterými se má řídit a zároveň by sám kontroloval, zda je dodržuje a jejich dodržování vymáhal. Absurdnost této situace je patrná na první pohled.

Organizační bezpečnost standardně spočívá v tom, že určené subjekty s ohledem na systém řízení bezpečnosti informací:

- **zajistí stanovení bezpečnostní politiky a cílů ISMS** tak, aby byly slučitelné se strategickým směřováním povinné osoby,
- **zajistí integraci ISMS** do procesů povinné osoby,
- **zajistí dostupnost zdrojů** potřebných **pro ISMS**,
- **informují zaměstnance o významu ISMS** a významu dosažení shody s jeho požadavky se všemi dotčenými stranami,
- **zajistí podporu** k dosažení zamýšlených výstupů **ISMS**,
- **vedou zaměstnance k rozvíjení efektivity ISMS** a podporují je při tomto rozvíjení,
- **prosazují neustálé zlepšování ISMS**,
- **podporují osoby zastávající bezpečnostní role** při prosazování kybernetické bezpečnosti v oblastech jejich odpovědnosti,
- **zajistí stanovení pravidel pro určení administrátorů** a **osob, které budou zastávat bezpečnostní role**,

  Bezpečnostními rolemi se rozumí:

  - **manažer** kybernetické bezpečnosti,
  - **architekt** kybernetické bezpečnosti,
  - **garant aktiva**,
  - **auditor** kybernetické bezpečnosti.
- **zajistí, aby byla zachována mlčenlivost** administrátorů a osob zastávajících bezpečnostní role,
- **pro osoby zastávající bezpečnostní role zajistí příslušné pravomoci** a zdroje včetně rozpočtových prostředků k naplňování jejich rolí a plnění souvisejících úkolů,
- **zajistí testování plánů kontinuity činností, obnovy a procesů spojených se zvládáním kybernetických bezpečnostních incidentů**.

Pro přiřazení a zobrazení (v rámci tabulky) odpovědností jednotlivých osob (bezpečnostních rolí dle VoKB) v rámci organizace je vhodné použít **matici odpovědnosti RACI (matice RACI).** RACI je akronym z počátečních písmen slov:

R - Responsible	kdo je odpovědný za vykonání svěřeného úkolu (dané aktivity)
A – Accountable (či Approver)	kdo je odpovědný za celý úkol, respektive za to, že je daný proces vykonán tak, jak bylo předdefinováno
C - Consulted	kdo může poskytnout cenou radu či konzultaci k úkolu, avšak nepřebírá odpovědnost za výkon procesu
I - Informed	kdo má být informován o průběhu úkolu či rozhodnutích v úkolu

Platí pravidlo, že celkovou odpovědnost (A - Accountability) má k danému úkolu pouze jedna osoba, zapojených lidí (R - Responsibility) by mělo být přiměřeně k danému úkolu. Metoda RACI je jednoduchou formou modelu kompetencí.[2]

Procesy:	**Role:**	**Výbor KB**	**Manažer KB**	**Architekt KB**	**Auditor KB**	**Garant aktiva**
Celkové řízení a rozvoj KB		**A**	**R**	**R**		**C**
Systém řízení bezpečnosti informací		**A**	**R**	**C**		**C**
Návrh bezpečnostních opatření		**C**	**A**	**R**		**C**
Implementace bezpečnostních opatření		**C**	**A**	**R**		**C**
Zajištění rozvoje, použití a bezpečnostní aktiva			**A**	**C**		**R**
Audit KB		**I**	**C**	**C**	**A/R**	**C**

Obrázek: RACI matice[3]

[1] Srov. *Bezpečnostní role a jejich začlenění v organizaci.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf s. 3

[2] Blíže viz např. *Matice odpovědnosti RACI (RACI Responsibility Matrix)*. [online]. [cit. 21. 8. 2018]. Dostupné z: https://managementmania.com/cs/matice-odpovednosti-raci či *Bezpečnostní role a jejich začlenění v organizaci.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf s. 6

[3] RACI matice při popisu základních procesů s pojených s bezpečnostními rolemi. Vztahy jednotlivých bezpečnostních rolí a procesů se v závislosti na dané organizaci mohou lišit. *Bezpečnostní role a jejich začlenění v organizaci.* [online]. [cit. 21. 8. 2018]. Dostupné z: https://nukib.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf s. 7

5.5. Řízení aktiv

Aktivem se rozumí cokoliv, co má určitou hodnotu pro osobu, organizaci či stát.

Aktivum může být věcí **hmotnou** (budova, počítačový systém, sítě, energie, zboží aj.) či **nehmotnou** (informace, znalosti, data, programy aj.) z pohledu občanského práva.

Aktivem však může být i **vlastnost** (např. dostupnost a funkčnost systému a dat aj.) či **dobré jméno**, reputace atd. **Lidé** (uživatelé, administrátoři aj.) a jejich znalosti a zkušenosti jsou také z pohledu kybernetické bezpečnosti aktivem.

Podpůrným aktivem je technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému.

Primárním aktivem je informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém.

„V rámci spolehlivého řízení bezpečnosti informací je důležité mít přehled o vazbách a závislostech mezi primárními a podpůrnými aktivy."[1]

V rámci správy aktiv jsou subjekty povinny:

- **stanovit metodiku pro identifikaci aktiv**,
- stanovit metodiku pro **hodnocení aktiv**,
- **identifikovat a evidovat aktiva**,
- **určit** a evidovat **garanty aktiv**,
- **hodnotit a evidovat primární aktiva** z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní aktiv,
- **určit a evidovat vazby mezi primárními a podpůrnými aktivy** a hodnotit důsledky závislostí mezi primárními a podpůrnými aktivy,
- **hodnotit podpůrná aktiva** a zohlednit vzájemné závislosti mezi primárními a podpůrnými aktivy,
- stanovit a **zavést pravidla ochrany** nutná pro zabezpečení **jednotlivých úrovní aktiv**,
- stanovit přípustné způsoby používání aktiv a pravidla pro manipulaci s aktivy s ohledem na úroveň aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv,
- určit způsob likvidace dat, provozních údajů, informací a jejich kopií nebo likvidaci technických nosičů dat s ohledem na úroveň aktiv.

Při hodnocení významu primárních aktiv je třeba povinně posoudit:

- rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství,
- rozsah dotčených právních povinností nebo jiných závazků,
- rozsah narušení vnitřních řídicích a kontrolních činností,
- poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty,
- dopady na poskytování důležitých služeb,
- rozsah narušení běžných činností,
- dopady na zachování dobrého jména nebo ochranu dobré pověsti,
- dopady na bezpečnost a zdraví osob,
- dopady na mezinárodní vztahy,
- dopady na uživatele informačního a komunikačního systému.

---

[1] MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015. s. 85

5.6. Bezpečnost lidských zdrojů

Subjekty jsou povinny v rámci ISMS dbát i na bezpečnost lidských zdrojů, jakožto jednoho z aktiv. Jak již bylo uvedeno dříve, člověk bývá zpravidla oním nejslabším článkem v rámci kybernetické bezpečnosti. Zejména jsou tytop subjekty povinny:

- **stanovit plán rozvoje bezpečnostního povědomí** s cílem zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí,
  - tento plán obsahuje formu, obsah a rozsah
  - poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice,
  - potřebných teoretických i praktických školení uživatelů, administrátorů a osob zastávajících bezpečnostní role.
- **určit osoby odpovědné** za realizaci jednotlivých činností uvedených v plánu,
- **zajistit poučení** uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení,
- **pro osoby zastávající bezpečnostní role zajistit pravidelná odborná školení**,
- zajistit **pravidelné školení** a ověřování bezpečnostního povědomí **zaměstnanců** v souladu s jejich pracovní náplní,
- zajistit **kontrolu dodržování bezpečnostní politiky ze strany uživatelů**, administrátorů a osob zastávajících bezpečnostní role,
- v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role **zajistit předání odpovědností**,
- **hodnotit účinnost plánu rozvoje** bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí,
- **určit pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel** ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.

O výše uvedených školeních je povinnost vést přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

> **Příklad:** Protože standardní školení, které uživatelé pouze povinně absolvují, se ukazují jako ne zcela účinná, přistupují některé organizace i k metodám ověřujícím skutečné pochopení informací předaných ve vlastním školení. Může jít například o rozeslání phishingových zpráv uživatelů po školení zaměřeném právě na tuto oblast. Organizace následně sleduje, kolik uživatelů na útok chybně reagovalo. Je však třeba upozornit, že takovéto testy musí být dobře promyšleny a při jejich plánování by neměl chybět právník, který posoudí, zda použitý test nebude například přílišným zásahem do soukromí zaměstnanců.

5.7. Řízení kontinuity činností

Řízení kontinuity činností (**B**usiness **C**ontinuity **M**anagement - **BCM**) představuje proces spočívající identifikaci klíčových prvků (systémů a procesů) v organizaci a následném nastavení procesů a postupů umožňujících zajištění kontinuity či obnovy těchto prvků, na předem definované úrovni, na které bude ještě možno plnit základní úlohy organizace.

V případě řízení kontinuity činností je třeba provést hodnocení rizik a analýzu stávajících informačních a komunikačních systémů a služeb a na základě takto získaných dat stanovit:

- **minimální úroveň poskytovaných služeb**, která je přijatelná pro užívání, provoz a správu informačního a komunikačního systému,
- **dobu obnovení chodu**, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačního a komunikačního systému,
- **bod obnovení dat** jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání.

Povinná osoba dále v rámci řízení kontinuity činností:

- **stanoví práva a povinnosti** administrátorů a **oso**b zastávajících bezpečnostní role,
- pomocí hodnocení rizik a analýzy dopadů vyhodnotí a **dokumentuje možné dopady kybernetických bezpečnostních incidentů a posoudí možná rizika** související s ohrožením kontinuity činností,
- **stanoví politiku řízení kontinuity činností**,
- **vypracuje, aktualizuje a pravidelně testuje plány kontinuity činností a havarijní plány** související s provozováním informačního a komunikačního systému a souvisejících služeb,
- **realizuje opatření pro zvýšení odolnosti informačního a komunikačního systému** vůči kybernetickým bezpečnostním incidentům a omezením dostupnosti.

5.8. Technická opatření

Technická opatření spolu s opatřeními organizačními představují základní prvky bezpečnostních opatření. Zatímco organizační opatření jsou primárně zaměřena na nastavení pravidel a politik v organizaci, technická opatření se primárně věnují pravidlům pro nastavení informačních a komunikačních systémů a služeb.

V rámci jednotlivých technických opatření budou demonstrovány i možné open source nástroje aplikovatelné pro dané opatření.

5.8.1 Fyzická bezpečnost

Fyzická bezpečnost je primárně zaměřena na ochranu technických aktiv daného subjektu. Maisner k fyzické bezpečnosti uvádí, že *„cílem tohoto opatření je především zamezení přístupu nepovolaných osob k jednotlivým prvkům infrastruktury, do serveroven, pracovišť správců systému apod. Snahou je vyloučit zcizení majetku přímo i nepřímo souvisejícího s informačním systémem, případně zamezit poškození hmotného i nehmotného vybavení nebo vybavení prostor. V neposlední řadě se snaží zamezit úniku informací a dat.“*[1]

Povinná osoba v rámci fyzické bezpečnosti

- **předcházet poškození**, krádeži nebo zneužití aktiv nebo přerušení poskytování služeb informačního a komunikačního systému,
- stanovit **fyzický bezpečnostní perimetr** ohraničující oblast, ve které jsou uchovávány a zpracovávány informace a umístěna technická aktiva informačního a komunikačního systému,
- **uplatnit** u fyzického perimetru **prostředky fyzické bezpečnosti:**
  - **k zamezení neoprávněnému vstupu,**
  - **k zamezení poškození a neoprávněným zásahům,**
  - **pro zajištění ochrany na úrovni objektů a v rámci objektů.**

Pojem fyzický **bezpečnostní perimetr** vymezuje určený prostor, respektive hranice tohoto prostoru. Oním prostorem může být například soubor objektů, objekt samotný či část objektu.

Objektem se rozumí budova nebo jiný ohraničený prostor. **Hranicí objektu** se rozumí plášť budovy, fyzická bariéra (oplocení) nebo jinak viditelně vymezená hranice oblasti. **Zabezpečenou oblastí** se rozumí stavebně nebo jinak viditelně ohraničený prostor v objektu.

Prostředky fyzické bezpečnosti mohou být:

- **mechanické zábranné prostředky** (např. zámky, dveře, mříže, folie, skla a další bezpečnostní konstrukční a stavební prvky, skříňové trezory, trezorové dveře a komorové trezory,
- **systém kontroly vstupu do zabezpečené oblasti** [poplachové a elektronické bezpečnostní systémy, detektory (pohybu, tříštění skla aj.) stanovení podmínek pro vstup: identifikační prvek, PIN, biometrie (případně jejich kombinace)],
- **zařízení elektrické zabezpečovací signalizace** (poplachové zabezpečovací a tísňové systémy – ústředny elektrické zabezpečovací signalizace, detektory elektrické zabezpečovací signalizace, otřesové detektory, perimetrické detekční systémy, tísňové systémy aj.),
- **speciální televizní systémy (kamerové systémy,** CCTV sledovací systémy aj.),
- **zařízení elektrické požární signalizace** (napojení do ústředny elektrické požární signalizace, nebo do ústředny elektrické zabezpečovací signalizace,
- **prostředky omezující působení požárů a živelných událostí** (poplachové systémy, detektory kouře, samočinné hasící systémy aj.,
- **zařízení pro zajištění ochrany před selháním dodávky elektrického napájení** (záložní zdroje – UPS, diesel agregáty aj.).

Dále lze implementovat například i:

- **zařízeními proti pasivnímu a aktivnímu odposlechu.**[2]

Do prostor, u kterých by z pohledu bezpečnosti informačních a komunikačních systémů měl být omezen, resp. regulován vstup, patří zejména **serverovny** (primární, záložní)**, prostory se síťovými prvky** (router, switch aj.), **úložiště dat** (kartotéky, NAS úložiště aj.), **prostory administrátorů ICT** aj.

> **Příklad:** Fyzická bezpečnost je jednou z oblastí, kde typicky dochází k porušování organizačních pravidel a kde je potřeba provádět periodické audity. Zatímco většinu ostatních činností vykonávají v organizaci administrátoři, správa fyzických přístupů bývá po samotné implementaci zabezpečení svěřena, například z důvodů úspor, méně kvalifikované pracovní síle, která navíc nemusí mít takové povědomí o vlastní problematice bezpečnosti.

Autor zažil několik situací, kdy po určité době začala osoba odpovědná za řízení fyzických přístupů udělovat oprávnění ke vstupům osobám, které do daných oblastí (např. serverovny) neměly mít přístup, například jen proto, že o přístup do chráněné oblasti požádal nadřízený manažer, který však k udělení souhlasu neměl dostatečná oprávnění.

V rámci fyzické bezpečnosti je možné využít i nástroje open source. Zejména půjde o případy *„realizace pultů centrální ochrany včetně kamerových přehledových systémů. Pro tento účel lze využít nástroje určené pro dohled síťových prvků (**Icinga, Nagios** a další), doplněné o rozhraní pro odpovídající čidla, propojené s pro gramy pro přenos a zachycení obrazového signálu z bezpečnostních kamer.“*[3]

5.8.2 Nástroj pro ochranu integrity komunikačních sítí

Někteří správci jsou v rámci fyzické bezpečnosti povinni:

- **zajistit segmentaci** komunikační **sítě**,
- zajistit řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě (tj. **řídit bezpečný přístup mezi vnitřní a vnější sítí**),

- **pomocí kryptografie zajistit důvěrnost a integritu dat při vzdáleném přístupu**, vzdálené **správě nebo při přístupu do** komunikační **sítě pomocí bezdrátových technologií** (tj. zajistit pomocí kryptografie například VPN, připojování ICT na Wi-Fi aj.),
- **aktivně blokovat nežádoucí komunikaci** (např. spam filtry aj.),
- pro zajištění segmentace sítě a pro řízení komunikace mezi jejími segmenty využívat nástroj, který zajistí ochranu integrity komunikační sítě.

*„Nástrojem pro ochranu integrity komunikačních sítí se tady rozumí **vhodně navržená topologie sítě** včetně použití síťových prvků umožňujících požadovanou segmentaci sítě a filtraci provozu mezi jednotlivými prvky. Použitá zařízení pro dosažení těchto požadavků představují ethernetové switche, routery a firewally. Pokud nelze zajistit segmentaci sítě pomocí VLAN na upravovatelném přepínači, je možné ji zabezpečit prostřednictvím několika menších nemanagovatelných switchů, z nich každý realizuje jednu fyzickou LAN.*

Při segmmentaci některých sítí je možné využít např. i routery Turris (https://www.turris.cz/cs/), kde je garantována vysoká bezpečnost (mj. díky firmwaru, který byl navržen s ohledem a dosažení maximálního možného zabezpečení) a rovněž nízký elektrický příkon.

*Softwarové **routery/firewally**: www.ipcop.org/ ; https://www.ipfire.org/*

*Ethernetový **switch** pro virtualizované prostředí: http://www.openvswitch.org/".*[4]

5.8.3 Nástroj pro ověřování identity uživatelů

Někteří správci jsou v rámci fyzické bezpečnosti povinni používat nástroj pro správu a ověření identity uživatelů, administrátorů a aplikací informačního a komunikačního systému.

Tento nástroj je v současnosti de facto součástí všech běžně používaných operačních systémů (Linux, iOS, Windows). Dle VoKB má tento nástroj zajistit

- **ověření identity osoby** (před zahájením aktivit v informačním a komunikačním systému),
- **řízení počtu** možných neúspěšných **pokusů o přihlášení**,
- **odolnost** uložených nebo přenášených **autentizačních údajů proti neoprávněnému odcizení a zneužití**,
- **ukládání autentizačních** údajů ve formě odolné proti off-line útokům,
- **opětovné ověření identity** po určené době nečinnosti,
- **dodržení důvěrnosti autentizačních údajů** při obnově přístupu,
- **centralizovanou správu identit**.

Povinná osoba pro ověření identity uživatelů, administrátorů a aplikací využívá:

1. **autentizační mechanizmus**, který není **založený** pouze na použití identifikátoru účtu a hesla, nýbrž **na vícefaktorové autentizaci s nejméně dvěma různými typy faktorů,**

2. nástroj pro ověření identity uživatelů, administrátorů a aplikací, používat **autentizaci pomocí kryptografických klíčů** a zaručit obdobnou úroveň bezpečnosti[5],

3. nástroj pro ověření identity uživatelů, administrátorů a aplikací, který používá k **autentizaci identifikátor účtu a heslo.**[6]

V případě, že je k autentizaci využito účtu a hesla, musí být splněny následující podmínky:

- minimální délka hesla:
  - **12 znaků u uživatelů** a
  - **17 znaků u administrátorů a aplikací.**
- **možnost zadat heslo o délce alespoň 64 znaků,**
- možnost použít v hesle **malá a velká písmena, číslice a speciální znaky,**
- **možnost změny hesla**, přičemž **doba mezi dvěma změnami** hesla **nesmí být kratší než 30 minut,**
- **neumožnit uživatelům a administrátorům:**
  - **zvolit si nejčastěji používaná hesla,**
  - **tvořit hesla na základě** mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem,
  - opětovné použití dříve používaných hesel **s pamětí alespoň 12 předchozích hesel.**
- pro **povinnou změnu hesla v intervalu maximálně po 18 měsících**, přičemž toto pravidlo se nevztahuje na účty sloužící k obnově systému v případě havárie,
- **vynutí bezodkladnou změnu výchozího hesla po jeho prvním použití,**
- **bezodkladně zneplatní heslo sloužící k obnovení přístupu po jeho prvním použití nebo uplynutím nejvýše 60 minut od jeho vytvoření**,
- **zahrne pravidla tvorby bezpečných hesel do plánu rozvoje bezpečnostního povědomí.**

> **Příklad:** Doporučujeme při školení uživatelů využít i praktické ukázky. Například nástroje CEWL, nebo CUPP. Oba lze nalézt například v linuxové distribuci Kali. Nástroj CEWL umí vytvořit slovník pro slovníkový útok na míru konkrétní organizaci a to na základě obsahu jejích webových stránek. Nástroj CUPP pak umí vytvořit slovník konkrétnímu uživateli na míru. Tyto praktické ukázky jsou dle zkušenosti autorů pro uživatele velmi přínosné, neboť na nich prakticky vidí, že jejich dosud používané heslo složené například z data narození a jména rodinného psího mazlíčka lze skutečně vygenerovat, pokud o nich má útočník dostatek informací.

„Pro praktické ověřování identity uživatelů nabízí komunita open source dostatek softwaru kompatibilního se svými komerčními protějšky. Jde například o:

FreeRADIUS - http://freeradius.org/ /RADIUS

OpenLDAP - http://www.openldap.org/ /Microsoft AD, Oracle Internet Directory

Kerberos - https://www.gnu.org/software/shishi/

OpenDiameter - https://sourceforge.net/projects/diameter/

Všechny tyto nástroje poskytují prostředky pro vynucení určené složitosti hesla, jakož i dalších atributů požadovaných ZoKB, buď samy o sobě prostřednictvím login.conf*, nebo s využitím externích mechanismů jako cracklib a slovníků oblíbených „hesel".*[7]

5.8.4 Nástroj pro řízení přístupových oprávnění

Někteří správci jsou v rámci fyzické bezpečnosti povinni používat centralizovaný nástroj pro řízení přístupových oprávnění.

Pojmem **oprávnění** se rozumí právo přístupu k některému z aktiv (typicky informačnímu či komunikačnímu systému, aplikacím aj.). V praxi se jedná o nástroj „správy uživatelů a skupin" a nástroj nastavování oprávnění k souborům a adresářům. Tyto nástroje jsou proprietární součástí všech standardně využívaných operačních systémů.

Centralizovaný nástroj pro řízení přístupových oprávnění, má zajistit řízení oprávnění:

- pro přístup k jednotlivým aktivům informačního a komunikačního systému a
- pro čtení dat, zápis dat a změnu oprávnění.

Je vhodné aplikovat nástroje pro centralizovanou správu přístupových oprávnění, **které budou komunikovat s centrálním AAA** (**A**uthentication, **A**uthorisation, **A**ccounting) **serverem**.

> **Příklad:** Důležité je pamatovat na řízení přístupových oprávnění již při samotném návrhu softwaru. Autor zná aplikaci, která měla velmi obecná oprávnění a v podstatě v ní existovaly pouze role administrátora a uživatele. Administrátor byl oprávněn přidávat další uživatele a administrátory a uživatel byl oprávněn k ostatním činnostem. Tato aplikace však uchovávala důležité informace o zákaznících dané organizace. Protože tato aplikace neumožňovala žádnou granuralitu oprávnění, všichni uživatelé, bez ohledu na jejich skutečné pracovní potřeby, byli oprávněni přistupovat do jakékoliv části informací o zákaznících. Tato situace nakonec vyústila v únik dat týkajících se konkrétní zákaznice.

5.8.5 Nástroj pro ochranu před škodlivým kódem

Někteří správci jsou v rámci fyzické bezpečnosti nastavit ochranu před škodlivým kódem a to tak, že:

- **zajišťují** (s ohledem na důležitost aktiv) **použití nástroje pro nepřetržitou automatickou ochranu**
  - koncových stanic,
  - mobilních zařízení,
  - serverů,
  - datových úložišť a výměnných datových nosičů,
  - komunikační sítě a prvků komunikační sítě,
  - obdobných zařízení.
- **monitorují a řídí používání výměnných zařízení a datových nosičů,**
- **řídí automatické spouštění obsahu** výměnných zařízení a datových nosičů,
- **řídí oprávnění ke spouštění kódu,**
- **provádí pravidelnou a účinnou aktualizaci** nástroje pro ochranu před škodlivým kódem.

*„**Ochrana před škodlivým softwarem šířeným prostřednictvím e-mailu.** Open source řešením e-mailové proxy, zajišťujícím ochranu před škodlivým softwarem, je projekt ASSP (AntiSpam SMTP Proxy, https://sourceforge.net/projects/assp/), umožňující komplexní konfiguraci chování mail proxy prostřednictvím webového rozhraní.*

***Ochrana před škodlivým softwarem šířeným prostřednictvím webu.** Vhodným řešením je například projekt HTTP AntiVirus Proxy (http://www.havp.org/) nebo www.cacheguard.com. I zde je nutné zajistit také odpovídající ochranu koncových pracovních stanic, protože šifrovaný provoz není možné v reálném čase skenovat v pozici ‚muže uprostřed'.*

Blokování jeho síťového provozu, a to jak na úrovni datové infrastruktury, tak na úrovni ‚osobních firewallů' koncových stanic. Pravidla síťové komunikace by se měla nastavit ‚paranoidně', tj. povolit jen provoz nezbytný k fungování legitimního softwaru, vše ostatní zakázat. Opatření na straně serveru, proxy serveru či prvku síťové infrastruktury ale v žádném případě plně nenahrazuje ochranu proti škodlivému softwaru na koncových pracovních stanicích, zejména proto, že nemusí být vždy schopné zachytit šifrovaný provoz, který je dešifrován až na klientském programu."[8]

5.8.6 Nástroj pro detekci kybernetických bezpečnostních událostí

Někteří správci jsou v rámci fyzické bezpečnosti povinni implementovat, v rámci komunikační sítě, jejíž součástí je informační a komunikační systém, nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí:

- **ověření a kontrolu přenášených dat v rámci komunikační sítě** a mezi komunikačními sítěmi,
- **ověření a kontrolu přenášených dat na perimetru** komunikační sítě a
- **blokování nežádoucí komunikace**.

„K detekci kybernetických bezpečnostních událostí lze využít výstupů z mnoha softwarových nástrojů, například prohledávačů logů Logwatch (https://sourceforge.net/projects/logwatch/files/), Epylog (https://fedoraproject.org/wiki/Infrastructure/Fedorahosted-retirement), intrusion detection systémů jako OpenVAS (http://openvas.org/), Suricata (https://suricata-ids.org/), Snort (https://www.snort.org/) nebo Samhain (la-samhna.de/Samoin)."[9]

5.8.7 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Někteří správci jsou v rámci fyzické bezpečnosti musí používat **nástroj pro sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí**, který umožní

- **sběr a vyhodnocování událostí**,
- **vyhledávání a seskupování souvisejících záznamů,**
- **poskytování informací pro určené bezpečnostní role** o detekovaných kybernetických bezpečnostních událostech,
- **vyhodnocování kybernetických bezpečnostních událostí** s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí,
- omezení případů nesprávného vyhodnocení událostí pravidelnou aktualizací nastavení pravidel pro:
  - vyhodnocování kybernetických bezpečnostních událostí,
  - včasné varování,
- využívání informací získaných nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí pro optimální nastavení bezpečnostních opatření informačního a komunikačního systému.

Nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí se rozumí nástroje, které jsou označovány jako **SIEM** (**S**ecurity **I**ncident and **E**vent **M**anagement).

V rámci open source řešení SIEM je možné využít například OSSIM/USM (https://www.alienvault.com/products/usm-anywhere/try-it-now), OSSEC (www.ossec.net/) nebo logalyze (www.logalyze.com).[10]

5.8.8 Aplikační bezpečnost

V případě aplikační bezpečnosti je pozornost věnována aplikacím, které jsou využívané v informačních systémech (ať již v rámci počítačového systému, mobilního zařízení, či jako webová aplikace). Aplikační bezpečnost je mimo jiné zajišťována penetračním testováním aplikací, či aplikačními firewally.

Někteří správci jsou v rámci fyzické bezpečnosti povinni provádět **penetrační testy** informačního a komunikačního systému se zaměřením na důležitá aktiva, a to:

- **před** jejich **uvedením do provozu a**
- **v souvislosti s významnou změnou**.

Povinná osoba v rámci aplikační bezpečnosti dále musí **zajistit trvalou ochranu aplikací**, **informací a transakcí před:**

- neoprávněnou činností,
- popřením provedených činností.

„Z aplikačních firewallů je možné uvést například bezpečnostní moduly webserveru (www.modsecurity.org) nebo OWASP Web Application Firewall. Z komerčních nástrojů pro testování aplikační bezpečnosti jde zejména o nástroj Nessus (www.tenable.com/products/nessusvulnerability-scanner). Jeho open source alternativou je pak projekt Open-VAS (www.openvas.org/).“ [11]

5.8.9 Kryptografické prostředky

Kryptografie (šifrování) je vědní obor, který se zabývá převodem informací srozumitelných do podoby nesrozumitelné pro příjemce, pokud tento nevlastní klíče, kterým je možné provést rozšifrování dané informace.

S přesunem značného množství dat a informací do systémů ICT je nezbytné věnovat zvýšenou pozornost právě možnostem šifrování (utajování obsahu) přenášených dat.

Někteří správci jsou v rámci fyzické bezpečnosti povinni pro ochranu aktiv informačního a komunikačního systému:

- používat aktuálně odolné kryptografické algoritmy a kryptografické klíče,
- používat systém správy klíčů a certifikátů, který:
  - zajistí generování, distribuci, ukládání, změny, omezení platnosti, zneplatnění certifikátů a likvidaci klíčů,
  - umožní kontrolu a audit.
- prosazovat bezpečné nakládání s kryptografickými prostředky,
- zohledňovat doporučení v oblasti kryptografických prostředků vydaná Úřadem (NÚKIB), zveřejněná na jeho internetových stránkách.

„Pro účely zajištění dostatečně odolného šifrování síťového provozu se používají knihovny OpenSSL (openssl.org*), avšak je třeba mít zajištěnou jejich aktuálnost a správnou konfiguraci, tak aby se vyhovělo podmínkám této vyhlášky. Je nutné sledovat aktuální zprávy o zranitelnostech a nevyhovující verze knihoven bez otálení upgradovat na varianty bez známých zranitelností. V tomto ohledu lze doporučit projekt bettercrypto (https://bettercrypto.org/), který má administrátorům pomoci s co nejlepším zabezpečením jimi používaných služeb a používané kryptografie.“*[12]

5.8.10 Nástroj pro zajišťování úrovně dostupnosti informací

Někteří správci jsou v rámci fyzické bezpečnosti povinni zavést opatření pro zajišťování úrovně dostupnosti, kterými zajistí:

- **dostupnost informačního a komunikačního systému**,
- **odolnost informačního a komunikačního systému** vůči kybernetickým bezpečnostním incidentům, které by mohly snížit jeho dostupnost,
- **dostupnost důležitých technických aktiv** informačního a komunikačního systému,

- **redundanci aktiv** nezbytných pro zajištění dostupnosti informačního a komunikačního systému.

Implementací nástroje pro zajišťování úrovně dostupnosti informací dochází k naplňování organizačního aktiva: řízení kontinuity činností (**B**usiness **C**ontinuity **M**anagement – **BCM**).

„Pro dosažení předepsané úrovně dostupnosti lze použít clusterové a cloudové technologie vyvíjené jako open source (KVM, OpenStack), případně zajistit dostupnost náhradního aktiva v určeném čase prostřednictvím back-up/restore softwaru (https://sourceforge.net/projects/bacula/).“ ***[13]***

---

[1] MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015. 91

[2] Proti pasivnímu a aktivnímu odposlechu musí být oblast zajištěna dostatečně zvukotěsnými stěnami, dveřmi, podlahou a stropem, okna, větrací otvory nebo prostupy klimatizace musí být chráněny technickými prostředky. Oblast musí být chráněna proti odezírání z míst nacházejících se vně jednací oblasti. Do oblasti nesmí být umístěn jakýkoliv nábytek nebo jakékoliv zařízení, pokud neprošly kontrolou, zda v jednací oblasti nedochází k nedovolenému použití technických prostředků určených k získávání informací. Nábytek a zařízení oblasti musí být evidováno (včetně typu, případně sériového a inventárního čísla), včetně historie pohybu. Umísťovat telefonní přístroje v oblasti není žádoucí. Pokud je jejich instalace bezpodmínečně nutná, musí být vybaveny odpojovačem nebo odpojovány ručně před jednáním. Do oblasti nelze vnášet mobilní telefony, jakákoliv nahrávací zařízení, vysílací zařízení, jakákoliv testovací, měřící a diagnostická zařízení a další elektronická zařízení (toto neplatí v případě, že jde o zařízení používané v rámci prováděné prohlídky s vědomím odpovědné osoby nebo jí pověřené osoby. Pro oblast musí být zpracována pravidla pro evidenci a pohyb osob a zařízení.

[3] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[4] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[5] Za předpokladu, že povinná osoba doposud nesplnila první z preferovaných autentizačních mechanismů.

[6] Za předpokladu, že povinná osoba doposud nesplnila první či druhý z preferovaných autentizačních mechanismů

[7] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[8] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[9] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[10] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[11] Tamtéž

[12] KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

[13] Tamtéž

5.9. SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

- Důvodů pro zavádění a implementaci kybernetické bezpečnosti existuje celá řada. Mezi ty nejběžnější je možné zařadit například negativní ekonomický dopad v případě úspěšného kybernetického útoku, při kterém jsou zcizena citlivá data. Úspěšný kybernetický útok také může ohrozit vlastní chod a fungování organizace, neboť může dojít například k omezení přístupu k počítačovým systémům nebo datům pomocí ransomware. Dalším z důvodů pro zavedení kybernetické bezpečnosti také může být i ztráta kredibility dané napadené organizace.
- V současné době je nejvýznamějším dokumentem Evropské unie, vztahujícím se k problematice kybernetické bezpečnosti, DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union.
- Systém řízení bezpečnosti informací (angl. Information Security Management System - ISMS) představuje soubor pravidel, jejichž cílem je zachovat důvěrnost, integritu a dostupnost informací aplikováním procesu řízení rizik a dát jistotu zainteresovaným stranám, že jsou rizika přiměřeně řízena.
- Řešení ISMS vyžaduje systémový a komplexní přístup, respektující principy a prvky v rámci celého životního cyklu kybernetické bezpečnosti. Systém řízení ISMS je založen na Demingově cyklu, neboli též na PDCA cyklu (Plan-Do-Check-Act; Plánuj-Dělej-Kontroluj-Jednej).
- PDCA cyklus je jedním ze základních manažerských principů spočívající v postupném zlepšování kvality procesů, služeb, dat, výrobků aj. díky neustálému opakování jeho čtyř základních činností: Plan-Do-Check-Act.
- Hodnota rizika je nejčastěji vyjádřena jako funkce, kterou ovlivňuje dopad, hrozba a zranitelnost. Pro vlastní hodnocení rizika lze využít například následující funkci:
    - Riziko = dopad * hrozba * zranitelnost
- Bezpečnostní politikou rozumí soubor zásad a pravidel, které určují způsob zajištění ochrany aktiv.
- Vymezení organizační bezpečnosti a zejména ukotvení kybernetické či ICT bezpečnosti v rámci již fungujících struktur organizace je velmi zásadní pro případné zvládání kybernetických hrozeb či útoků.
- Aktivem se rozumí cokoliv, co má určitou hodnotu pro osobu, organizaci či stát.
- Podpůrným aktivem je technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému.
- Primárním aktivem je informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém
- Řízení kontinuity činností (Business Continuity Management - BCM) představuje proces spočívající identifikaci klíčových prvků (systémů a procesů) v organizaci a následném nastavení procesů a postupů umožňujících zajištění kontinuity či obnovy těchto prvků, na předem definované úrovni, na které bude ještě možno plnit základní úlohy organizace.

KLÍČOVÁ SLOVA K ZAPAMATOVÁNÍ

- NIS directive
- ISMS
- PDCA
- Hrozba
- Riziko
- Dopad
- Zranitelnost
- Bezpečnostní politika
- Aktivum
- Fyzická bezpečnost
- Business Continuity Management

KONTROLNÍ OTÁZKY

- Definujte ISMS.
- Co je to PDCA cyklus a jak se uplatňuje?
- Jaké komponenty je možné zařadit do fyzické bezpečnosti?
- Co znamená: Business Continuity Management?
- Definujte pojem hrozba.
- Definujte pojem riziko.
- Definujte pojem dopad.
- Definujte pojem zranitelnost.
- Definujte pojem aktivum.
- Jaká aktiva rozeznáváme a co vše je aktivem?

6. Ochrana osobních údajů v kyberprostoru

Na prvním místě se chci věnovat ochraně fyzické osoby, konkrétně ochraně podoby a soukromí jedince. Soukromí je jedním ze základních lidských práv, zakotvených ve Všeobecné deklaraci lidských práv z roku 1948[1].

---

[1] Dostupné online: http://www.osn.cz/wp-content/uploads/2015/03/vseobecna-deklarace-lidskych-prav.pdf

Ve všeobecné deklaraci lidských práv jsou tato práva primárně zakotvena v článcích 12 a 18.

Čl. 12: *„**Nikdo nesmí být vystaven svévolnému zasahování do soukromého života**, do rodiny, domova **nebo korespondence**, ani útokům na svou čest a pověst. **Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.**“*

Čl. 18: *„Každý má právo na svobodu myšlení, svědomí a náboženství; toto právo zahrnuje v sobě i volnost změnit své náboženství nebo víru, jakož i svobodu projevovat své náboženství nebo víru, sám nebo společně s jinými, ať veřejně nebo soukromě, vyučováním, prováděním náboženských úkonů, bohoslužbou a zachováváním obřadů.“*

6.1. Exkurze do práv a povinností vyplývajících z některých právních norem

Jsme bytostně přesvědčeni o tom, že **není vhodné odděleně řešit problematiku kybernetické bezpečnosti a dalších oblastí** (např. ochrany osobních údajů, dat souvisejících s elektronickými komunikacemi a jiných obdobných dat).

Důvod pro toto přesvědčení spočívá ve stále větší integraci a vzájemné provázanosti různých kategorií dat s počítačovými systémy a aplikacemi v nich provozovanými. Tato provázanost a digitalizace analogových dat do budoucna jen poroste.

Z tohoto důvodu se jako vhodné východisko jeví řešit problematiku bezpečnosti komplexně, a nejen v souvislosti s právy a povinnostmi vyplývajícími ze zákona o kybernetické bezpečnosti, či z jiného právního předpisu.

Cílem organizace či jednotlivce by mělo být zavedení takových pravidel, procesů, postupů a bezpečnostních opatření, která budou splňovat jak požadavky vyplývající z NIS, tak i například z GDRP, ePrivacy, eIDAS aj. Takovýto postup umožní vytvořit **integrovanou bezpečnost**.[1]

Obrázek: Ukázka řešení integrované bezpečnosti[2]

---

[1] Blíže viz např. GREENFIELD, David. *Integrovaná bezpečnost: Už nastal její čas?* [online]. [cit. 1. 3. 2018]. Dostupné z: http://www.controlengcesko.com/hlavni-menu/artykuly/artykul/article/integrovana-bezpecnost-uz-nastal-jeji-cas/

[2]*Integrovaná multidisciplinární bezpečnost.* [online]. [cit. 17. 2. 2018]. Dostupné z: https://www2.deloitte.com/cz/cs/pages/risk/solutions/integrovana-multidisciplinarni-bezpecnost.html

6.2. GDPR

Obecné nařízení o ochraně osobních údajů (EU) 2016/679 (anglicky: General Data Protection Regulation neboli GDPR)[1] je jedním z významných mezinárodních právních dokumentů, který s problematikou kybernetické bezpečnosti bezprostředně souvisí, byť není primárně cílen do oblasti ICT.

*„**GDPR ≠ IT + software.***

Nové nařízení o ochraně osobních údajů má 778 řádků a z toho jen 26 se přímo týká IT bezpečnosti. Máte představu, co obsahují ty ostatní?“

Mgr. Eva Škorničková[2]

Právě na GDPR a implementaci povinností z tohoto nařízení vyplývajících je možné demonstrovat tu skutečnost, že je vhodné řešit komplexně problematiku bezpečnosti, a ne uměle izolovat povinnosti vyplývající z různých právních norem (v tomto případě ze zákona o kybernetické bezpečnosti a GDPR).

Cílem této publikace není provést samostatný a komplexní rozbor problematiky GDPR. Na tomto místě budou definovány pouze dílčí pojmy a práva a povinnosti, které z GDPR vyplývají a zároveň mají přesah do oblasti kybernetické bezpečnosti.

Nařízení GDPR představuje **obecný právní rámec ochrany osobních údajů** platný a účinný na celém území EU a v určitých případech i mimo toto teritorium. Hlavním cílem GDPR je zajistit komplexní ochranu práv subjektů údajů proti neoprávněnému zacházení s jejich daty a osobními údaji, nastolit rovnováhu mezi oprávněnými zájmy správců, zpracovatelů a subjektů údajů, vytvořit systém jednotné vymahatelnosti práva a jednotného sankčního mechanismu v této oblasti atd.

Rozsah shromažďování a sdílení osobních údajů právě díky informačním a komunikačním technologiím a službám, které jsou na ně navázány, významně vzrostl. Informační a komunikační technologie umožňují jak soukromým společnostem, tak orgánům veřejné moci využívat při provádění jejich činností osobní údaje v nebývalém rozsahu. Na druhou stranu je také možné pozorovat masivní dobrovolné zveřejňování osobních údajů samotnými fyzickými osobami, jichž se tyto údaje týkají.

Informační a komunikační technologie výrazně změnily ekonomiku i společenský život a měly by usnadňovat volný pohyb osobních údajů v rámci Evropské unie a předávání těchto údajů do třetích zemí a mezinárodním organizacím. Současně by však tyto technologie a procesy s nimi spojené měly zajistit vysokou úroveň ochrany osobních údajů.[3]

Díky výše uvedenému však **vzniká zajímavý paradox**, který spočívá v následujících bodech:

- **fyzické osoby samy a dobrovolně o sobě zveřejňují stále větší množství dat** (fotografie, videa aj.), přičemž k distribuci těchto dat typicky využívají služby informační společnosti, které jsou založeny na EULA[4] či SLA[5] mezi uživatelem a poskytovatelem služby,
- **nejvíce jsou osobní údaje zveřejňovány v rámci sociálních sítí**, které z podstaty své funkce takovéto zveřejňování předpokládají a zakotvují ve smluvních podmínkách pravidla, na základě kterých je s takovýmito daty zacházeno,
- **fyzické osoby při využívání řady služeb informační společnosti předpokládají, a mnohdy i očekávají interakci mezi těmito technologiemi a jejich kyberosobností**[6],
- mezinárodní společenství, stát, ale i **fyzické osoby** samy **vyžadují vyšší zabezpečení osobních údajů a znemožnění přístupu k těmto údajům jiným** (zpravidla neoprávněným) **subjektům, a to vše za podmínky zachování existence prvních tří bodů tohoto paradoxu.**

Důsledek tohoto paradoxu je zřejmý. Poskytovatelé služeb informační společnosti[7] tak musí věnovat vyšší úsilí zabezpečení jednotlivých služeb, které koncovému uživateli poskytují, vyšší úrovni zabezpečení dat vztahujících se k uživateli, modifikaci stávajících smluvních podmínek a zavedení dalších požadavků vyplývajících z GDPR.

6.2.1 Místní působnost GDPR

Někoho by mohlo napadnout, že způsobem, jak se vyhnout GDPR, by bylo přesunout se mimo jeho dosah, tedy mimo teritorium EU. Nařízení GDPR se však uplatní v případech, kdy:

- **provozovna správce nebo zpracovatele je v EU**, bez ohledu na to, zda zpracování probíhá v EU,
- **správci nebo zpracovatelé nejsou usazení v EU**, **ale**
  - zboží nebo služby jsou nabízeny subjektům údajů v EU (bez ohledu na úplatu),
  - je monitorováno chování subjektů údajů v rámci EU.[8]

Díky takto vymezené místní působnosti má GDPR exteritoriální dosah a de facto se bude vztahovat na všechny služby informační společnosti, ke kterým lze získat přístup z geografického teritoria EU, nebo které monitorují chování subjektů údajů v rámci EU.

6.2.2 Osobní údaj

Osobním údajem dle čl. 4 odst. 1 GDPR jsou *„**veškeré informace** o **identifikované nebo identifikovatelné fyzické osobě**. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat zejména odkaz na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“*

Osobním údajem je dle GDRP **jakákoliv informace** (např. obrazová, písemná, slovní, digitální, genetická, zdravotnická aj.), která **má vztah** (obsahem – např. jméno, adresa, pracovní zařazení, e-mail aj.), **k subjektu údajů.**[9] Z tohoto pohledu a v souladu s výkladem uvedeným v recitálech 30, 34, 35, 38 GDPR[10] je třeba za osobní údaj považovat:

- jméno a příjmení,
- **identifikační číslo**,
- rodné číslo,
- **lokační údaje (geo-)**,
- věk a datum narození,
- pohlaví,
- osobní stav,
- občanství,
- **síťové identifikátory**,
  - **IP adresa**,
  - **identifikátory cookies**,
  - radio frequency identification tags aj.,
- **fotografie**,
- **prvky** fyzické, fyziologické, genetické, psychické, ekonomické, **kulturní nebo společenské identity**,
- osobní či pracovní adresa,
- osobní či pracovní telefonní číslo,
- **osobní či pracovní e-mail**,
- **ověřovací identifikační údaje**,
- identifikační čísla vydaná státem.

Tučně vyznačené osobní údaje mají typicky vztah k informačním a komunikačním technologiím a aplikacím, které tyto technologie využívají. Rozšíření okruhu dat, jež je možné považovat za osobní údaje, výrazným způsobem zasahuje do problematiky kybernetické bezpečnosti a zajištění ochrany dat, která jsou spravována v dané organizaci.

Pokud se zaměříme na **položku síťových identifikátorů a ověřovacích identifikačních údajů, zjistíme, že za osobní údaj může a zřejmě i bude považována řada dat umožňujících základní fungování počítačového systému v síti.**

Velmi často byla v praxi diskutována otázka - je IP adresa osobním údajem?

V této věci je vhodné krom GDPR přihlédnout i k judikatuře Soudního dvora EU, který mimo jiné rozhodoval v kauze: **Patrick Breyer** proti **Bundesrepublik Deutschland.**[11]

Patrick Bayer se u německých soudů domáhal, aby Německo přestalo uchovávat jeho IP adresy, které získalo při jeho „návštěvách" několika internetových stránek německých spolkových orgánů, které byly veřejně přístupné. Z pohledu činnosti provozovatelů dotčených webových stránek se jednalo o klasické logování služeb tímto ISP[12] nabízených.

Německé soudy přerušily řízení a položily předběžnou otázku soudnímu dvoru EU, protože v dané věci neexistuje jednotný výklad práva EU.

Jde zejména o to, jestli k tomu, aby nějaký údaj byl osobním údajem, a tedy identifikoval konkrétní osobu, je třeba vycházet z *„objektivního"*, či *„relativního"* kritéria.

„Objektivní" kritérium znamená, že údaje, jako jsou **IP adresy**, **by mohly být považovány za osobní údaje** zpracovávané ISP jiných služeb než připojení (např. provozovatelem internetové stránky), **a to i tehdy, pokud by byla schopna identifikovat konkrétního uživatele jen třetí osoba** (typicky ISP připojení).

„Relativní" kritérium znamená, že **IP adresy by mohly být považovány za osobní údaj u ISP připojení**, neboť mu umožňují přesně určit totožnost uživatele, **ale už ne u ISP služeb, který disponuje skutečně pouze údajem o IP adrese a nezná jméno návštěvníka.**

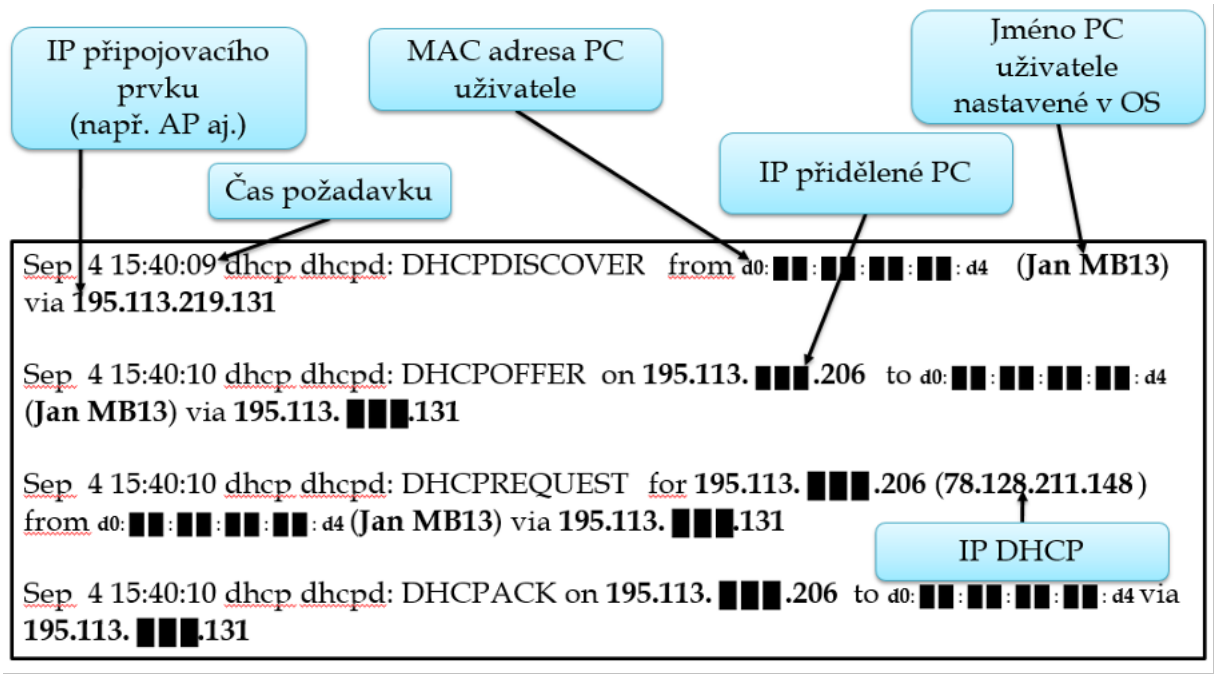
Soudní dvůr EU konstatoval, že **je nesporné, že dynamická IP adresa nepředstavuje informaci o „identifikované osobě"**, neboť **adresa přímo neodhaluje totožnost fyzické osoby**, která je majitelem počítače, ze kterého byla navštívena internetová stránka, **ani totožnost jiné osoby, která mohla tento počítač používat**.

Na druhou stranu však Soudní dvůr (druhý senát) také uvedl (následně i rozhodl), že **dynamická adresa** internetového protokolu, **kterou poskytovatel on-line mediálních služeb uchovává v souvislosti s přístupem osoby na internetovou stránku,** kterou tento poskytovatel zpřístupnil veřejnosti, pro uvedeného poskytovatele **představuje osobní údaj ve smyslu** článku 2 písm. a) směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, **pokud má poskytovatel k dispozici právní prostředky, které mu umožňují nechat identifikovat subjekt údajů díky dalším informacím, kterými disponuje poskytovatel internetového připojení tohoto subjektu.**

Dynamická IP adresa může být dle tohoto rozsudku, z 19. října 2016, za určitých okolností osobním údajem.

Dopad té skutečnosti, že **IP adresa, jakožto i další síťové identifikátory mohou být osobním údajem,** demonstrujeme na dvou příkladech.

Na následujícím obrázku je možné vidět komunikaci PC a jednotlivých prvků sítě (AP, DHCP server) a následné připojení PC do sítě.

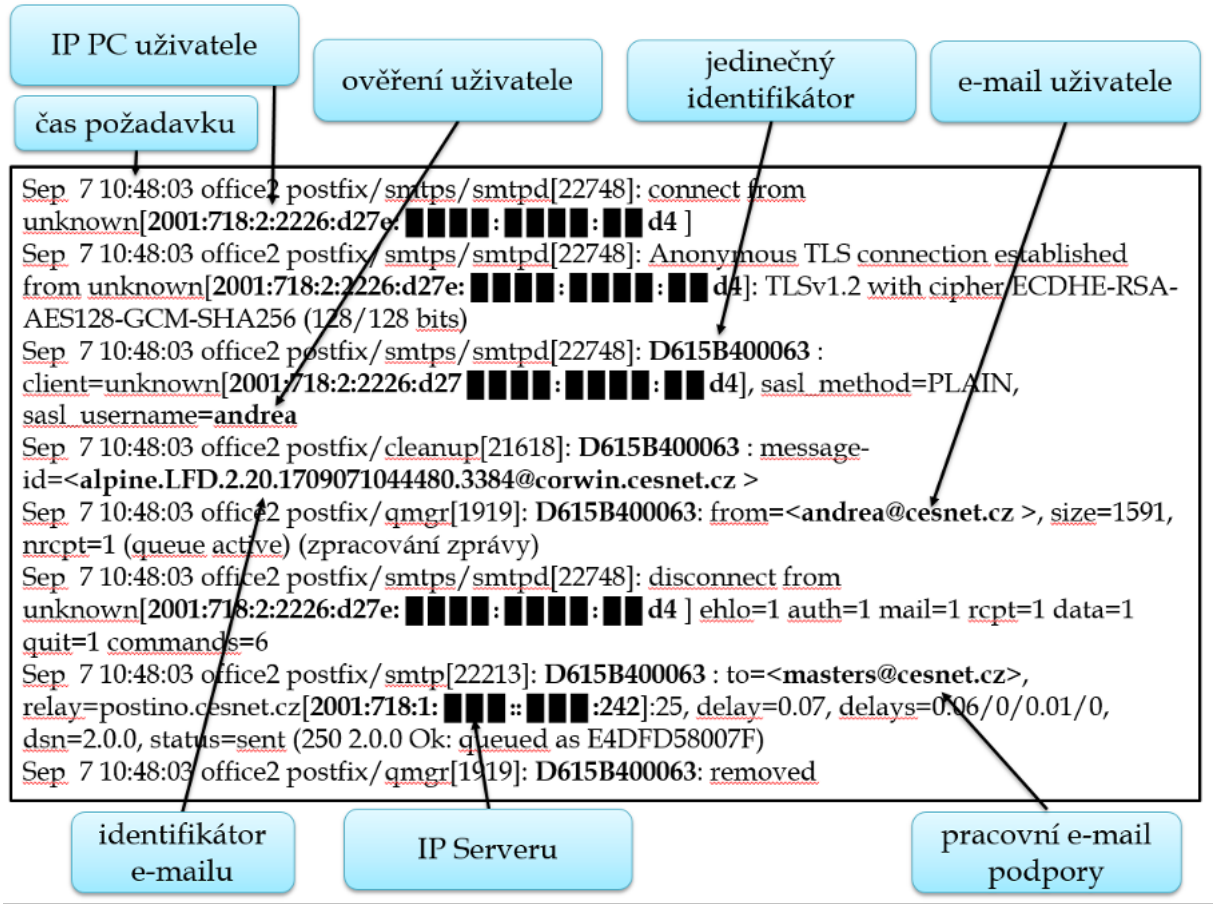


Obrázek: DHCP

Pokud se důsledně zaměříme na **data** (informace)**, která mají vztah k subjektu údajů a jsou jej schopny identifikovat**, pak osobním údajem v tomto případě nebude pouze IP adresa připojovacího prvku a IP adresa DHCP serveru.

Osobním údajem je teoreticky i čas daného požadavku, neboť se jedná o stopu, která může být zejména v kombinaci s jedinečnými identifikátory a dalšími informacemi, které servery získávají, použita k identifikaci fyzické osoby.[13] Zároveň se jedná o velmi podstatnou informaci, neboť bez přesného času není možné identifikovat, komu (jakému počítačovému systému) byla přidělena konkrétní IP adresa.

Dalším příkladem zobrazujícím rozsah zpracovávání dat, která je možné považovat za osobní údaje, je zpracování osobních údajů při odeslání e-mailu prostřednictvím SMTP.



Obrázek: SMTP

Pokud se opět důsledně zaměříme na **data** (informace)**, která mají vztah k subjektu údajů a jsou schopna jej identifikovat**, pak osobním údajem v tomto případě nebude pouze IP adresa serveru.

Pracovní e-mail podpory by mohl být opět osobním údajem, pokud k němu budou přiřazeny další identifikátory, které jsou schopné identifikovat fyzickou osobu.

Klíčovou otázkou je, zda jsme v rámci veškerých procesů, které se odehrávají v počítačových systémech (prvcích ICT), které jsou daným subjektem (fyzická či právnická osoba) spravovány, **schopni rozlišit situaci, kdy dochází k přenosu dat čistě mezi počítačovými systémy, bez vztahu k jakékoliv fyzické osobě, a kdy už se do těchto procesů zapojí fyzická osoba jakožto subjekt údajů dle GDPR**.

Domníváme se, že až na specifické výjimky nebudeme schopni vyčlenit procesy, které se odehrávají bez lidské interakce. Na základě tohoto tvrzení je následně třeba aplikovat požadavky vyplývající z GDPR na veškeré procesy, při nichž dochází k manipulaci s informacemi, které mají vztah k subjektu údajů a jsou jej schopny identifikovat. Zároveň bude třeba přijmout dostatečná bezpečnostní opatření, aby byla dostatečně chráněna jak přenosová soustava, počítačové systémy a aplikace, které s takovýmito informacemi pracují, tak informace (resp. data) samotná.

Vedle shora uvedených osobních údajů definuje GDPR zvláštní kategorie osobních údajů, mezi které patří údaje o:

- rasovém či etnickém původu,
- vyznání,
- politických názorech,
- členství v odborech či jiných organizacích,
- sexuální orientaci,
- spáchání deliktů (trestný čin/přestupek aj.) a potrestání za ně,
- genetické údaje (DNA & RNA),
- biometrické údaje,
- údaje o zdravotním stavu.

6.2.3 Zpracování osobních údajů

Zpracováním osobních údajů se dle čl. 4 odst. 2 GDRP rozumí **jakákoliv operace** nebo soubor operací **s osobními údaji** nebo soubory osobních údajů, **který je prováděn pomocí či bez pomoci automatizovaných postupů**, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

Ochrana subjektu údajů se vztahuje na zpracování osobních údajů, pokud jsou tyto údaje uloženy v evidenci nebo do ní mají být vloženy.[14]

Pojem **zpracování** dle GDPR však **nelze chápat jako jakékoli nakládání s osobním údajem. Zpracování osobních údajů je nutné považovat již za sofistikovanější činnost, kterou správce s osobními údaji provádí za určitým účelem a z určitého pohledu tak činí systematicky.**[15]

Ze zpracování osobních údajů dle GDPR je mimo jiné **vyňata činnost prováděná fyzickou osobou v rámci čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti, a tedy bez jakékoliv souvislosti s profesní nebo obchodní činností.**[16]

V čl. 5 odst. 1 písm. a) GDPR jsou stanoveny zásady zpracování osobních údajů. Mezi tyto zásady dle GDPR patří:

- **zákonnost, korektnost, transparentnost** [čl. 5 odst. 1 písm. a) GDPR] – správce osobních údajů je povinen:
  - informovat subjekt údajů o probíhající operaci zpracování a jejích účelech,
  - informovat subjekt údajů o profilování a o jeho důsledcích,
  - informovat subjekt údajů, pokud jsou osobní údaje získávány od něj, zda je povinen tyto údaje poskytnout, a o důsledcích jejich případného neposkytnutí,
  - **prokázat existenci nejméně jednoho právního důvodů pro zpracování osobních údajů**,
  - **dokumentovat:**

o co, jak, proč zpracovává,

o souhlas a zákonný důvod,

o čas, po který zpracovává,

o **přijaté záruky a bezpečnostní opatření**.

- **omezení účelu** [čl. 5 odst. 1 písm. b) GDPR] – osobní údaje musí být shromažďovány pro určité, výslovně vyjádřené a legitimní účely a nesmějí být dále zpracovávány způsobem, který je s těmito účely neslučitelný,
- **minimalizace údajů** [čl. 5 odst. 1 písm. c) GDPR] – osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány,
- **přesnost** [čl. 5 odst. 1 písm. d) GDPR] – osobní údaje musí být přesné a v případě potřeby aktualizované; musí být přijata veškerá rozumná opatření, aby osobní údaje, které jsou nepřesné s přihlédnutím k účelům, pro které se zpracovávají, byly bezodkladně vymazány nebo opraveny,
- **omezení uložení** [čl. 5 odst. 1 písm. e) GDPR] – osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány,
- **integrita a důvěrnost** [čl. 5 odst. 1 písm. f) GDPR] – osobní údaje musí být **zpracovávány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením technické a organizační zabezpečení osobních údajů**.

6.2.4 Zabezpečení osobních údajů

Jednou z oblastí, které se GDPR explicitně věnuje, je i **problematika zabezpečení zpracování osobních údajů**.

V čl. 32 GDPR je uvedeno, že **správce** (případně zpracovatel) **musí** s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, **přijmout vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku**, případně včetně:

- **pseudonymizace a šifrování osobních údajů,**
- **schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování,**
- **schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů,**
- **procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.**

*„**Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika**, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.“*[17]

Při určování rizika je třeba vycházet zejména z kategorie osobních údajů, které by mohly být porušením zabezpečení dotčeny, charakteru porušení zabezpečení a počtem dotčených subjektů údajů. Vyšší riziko představují „citlivější“ osobní údaje (viz např. zvláštní kategorie osobních údajů), rozsáhlejší soubor osobních údajů, případně údaje, jimiž lze způsobit subjektu údajů újmu či zásah do jeho práv.

Dle čl. 32 odst. 4 GDPR přijmou správce a zpracovatel opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

6.2.5 Posouzení vlivu na ochranu osobních údajů (DPIA)

Posouzení vlivu na ochranu osobních údajů (**D**ata **P**rotection **I**mpact **A**ssessment **– DPIA)** je nástrojem, který se využije v případě, kdy **je pravděpodobné, že** určitý druh **zpracování, zejména při využití nových technologií, bude** s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování **mít za následek vysoké riziko pro práva a svobody fyzických osob.** Jde o nástroj, který může správcům pomoci identifikovat případná rizika zpracování osobních údajů a zavedení vhodných opatření.

Posouzení vlivu na ochranu osobních údajů je třeba provést v případech:

- **systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování**, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad,
- **zpracování zvláštních kategorií osobních údajů** (biometrických údajů, nebo údajů o odsouzení v trestních věcech a o trestných činech či souvisejících bezpečnostních opatřeních),
- rozsáhlého systematického monitorování veřejně přístupných prostor,
- **jakýchkoliv jiných operací, kdy má příslušný dozorový úřad za to, že je pravděpodobné, že zpracování bude představovat vysoké riziko pro práva a svobody subjektů údajů.**

Obsahem posouzení vlivu na ochranu osobních údajů by měl být:

- popis zamýšlených operací zpracování,
- posouzení nezbytnosti a přiměřenosti operací z hlediska účelu (**test proporcionality)**,
- **posouzení rizik pro práva a svobody subjektů**,
- **plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření aj.**

Vlastní nařízení GDPR obsahuje i další instituty (např. pseudonymizace, požadavky na výmaz či přenositelnost osobních údajů aj.), které se mohou vztahovat k činnosti, jež je prováděna v rámci informačních a komunikačních systémů, a které vyžadují náležitou úroveň zabezpečení a ochrany.

Podstatné je identifikovat vliv (dopad) GDPR na organizaci, na její jednotlivé části a procesy. De facto jde o provedení auditu, kde všude v organizaci, případně u jednotlivce se pracuje s osobními údaji ve vztahu ke GDPR. Následně postup spočívá v modifikaci či tvorbě pravidel a procesů (pokud je to třeba) jak uvnitř organizace, tak ve vztahu k subjektu údajů. Veškerá tato činnost by současně měla respektovat základní principy bezpečnosti.

Stejně jako při zavádění bezpečnostních pravidel obecně, tak při implementaci GDPR či jiných dokumentů a doporučení je třeba si uvědomit, že neexistuje jedno pravidlo, vzor, nástroj, řešení či postup aplikovatelný pro každou organizaci a každou situaci či každou organizaci.

Je třeba přijmout a implementovat vlastní řešení v souladu s GDPR.

Je třeba individualizovat…

---

[1] [online]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&qid=1488972453767&from=CS

[2] ŠKORNIČKOVÁ, Eva. *Jednoduchý test: Jak jste na tom s přípravou na GDPR?* [online]. [cit. 10. 11. 2017]. Dostupné z: *https://www.gdpr.cz/blog/jednoduchy-test-jak-jste-na-tom-s-pripravou-na-gdpr/*

[3] Srov. recitál 6 GDPR

[4] **EULA** (**E**nd **U**sers **L**icence **A**greement) je označení pro smluvní podmínky, umožňující využití služby daného poskytovatele služby. EULA představuje smlouvu, která je zpravidla jednostranně vymezena poskytovatelem služby. Uživatel však není nikterak omezován na svých právech, neboť má možnost volby v podobě nevyužití takto jednostranně stanovených smluvních podmínek. V případě souhlasu s využíváním takovýchto služeb je možné obecně konstatovat, že dojde primárně k aplikaci soukromoprávních norem.

Otázkou je, zda si uživatel skutečně uvědomuje, jaké smluvní podmínky odsouhlasil, kdy se pro něj stávají závaznými a jaký možný (legální) zásah do jeho základních lidských práv a svobod takto vyslovený souhlas představuje. Další neopomenutelnou skutečností pak je, že takto poskytovaná služba může ovlivnit práva a oprávněné zájmy (např. bezpečnost IT, důvěryhodnost dat aj.) třetích osob (např. zaměstnavatele aj.), které k využívání předmětné služby explicitně souhlas nevyjádřily.

Smutným faktem zůstává ta skutečnost, že velmi malé procento uživatelů je ochotno číst smluvní podmínky, vztahující se k té které poskytované službě.

[5] **SLA (S**ervice**-L**evel **A**greement) označuje smlouvu sjednanou mezi poskytovatelem služby a jejím uživatelem.

[6] **Tuto interakci je možné sledovat při využívání polohových a geolokačních služeb** (např. Google Maps, Waze, Seznam mapy aj.), neboť fyzická osoba předpokládá, že ji bude počítačový systém schopen lokalizovat a zobrazit jí nejvýhodnější cestu. Stejně tak je ona interakce očekávána např. **u služeb umožňujících prodej a nákup zboží** (např. Letgo – viz doporučené inzeráty dle geolokace či již nakoupeného zboží), **restauračních a ubytovacích službách** (např. Tripadvisor, Booking.com, Airbnb aj.) aj.

[7] Blíže viz KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 78 a násl. a s. 109 a násl.

[8] Viz Čl. 3 GDPR – Místní působnost

[9] **Subjektem údajů je** dle čl. 4 odst. 1 GDPR identifikovaná nebo identifikovatelná **fyzická osoba**. **Subjekt může být identifikován:**

§ **přímo,**

§ **nepřímo (např. výběr vyčleněním aj.).**

[10] Recitály jsou ustanovení předcházející vlastnímu textu nařízení GDPR a jsou v některých případech výkladem či do jisté míry důvodovou zprávou k vlastnímu textu nařízení.

[11] Blíže viz: [online]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=cs&mode=lst&dir=&occ=first&part=1&cid=1403270

[12] K vlastnímu pojmu ISP, právům a povinnostem jednotlivých ISP viz blíže např. KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 78 a násl. a s. 109 a násl.

[13] Blíže viz recitál 30 GDPR

[14] Viz recitál 15 GDPR

[15] Blíže viz *Základní příručka k GDPR.* [online]. [cit. 7. 8. 2018]. Dostupné z: *https://www.uoou.cz/zakladni%2Dprirucka%2Dk%2Dgdpr/ds-4744/archiv=0&p1=3938*

[16] Viz recitál 15 GDPR

[17] Čl. 32 odst. 2 GDPR

6.3. SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

- Nařízení GDPR představuje obecný právní rámec ochrany osobních údajů platný a účinný na celém území EU a v určitých případech i mimo toto teritorium. Hlavním cílem GDPR je zajistit komplexní ochranu práv subjektů údajů proti neoprávněnému zacházení s jejich daty a osobními údaji, nastolit rovnováhu mezi oprávněnými zájmy správců, zpracovatelů a subjektů údajů, vytvořit systém jednotné vymahatelnosti práva a jednotného sankčního mechanismu v této oblasti atd.
- Nařízení GDPR se však uplatní v případech, kdy:
  - provozovna správce nebo zpracovatele je v EU, bez ohledu na to, zda zpracování probíhá v EU,
  - správci nebo zpracovatelé nejsou usazení v EU, ale
    - zboží nebo služby jsou nabízeny subjektům údajů v EU (bez ohledu na úplatu),
    - je monitorováno chování subjektů údajů v rámci EU.
- Osobním údajem dle čl. 4 odst. 1 GDPR jsou *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat zejména odkaz na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“*
- Zpracováním osobních údajů se dle čl. 4 odst. 2 GDRP rozumí jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.
- Správce (případně zpracovatel) musí s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, přijmout vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:
  - pseudonymizace a šifrování osobních údajů,
  - schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování,
  - schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů,
  - procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.
- Posouzení vlivu na ochranu osobních údajů (Data Protection Impact Assessment – DPIA) je nástrojem, který se využije v případě, kdy je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování mít za následek vysoké riziko pro práva a svobody fyzických osob. Jde o nástroj, který může správcům pomoci identifikovat případná rizika zpracování osobních údajů a zavedení vhodných opatření.

KLÍČOVÁ SLOVA K ZAPAMATOVÁNÍ

- GDPR
- Osobní údaj
- Správce osobních údajů
- Zpracování osobních údajů
- Data Protection Impact Assessment

KONTROLNÍ OTÁZKY

- Jaká je místní působnost GDPR?
- Co vše je osobním údajem?
- Je IP adresa osobním údajem?
- Jaké povinnosti má správce osobních údajů?
- Co se rozumí zpracováním osobních údajů?
- Coto znamená Data Protection Impact Assessment?

7. Soukromí a bezpečnost v ICT, ochrana dat v kyberprostoru

Žít v digitální době s představou či pocitem, že mé jednání je anonymní či skryté před zraky jiných uživatelů,[1] je dle mého názoru naivní. S nástupem doby digitální se neobjevují pouze její pozitivní, ale i negativní aspekty.[2] Jedním z těchto negativ je i ta skutečnost, že se čím dál méně zajímáme o podstatu fungování služeb poskytovaných v kyberprostoru.

Náš svět, který stále častěji chápeme jako „svět informací" či „svět Internetu" je pevně spojen s informačními a komunikačními technologiemi, které zasahují do života jedince velmi výrazným způsobem. Tyto technologie usnadňují přístup k informacím a zjednodušují či zrychlují vzájemnou komunikaci mezi jednotlivými uživateli atd. Na straně druhé je však třeba si uvědomit, že jakékoli uveřejnění informací z našeho soukromí na Internetu je rizikem, kterého může v kyberprostoru kdokoliv zneužít.

Veškeré aplikace, ať už jsou využívány v jakémkoli počítačovém systému, webové služby[3] a zejména sociální sítě,[4] shromažďují o svých uživatelích značné množství informací, které majoritně nepotřebují ke svému fungování, ale které jednak umožňují dotyčnému ISP poskytovat službu „zadarmo", a jednak „cílit" či modifikovat jím nabízené služby. Mezi informace, které standardně nejsou nezbytně nutné k přímé funkčnosti jednotlivých služeb, patří například informace mající povahu **osobních** (jméno, příjmení, e-mailová adresa, telefonní číslo, bydliště aj.), **citlivých** (např. informace o využívaném operačním systému počítače, verzích jednotlivých aplikací, soubory cookies aj.), **lokalizačních údajů** (souřadnice GPS, informace o WiFi, GPRS aj.), provozních údajů aj.[5]

Uvedené informace mohou být využity značně různorodě. Poskytovatel služby může dle těchto informací nabízet např. doplňkové služby či reklamu na základě požadavků, zájmů či zálib uživatelů. Policie je díky nim schopna vytvořit rámec denní činnosti osoby, která se například ztratila či byla unesena, a tím urychlit vlastní činnost při pátrání po této osobě. Zároveň však tyto informace mohou být velmi jednoduše zneužity pachateli trestné činnosti, ať již pro navázání kontaktu s obětí, či k naplánování činu samotného.

Poskytnutím (byť i nedobrovolným či nevědomým) těchto údajů umožňuje uživatel dané služby získat jiným osobám důležité informace o svém životě (např. informace o svém chování v průběhu dne, navštěvovaných místech, aktivitách a osobách, se kterými je v kontaktu).[6] V tento okamžik **se sami stáváme informací či komoditou, se kterou může někdo jiný obchodovat**.

Různé dostupné statistiky[7] uvádějí, že v současnosti je celková populace přibližně 7,359,244,000 lidí. Z tohoto počtu zhruba 3,6 miliardy lidí jsou aktivními uživateli Internetu a více než 2,1 miliardy lidí jsou aktivní uživatelé sociálních sítí. Mobilní zařízení vlastní více než 3,6 miliardy uživatelů a k sociálním sítím se přes tato zařízení připojuje více než 1,7 miliardy uživatelů. Sociálním sítím vévodí Facebook s více než 1,59 miliardami uživatelů:[8]

V této části se pokusím upozornit na možné bezpečnostní hrozby, které jsme si zvykli de facto přijímat či nevnímat a u kterých si většina jedinců či organizací vůbec neuvědomuje možné nebezpečí.

---

[1] Pod pojmem uživatel zahrnuji veškeré subjekty, které svým působením ovlivňují dění v kyberprostoru. Primárně je potřeba do této skupiny zařadit **ISP**. Ne všichni ISP však spadají do jurisdikce českého práva (ať již z důvodů geolokačních, či spíše proto, že jejich činnost není právní normou upravena). Dalšími „uživateli" pak bezesporu budou **LEA** (Law Enforcement Agencies - jimž právní normy jednotlivých zemí umožňují jeden z nejintenzivnějších zásahů do základních lidských práv a svobod), **CERT/CSIRT týmy, správci IT oddělení, koncoví uživatelé (end user) aj.**

[2] Např. kyberkriminalita, závislosti a mimo jiné i tzv. digitální demence. Blíže viz: SPITZER, Manfred. *Digitátlní demence.* Brno: Host, 2014. ISBN 978-80-7294-872-7

[3] Viz např. *Zlepšování zabezpečení, ochrana soukromí a vytváření jednoduchých nástrojů, které vám dávají možnost kontroly a výběru, je pro nás velmi důležité.* [online]. [cit.4.4.2014]. Dostupné z: https://www.google.cz/intl/cs/policies/?fg=1

[4] Viz *Prohlášení o právech a povinnostech.* [online]. [cit.4.4.2014]. Dostupné z: https://www.facebook.com/legal/terms

[5] **Některé autentizační systémy přesto potřebují pro svoji funkčnost i tyto uvedené doplňkové informace.**

[6] KOLOUCH, Jan, Michal DVOŘÁK, Tomáš NAJMAN a Terezie JANÍKOVÁ. neBezpečné chování na Facebooku. In: *Sborník příspěvků ke konferenci: Sociální sítě. Mobilní aplikace.* Plzeň: Západočeská univerzita v Plzni, 2014, s. 39 – 47. ISBN 978-80-261-0362-2 s. 40

[7] Blíže viz např.:

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

Digital, Social & Mobile Worldwide in 2015. [online]. [cit.9.8.2015]. Dostupné z: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

Největší sociální sítě na světě? Facebook je sice jednička, ale... [online]. [cit.10.8.2015]. Dostupné z: http://www.lupa.cz/clanky/nejvetsi-socialni-site-na-svete-facebook-je-sice-jednicka-ale/

Current World Population. [online]. [cit.10.8.2015]. Dostupné z: http://www.worldometers.info/world-population/

[8] *Leading social networks worldwide as of April 2016, ranked by number of active users (in millions)* [online]. [cit.10.8.2015]. Dostupné z: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

7.1. Digitální stopa neovlivnitelná

Uvedené hrozby, či spíše rizika, spočívají velmi často v zanechávání digitálních stop v kyberprostoru. Digitální stopy, na základě toho, zda mohou, či nemohou být ovlivněny uživatelem, je obecně možné **rozdělit na stopy ovlivnitelné a neovlivnitelné**.

Dělení digitálních stop:

- **Digitální stopa neovlivnitelná**
  - Informace z počítačového systému;
  - připojení k počítačovým sítím, zejména Internetu;
  - využívání poskytovaných služeb aj.
- **Digitální stopa ovlivnitelná**
  - vědomé využití služeb;
  - dobrovolné zveřejnění informace
    - blogy, fóra
    - sociální sítě,
    - e-mail,
    - datová úložiště,
    - cloudové služby aj.

V následující části se budu věnovat některým aspektům jednotlivých digitálních stop a informacím v nich obsažených. Smyslem je upozornit uživatele na to, že jeho jednání v prostředí informačních a komunikačních systémů není tak anonymní, jak si možná myslí.

Ve světě ICT platí jedno pravidlo: **pokud kdykoliv cokoliv nahrajete, přenesete, zprostředkujete, vložíte do kyberprostoru, zůstane to tam „navždy“**. Vždy bude existovat kopie (vzniklá na základě funkcionality počítačového systému či kopie uložená některým jiným uživatelem) vašich dat. A i když tato data následně odstraníte, k jejich skutečnému, trvalému a nezvratnému odstranění nedojde. Je proto vhodné věnovat pozornost své digitální stopě a informacím či datům, jež za sebou v prostředí kyberprostoru zanecháváme.

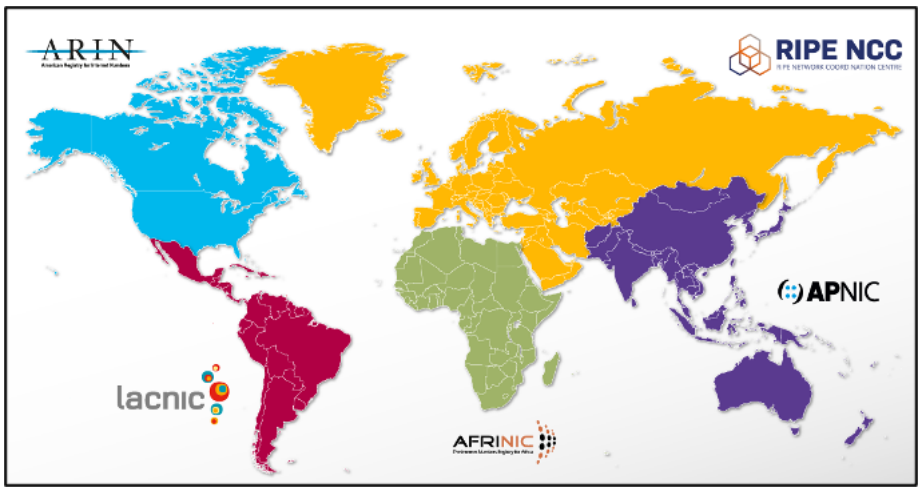
7.1.1 Digitální stopa neovlivnitelná

Neovlivnitelné stopy nejčastěji vznikají na základě interakce jednoho počítačového systému s počítačovým systémem jiným nebo na základě funkčnosti počítačového systému (a přidruženého software). Příkladem těchto stop mohou být například informace z operačního sytému (např. hlášení o chybách systému Windows či systémové informace), nebo další informace a data, jež jsou ukládány na základě funkčnosti tohoto systému, aniž by muselo dojít k jejich předání (např. počítačový systém nebyl nikdy připojen k žádné síti či jinému počítačovému systému).[1] Tvrdit zcela nekompromisně, že nelze tyto stopy ovlivnit, by nebylo zcela korektní. V případě, že je uživatel dostatečně zkušený, je schopen celou řadu „neovlivnitelných“ digitálních stop pozměnit, maskovat nebo potlačit (např. prostým anonymním režimem webového prohlížeče, který vypne cookies). Nicméně pohyb uživatele po Internetu se dá sledovat nejrůznějšími způsoby.

IP adresa

Připojení počítačového systému k Internetu je typickým příkladem relativně neovlivnitelné stopy. IP adresa či MAC adresa, jež jsou předávány spolu s dalšími informacemi ISP. IP adresa není standardně anonymní a počítačový systém ji využívá při komunikaci s jinými počítačovými systémy jakožto jeden z identifikátorů. IP adresy jsou přidělovány hierarchicky, přičemž dominantní roli zde má **ICANN**, který rozdělil reálný svět na regiony, nad nimiž vykonávají správu regionální internetoví registrátoři (**RIR** - **Regional Internet Registry**). Tito registrátoři dostali od ICANN přidělen určitý rozsah IP adres, které přidělují LIRům v rámci svého regionu. Regionální registrátoři jsou rozděleni do následujících pěti teritorií

1. „Euro-asijská“ oblast - RIPE NCC: https://www.ripe.net/
2. „Asijsko pacifická“ oblast – APNIC: https://www.apnic.net/
3. „Severo-americká“ oblast – ARIN: https://www.arin.net/
4. „Jiho-americká“ oblast – LACNIC: http://www.lacnic.net/
5. „Africká“ oblast – AFRINIC: http://www.afrinic.net/



Obrázek - Rozdělení světa mezi RIR

Regionální registrátoři[2] provozují na svých stránkách službu *Whois*, což je označení pro databázi, v níž jsou evidovány údaje o držitelích IP adres. Tyto databáze obsahují celou řadu informací, na jejichž základě je možné identifikovat např. rozsah používaných veřejných IP adres, kontaktní údaje, abuse kontakt[3], hierarchicky nadřazeného poskytovatele připojení aj. K vlastnímu zjištění „vlastníka" (operátora, poskytovatele) konkrétní IP adresy je mnohdy možné využít právě těchto volně dostupných databází.[4]

Regionální registrátoři dále rozdělují přidělené IP rozsahy mezi lokální internetové registrátory (**LIR - Local Internet Registry**). Lokálním registrátorem je zpravidla ISP (v ČR poskytovatel služeb informační společnosti, konkrétně pak poskytovatel připojení, ať veřejný, či neveřejný). Tento registrátor pak může dále svůj rozsah IP adres poskytnout například části své organizace, či jiným subjektům.

```
Responsible organisation: Policejni akademie CR v Praze
Abuse contact info: abuse@polac.cz

inetnum:          195.113.149.160 - 195.113.149.175
organisation:     ORG-PACV1-RIPE
org-name:         Policejni akademie CR v Praze
org-type:         OTHER
address:          Policejni akademie CR v Praze
address:          Lhotecka 559/7
address:          P. O. Box 54
address:          Praha 4
address:          143 01
address:          The Czech Republic
phone:            +420 974 828 551
e-mail:           polac@polac.cz
abuse-mailbox:    abuse@polac.cz

route:            195.113.0.0/16
descr:            CESNET-TCZ
origin:           AS2852
mnt-by:           AS2852-MNT
remarks:          Please report abuse -> abuse@cesnet.cz
created:          1970-01-01T00:00:00Z
last-modified:    2006-06-26T14:36:38Z
source:           RIPE
```

Obrázek - Výpis informací z databáze RIR

Na zkráceném výběru z databáze RIR je zobrazen LIR (v tomto případě sdružení CESNET, z. s. p. o. využívající rozsah IP adres: 195.113.0.0/16) a organizace, jíž CESNET přidělil část veřejných adres [Policejní akademie ČR s rozsahem IP adres 195.113.149.160 – 195.113.149.175. Policejní akademie pak opět může rozdělit tyto adresy mezi další části organizace (např. fakulty, laboratoře, či jiné sub sítě, jež spravuje)]. Dle IP adresy a přesného času je možné na základě hierarchického přidělování adres určit konkrétní počítačový systém. Informace o připojení koncového počítačového systému (zdroje) k cílovému počítačovému systému (např. připojení počítače k Internetu a zobrazení si požadované webové stránky) jsou uchovávány jednotlivými ISP v rámci celé cesty mezi zdrojem a cílem.

Díky přísným pravidlům definujícím hospodaření s IP adresami a veřejně přístupnými databázemi RIRů, které obsahují informace o držitelích jednotlivých adresových bloků, je možné velmi rychle zjistit, do které sítě patří určitá IP adrea a kdo danou síť provozuje. Provozovatel dané sítě pak díky logování informací ze síťového provozu dokáže identifikovat, kdo (respektive jaký počítačový systém) v konkrétním čase používal konkrétní IP adresu. Toto určení je velmi důležitým zdrojem informací při řešení bezpečnostních incidentů (kybernetických útoků) a při pátrání jejich po zdroji (původci).

e-mail

E-mail jakožto jedna z nejčastěji využívaných služeb v prostředí Internetu rozhodně není anonymní službou. Zpráva, která je odeslána od zdroje k cíli (adresátovi), v sobě typicky nese celou řadu informací, které mohou identifikovat jednak poskytovatele služby (e-mailu), tak i poskytovatele připojení zařízení, z nějž byl e-mail odeslán. Tyto informace nejsou zobrazeny v těle zprávy (tedy textu, který odesíláme konkrétní osobě), ale ve zdrojovém kódu (hlavičce) zprávy. Z toho zdrojového kódu je například možné zjistit cestu přes servery, skutečného odesílatele, zdrojové jméno počítače, název počítače, čas odeslání zprávy (včetně časové zóny) používaný operační systém, mailového klienta aj. Níže je uvedený příklad hlavičky přeposlaného[5] podvodného e-mailu s vyznačením potenciálně zajímavých informací.

```
From - Wed Aug 19 15:14:52 2015
X-Account-Key: account1
X-UIDL: 7
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Mozilla-Keys:
Received: from relay.fit.cvut.cz (relay.fit.cvut.cz [147.32.232.237])
    by email-smtpd5.ko.seznam.cz (Seznam SMTPD 1.3.4) with ESMTP;
    Wed, 19 Aug 2015 15:14:16 +0200 (CEST)
Received: from imap.fit.cvut.cz (imap.fit.cvut.cz [IPv6:2001:718:2:2901:0:0:0:238])
    by relay.fit.cvut.cz (8.15.2/8.15.2) with ESMTP id t7JDE1Mm072888
    for <kyber.test@seznam.cz>; Wed, 19 Aug 2015 15:14:01 +0200 (CEST)
    (envelope-from jan.kolouch@fit.cvut.cz)
Received: from PCP[redacted] (cust-178.17.4.174.uvt.cz [178.17.4.174] (may be forged))
        (authenticated bits=0 as user ko[redacted])
        by imap.fit.cvut.cz (8.15.2/8.15.2) with ESMTPSA id t7JDE139012575
        (version=TLSv1.2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128 verify=NOT)
        for <kyber.test@seznam.cz>; Wed, 19 Aug 2015 15:14:01 +0200 (CEST)
    (envelope-from jan.kolouch@fit.cvut.cz)
X-Authentication-Warning: imap.fit.cvut.cz: Host cust-178.17.4.174.uvt.cz [178.17.4.
From: "JUdr. Jan Kolouch, Ph.D." <jan.kolouch@fit.cvut.cz>
To: <kyber.test@seznam.cz>
References: <20150817015549.C54655DA12CC@mail.nbfgr.res.in>
In-Reply-To: <20150817015549.C54655DA12CC@mail.nbfgr.res.in>
Subject: =?UTF-8?Q?FW:_Chci=2C_aby_partner_s_v=C3=A1mi_na_?=
    =?UTF-8?Q?tomto_projektu?=
Date: Wed, 19 Aug 2015 15:14:15 +0200
Message-ID: <006901d0da80$f3599db0$da0cd910$@fit.cvut.cz>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="----=_NextPart_000_006A_01D0DA91.B6E2BBD0"
X-Mailer: Microsoft Outlook 14.0
Thread-Index: AQDP5b3kQbONWI2VUUpla1oprzeNE6AVNk1w
Content-Language: cs
X-FIT-MailScanner-ID: t7JDE1Mm072888
X-FIT-MailScanner: Found to be clean
X-FIT-MailScanner-SpamCheck: not spam, SpamAssassin (not cached,
    score=-0.381, required 7, autolearn=not spam, RP_MATCHES_RCVD -0.38)
X-FIT-MailScanner-From: jan.kolouch@fit.cvut.cz
X-FIT-MailScanner-Watermark: 1440594843.20583@MBoaO3F9jzMModBIjGdzYg
X-Spam-Status: No
```

Obrázek - Zobrazení informací z hlavičky e-mailové zprávy

Web browser

Webový prohlížeč je další aplikací, která standardně předává informace o uživateli a jeho počítačovém systému, počítačovému systému (serveru) navštívené stránky. Tento server pak v rámci dotazu od klienta zjistí například referer (což je stránka, ze které uživatel přichází), používaný webový prohlížeč a operační systém (včetně přesné verze), cookies, flash cookies, historie, cache aj.

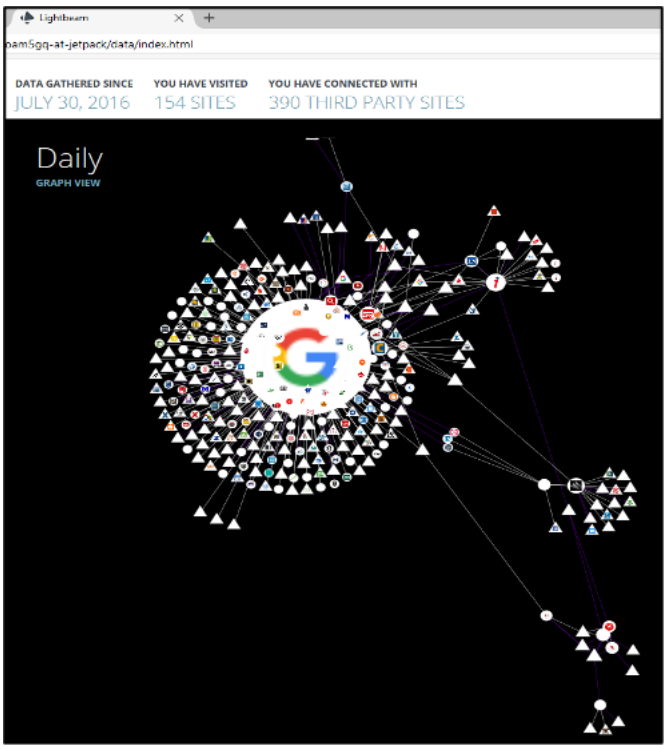
Kromě IP adresy jsou to právě mimo jiné i soubory cookies[6], jež pomáhají vytvořit „otisk" („fingerprint") uživatelova počítačového systému (počítače, smartphonu aj.). Tento otisk umožňuje určit konkrétní počítačový systém[7], a to i v případě, že uživatel používá jiný webový prohlížeč, či promaže cookies, přihlašuje se z jiné IP adresy, atd.

Jeden z mnoha v současnosti požívaných způsobů tvorby „fingerprintingu" je canvas fingerprinting.[8] Canvas fingerprinting funguje tak, že navštívený webserver nařídí webovému prohlížeči uživatele „nakreslit skrytý obrázek". Tento obrázek je unikátní pro ten který webový prohlížeč a počítačový systém. Nakreslený obrázek je pak převeden do ID kódu, který je na webovém serveru uchován pro případ, že by jej uživatel navštívil znovu.[9]

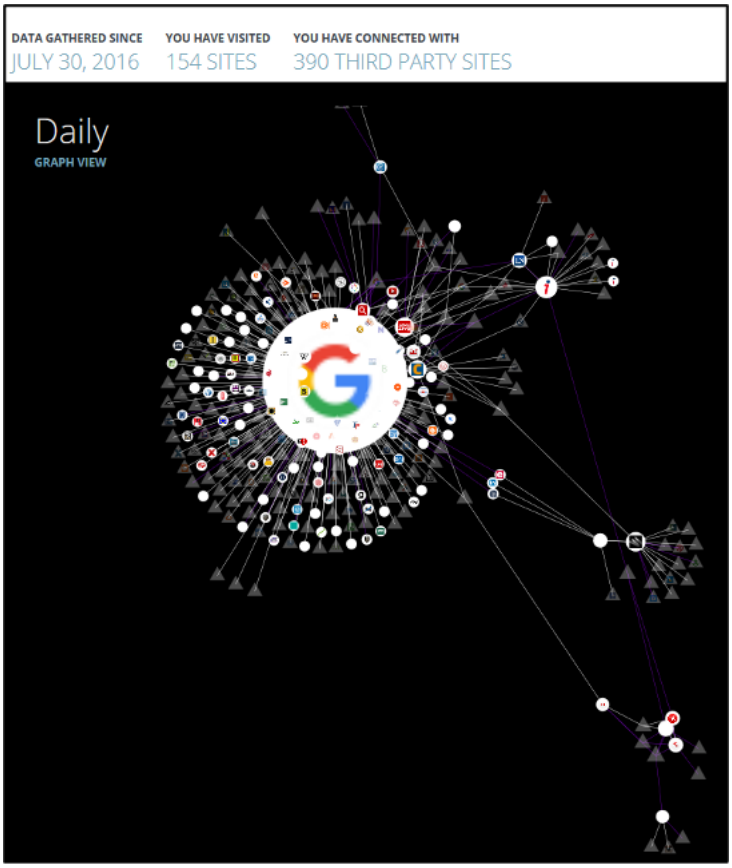
Obrázek - Ukázka Canvas Fingerprintingu

Kromě fingerprintingu je u webového prohlížeče dále zajímavé sledovat předávání informací třetím stranám (jak subjektům, tak službám, které informace o uživateli mohou dále využít). Toto předávání se standardně děje na základě smluvních podmínek uzavřených s ISP. Každý koncový uživatel může například využít aplikaci Light Beam[10], která zobrazí všechny stránky, se kterými na webu uživatel (mnohdy nevědomky) komunikuje (dochází k předávání dat třetím stranám). Předávání informací o uživatelích třetím stranám rozhodně není něco výjimečného, naopak, v digitálním světě se jedná o samozřejmost a „nezbytný předpoklad" pro fungování řady ISP.

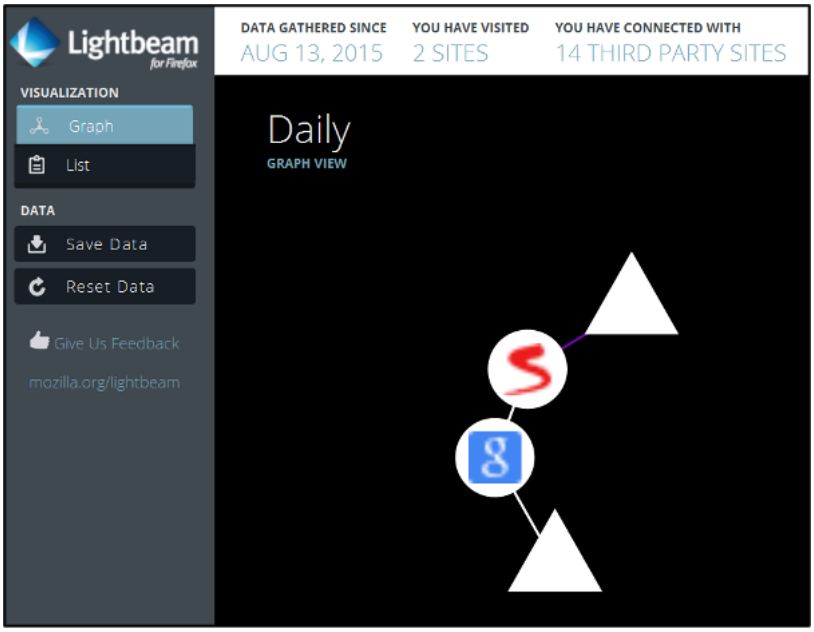
1. První snímek zobrazuje činnost Firefoxu za období od 30. července 2016 do 4. srpna 2016. V daném období došlo k navštívení 154 stránek a došlo k propojení na **390 stránek třetích stran.**



2. Druhý printscreen zobrazuje stejnou mapu, avšak odfiltrovává stránky třetích stran, které jsou znázorněny pomocí trojúhelníků.



3. Poslední printscreen zobrazuje aplikaci LightBeam po vyčištění a zobrazení následujících stránek: www.seznam.cz; www.google.com;



Ostatní aplikace

V následující části textu se částečně zaměřím na smart devices (smartphone, tablet aj.) a aplikace spojené s vlastní činností „smart devices“. Cíleně si vybírám právě tato zařízení, neboť se jedná o počítačové systémy, do kterých uživatelé instalují asi největší množství programů (velmi často neověřených, pouze doporučených „kamarádem“). Právě tato zařízení, která mimo jiné i díky smluvním podmínkám, nemusí být pod plnou kontrolou uživatele, administrátora aj., představují bezpečnostní riziko a to jak pro uživatele koncového, tak pro společnost (organizaci).

Z již dříve zmíněného statistického průzkumu[11] vyplývá, že průměrně strávíme na Internetu: 4,4 hod. (přístup přes počítač v podobě stolního PC či notebooku aj.) a 2,7 hod (přístup skrze mobilní zařízení) denně. V případě počítače je zpravidla bezpečnost zařízení zajištěna, avšak mobilní zařízení (smartphone, tablet aj.) běžně nemají nastavené politiky týkající se možné instalace software (ať již z důvěryhodných, či nedůvěryhodných zdrojů) a mnohdy chybí i základní ochrana v podobě antivirového programu.[12]

Koncový uživatel si právě primárně do zařízení s OS Android má možnost nainstalovat software, který bude předávat (dalším subjektům) a uchovávat informace o jeho činnosti, a to včetně uchování a předání obsahu přenášených informací. Služba Obchod Play, která je společností Google v rámci OS Android poskytována, umožňuje jakémukoli vývojáři nastavit pravidla toho, co má daná aplikace např. sbírat a kam má tato data posílat.

Osobně se domnívám, že není chybou umožňovat vývojářům a tvůrcům aplikací získávat dostatečné informace o svých aplikacích, jejich funkčnosti atd. Pokud bychom sběr těchto informací regulovali, pak nepochybně budeme regulovat a brzdit možný pokrok a následný vývoj těchto a jiných aplikací. Na straně druhé však stojí útočníci, kteří díky tomu, že ve službě Obchod Play nedochází k ověřování a prověřování aplikací, mohou nabízet malwarem infikované aplikace, po jejichž instalaci do koncového počítačového systému může dojít například i k získání kontroly nad smartphonem koncového uživatele.

Určení počítačového systému na základě informací z jeho komponent

Jedním z unikátních, avšak za určitých okolností změnitelných, identifikátorů počítačového systému, je MAC adresa, která je pevně svázána se síťovou kartou počítačového systému. Síťová karta není však jedinou hardwarovou komponentou, která je schopna předávat unikátní identifikátor počítačového systému jinému počítačovému systému.

Vědci z Princeton University zjistili, že počítačový systém je možné identifikovat například i na základě informací o baterii tohoto systému, přičemž webové prohlížeče jsou nezbytnou součástí předávání těchto informací.[13]

V praxi je užíván postup, který využívá možnosti HTML5. Součástí tohoto standardu je totiž funkce, která umožňuje webovým stránkám (resp. web serveru) zjistit stav baterie počítačového systému, který na ně přistupuje (předávány jsou informace o tom, kolik procent baterie zbývá, za jak dlouho se přibližně vybije nebo nabije). Představa vlastníků web serverů je taková, že uživateli, kterému se vybíjí baterie, bude zobrazena úsporná verze webové stránky. Dva skripty, které popsali právě vědci z Princeton University, data o baterii už skutečně využívají, zároveň sbírají další informace - například IP adresu nebo otisk z canvas fingerprinting. Takové kombinace už mohou poskytnout velmi přesnou identifikaci počítačového systému.[14]

7.1.2 Digitální stopa ovlivnitelná

Digitální stopa ovlivnitelná představuje veškeré informace, které o sobě uživatel sám dobrovolně předá jiné osobě (ať fyzické či právnické, nebo i např. ISP). Pod pojmem předání si je třeba představit celou řadu činností, které mohou spočívat například v odeslání e-mailu, přidání příspěvku do diskuse, fóra, zveřejnění jakýchkoli médií (foto, video, audio aj.) v rámci sociálních sítí, atd. Dále pod tento pojem spadají i registrace a využívání všech představitelných služeb v rámci kyberprostoru [např. operační systémy, e-maily (včetně freemailu), sociální sítě, seznamky, P2P sítě, chaty, blogy, BBS, webové stránky, cloudové služby, datová úložiště aj.].

Digitální stopy ovlivnitelné jsou stopami, nad kterými může mít uživatel relativní kontrolu a je pouze na něm, jaké informace o sobě hodlá zpřístupnit jiným. Je však třeba upozornit na již uvedenou premisu: jakákoli data či informace vložené do kyberprostoru již v kyberprostoru zůstanou.

Teoreticky by bylo možné definovat i kategorii **hypoteticky ovlivnitelných stop**, což je svým způsobem oxymóron, nicméně tato kategorie zahrnuje jisté skutečnosti, na které může mít uživatel teoreticky vliv, tedy je schopen je ovlivnit, ale běžně to nedělá, neboť by de facto značně omezil možnosti svého fungování v digitálním světě. Mezi tyto stopy by pak bylo možné zařadit například používání služeb největších ISP (Microsoft, Apple, Google, Facebook aj.), u

nichž je využívání služby podmíněno odsouhlasením smluvních podmínek (EULA), které umožňují těmto ISP získávat značné množství informací. Dále je pak do těchto stop možné zahrnout i stopy, jež vznikly např. korelací neovlivnitelných a ovlivnitelných stop; informace, jež o nás zveřejní jiní uživatelé; data, jež jsou zrcadlena; EXIF data[15]

---

[1] Neboli převážně informace, které se o činnosti uživatelů logují a archivují na místech, k nimž nemá uživatel přístup a nemá je pod kontrolou [např. uživatel není schopen smazat logy prokazující jeho aktivitu (např. přístup, odesílání e-mailu aj.) na mail serveru]. Na vlastním počítači může uživatel ovlivňovat uložená data a informace. Je oprávněn mazat (např. historii, e-maily aj.), editovat aj.

[2] *Regional internet registries.* [online]. [cit.4.8.2015]. Dostupné z: https://www.nro.net/about-the-nro/regional-internet-registries

[3] Jedná se o kontakt, na nějž se uživatel může obrátit, pokud je mu z dané IP adresy, nebo rozsahu adres způsobována újma (dochází např. ke kybernetickému útoku v podobě spamu, phishingu aj.). Jde o kontakt nejbližší zdroji útoku.

[4] Nejedná se však o databáze jediné. Existuje celá řada služeb, jež nabízejí stejné informace. Jako příklad uvádím i další databáze: http://whois.domaintools.com/; https://www.whois.net/; http://www.nic.cz/whois/; https://whois.smartweb.cz/ aj.

[5] e-mail byl přeposlán z adresy: jan.kolouch@fit.cvut.cz na e-mail: kyber.test@seznam.cz

[6] V protokolu HTTP označuje pojem cookie malé množství dat, která odešle navštěvovaný webserver (zjednodušeněji: navštěvovaná webová stránka) webovému prohlížeči, který je následně uloží na počítači uživatele. Tato data jsou pak zpětně posílána webovému serveru, při každém navštívení téhož serveru.

[7] Pokud si chce uživatel zjistit více informací o tom, co o jeho činnosti prozrazuje webový prohlížeč, doporučuji následující URL: http://panopticlick.eff.org , http://browserspy.dk/, http://samy.pl/evercookie.

[8] ANGWIN, Julia. *Meet the Online Tracking Device That is Virtually Impossible to block.* [online]. [cit.10.6.2016]. Dostupné z: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

[9] Ukázka Canavas fingerprintingu. Test, ukazující otisk Vašeho webového prohlížeče, je možné vyzkoušet v rámci článku ANGWIN, Julia. *Meet the Online Tracking Device That is Virtually Impossible to block.* [online]. [cit.10.6.2016]. Dostupné z: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block

[10] Aplikace umožňuje grafické zobrazení propojování jednotlivých služeb a předávání informací třetím stranám. Jedná se o doplněk webového prohlížeče Firefox, který je dostupný na: https://www.mozilla.org/en-US/lightbeam/.

[11] *Digital, Social & Mobile Worldwide in 2015.* [online]. [cit.9.8.2015]. Dostupné z: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

[12] Přičemž je třeba uvést, že např. ze zprávy vydané společností Kaspersky Lab vyplývá, že existuje více než 340 000 druhů malware určeného primárně pro mobilní zařízení. Kaspersky Lab dále uvádí, že 99 % tohoto malware cílí na zařízení s operačním systémem Android. Je třeba uvést, že toto cílení je naprosto pochopitelné, neboť variabilita jednotlivých zařízení a verzí OS Android je značná (některé zprávy uvádí, že Android OS využívá více jak 24 000 druhů různých zařízení).

Blíže viz např.:

The very first mobile malware: how Kaspersky Lab discovered Cabir. [online]. [cit.1.8.2016]. Dostupné z: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir

Dále: *Interesting Statistics On Mobile Strategies for Digital Transformations.* [online]. [cit.15.7.2016]. Dostupné z: http://www.smacnews.com/digital/interesting-statistics-on-mobile-strategies-for-digital-transformations/

The fragmentation of Android has new records: 24 000 different devices. [online]. [cit.15.7.2016]. Dostupné z: http://appleapple.top/the-fragmentation-of-android-has-new-records-24-000-different-devices/

[13] Blíže viz ENGLEHARDT, Steven a Ardvin NARAYANAN. *Online tracking: A 1-million-site measurement and analysis.* [online]. [cit.5.8.2016]. Dostupné z: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

[14] Blíže viz VOŽENÍLEK, David. *Promazání „sušenek" nepomůže, na internetu vás prozradí i baterie.* [online]. [cit.4.8.2016]. Dostupné z: http://mobil.idnes.cz/sledovani-telefonu-na-internetu-stav-baterie-faz-/mob_tech.aspx?c=A160802_142126_sw_internet_dvz

[15] EXIF - *Exchangeable image file format*. Jedná se o formát metadat, která jsou vkládána do digitálních fotografií, digitálními fotoaparáty. Tato metadata mohou například:

- Značku a model fotoaparátu.
- Datum a čas pořízení snímku.
- GPS pozici.
- Informace o autorovi (osobě, která si fotoaparát zaregistrovala).
- Nastavení fotoaparátu.
- Náhled snímku aj.

7.2. Smluvní podmínky (EULA)

V následující části této kapitoly se pokusím popsat, jaké informace jsou standardně o uživatelích sbírány největšími ISP.[1] Specificky jsem si vybral společnost Google Inc., neboť se domnívám, že existuje minimum uživatelů, jež by nikdy nevyužili některý z produktů (např. OS Android, vyhledávací nástroj na www.google.com, Gmail, Google Chrome aj.) této společnosti.[2] Mým cílem v žádném případě není „útok" na společnost Google Inc. či jiné společnosti (včetně jejich produktů). Smyslem je prezentovat možná bezpečnostní rizika, která jsou spojena s využíváním některých poskytovaných služeb a s akceptací smluvních podmínek (EULA - End Users Licence Agreement), na něž je využívání uvedených služeb vázáno.

Smluvní podmínky, umožňující využití služby daného poskytovatele služby nejsou ve své podstatě ničím jiným než zpravidla jednostranně vymezeným definováním práv a povinností ze strany poskytovatele služby (ISP). Uživatel však není nikterak omezován na svých právech, neboť má možnost volby v podobě nevyužití takto jednostranně stanovených smluvních podmínek. V případě souhlasu s využíváním takovýchto služeb je možné obecně konstatovat, že dojde primárně k aplikaci soukromoprávních norem.

Otázkou je, zda si uživatel skutečně uvědomuje, jaké smluvní podmínky odsouhlasil, kdy se pro něj stávají závaznými a jaký možný (legální) zásah do jeho základních lidských práv a svobod takto vyslovený souhlas představuje. Další neopomenutelnou skutečností pak je, že takto poskytovaná služba může ovlivnit práva a oprávněné zájmy (např. bezpečnost IT, důvěryhodnost dat aj.) třetích osob (např. zaměstnavatele aj.), které k využívání předmětné služby explicitně souhlas nevyjádřily.

Teoreticky je možné konstatovat, že soukromoprávní smlouvu s touto společností za celé období existence této společnosti uzavřely téměř 3 miliardy uživatelů.[3] Smutným faktem zůstává ta skutečnost, že velmi malé procento uživatelů je ochotno číst smluvní podmínky, vztahující se k té které poskytované službě.[4]

Výňatky ze smluvních podmínek společnosti Google Inc.[5]

Google explicitně uvádí, že pokud kterýkoli uživatel začne využívat jakékoli služby společnosti Google, souhlasí s platnými smluvními podmínkami. Dále jasně definuje vztah uživatele a sebe, jakožto poskytovatele služby, v případě, že je uživatel povinen akceptovat další smluvní podmínky. Tento vztah je vyjádřen následujícím způsobem: *„Nabídka našich služeb je široká, a na některé se proto mohou vztahovat dodatečné podmínky nebo požadavky (včetně omezení věku). **Dodatečné podmínky** budou k dispozici spolu s příslušnými službami. **Pokud tyto služby použijete, stávají se dodatečné smluvní podmínky součástí smluvních ujednání mezi oběma stranami.“***

Již v úvodu smluvních podmínek Google stanoví, že: *„**Obsah**[6] **můžeme kontrolovat**, **abychom určili, zda je legální a splňuje naše zásady**, a pokud se domníváme, že naše zásady nebo právní předpisy porušuje, můžeme obsah odstranit nebo zamezit jeho zobrazování. Berte prosím na vědomí, že **výše uvedené neznamená, že obsah prověřujeme**.“*

Z hlediska bezpečnosti je dle mého názoru zásadní částí smluvních podmínek sekce, která pojednává o **Ochraně osobních údajů a autorských práv**.[7] V této části Google definuje, jaké informace o uživatelích shromažďuje a jak s nimi nakládá. Z pohledu bezpečnosti a „pocitu anonymity" jsou následující informace klíčové. Domnívám se, že deklarace toho, že následující informace jsou shromažďovány *„proto, abychom mohli všem našim uživatelům poskytovat lepší služby – od určení jednoduchých věcí, jako je jazyk, kterým mluvíte, až po věci složitější, například reklamy, které pro vás budou nejužitečnější, lidé o které se na webu nejvíce zajímáte, nebo která videa na YouTube by se vám mohla líbit“* je možná chvályhodná, avšak minimálně zarážející. Přirovnání k již zmíněnému Minority Reportu v podobě cílení reklamy je po takovémto prohlášení více než nasnadě. Mimoto se mi opět vybaví Manfred Spitzer a *Digitální demence*, neboť po čase to již nejsem já, kdo rozhoduje, na co se budu dívat či co budu vyhledávat (resp. mi nemusí být a nejsou nabízeny všechny relevantní odpovědi).

Google shromažďuje informace o uživateli v zásadě dvěma způsoby:

1. **Informace, které uživatel sám sdělí.** Typicky se jedná o:

- *jméno, e-mailovou adresu, telefonní číslo nebo platební kartu.*

2. **Informace získávané při používání služeb Google.** Jsou shromažďovány informace o službách, které jsou uživatelem používány, včetně způsobu, jakým jsou používány (*„například když se podíváte na video na YouTube, navštívíte webové stránky, které využívají naše reklamní služby, nebo sledujete naše reklamy a obsah nebo na ně reagujete*"). Dle Google se jedná o:

- ***Informace o zařízení** (např. model hardwaru, verze operačního systému, jedinečné identifikátory zařízení*[8] *a údaje o mobilní síti včetně telefonního čísla)*. Google je oprávněn přiřadit k vašemu uživatelskému účtu na Google identifikátory vašeho zařízení nebo vaše telefonní číslo

- ***Informace z protokolu:***

  - *podrobnosti o tom, jakým způsobem uživatel využil službu Google,*
  - *informace z protokolu telefonování (např. telefonní číslo, číslo volajícího, čísla přesměrování, čas a datum hovorů, trvání hovorů, údaje o směrování zpráv SMS a typy hovorů),*
  - *adresa internetového protokolu,*
  - *informace o událostech zařízení (např. selhání, činnost systému, nastavení hardwaru, typ prohlížeče, jazyk prohlížeče, datum a čas vašeho požadavku nebo odkazující adresa URL,*
  - *soubory cookie, které mohou být jedinečnými identifikátory vašeho prohlížeče nebo účtu Google*.

- ***Informace o poloze.*** Google je oprávněn shromažďovat a dále zpracovávat informace o skutečné poloze svého uživatele. Polohu může Google určovat pomocí různých technologií, jako jsou IP adresa, systém GPS a další senzory, které společnosti Google mohou poskytovat například údaje o zařízeních v okolí, přístupových bodech sítě Wi-Fi a vysílačích mobilních sítí.

- ***Jedinečná čísla aplikací*. Typicky se jedná o licenční číslo a typ (verzi) příslušného nainstalovaného softwarového produktu. Ze smluvních podmínek** nevyplývá, že by se jedinečná čísla aplikací zaznamenávala pouze ze zařízení, jejichž primárním operačním systémem je systém Android. Lze tedy dojít k závěru, že pokud dochází k využívání služeb Google, pak jsou sbírány i informace o jedinečných číslech aplikací i z jiných operačních systémů (iOS,

Linux, Windows aj.).

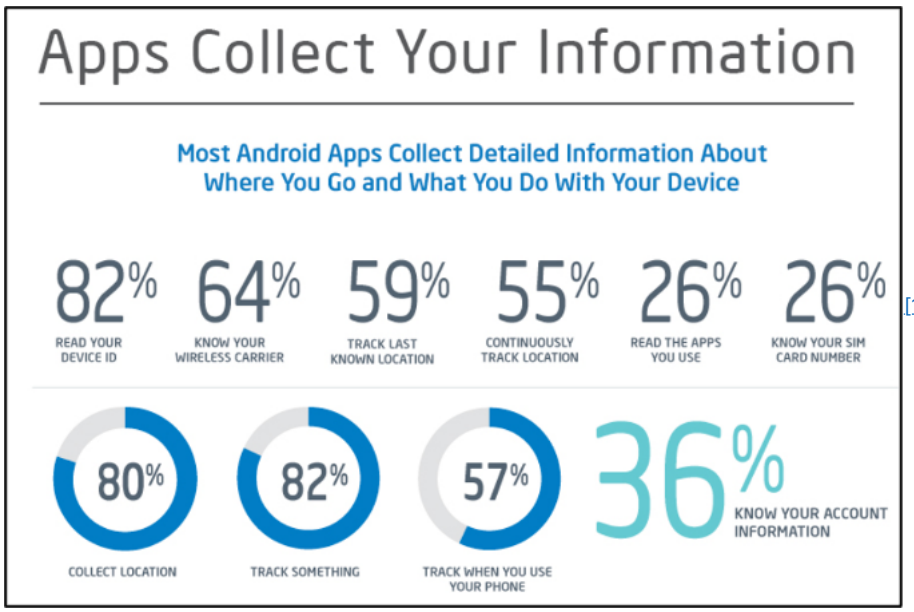
- ***Místní úložiště.*** **Dle smluvních podmínek může Google: „***shromažďovat a uchovávat informace (včetně osobních údajů) v místním úložišti vašeho zařízení.*“ I v tomto případě lze dojít ke stejnému závěru, jako tomu bylo u jedinečných čísel aplikací.

Problémem je dle mého názoru i ta skutečnost, že nikde v obecných smluvních podmínkách není přesně vymezeno[9], jaké umístění a především jaké zabezpečení bude službou Google využito, a tím pádem je teoreticky možné využívat úložiště jako celek. Lze získávat informace o souborech (např. jejich názvy, lokaci, a ad absurdum i hash, který bude následně porovnán např. s databází jiné služby, kde se ukládají data – např. DropBox, OneDrive aj.).

Hrozbou pro uživatele pak je dle mého názoru i možnost zneužití takto uložených dat útočníkem. Informace (které se typicky nabalují na cookies aj.) uložené v uživatelově místním úložišti se mohou stát i zajímavým cílem pro útočníka, neboť právě z těchto informací je možné zjistit např. vzorce chování uživatele.

- ***Soubory cookie a podobné technologie. „****Když navštívíte nějakou službu Google, používáme my* ***i naši partneři*** *různé technologie ke shromažďování a ukládání informací. To může mimo jiné zahrnovat používání souborů cookie nebo podobných technologií k identifikaci vašeho prohlížeče nebo zařízení. Pomocí těchto technologií* ***shromažďujeme a ukládáme informace i v případě, kdy využíváte služby, které nabízíme našim partnerům****, jako jsou reklamní služby nebo funkce Google, které se mohou zobrazit na jiných webech.*“

Jaké informace sbírají aplikace fungující v rámci Android OS:



[10]

Google je na základě odsouhlasených smluvních podmínek s těmito informacemi dále oprávněn nakládat. Mimo jiné je Google oprávněn analyzovat obsah (včetně e-mailů) pomocí automatizovaných systémů. Dále je oprávněn spojovat osobní údaje z jedné služby s informacemi a osobními údaji ze služby další (využívající Google).

Nakládáním s uvedenými informacemi se pak rozumí i jejich sdílení, a to ať již se souhlasem uživatele, nebo bez tohoto souhlasu.[11] Za doslovnou citaci stojí dikce smluvních podmínek umožňující **sdílení za účelem externího zpracování a z právních důvodů:**

„Osobní údaje poskytujeme spřízněným společnostem, nebo jiným důvěryhodným firmám či osobám, aby je pro nás mohli zpracovat na základě našich pokynů a v souladu s našimi zásadami ochrany osobních údajů a dalšími příslušnými opatřeními ohledně důvěrnosti a zabezpečení.

„Osobní údaje sdílíme se společnostmi, organizacemi či jednotlivci *mimo společnost Google,* ***pokud jsme v dobré víře přesvědčeni, že přístup k takovým údajům, jejich použití, uchování nebo zveřejnění jsou rozumně nutné za účelem:***

- *dodržení platného zákona, nařízení, právního postupu nebo vynutitelného vládního požadavku,*
- *uplatnění příslušných smluvních podmínek včetně vyšetření jejich možného porušení,*
- *zjištění, zabránění nebo jiného postupu proti podvodu, technickým potížím či bezpečnostním problémům,*
- *ochrany před poškozením práv, majetku nebo bezpečnosti společnosti Google, našich uživatelů nebo veřejnosti tak, jak to vyžaduje nebo povoluje zákon.*“

Z pohledu bezpečnosti a ztráty anonymity však považuji za asi nejproblematičtější následující pasáž smluvních podmínek, která se věnuje uživatelskému obsahu ve službách poskytovaných Google:

„Pokud ***nahrajete, odešlete, uložíte nebo přijmete obsah do nebo prostřednictvím našich služeb, poskytujete společnosti Google*** *(a subjektům, se kterými společnost Google spolupracuje)* ***celosvětově platnou licenci k užití, hostování, uchovávání, reprodukování, upravení, vytvoření odvozených děl*** *(například děl, jež jsou výsledkem překladu, přizpůsobení/adaptací či úprav provedených za účelem jeho lepšího fungování v rámci našich služeb)*[12]*,* ***komunikaci, publikování, provozování a zobrazování na veřejnosti a distribuci takového obsahu****.....Licence přetrvává i poté, co přestanete naše služby používat (např. firemní zápis přidaný do služby Mapy Google).* ***Některé služby umožňují k obsahu, který jste do služby odeslali, získat přístup nebo jej odebrat****....*“

Osobně se domnívám, že minimálně v této části smluvních podmínek došlo k překročení oné pomyslné hranice vymezující přiměřenost sbíraných informací o jednotlivých uživatelích. V této části de facto jde o „legální využití“ jakéhokoli obsahu, se kterým Google „přijde do styku“. Osobně se domnívám, že právě zásah do obsahu např. přenášených informací by měl být tím nejzazším možným prostředkem, a ne jakousi „samozřejmostí“ zakotvenou ve smlouvě.

[1] Pro tuto část textu byly použity teze, jež byly uveřejněny v článku: KOLOUCH, Jan. Pseudoanonymita – bezpečnostní riziko pro uživatele Internetu. *DSM –data security management* [online]. 2015. Roč. 19, číslo 3, s. 24-29 ISSN 1211-8737. Dostupné z: http://www.tate.cz/cz/casopis/clanek/dsm-2015-3-456/

[2] Je třeba konstatovat, že velmi obdobné smluvní podmínky (umožňující zajišťovat informace ve srovnatelném rozsahu) mají i následující společnosti: Microsoft, Apple, Facebook, aj.

[3] Dle článku SMITH, Craig. *By the Numbers: 100 Amazing Google Search Statistics and Facts.* [online]. [cit. 4. 8.2016]. Dostupné z: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/ dochází měsíčně k 100 miliardám vyhledávání právě prostřednictvím Google search.

[4] A dle vyjádření jednoho účastníka konference Security 2015 by normální člověk čtením všech, neustále se měnících smluvních podmínek strávil cca 10-20 let života.

[5] Dále jen Google. Veškeré výňatky ze smluvních podmínek byly čerpány z: *Smluvní podmínky společnosti Google.* [online]. [cit.14.6.2016]. Dostupné z: *https*://www.google.cz/intl/cs/policies/terms/regional.html

[6] Obsahem je míněn obsah (data), která nepatří společnosti Google. Za obsah nese odpovědnost ten subjekt, který jej zveřejnil.

[7] Specificky pak, *Zásady ochrany osobních údajů.* [online]. [cit.14.6.2016]. Dostupné z: https://www.google.cz/intl/cs/policies/privacy/

[8] Definice Google. *Jedinečný identifikátor zařízení.* [online]. [cit.14.6.2016]. Dostupné z: https://www.google.cz/intl/cs/policies/privacy/key-terms/#toc-terms-unique-device-id

„Jedinečný identifikátor zařízení (někdy zvaný také univerzálně jedinečné ID nebo UUID) je řetězec znaků, který do zařízení zakódoval výrobce a slouží k jednoznačné identifikaci zařízení (například číslo IMEI mobilního telefonu). Různé identifikátory zařízení se liší podle toho, zda jsou trvalé, zda je mohou uživatelé resetovat a jak k nim lze získat přístup. Dané zařízení může obsahovat několik různých jedinečných identifikátorů. Jedinečné identifikátory zařízení lze použít k různým účelům, například k zabezpečení, zjišťování podvodů, synchronizaci služeb, jako je doručená e-mailová pošta, nebo k uchování nastavení uživatele a poskytování relevantních reklam.“

[9] Resp. dle požadované funkce půjde především o ukládání informací a dat do složky daného prohlížeče (webbrowser), avšak dle smluvních podmínek může jít i o jiné aplikace, než je webbrowser.

[10] CAETANO, Lianne. *Are Your Apps Oversharing? 2014 Mobile Security Report Tells All.* [online]. [cit.10.4.2015]. Dostupné z: https://blogs.mcafee.com/consumer/mobile-security-report-2014/

[11] Např. s administrátory domén; za účelem externího zpracování, či z právních důvodů.

[12] Je pochopitelné, že se společnost Google snaží např. o překlady děl, stánek, či jiného obsahu, aby měl možnost si jej přečíst i uživatel, který nezná originální jazyk uvedeného díla. Nicméně, ad absurdum si je možné představit, že dojde k zveřejnění vaší soukromé milostné básně, kterou jste pomocí některé ze služeb Google odeslali, vaší fotografie, vašeho geniálního nápadu na perpetum mobile aj.

7.3. SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

SHRNUTÍ/ HLAVNÍ VÝSTUPY Z KAPITOLY

- Veškeré aplikace, ať už jsou využívány v jakémkoli počítačovém systému, webové služby a zejména sociální sítě, shromažďují o svých uživatelích značné množství informací, které majoritně nepotřebují ke svému fungování, ale které jednak umožňují dotyčnému ISP poskytovat službu „zadarmo", a jednak „cílit" či modifikovat jím nabízené služby. Mezi informace, které standardně nejsou nezbytně nutné k přímé funkčnosti jednotlivých služeb, patří například informace mající povahu osobních (jméno, příjmení, e-mailová adresa, telefonní číslo, bydliště aj.), citlivých (např. informace o využívaném operačním systému počítače, verzích jednotlivých aplikací, soubory cookies aj.), lokalizačních údajů (souřadnice GPS, informace o WiFi, GPRS aj.), provozních údajů aj.
- Digitální stopy, na základě toho, zda mohou, či nemohou být ovlivněny uživatelem, je obecně možné rozdělit na stopy ovlivnitelné a neovlivnitelné.
- Ve světě ICT platí jedno pravidlo: pokud kdykoliv cokoliv nahrajete, přenesete, zprostředkujete, vložíte do kyberprostoru, zůstane to tam „navždy". Neovlivnitelné stopy nejčastěji vznikají na základě interakce jednoho počítačového systému s počítačovým systémem jiným nebo na základě funkčnosti počítačového systému (a přidruženého software). Příkladem těchto stop mohou být například informace z operačního sytému (např. hlášení o chybách systému Windows či systémové informace), nebo další informace a data, jež jsou ukládány na základě funkčnosti tohoto systému, aniž by muselo dojít k jejich předání (např. počítačový systém nebyl nikdy připojen k žádné síti či jinému počítačovému systému). Tvrdit zcela nekompromisně, že nelze tyto stopy ovlivnit, by nebylo zcela korektní. V případě, že je uživatel dostatečně zkušený, je schopen celou řadu „neovlivnitelných" digitálních stop pozměnit, maskovat nebo potlačit (např. prostým anonymním režimem webového prohlížeče, který vypne cookies). Nicméně pohyb uživatele po Internetu se dá sledovat nejrůznějšími způsoby.
- Digitální stopa ovlivnitelná představuje veškeré informace, které o sobě uživatel sám dobrovolně předá jiné osobě (ať fyzické či právnické, nebo i např. ISP). Pod pojmem předání si je třeba představit celou řadu činností, které mohou spočívat například v odeslání e-mailu, přidání příspěvku do diskuse, fóra, zveřejnění jakýchkoli médií (foto, video, audio aj.) v rámci sociálních sítí, atd. Dále pod tento pojem spadají i registrace a využívání všech představitelných služeb v rámci kyberprostoru [např. operační systémy, e-maily (včetně freemailu), sociální sítě, seznamky, P2P sítě, chaty, blogy, BBS, webové stránky, cloudové služby, datová úložiště aj.].

KLÍČOVÁ SLOVA K ZAPAMATOVÁNÍ

- Digitální stopa
- Digitální stopa neovlivnitelná
- Digitální stopa ovlivnitelná
- EULA

KONTROLNÍ OTÁZKY

- Definujte pojem digitální stopa.
- Jak se od sebe digitální stopy odlišují?
- Jakými prvky je tvořena digitální stopa neovlivnitelná?
- Kdo je to LIR?
- Jakou informaci o uživateli nese IP adresa?
- Co je to EULA?

8. Závěr

Při používání informačních a komunikačních technologií a stále většímu objemu dat zveřejňovaných samotnými uživateli nutně došlo ke vzniku žádostí o potlačení či smazání dat, která nejsou aktuální, či která nějakým způsobem poškozují uživatele samotného.

Vize, že digitální svět a jeho uživatelé začnou být anonymní, je dle mého názoru utopií. Nic na tomto tvrzení nezmění ani různé možnosti anonymizace v podobě např. služeb TOR network[1] aj., neboť vždy bude docházet k interakci se světem reálným a vždy budou v digitálním světě figurovat uživatelé, kteří jsou omylní a kteří při sebelepším zakrývání informací o své činnosti chybují. Stejně tak je utopií se domnívat, že technika bude zapomínat. O uživatelích budou nadále sbírána data. To, k čemu dojde, bude další technické nastavení toho, komu se uvedená data budou zobrazovat a komu nikoli.

K „deanonymizaci" uživatelů bezesporu přispívá jak provázanost jednotlivých nabízených služeb a možnost předávání informací o uživatelích třetím stranám, tak i **Internet věcí** (**IoT**).

Se zajímavým řešením „deanonymizace" uživatelů přišla např. společnost Facebook, vyvíjející metodu **DeepFace**, která je založena na vytvoření 3D modelu obličeje na základě definovaných výchozích bodů na fotografii.[2] Na základě této metody lze identifikovat i osoby, které nemají Facebookový účet a byly pouze označeny (identifikovány) jako konkrétní osoba. Metoda DeepFace je zde uvedena záměrně, neboť možnost využití této metody je zakotvena ve smluvních podmínkách služby Facebook a umožňuje, byť si to uživatel nebude přát (např. sám se úmyslně neoznačí pod fotografií), jeho identifikaci.

Pokud jde o **IoT**, pak zásah nových technologií a naše „deanonymizace" je ještě patrnější. Jako příklad uvedu „smart TV"[3], která při vlastní instalaci opět nabídne smluvní podmínky k odsouhlasení a okamžitě poté „se ptá" po možnosti připojení k síti Internet. Podrobnějším prostudováním smluvních podmínek můžete například zjistit, že tato televize je oprávněna poskytnout záznam důvěrných a osobních hovorů či aktivit, které *„před ní vedete"*, a to za předpokladu, že využíváte funkci voice či motion control. V rámci smluvních podmínek budete upozorněni i na tu skutečnost, že zaznamenaná data jsou předávána výrobci a třetím stranám. Jediným řešením, jak zabránit předávání těchto informací, je vypnutí voice či motion recognition. Otázkou je, zda je to skutečně řešení. Osobně si myslím, že řešením by bylo vypnutí či omezení přenosu dat, případně určení subjektu, s nímž jsem ochoten tato osobní data sdílet.

Pokud jde o právo být zapomenut, dokáži si představit hypotetickou situaci, kdy uživatel bude žádat, aby společnost, jež vyrobila danou televizi či jiný počítačový systém s podobnými smluvními podmínkami, vymazala záznam hovoru např. z 1. 3. 2016. Soud i na tento případ aplikuje právo „být zapomenut", avšak je otázkou, kdo skutečně zaručí uživateli, že jeho data byla smazána ze všech datových úložišť.

Výňatek ze Samsung EULA:

Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

Anonymita na Internetu není a rozhodně v blízké budoucnosti ani nebude. Uživatelé mnohdy, zcela logicky, oprávněně intenzivně bojují proti intervenci státu do svého soukromí, avšak na straně druhé toto soukromí sami dobrovolně a mnohem vstřícněji nabízí všem v okolí (např. na sociálních sítích, v rámci cloudových služeb aj.).

Nemyslím si, že by propast mezi světem reálným a digitálním byla natolik obrovská, a možná i proto mnohdy nechápu bezmyšlenkové chování uživatelů, pokud jde o nabízené služby ze strany ISP. Ano, jako uživatelé získáme v rámci smluvních podmínek, které uzavíráme, nějakou službu. Otázkou je, zda je tento obchod výhodný a zda cena, kterou za tuto službu platíme, je přiměřená.

Osobně si plně uvědomuji tu skutečnost, že moje svoboda, včetně jisté míry „anonymity" na Internetu, je již v současnosti utopií. Domnívám se, že tato utopie bude v brzké budoucnosti i díky IoT a stále většímu propojování všech „services" dovedena téměř do situace, ne nepodobné té v Minority Report. Na druhou stranu však věřím, nebo spíše chci věřit tomu, že jsem pořád svobodný a mám právo volby.

Toto mé právo volby pak minimálně spočívá v mém rozhodnutí, zda, případně jaké služby (services) chci využívat a za jakých podmínek. Myslím si, že uživatelé by se měli stát onou skutečnou definiční autoritou Internetu, a to minimálně v té podobě, že projeví svoji vůli a budou se snažit vydobýt si svá práva i na poskytovateli služeb, neboť v případě intervence státu do jejich soukromí se jim to v řadě případů daří.

Ostatně zhodnotit, jak moc je daná služba „agresivní", respektive jak moc zasahuje do vašeho soukromí, je možné nalézt např. na stránkách: Terms of Service, Didn't Read: https://tosdr.org/. Když už nic jiného (byť je zde možné použít analogii o "Digitální demenci"), tak alespoň kontrola základních podmínek na této stránce může pomoci uživatelům, aby se v dané problematice částečně zorientovali.

Žijeme v době, kdy jsou informační a komunikační technologie již neodmyslitelně propojeny s každým aspektem našeho bytí. Určitým paradoxem je, že de facto nemáme možnost se tomuto prostupu a vzájemné interakci s ICT vyhnout, což nás současně činí více zranitelnými.

Díky informačním a komunikačním technologiím a propojeným službám vytváříme odraz své identity či osobnosti ve světě virtuálním.

Naše digitální „já" má všechny předpoklady pro to být „mnohem trvanlivější" než naše fyzické tělo. Informace o našich aktivitách v kyberprostoru, naše kyberosobnosti, účty a digitální stopy budou díky archivaci dat a informací o nás žít i po naší smrti.

S tím, jak roste objem dat a informací ukládaných v jednotlivých ISP, začínají být stále více řešeny i otázky jejich efektivního zabezpečení, předávání či vymazání, a to nejen na základě smlouvy uzavřené mezi poskytovatelem dané služby a koncovým uživatelem, ale i na základě nově vznikajících právních předpisů.

Státy, organizace, ale i jednotlivci si čím dál více uvědomují, že informace a data představují významný potenciál, který je ve stále větší míře napadán kybernetickými útoky ať již s cílem zcizení, poškození, znepřístupnění, či vymazání dat.

Pokud chceme v současné společnosti žít a využívat její benefity, není možné se od ICT oprostit a rozhodně nemá smysl tyto technologie přestat využívat. Je třeba se začít učit, jak tyto technologie a služby využívat, jak se vyhnout či alespoň eliminovat následky způsobené kybernetickými útoky.

V kyberprostoru, stejně jako ve světě reálném, neexistuje jedna bezpečnost a jedno zabezpečení, které by bylo možné univerzálně aplikovat na každého. Pokud chceme řešit bezpečnost, je třeba ji řešit komplexně a je třeba individualizovat.

---

[1] Některé případy narušení bezpečnosti TOR network:

FBI Exploits Flash Vulnerability to Breach Tor Network Security. [online]. [cit.23.7.2016]. Dostupné z: https://nordvpn.com/blog/fbi-exploits-flash-vulnerability-to-breach-tor-network-security/

Tor security advisory: "relay early" traffic confirmation attack. [online]. [cit.23.7.2016]. Dostupné z:https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack

[2] Blíže viz např.: *Facebook will soon be able to ID you in any photo.* [online]. [cit.9.8.2015]. Dostupné z: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

[3] Dále viz např. ČÍŽEK, Jakub. *Chytré televizory nás monitorují. Smiřte se s tím.* [online]. [cit.9.8.2015]. Dostupné z: http://www.zive.cz/clanky/chytre-televize-nas-monitoruji-smirte-se-s-tim/sc-3-a-171676/default.aspx

9. Seznam použitých pramenů a dalších zdrojů

1. ANGWIN, Julia. *Meet the Online Tracking Device That is Virtually Impossible to block.* [online]. [cit.10.6.2016].

2. BARLOW, Perry John. *A Declaration of the Independence of Cyberspace.* [online]. [cit.23.9.2014]. Dostupné z: https://www.eff.org/cyberspace-independence.

3. CAETANO, Lianne. *Are Your Apps Oversharing? 2014 Mobile Security Report Tells All.* [online]. [cit.10.4.2015]. Dostupné z: https://blogs.mcafee.com/consumer/mobile-security-report-2014/

4. ČÍŽEK, Jakub. *Chytré televizory nás monitorují. Smiřte se s tím.* [online]. [cit.9.8.2015]. Dostupné z: http://www.zive.cz/clanky/chytre-televize-nas-monitoruji-smirte-se-s-tim/sc-3-a-171676/default.aspx

5. *CNN on pedophile sex in Second Life*. [cit.18.6.2009].

6. *Current World Population.* [online]. [cit.10.8.2015]. Dostupné z: http://www.worldometers.info/world-population/

7. Dále: *Interesting Statistics On Mobile Strategies for Digital Transformations.* [online]. [cit.15.7.2016]. Dostupné z: http://www.smacnews.com/digital/interesting-statistics-on-mobile-strategies-for-digital-transformations/

8. *Data retention unconstitutional in its present form.* [online]. [cit.16.7.2016]. Dostupné z: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html?nn=5404690

9. *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

10. *Digital, Social & Mobile Worldwide in 2015.* [online]. [cit.9.8.2015]. Dostupné z: http://www.slideshare.net/wearesocialsg/digital-social-mobile-in-2015?ref=http://wearesocial.net/blog/2015/01/digital-social-mobile-worldwide-2015/

11. ENGLEHARDT, Steven a Ardvin NARAYANAN. *Online tracking: A 1-million-site measurement and analysis.* [online]. [cit.5.8.2016]. Dostupné z: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

12. *Facebook will soon be able to ID you in any photo.* [online]. [cit.9.8.2015]. Dostupné z: http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo

13. *FBI Exploits Flash Vulnerability to Breach Tor Network Security.* [online]. [cit.23.7.2016]. Dostupné z: https://nordvpn.com/blog/fbi-exploits-flash-vulnerability-to-breach-tor-network-security/

14. *First Amendment.* [online]. [cit.10.7.2016]. Dostupné z: https://www.law.cornell.edu/constitution/first_amendment.

15. *German Bundestag Passes New Data Retention Law.* [online]. [cit.16.7.2016]. Dostupné z: http://www.gppi.net/publications/global-internet-politics/article/german-bundestag-passes-new-data-retention-law/

16. GREENFIELD, David. *Integrovaná bezpečnost: Už nastal její čas?* [online]. [cit. 1. 3. 2018]. Dostupné z: http://www.controlengcesko.com/hlavni-menu/artykuly/artykul/article/integrovana-bezpecnost-uz-nastal-jeji-cas/

17. HAINES, Lester. *Online gamer stabbed over „stolen" cybersword.* [online]. [cit.3.10.2006]. Dostupné z: http://www.theregister.co.uk/2005/03/30/online_gaming_death/

18. http://news.bbc.co.uk/2/hi/technology/6638331.stm

19. http://www.austlii.edu.au/au/cases/cth/HCA/2002/56.html

20. HUSOVEC, Martin. *Zodpovednosť na Internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014. ISBN: 978-80-904248-8-3, s. 101-102.

21. *Internet censorship.* [online]. [cit.10.8.2016]. Dostupné z: http://www.deliveringdata.com/2010_10_01_archive.html

22. *Internet History of 1980s.* [online]. [cit. 7. 6. 2016]. Dostupné z: http://www.computerhistory.org/internethistory/1980s/

23. *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

24. JOHNSON, David R. a David POST. *The Rise of Law in Cyberspace.* [online]. [cit.10.7.2016]. Dostupné z: http://poseidon01.ssrn.com/delivery.php?ID=797101088103069021099122095084084095061040041017050027018013071117008115007025117112101013061121056036119084118089028085067043

25. KODET, Jaroslav. *Kybernetický zákon: Využijte naplno open source nástroje.* [online]. [cit. 25. 4. 2018]. Dostupné z: https://www.nic.cz/files/nic/doc/Securityworld_CSIRTCZ_112015.pdf

26. KOLOUCH, Jan a Andrea KROPÁČOVÁ. Liability for Own Device and Data and Applications Stored therein. In: *Advances in Information Science and Applications Volume I: Proceedings of the 18th International Conference on Computers (part of CSCC '14).* [B.m.], c2014, s. 321 – 324. Recent Advances in Computer Engineering Series, 22. ISBN 978-1-61804-236-1 ISSN 1790-5109.

27. KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou.* Praha: Policejní akademie České republiky v Praze, 2013, s. 65

28. KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016, s. 78 a násl. a s. 109 a násl.

29. KOLOUCH, Jan. Pseudoanonymita – bezpečnostní riziko pro uživatele Internetu. *DSM –data security management* [online]. 2015. Roč. 19, číslo 3, s. 24-29 ISSN 1211-8737. Dostupné z: http://www.tate.cz/cz/casopis/clanek/dsm-2015-3-456/

30. *Leading social networks worldwide as of April 2016, ranked by number of active users (in millions)* [online]. [cit.10.8.2015]. Dostupné z: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

31. LESSIG, Lawrence. *Code v. 2. str.* 6 Dostupný v plném znění (Angl.) [online]. [cit.13.3.2008]. Dostupné z: http://pdf.codev2.cc/Lessig-Codev2.pdf

32. MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti. Komentář.* Praha: Wolters Kluwer, 2015. s. 85

33. MATEJKA, Ján. *Internet jako objekt práva: hledání rovnováhy autonomie a soukromí.* Praha: CZ.NIC, 2013. ISBN 978-80-904248-7-6 s. 25

34. *National legal challenges to the Data Retention Directive.* [online]. [cit.16.7.2016]. Dostupné z: https://eulawanalysis.blogspot.cz/2014/04/national-legal-challenges-to-data.html

35. *Největší sociální sítě na světě? Facebook je sice jednička, ale...* [online]. [cit.10.8.2015]. Dostupné z: http://www.lupa.cz/clanky/nejvetsi-socialni-site-na-svete-facebook-je-sice-jednicka-ale/

36. *PDCA cycle.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.creativesafetysupply.com/glossary/pdca-cycle/

37. PETERKA, Jiří. *Uchovávat provozní a lokalizační údaje nám už EU nenařizuje. My to v tom ale pokračujeme.* [online]. [cit. 10. 11. 2015]. Dostupné z: http://www.earchiv.cz/b14/b0428001.php3

38. POLČÁK, Radim. *Právo na internetu. Spam a odpovědnost ISP.* Brno: Computer Press, 2007, s. 7

39. POŽÁR, Josef a Luděk NOVÁK. *Pracovní příručka bezpečnostního manažera.* Praha: AFCEA, 2011. ISBN 978-80-7251-364-2, s. 5 případně: POŽÁR, Josef a Luděk NOVÁK. *Systém řízení informační bezpečnosti.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.cybersecurity.cz/data/srib.pdf s. 1

40. REED, Chris. *Internet Law*. Cambridge: Cambridge University Press, 2004, str. 218

41. *Regional internet registries.* [online]. [cit.4.8.2015]. Dostupné z: https://www.nro.net/about-the-nro/regional-internet-registries

42. ROSER, Christoph. *The Many Flavors of the PDCA.* [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.allaboutlean.com/pdca-variants/

43. ŠKORNIČKOVÁ, Eva. *Jednoduchý test: Jak jste na tom s přípravou na GDPR?* [online]. [cit. 10. 11. 2017]. Dostupné z: *https://www.gdpr.cz/blog/jednoduchy-test-jak-jste-na-tom-s-pripravou-na-gdpr/*

44. SMEJKAL, Vladimír. *Internet a §§§.* 2. aktualiz. a rozš. vyd. Praha: Grada, 2001, s. 32

45. SMITH, Craig. *By the Numbers: 100 Amazing Google Search Statistics and Facts.* [online]. [cit. 4. 8.2016]. Dostupné z: http://expandedramblings.com/index.php/by-the-numbers-a-gigantic-list-of-google-stats-and-facts/

46. Soudní dvůr Evropské unie. Tisková zpráva č. 54/14, ze dne 8. 4. 2014. Rozsudek ve spojených věcech C-293/12 a C-594/12. [online]. [cit.15.7.2016]. Dostupné z: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054cs.pdf

47. SPITZER, Manfred. *Digitální demence.* Brno: Host, 2014. ISBN 978-80-7294-872-7

48. Stanovisko Generálního advokáta Pedra Cruz Villalóna. Věc C-293/12 a C-594/12. [online]. [cit.15.7.2016]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=727954

49. Stanovisko Generálního advokáta SAUGMANDSGAARD ØE, ze dne 19. 7. 2016. Ve spojených věcech C-203/15 a C-698/15. [online]. [cit.10.8.2016]. Dostupné z: http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=111650

50. ŠTOČEK, Milan. *V Hitlerově duchu proti Hitlerovi.* [online]. [cit.10.7.2016]. Dostupné z: http://www.euro.cz/byznys/v-hitlerove-duchu-proti-hitlerovi-814325

51. *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

52. *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

53. *The fragmentation of Android has new records: 24 000 different devices.* [online]. [cit.15.7.2016]. Dostupné z: http://appleapple.top/the-fragmentation-of-android-has-new-records-24-000-different-devices/

54. *The very first mobile malware: how Kaspersky Lab discovered Cabir.* [online]. [cit.1.8.2016]. Dostupné z: http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir

55. THOMAS, Douglas. *Criminality on the Electronic Frontier.* In Cybercrime. London: Routledge, 2003, s. 17 a násl.

56. *Tor security advisory: "relay early" traffic confirmation attack.* [online]. [cit.23.7.2016]. Dostupné z:https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack

57. TRADOC. Cyberspace Operations: Concept Capability Plan 2016-2028. [online]. [cit. 18. 2. 2018], s. 8-9 Dostupné z: www.fas.org/irp/doddir/army/pam525-7-8.pdf?

58. VOŽENÍLEK, David. *Promazání „sušenek" nepomůže, na internetu vás prozradí i baterie.* [online]. [cit.4.8.2016]. Dostupné z: http://mobil.idnes.cz/sledovani-telefonu-na-internetu-stav-baterie-faz-/mob_tech.aspx?c=A160802_142126_sw_internet_dvz

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

60. *Zlepšování zabezpečení, ochrana soukromí a vytváření jednoduchých nástrojů, které vám dávají možnost kontroly a výběru, je pro nás velmi důležité.* [online]. [cit.4.4.2014]. Dostupné z: https://www.google.cz/intl/cs/policies/?fg=1