LEGISLATIVNÍ ASPEKTY MONITORINGU SÍTÍ

Jan Kolouch

DŮVODY MONITORINGU ICT

- **Bezpečnostní** (odhalování úniku dat a informací, nalezení malware či jiného útoku, zamezení šíření nákazy aj.),
- **Ekonomické** (produktivita, motivace zaměstnanců, pracovní kázeň, snížení nákladů o již způsobenou škodu, prevence škod budoucích aj.),
- **Právní** (protože mi to zákon přikazuje…)

PRACOVNÍ MORÁLKA A ICT - MINULOST-

Zdroj: Prezentace Markéty Románkové na Odborné konferenci IIR: IT Security, 15.-16.5.2012. **Máte IT zabezpečené i proti právníkům?**

- **46 %** pracovní doby hrál zaměstnanec **Solitaire**,
- **80 %** pracovní doby si pracovnice městského úřadu **trénovala strategické myšlení** hraním **Age of Empires**,
- **106 %** (**započítány jsou i přesčasy**) pracovní doby strávila administrativní pracovnice státní instituce **chatováním**….**ne pracovním**….**i když zcela jistě o práci**,
- **pouze 4 %** pracovní doby **prokazatelně odpracoval webmaster** velké společnosti v průběhu 1 měsíce,
- **45 % pracovní doby** měl člověk, který má v popisu práce celý den pracovat s PC, **vypnutý počítač**.


Candy Crush Saga
Subway Surfers
Clash of Clans
Criminal Case
8 Ball Pool
Farm Heroes Saga
Words With Friends
Texas HoldEm Poker
Dragon City
Hay Day
Users Stats:
Monthly: 5,000,000
Weekly: 5,000,000
Daily: 1,000,000
Viral: 84,132
aMOOzing farm!
ayDL Hay Day is a
smooth gest...
YouTube

DALŠÍ AKTIVITY

- běžné surfování….aka…**kill the time**….
- soukromé emaily
- výběr a nákup zboží

Surfování na internetu není levná záležitost. Z uživatelských dat klientů společnosti SODATSW vyplývá, že **v průměru tráví zaměstnanci 12 % času nepracovní aktivitou**.
Pokud tuto časovou ztrátu vyčíslíme **u firmy o 50 zaměstnancích, dostáváme se na úctyhodných 2,4 milionů korun ročně.** Díky monitoringu se nepracovní aktivita zaměstnanců v průměru snižuje až o 80 %,“uzavírá Roman Rous.

http://finexpert.e15.cz/co-muze-zamestnavatel-sledovat-a-co-uz-je-pres-caru

FAKT BYCH MĚL MONITOROVAT?

VŠE UVEDENÉ JE PRO MĚ NAPROSTO OK…

Občanskoprávní důsledky

Trestněprávní důsledky

Správněprávní důsledky

Splnění povinnosti dle ZKB, ZoEK aj.

Ale zasahuji do práv UŽIVATELE!

Čl. 1 Listiny

Lidé jsou svobodní a rovní v důstojnosti i v právech. *Základní práva a svobody jsou nezadatelné, nezcizitelné, nepromlčitelné a nezrušitelné.*

SOUKROMÍ

základní lidské právo, zakotvené ve Všeobecné deklaraci lidských práv z roku 1948:

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.“*

ČR

Čl. 7 odst. 1 Listiny:

„Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.“

Čl. 10 odst. 2 a 3 Listiny:

„Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.“

„Každý má právo na ochranu před NEOPRÁVNĚNÝM shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“

ČL. 13 Listiny:

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

JAK VLASTNĚ MONITORUJI?

- **Kamery**
- Sledování výpisu firemních telefonů
- Docházkový systém
- **Monitoring ICT** (např. uchovávání provozních a lokalizačních údajů) aj.

Paralela mezi kamerami a monitoringem ICT

- stanovit hranice, **co a jak moc se bude sledovat**
- stanovit jasná **pravidla, které prostory se nesmí sledovat** vůbec, **a které naopak celé** a s podrobným náhledem.
- definovat **jak se budou záznamy dlouho archivovat, jak budou tyto záznamy chráněné a zabezpečené proti zneužití.**

http://www.newyorker.com/culture/culture-desk/gold-toilet

https://lovetha

-applications.htm

CESNET

KAMERY A UOOU?

https://www.uoou.cz/files/stanovisko_2006_1.pdf

- **Provozování kamerového systému je považováno za zpracování osobních údajů, pokud je** vedle kamerového sledování **prováděn záznam pořizovaných záběrů, nebo jsou v záznamovém zařízení uchovávány informace** a zároveň účelem pořizovaných záznamů, případně vybraných informací, je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním.
- **Údaje uchovávané v záznamovém zařízení**, ať obrazové či zvukové, **jsou osobními údaji za předpokladu, že na základě těchto záznamů lze přímo či nepřímo identifikovat konkrétní fyzickou osobu** (tedy: informace z obrazových či zvukových nahrávek umožňují, byť nepřímo, identifikaci osoby).

Zpracování osobních údajů provozováním kamerového systému je přípustné:

a) v rámci **plnění úkolů uložených zákonem** (např. Policii České republiky); v těchto případech je třeba dbát ustanovení příslušného zákona,

b) dále je toto možné na základě řádného **souhlasu subjektu údajů**;

c) užití kamerového systému však je možné i bez souhlasu subjektu údajů s využitím **ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.:**

„pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; *takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života,“*

Povinnosti správce při provozování kamerového systému vybaveného záznamovým zařízením:

a) Kamerové sledování nesmí nadměrně zasahovat do soukromí. Sledovaného účelu nelze účinně dosáhnout jinou cestou (např. majetek je možno chránit před odcizením uzamčením místnosti). **Je vyloučeno užití kamerového systému v prostorách určených k ryze soukromým úkonům** (např. toalety, sprchy). Je ovšem možné řešení, kdy subjekt údajů má na výběr z alternativ (např. lze monitorovat prostory šatny plaveckého stadionu za předpokladu, že je vymezen prostor pro převlékání, který není kamerami sledován).

b) **Specifikace sledovaného účelu. Je třeba předem jednoznačně stanovit účel pořizování záznamů, který musí korespondovat s důležitými, právem chráněnými zájmy správce** (např. ochranou majetku před krádeží). Záznamy tak mohou být využity pouze v souvislosti se zjištěním události, která poškozuje tyto důležité, právem chráněné zájmy správce. Přípustnost využití záznamů pro jiný účel musí být omezena na významný veřejný zájem, např. boj proti pouliční kriminalitě.

c) Je třeba **stanovit lhůtu pro uchovávání záznamů.**

d) Je třeba řádně **zajistit ochranu** snímacích **zařízení, přenosových cest a datových nosičů, na nichž jsou uloženy záznamy**, před neoprávněným nebo nahodilým přístupem, změnou, zničením či ztrátou nebo jiným neoprávněným zpracováním - viz § 13 zákona č. 101/2000 Sb.

e) Subjekt údajů musí být o užití kamerového systému **vhodným způsobem informován** (např. nápisem umístěným v monitorované místnosti), viz § 11 odst. 5 zákona č. 101/2000 Sb., nejde-li o uplatnění zvláštních práv a povinností vyplývajících ze zvláštního zákona.

f) Je třeba **garantovat další práva subjektu údajů, zejména právo na přístup ke zpracovávaným datům a právo na námitku proti jejich zpracování, viz § 1 zákona č. 101/2000 Sb.**

g) **Zpracování osobních údajů je třeba registrovat** u Úřadu pro ochranu osobních údajů, nejde-li o uplatnění zvláštního práva či povinností vyplývajících ze zvláštního zákona, viz § 18 odst. 1 písm. b) zákona č. 101/2000 Sb.

Ok…kamery a ZOOU….ale… MONITORING ICT?

IP ADRESA JAKO OSOBNÍ ÚDAJ

Patrick Breyer proti **Bundesrepublik Deutschland**

http://curia.europa.eu/juris/document/document.jsf?text=&docid=184668&pageIndex=0&doclang=cs&mode=lst&dir=&occ=first&part=1&cid=1403270

dynamická IP adresa je dle rozsudku soudního dvora EU z 19.10.2016 za určitých okolností osobním údajem

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.**

Jednalo se o klasické logování ze strany ISP služeb.

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:

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:

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.

Rozsudek alá chytrá horákyně

- **Je nesporné, že dynamická IP adresa nepředstavuje informaci o „IDENTIFIKOVANÉ OSOBĚ“**
- **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.

Dále soud prohlásil (body 47 a 48):

- **„Existují-li právní prostředky umožňující poskytovateli online mediálních služeb obrátit se** zejména v případě kybernetických útoků **na příslušný orgán** za účelem, **aby podnikl kroky nezbytné k získání těchto informací od poskytovatele internetového připojení** a k zahájení trestních stíhání.

- **Poskytovatel on-line mediálních služeb má tedy patrně prostředky, které mohou být** rozumně **použity, aby nechal** s pomocí jiných osob, a sice příslušného orgánu a poskytovatele internetového připojení, **identifikovat subjekt údajů** na základě uchovaných IP adres.“

Z těchto důvodů Soudní dvůr (druhý senát) rozhodl takto:

1) Článek 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 musí být vykládán v tom smyslu, 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 tohoto ustanovení, pokud má k dispozici právní prostředky, které mu umožňují NECHAT IDENTIFIKOVAT subjekt údajů díky dalším informacím, kterými disponuje poskytovatel internetového připojení tohoto subjektu.**

DŮSLEDEK

- **ISP budou IP adresami muset** (minimálně z důvodu opatrnosti) **zacházet jako s osobním údajem**
- **Musí dodržovat všechny povinnosti stanovené zákonem č. 101/2000 Sb.**, o ochraně osobních údajů, potažmo novým Obecným nařízením o ochraně osobních údajů, které začne platit v květnu roku 2018 (**GDPR**).

DALŠÍ IMPULZ PRO MONITORING ICT

- **zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim.**
  - **právnické osobě lze přičítat spáchání trestného činu**, jestliže:
  - orgány právnické *„neprovedly taková opatření, která měly provést podle jiného právního předpisu nebo která po nich lze spravedlivě požadovat, zejména* ***neprovedly povinnou nebo potřebnou kontrolu nad činností zaměstnanců nebo jiných osob, jimž jsou nadřízeny, anebo neučinily nezbytná opatření k zamezení nebo odvrácení následků spáchaného trestného činu.“***
  - Zaměstnanci tak mohou být pro svého zaměstnavatele i vnitřním trestněprávním rizikem.
- **zákon č. 181/2014 Sb., o kybernetické bezpečnosti.**
  - **§ 7** (detekce kybernetické bezpečnostní události)
  - **§ 8** (hlášení kybernetického bezpečnostního incidentu)

INTERVENCE PRÁVA DO TOHO CO BĚŽNĚ DĚLÁM

Takže jsem permanentně jednou nohou….

K čemu mi tedy právo je?

http://zpravy.tiscali.cz/ve-svete-je-ve-vezeni-rekordni-pocet-232-novinaru-206486

Čl. 2 odst. 3 Listiny

Každý může činit vše, co není zákonem zakázáno, a nikdo nesmí být nucen činit, co zákon neukládá

Zákon č. 89/2012 Sb., občanský zákoník

§ 86

Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména **nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy** pořízené o soukromém životě člověka třetí osobou, nebo **takové záznamy** o jeho soukromém životě **šířit.** Ve stejném rozsahu jsou **chráněny i soukromé písemnosti osobní povahy.**

§ 88

(1) Svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí **k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob.**

(2) Svolení není třeba ani v případě, když se podobizna, písemnost osobní povahy nebo zvukový či obrazový záznam **pořídí nebo použijí na základě zákona k úřednímu účelu nebo v případě, že někdo veřejně vystoupí v záležitosti veřejného zájmu.**

§ 89

Podobizna nebo zvukový či obrazový záznam se mohou **bez svolení člověka** také pořídit nebo použít přiměřeným způsobem též **k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství.**

- **Generální prevenční povinnost**
- Možnost náhrady škody, když jsem ISP
- **Vhodně nastavená pravidla**

EULA

- Relativně **vyvážené vydefinování práv a povinností uživatele i správce**
- Stanovení toho co a v jakém rozsahu (v jakých případech budete monitorovat)
- Plošný vs. individualizovaný monitoring

- **Souhlas dotčeného**
- **Seznámení se i s možností zásahu do osobních údajů**
- **Možnost nesouhlasit**

Zákon č. 262/2006 Sb., zákoník práce

§ 301 písm. a) a d) ZP

- **Zaměstnavatel je oprávněn kontrolovat zda zaměstnanec všechny uložené úkoly plní řádně a včas.**
- **Základní povinností zaměstnance je dle § 301**

a) *pracovat řádně* podle svých sil, znalostí a schopností, *plnit pokyny nadřízených*, vydané v souladu s právními předpisy a spolupracovat s ostatními zaměstnanci,

d) ***řádně hospodařit s prostředky svěřenými jim zaměstnavatelem a střežit a ochraňovat majetek*** zaměstnavatele před poškozením, ztrátou, zničením a zneužitím a **nejednat v rozporu s oprávněnými zájmy zaměstnavatele.**

Hlava VIII: Ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance

§ 316 ZP

(1) Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.

(2) **Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.**

(3) Jestliže je u zaměstnavatele dán **závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele**, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, **je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.**

Informujte osoby, že dochází k monitoringu ICT

- **Povinnost** předem upozornit **dle § 316 odst. 3 ZP není úplně jasně vymezena** a je závislá vždy na způsobu kontroly.
- **Zaměstnavatel smí bez předchozího upozornění sledovat dobu strávenou na internetu či využití programů.**
- Kontrola firemních e-mailových schránek či paměti počítačů a externích nosičů je však již podložena povinností informovanost zaměstnance vyžaduje.
- **Obecně se doporučuje informovat zaměstnance v případě jakékoliv kontroly.**
- …..viz **EULA** …. Vhodné a **vyvážené nastavení pravidel**, či dodatku k pracovní smlouvě, kdy zaměstnanec svým podpisem stvrzuje, že se s informací seznámil.

Nejvyšší soud ve svém rozhodnutí **21 Cdo 2172/2002** konstatoval, že:

*„**K povinnostem zaměstnavatele náleží** nepochybně rovněž **povinnost** … **soustavně kontrolovat, zda zaměstnanci plní své pracovní úkoly tak, aby nedocházelo ke škodám. Jde o součást systému prevenčních povinností**, ukládající zaměstnavateli přijmout a soustavně uplatňovat takový souhrn způsobů a forem kontroly plnění pracovních úkolů zaměstnanci, který lze po něm vzhledem ke konkrétní časové a místní situaci rozumně požadovat a který – objektivně vzato – **je způsobilý co nejvíce omezit a snížit riziko vzniku škod.**“*

Zdroj:
http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/D5C7441DD038DFE6C1257A4E0065A236?openDocument&Highlight=0,

Nejvyšší soud ve svém rozhodnutí **21 Cdo 1771/2011** konstatoval, že:

*„**cílem kontroly** prováděné zaměstnavatelem **nebylo zjišťování obsahu** e-mailových zpráv, obsahu SMS nebo MMS, případně odeslaných či přijatých zaměstnancem, **nýbrž toliko zjištění, zda zaměstnanec respektuje** (a když nerespektuje, tak v jaké míře) **zákaz užívat pro svou osobní potřebu výpočetní techniku zaměstnavatele** včetně jeho telekomunikačních zařízení, vyplývající ze zákona, **a to s přihlédnutím k zákazu nepoužívat internetové stránky s pochybným či citlivým obsahem nebo stránky typu on-line zpravodajství, sledování TV přes internet nebo poslech rozhlasu přes internet, které mohou nadměrně zatěžovat počítačovou síť a které nesouvisí s výkonem sjednané práce** (vyplývajícímu z Pracovního řádu). **Je tedy zřejmé, že prováděná kontrola směřovala toliko k ochraně majetku zaměstnavatele.**“*

Zdroj:
http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/B0ED0CEF751D472DC1257A61004D599C?openDocument&Highlight=0,

Niemetz vs. Německo

Evropský soud v odůvodnění dospěl k závěru, že **soukromý život je otázkou respektování vzájemných vztahů mezi lidskými bytostmi** a je irelevantní, zda se tak děje na pracovišti či kdekoliv jinde.

Zaměstnavatel je tak **oprávněn kontrolovat zaměstnance adekvátním způsobem, tak aby nebyla snížena jejich lidská důstojnost nepřiměřeným zásahem do práva na soukromí.**

http://hudoc.echr.coe.int/eng?i=001-61853#{%22fulltext%22:[%2213710/88%22],%22itemid%22:[%22001-57887%22]}

http://spcp.prf.cuni.cz/judikat/es27-96.htm

Bărbulescu proti Rumunsku

Dne 12. 1. 2016 vydal Evropský soud pro lidská práva rozhodnutí ve věci sledování osobní elektronické komunikace zaměstnanců zaměstnavatelem během pracovní doby – Rozhodnutí ve věci č. 61496/08 Bărbulescu proti Rumunsku.

Evropský soud pro lidská práva nejprve na základě své předchozí judikatury **shrnul, že pojem soukromí či soukromý život je nutno chápat široce, nicméně nikoli neomezeně. Důležité pro posouzení toho, zda monitorování činnosti zaměstnance**, například nahrávání jeho telefonních hovorů, **sledování činnosti na internetu či elektronické komunikace**, je či není v rozporu s čl. 8 Úmluvy, **je, zda dotyčný stěžovatel na základě objektivních skutečností** (informace prokazatelně zprostředkované zaměstnavatelem, vnitřní pravidla pro využívání výpočetní techniky a telekomunikačního zařízení, běžná praxe na pracovišti) **mohl při komunikaci,** v tomto případě při využívání programu Yahoo Messenger, **odůvodněně očekávat soukromí či nikoliv.**

Evropský soud pro lidská práva pokračoval obecným tvrzením, že není nedůvodné, aby zaměstnavatel kontroloval, zda zaměstnanci v pracovní době skutečně pracují. Podle názoru Evropského soudu pro lidská práva **nebylo doloženo, že by zaměstnavatel přistupoval k dalším informacím v počítači daného zaměstnance**, např. k uloženým dokumentům, naproti tomu využívání účtu v programu Yahoo Messenger bylo kontrolováno pouze v krátkém časovém období. Z toho soud dovodil, že v tomto případě se jednalo o omezený a přiměřený zásah do soukromí stěžovatele. K porušení čl. 8 Úmluvy tak podle názoru soudu v tomto případě nedošlo.

Každý člověk má i při výkonu práce jistou míru soukromí, byť s ohledem na charakter práce více či méně sníženou. Zaměstnavatel má na druhé straně LEGITIMNÍ PRÁVO rozhodovat o tom, jak bude využíván jeho majetek (výrobní prostředky) **a rovněž právo jejich využívání kontrolovat.**

- http://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159906%22]}
- http://www.cak.cz/assets/barbulescu-proti-rumunsku.pdf
- Dále viz: https://www.epravo.cz/top/clanky/sledovani-aktivity-zamestnance-na-internetu-ve-svetle-aktualni-judikatury-evropskeho-soudu-pro-lidska-prava-100316.html

e-mail

Stanovisko č. 2/2009 UOOU

https://www.uoou.cz/files/stanovisko_2009_2.pdf

*„**zaměstnavatel není oprávněn** sledovat, **monitorovat a zpracovávat obsah korespondence svých** korespondence svých **zaměstnanců**. Zaměstnavatel případně **smí u svých zaměstnanců pouze sledovat počet došlých a odeslaných e-mailů, případně** (tj. zejména vznikne-li podezření ze zneužití pracovních prostředků, resp. využití k jiným než pracovním účelům) **včetně hlavičky**, tj. komu píší a od koho je dostávají.“*

*Stanovisko dále pokračuje: „**Soukromý e-mail** zaměstnance **smí zaměstnavatel na základě oprávnění daných mu novým zákoníkem práce otevřít a přečíst pouze výjimečně, v zájmu ochrany svých práv, především jestliže je zřejmé, že se jedná o pracovní e-mail, tj. lze-li tento závěr učinit na základě údajů uvedených v hlavičce, a jestliže je pravděpodobné, že z objektivních důvodů**, jako je dlouhodobá nemoc zaměstnance, by k jejímu vyřízení zaměstnancem mohlo dojít natolik pozdě, že by zaměstnavatel mohl utrpět újmu na svých právech.*

***Zaměstnavatel tak fakticky využívá svého práva chránit majetek podle nového zákoníku práce.** Při nařizování dovolené by měl zaměstnavatel předem přijmout taková opatření k zastupování, aby k poškození soukromí zaměstnance nedošlo.“*

MOŽNÁ OBČANSKOPRÁVNÍ ODPOVĚDNOST

Vyžadují-li to okolnosti případu nebo zvyklosti soukromého života, **je každý povinen počínat si při svém konání tak, aby nedošlo k nedůvodné újmě na svobodě, životě, zdraví nebo na vlastnictví jiného.**

§ 2909 a násl. OZ

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

§ 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.**

MOŽNÁ TRESTNĚPRÁVNÍ ODPOVĚDNOST

§ 182
Porušení tajemství dopravovaných zpráv

(1) Kdo **úmyslně poruší tajemství**

a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,

b) **datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo**

c) **neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data,**

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

(2) Stejně bude potrestán, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch

a) **prozradí tajemství, o němž se dozvěděl z** písemnosti, telegramu, telefonního hovoru nebo **přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu, nebo**

b) **takového tajemství využije.**

(3) Odnětím svobody na šest měsíců až tři léta nebo zákazem činnosti bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,
b) spáchá-li takový čin ze zavrženíhodné pohnutky,
c) způsobí-li takovým činem značnou škodu, nebo
d) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného značný prospěch.
(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,
a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako úřední osoba,
b) způsobí-li takovým činem škodu velkého rozsahu, nebo
c) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.
(5) **Zaměstnanec provozovatele** poštovních služeb, **telekomunikační služby nebo počítačového systému anebo kdokoli jiný vykonávající komunikační činnosti, který**
***a)* spáchá čin uvedený v odstavci 1 nebo 2,**
***b)* jinému úmyslně umožní spáchat takový čin, nebo**
***c)* pozmění nebo potlačí písemnost** obsaženou v poštovní zásilce nebo dopravovanou dopravním zařízením anebo zprávu **podanou neveřejným přenosem počítačových dat, telefonicky, telegraficky nebo jiným podobným způsobem**,
bude potrestán odnětím svobody na jeden rok až pět let, peněžitým trestem nebo zákazem činnosti.
(6) Odnětím svobody na tři léta až deset let bude pachatel potrestán,
a) způsobí-li činem uvedeným v odstavci 5 škodu velkého rozsahu, nebo
b) spáchá-li takový čin v úmyslu získat pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

(1) Kdo **překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části**, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo **získá přístup k počítačovému systému nebo k nosiči informací a**

a) neoprávněně **užije data** uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací **neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,**

c) **padělá nebo pozmění data** uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) **neoprávněně vloží data** do počítačového systému nebo na nosič informací **nebo učiní jiný zásah** do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat,

bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2

a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo

b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.

(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) způsobí-li takovým činem značnou škodu,

c) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,

d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo

e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.

(5) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo

b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) **Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c)** nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle **§ 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává**

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části,

bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo jiné majetkové hodnoty nebo zákazem činnosti.

(2) Odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny, nebo

b) získá-li takovým činem pro sebe nebo pro jiného značný prospěch.

(3) Odnětím svobody na šest měsíců až pět let bude pachatel potrestán, získá-li činem uvedeným v odstavci 1 pro sebe nebo pro jiného prospěch velkého rozsahu.

TAK CO MÁM DĚLAT, ABY TO BYLO DOBŘE?

TEST PROPORCIONALITY

je **standardním právním nástrojem soudů mezinárodních, tak soudů ústavních (národních)** posuzuje-li se **konflikt ustanovení právního řádu, sledující ochranu ústavně zaručených práv či veřejného zájmu, s jiným základním právem či svobodou.** Tato obecná zásada 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 nejšetrnějšího*** *- ve vztahu k dotčeným základním právům a svobodám -* ***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."*

Co ano a co ne?

Příklady přiměřeného monitoringu:

- **sledování doby strávené na internetu**, včetně přehledu o navštívených stránkách
- **sledování doby strávené chatováním**, včetně přehledu o tom, s kým se chatovalo,
- **přehled telefonické komunikace** (příchozí i odchozí hovory) zaměstnance,
- **obsah pevného disku firemního počítače** - zejména z hlediska legálnosti nebo nelegálnosti nainstalovaného a používaného software,
- **obsah přenosných médií** (typicky USB flashdisků apod.) – zejména ve kvůli ochraně firemních tajemství a možnému úniku dat.

Příklady nepřiměřeného monitoringu:

- **skenování monitoru zaměstnance** (některé dohledové systémy pravidelně snímají obsah toho, co je na obrazovce a ukládají tyto informace do své databáze),
- **použití keyloggerů**,
- **sledování obsahu soukromé konverzace**, ať už chatování či e-mailů (vyjma zákonem stanovených případů).
- **sledování zaměstnanců kamerami nad rámec zákonem stanovených oprávnění** (vyjma dříve uvedených výjimečných druhů zaměstnání),

Vztahuje se to vůbec na mě? Moji instituci?

ISP - ZSIS

Poskytovatel služeb spočívající v **přenosu informací poskytnutých uživatelem** (Mere Conduit nebo Access Provider).

ISP jiných služeb, než konektivity
Zák. 480/2004, ZoSIS

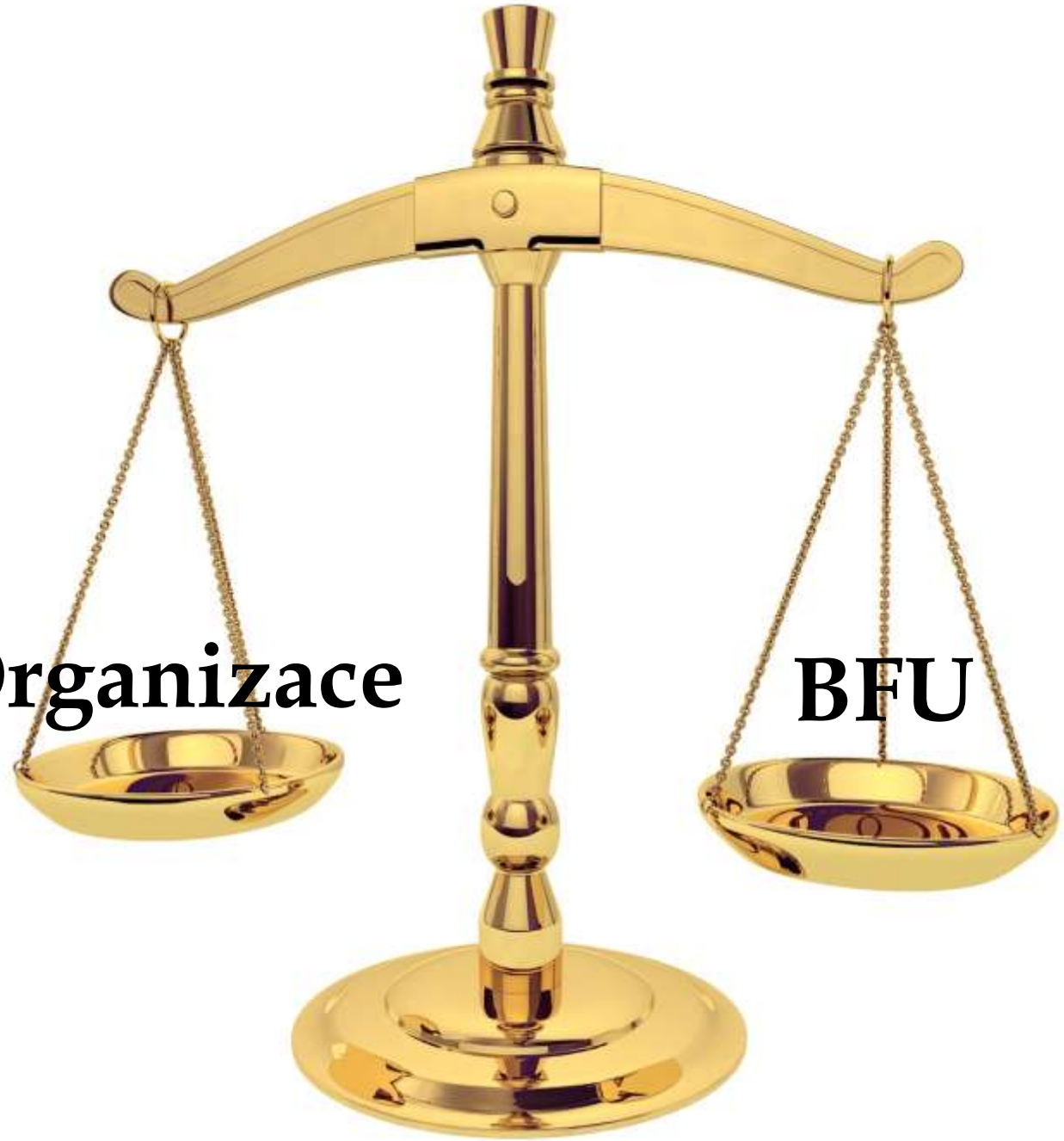
Veřejní
Zák. 127/2005, ZoEK

Neveřejní
Zák. 480/2004, ZoSIS

Poskytovatele služeb **spočívajících v automatickém meziukládání informací poskytnutých uživatelem** (tzv. caching).

- Proxy
- Aplikační cashing (exchange, cloudové řešení, aj.)
- Maily
- Blogy, aj.

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


Organizace
BFU

1) **Nastavte jasná a srozumitelná pravidla** pro užívání ICT pro koncové uživatele.
2) **Seznamte prokazatelně uživatele** s těmito pravidly.
3) **Umožněte** subjektu **nesouhlasit** s podmínkami použití služby.
4) **Definujte práva a povinnosti uživatele, správce, organizace.**
5) **Upozorněte subjekty na to, že sbíráte a uchováváte osobní údaje.**
6) **Zvolte prostředky přiměřené k dosažení sledovaného cíle** (viz princip minimalizace zásahu do základních lidských práv a test proporcionality).

   Např. o taxativní vymezení webových stránek, které určitý zaměstnanec může navštěvovat (tzv. **whitelist**) nebo naopak stránky, na které je přístup blokován (sociální sítě, pornografické stránky atd. - **blacklist**) aj.
7) **Využívejte osobní údaje pouze v souladu s účelem, ke kterému byly shromážděny.** K jiným účelům je využívejte pouze tehdy, pokud lze takové zpracování podložit § 5 odst. 2 zákona o ochraně osobních údajů.
8) **Nebojte se upravovat a modifikovat pravidla.**
9) **Spolupracujte při tvorbě pravidel a managementem, právníky, bezpečnostními týmy, IT aj.**
10) **VYTVOŘTE SI SVÁ VLASTNÍ PRAVIDLA**

Pozn. ***Využijte současné „turbulentní situace“***

Kvalitně a precizně nastavená pravidla Vám mohou pomoci značně eliminovat či redukovat střet světa IT a práva

Primárně je třeba pozornost věnovat oblastem:

- **osobních údajů a ochrany soukromí**
- **citlivých či důvěrných informací** poskytnutých v obchodní styku
- **autorských práv**
- **trestně právní odpovědnosti** (fyzické i právnické osoby)
- **obchodních sdělení aj.**

Neexistuje jedno pravidlo, vzor, matice aplikovatelná pro každou společnost a každou situaci.

Je třeba individualizovat…

Děkuji za pozornost

JUDr. Jan Kolouch, Ph.D.
sdružení CESNET, z.s.p.o.
jan.kolouch@cesnet.cz