Crypto-World

Informační sešit GCUCMP

Ročník 5, číslo 10/2003 **15. říjen 2003**

10/2003

Připravil : Mgr.Pavel Vondruška

Sešit je rozesílán registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(475 e-mail výtisků)

Obsah : **Str.**

A. Soutěž v luštění 2003 (P.Vondruška) **2**
B. Cesta kryptologie do nového tisíciletí III. (Od asymetrické kryptografie k elektronickému podpisu) (P.Vondruška) **3 - 7**
C. K oprávnění zaměstnavatele kontrolovat práci zaměstnance pomocí moderních technologií (J.Matejka) **8-19**
Jednoduchá a automatická aktualizace (D.Doležal) **20-21**
D. Recenze knihy „Řízení rizik“ autorů V. Smejkala a K. Raise (A. Katolický) **22-24**
E. Letem šifrovým světem **25-26**
F. Závěrečné informace **27**

(články neprocházejí jazykovou korekturou)

A. Soutěž v luštění 2003
Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

Soutěž v luštění jednoduchých kryptologických úloh, kterou jsem vyhlásil v minulém čísle Crypto-Worldu, má za sebou teprve první měsíc a již jsou známi její vítězové. Prvá tři místa (tj. místa, na nichž řešitel automaticky získal cenu) byla obsazena dokonce již v průběhu prvého týdne. První řešitel oznámil splnění všech úloh ve čtvrtek 18.9 kolem poledne a druhý v celkovém pořadí dokončil soutěž jen o půl hodiny později.

Vítězové soutěže 2003:

(registrační jméno,	pořadí vyřešených úloh,								e-mail)
1 CyberMage	01;	03;	02;	04;	05;	06;	09;	08;	07;	(jry2000@seznam.cz)
2 peta007	01;	04;	07;	02;	03;	05;	06;	08;	09;	(peta007@seznam.cz)
3 xnovakv	02;	05;	06;	03;	01;	04;	08;	07;	09;	(xnovakv@volny.cz)

Neznamená to však, že soutěž skončila! Stále (kromě radosti z hledání správného řešení) jsou ve hře tři ceny (replika historické číše Rudolfa II. s láhví portugalského vína MATEUS). Tyto ceny budou vylosovány po oficiálním ukončení soutěže (6.12.2003, 22.00 hod) mezi ty řešitele, kteří vyluští alespoň tři ze zadaných úloh.

Dostat se mezi účastníky, o nichž rozhodne los, by nemělo být velkým problémem, potvrzuje to i ukázka z e-mailu celkového vítěze :
"Největší můj problém byly úlohy 1-3, protože byly extrémně lehké. V okamžiku, když jsem rozluštil úlohu číslo 1, tak jsem málem 'bil hlavou do zdi'. Přece jen jsem očekával větší složitost už v prvním kole".

V současné době (sobota 11.10.2003) se zaregistrovalo do soutěže 85 řešitelů, pouze 20 však splnilo požadavek na zařazení do losování o zbývající 3 ceny (tj. jedná se o odběratele Crypto-Worldu, kteří vyřešili minimálně 3 úlohy), všech 9 úloh dosud vyřešilo 7 soutěžících.

Jako zajímavost uvádím, že první den www stránku s úlohami navštívilo přes 400 lidí (viz statistiky na http://crypto-world.info).

Podle přehledu vyřešených úloh a z korespondence, kterou jsem dostal, dělají řešitelům největší problém obě úlohy na transpozici (04, 07).
Naopak za nejlehčí považují soutěžící úlohu 01 a 03.

Poznámka (pro řešitele ze Slovenska): pokud se vám zdá, že jste úlohu 03 vyřešili, a přesto vám automat vaše řešení odmítá potvrdit – prosím zašlete e-mailem své řešení na moji adresu (pavel.vondruska@crypto-world.info) a já, pokud je řešení správné, zajistím připsání bodu. Proč tomu tak je nemohu více v této chvíli vysvětlit abych neprozradil podstatu úlohy.

Jména vylosovaných řešitelů, kteří získali zbývající tři ceny, jakož i řešení všech devíti úloh s průvodním komentářem bude zveřejněno v e-zinu Crypto-World 12/2003.

Závěrem vás srdečně zvu k zapojení do probíhající soutěže.
Úlohy, aktuální stav, pravidla a ceny najdete na http://crypto-world.info ikona Soutěž 2003.

B. Cesta kryptologie do nového tisíciletí III.
(Od asymetrické kryptografie k elektronickému podpisu)

Mgr. Pavel Vondruška, ČESKÝ TELECOM, a.s.

Jak jsem již psal v e-zinu Crypto-World 78/2000 seriál *Cesta kryptologie do nového tisíciletí* vznikl v roce 2000 a zde jej publikuji v původní, neupravené verzi. Z tohoto důvodu jsou v něm některé uvedené informace již zastaralé. Na dvou místech jsem proto vložil krátké upřesňující poznámky.

Asymetrická kryptografie

Asymetrická kryptografie je založena na této myšlence: Každý subjekt má svůj tajný (soukromý) klíč a k němu veřejný klíč. Tajný klíč je určen k zašifrování a veřejný klíč k odšifrování. V síti o n subjektech je tak potřeba připravit jen 2n klíčů, přičemž veřejné klíče lze opravdu zveřejnit a odpadá tedy nutnost složité, nákladné a nebezpečné distribuce těchto klíčů. Šifrování mezi subjekty A a B pak probíhá takto: A má dvojici klíčů "AS" (soukromý klíč), "AV" (veřejný klíč), B má k dispozici obdobně klíče "BS" a "BV". Klíče "AV", "BV" jsou zveřejněny a jsou tedy A i B známy. Subjekt A připraví text, který chce utajit, zašifruje jej svým klíčem "AS" a dále jej zašifruje veřejným klíčem příjemce "BV" (jinak by zprávu mohl odšifrovat každý, kdo má přístup k veřejnému klíči "AV"). Příjemce B potom nejprve zašifruje přijatou zprávu pomocí svého soukromého klíče "BS" (ten zná jen on) a dále pomocí veřejného klíče odesílatele.

Brzy po zveřejnění teoretického schématu asymetrické kryptografie (1978) se objevuje první šifrový systém založený na této myšlence. Vžil se pro něj název RSA (zkratka z prvých písmen tvůrců systému Rivest, Shamir a Adelmann). Tento systém se po malých úpravách (především prodloužení klíče a stanovení jistých pravidel, která musí klíče splňovat) používá dodnes. Je založen na obtížném matematickém problému - faktorizaci (rozkladu na prvočísla) velkých čísel. Vše si nejlépe uvědomíme na následujícím jednoduchém příkladě. Zkusíte najít celočíselné dělitele čísla 217502279? Jsou jimi dvě prvočísla 14713 a 14783. Zatímco vyhledání těchto čísel vyžadovalo relativně dost práce, pak vynásobení těchto dvou čísel je velice jednoduchým úkonem.

Vzhledem k tomu, že RSA ovlivnilo kryptologii konce dvacátého století a význam celého systému v souvislosti se zavedením elektronických podpisů neustále roste, řekněme si něco více o matematických principech tohoto systému.

Postup při vytváření dvojice klíčů (veřejného a tajného) pro RSA je následující:
a) nejprve náhodně (a nepredikovatelně) vygenerujeme dvě dostatečně velká prvočísla (jejich přibližná velikost, tj. počet bitů, je zadána)
b) Spočteme
$n = p*q$ a $F(n) = (p-1)*(q-1)$, kde $F(n)$ je Eulerova funkce určující počet přirozených čísel nesoudělných s n.
c) Zvolíme náhodné číslo e, kde $1 < e < F(n)$, tak, že největší společný dělitel $(e, F(n)) = 1$ (tj. e a $F(n)$ jsou nesoudělná) .
d) Užitím Eukleidova algoritmu spočteme jednoznačně definované číslo d takové, že
$1 < d < F(n)$ a $e*d \equiv 1 \bmod F(n)$.
Veřejným klíčem je potom dvojice (n,e), tajným klíčem uživatele je d.

Číslo n nazýváme modulem, číslo e šifrovacím exponentem a číslo d dešifrovacím exponentem. Patent na algoritmus RSA drží již od jeho vzniku americká společnost RSA Data Security Inc. Letos (20. 9. 2000) tento patent vyprší a algoritmus bude uvolněn k veřejnému použití bez poplatků. Jak se dále dozvíme, stane se tak právě v době, kdy může tento algoritmus sehrát rozhodující úlohu v zavádění elektronických podpisů dokumentů.

Jsme ale stále ještě na začátku osmdesátých let. Světová odborná společnost vývojem asymetrické kryptografie slaví velký úspěch. Tajné služby USA a Anglie mlčí a neprozrazují, že jim je celý systém asymetrické kryptografie již znám. Teprve v roce 1997 byl uveřejněn článek Jamese Ellise z britské CESG (Communications – Electronics Security Group), nazvaný "The history of Non-Secret Encryption" , ve kterém jeho autor popisuje, jak princip asymetrické kryptografie (jím nazývaný jako Non-Secret Encryption, NSE) objevil už v roce 1970. Dále uvádí, že speciální variantu RSA objevil jeho kolega Clifford Cocks v roce 1973. Tajným službám je však přesto jasné, že jejich náskok před světovou veřejností se zmenšuje.

První symetrický standard - DES

Přes zjevné výhody systému RSA se systém v na přelomu 70. a 80. let ještě moc neprosazuje. Výpočetní složitost je obrovská a tehdejší slabé počítače pracují pomalu. Šifrování dlouhých textů je tak pomalé, že není prakticky použitelné. Je stále potřeba používat symetrickou kryptografii. Asymetrická kryptografie má sloužit v budoucnu jen k distribuci klíčů a k identifikaci a autentizaci. Kryptologové se začínají zabývat hybridními systémy. Pomocí asymetrického šifrového systému se přenese klíč pro symetrický systém, a tím se dále šifruje. Na každou zprávu tak lze použít jiný symetrický klíč. Tato kombinace prakticky řeší a odstraňuje většinu problémů s distribucí klíčů. Zbývá maličkost - silný a bezpečný symetrický algoritmus. Na scéně se objevuje první celosvětově uznávaný symetrický algoritmus DES (Data Encryption Standard).

Vývoj DES navazuje na vývoj šifrovacího algoritmu Lucifer od Thomase Watsona (IBM). Potřeba standardu jeho vývoj urychluje a DES je v roce 1977 v USA formálně přijat za veřejný standard pro ochranu senzitivních informací, nikoliv však pro ochranu informací utajovaných. Způsob ochrany tajných informací v USA není zveřejněn.

DES šifruje text po blocích délky 64 bitů, aktivní délka klíče je 56 bitů, hlavní prvek tvořící potřebnou nelinearitu, která chrání šifrový text před útoky analytiků, jsou tzv. S-boxy. Hned od počátku jsou zde určité nejasnosti okolo návrhu celého systému. NSA (National Security Agency) přesvědčila IBM o "vhodnosti" redukce délky klíče z původních 128 bitů na 56 bitů. NSA také změnila vnitřní strukturu jednoho z S-boxů. Martin Hellmann poukazuje na nebezpečí, které vyplývá z malé délky symetrického klíče. Celkově se však zdá, že algoritmus DES je prvním opravdu bezpečným algoritmem tohoto typu.

O tom, jaký byl náskok pracovníků NSA před odbornou veřejností, svědčí událost, která se váže se k procesu přijímání DES za standard. V roce 1976 uspořádal NBS (Národní úřad pro standardizaci) dvoudenní konferenci k diskusi o DES. Na tuto konferenci byli pozváni všichni zástupci výzkumných organizací, univerzit, firem a další zájemci o kryptologii. Zástupce NSA pak ve svých vzpomínkách popisuje, že již během prvního dne bylo jasné, že toto shromáždění nemá dostatečné znalosti pro posouzení tohoto šifrového algoritmu. Dokonce tvrdí, že měl pocit, jako by byla pozvána skupina alchymistů k posouzení atomové bomby…

International Association for Cryptologic Research

Dalším možným mezníkem na naší pouti světem kryptologie je rok 1980. V tomto roce se koná v Santa Barbaře veliká konference věnovaná kryptologii. Konference má výjimečný ohlas a její další konání v roce 1981 (již pod názvem Crypto) zakládá tradici, která nepřetržitě trvá dodnes. Vytváří se nezávislá akademická skupina odborníků, kteří v roce 1982 zakládají IACR (International Association for Cryptologic Research). Od roku 1982 se také pod záštitou IACR konají pravidelná setkání vědců na evropském kontinentu - Eurocrypty. Tyto pravidelné konference Crypto a Eurocrypt se stávají synonymem pro toto sdružení. Od svého založení vydává tato společnost vlastní a ve své době jediný časopis svého druhu - Journal of Cryptology. Velice brzy získalo toto sdružení vůdčí postavení ve vědeckém a odborném světě kryptologie. V prostředí, kde po dlouhou dobu trvala absence jakýchkoliv odborných informací, sehrálo neocenitelnou roli a své vůdčí postavení si udržuje dodnes.

Kryptologická veřejnost sdružená v IACR podrobuje analýze blokovou šifru DES. Objevují se jisté teoretické útoky, lineární analýza, diferenční analýza. DES odolává. Dokonce jsou vyslovovány hypotézy, že NSA znala tyto metody již v době návrhu S-boxů.

Koncem osmdesátých a začátkem devadesátých let se objevuje celá řada dalších symetrických blokových algoritmů - FEAL, GOST, IDEA, CAST, BLOWFISH atd. Autoři těchto systémů jsou výrazné postavy z komunity IACR. Tato komunita spolu soutěží o vytvoření silného, rychlého a bezpečného symetrického algoritmu. Kompatibilita veřejných systémů se tím sice snižuje, ale DESu se v této komunitě nevěří a hlavně prodej licencí na nové šifrové algoritmy se stává obchodně zajímavý. V ČR se v té době komerčně vyvíjí vlastní šifrovací čip SIC5000 (s algoritmem DVK). Současně se zjišťuje, že některé z těchto systémů, ač na první pohled velice podobné svoji strukturou DES, nejsou tak kvalitní a jsou rozbitelné. Japonský FEAL je totálně rozbit. Je to upozornění - amatéři a poloprofesionálové nemají na poli kryptologie místo. Bez hluboké znalosti souvislostí nelze navrhnout bezpečný šifrový algoritmus.

Co však nedokázali kryptologové svými analytickými útoky, docílil rozvoj síly výpočetní techniky. Vyluštit šifrový text tzv. hrubou silou znamená, že odzkoušíme všechny možné klíče. Právě velikost klíče "pouze" 56 bitů se stala pro DES osudná. V roce 1993 J.Wiener z Bell Northern Research publikoval zprávu, v níž popsal zařízení, které vyzkouší všechny klíče DES do 7 hodin. Cenu takového zařízení odhaduje na jeden milion dolarů. V roce 1995 se na veřejnost dostává informace, že NSA vlastní stroj, který je schopen DES vyluštit do 15 minut. Toto zařízení sestrojila firma The Harris Corporation. Pro ty, kteří stále pochybovali, bylo komerčně sestrojeno a předvedeno speciální zařízení DES-cracker (1998), které je schopno otestovat všech 2^{56} klíčů do 9 dnů a nalézt tak příslušné řešení.

DES musel být nahrazen jiným standardem. Prozatímně jej NIST (National Institute of Standards and Technology) nahrazuje implementací 3DES (TripleDES). V podstatě se jedná o opakované použití algoritmu DES. Zašifrování nyní probíhá takto: zpráva se zašifruje pomocí algoritmu DES a klíče K1, odšifruje se pomocí klíče K2 a opět se zašifruje pomocí klíče K3 (resp. v jiné verzi klíčem K1). Délka klíče se tak vlastně 3x (resp.2x) prodloužila a toto řešení se tímto stalo odolné proti útoku hrubou silou. FIPS-PUB-46-3 ustavuje jako současně platnou normu obě výše popsané verze algoritmu 3DES. Kryptologické veřejnosti je jasné, že řešení není optimální, a proto v roce 1997 NIST vypisuje veřejnou soutěž na vytvoření nového komerčního standardu pro symetrické šifrování.

Advanced Encryption Standard

Pro název tohoto nového algoritmu se vžilo označení AES (Advanced Encryption Standard). Vybraný standard má být velice flexibilní, lehce implementovatelný, má pracovat s 32-bitovým mikroprocesorem, 64-bitovým procesorem, ale i 8-bitovým (v tzv. režimu smart card). AES má být 128-bitová bloková šifra, musí podporovat klíče délky 128, 192 a 256 bitů. Výběr takového algoritmu, který je určen pro všechny typy aplikací a nasazení (klasický software pro PC, terminály pro elektronickou komerci, čipové karty), není opravdu lehký. Autoři tvrdí, že nově vzniklý standard by snad mohl být standardem pro celé 21.století! Algoritmus nesmí být patentován a pro vítěze je připravena odměna - prestižní uznání kryptologické veřejnosti - tzv. "zlatý vavřín kryptologie".

V červnu 1998, kdy byla stanovena uzávěrka pro podání návrhu, bylo celkem předloženo 15 kandidátů (CAST-256, CRYPTON, DEAL, DFC, E2, FROG, HPC, LOKI97, MAGENTA, MARS, RC6, RIJNDAEL, SAFER+, SERPENT, TWOFISH) . Z nich bylo do dalšího kola vybráno v květnu 1999 pět kandidátů :
Rijndael **(**připravil jej vynikající tým belgických kryptologů -Vincent Rijmen, Joan Daemen), Serpent (navržený trojicí známých kryptologů - Ross Andrson, Eli Biham, Lars Knudsen) , RC6 (od RSA Data Security - Burt Kaliski, Ron Rivest), Twofish (návrh firmy Counterpane System v čele s Brucem Schneierem), Mars (vytvořen rozsáhlým týmem odborníků IBM a veřejnosti prezentován Nevenko Zunicem).

Letos 15. května 2000 byla publikována rozsáhlá zpráva o hardwarovém posouzení těchto pěti algoritmů. Koncem tohoto léta pak má být vybrán vítěz, který bude podroben procesu hodnocení NIST, a za rok - v létě roku 2001 - bude vyhlášen nový šifrový symetrický standard. Mezi kryptology se očekává, že tím vybraným algoritmem by mohl být Rijndael nebo Serpent (nebo oba ?).

Poznámka (vloženo 10/2003):
Za algoritmus AES byl vybrán algoritmus Rijndael. Blíže např. článek v našem e-zinu 10/2000 - Král DES je mrtev - ať žije král AES !

Elektronický podpis

Vraťme se k asymetrické kryptografii. Dalším závažným využitím, mimo šifrování, je možnost elektronicky podepisovat dokumenty. Popišme si stručně, jak obecně probíhá proces elektronického podpisu nějakého dokumentu.

K výkladu potřebujeme ještě jeden kryptografický modul kromě asymetrické šifry, o které jsme se již podrobně zmínili. Tím modulem je hash. Hashovací funkce mají za úkol vytvořit takzvaný otisk zprávy. Vstupem hashovací funkce může být libovolná zpráva (libovolně dlouhá), na výstupu obdržíme její otisk, který má pevnou délku (128 nebo 160 bitů). Pokud bychom ve zprávě změnili byť i jediné písmenko, dostaneme na výstupu úplně jiný otisk. Hashovací funkce jsou obecně známé a kdokoli si může z jakékoliv zprávy takový otisk udělat. Navíc platí, že je výpočetně velice obtížné vytvořit k libovolné zprávě jinou zprávu, která má stejný otisk. Obtížnost tohoto úkonu je ekvivalentní obtížnosti rozšifrování zprávy bez znalosti klíče.

Nejznámějšími a nejpoužívanějšími představiteli hashovacích funkcí jsou MD5 (message digest, otisk délky 128 bitů) a SHA-1 (Secure Hash Algorithm, otisk délky 160 bitů).

Podepisující osoba musí mít dále připravenu sadu svých klíčů (soukromý a veřejný klíč) pro některý asymetrický algoritmus . Nejznámějším je RSA, ale mohou se použít i asymetrické algoritmy založené na diskrétním logaritmu nebo eliptických křivkách.

Proces elektronického podpisu pak probíhá takto. Podepisující osoba vypočte hash dokumentu, který chce podepsat, hash dále zašifruje pomocí zvoleného asymetrického algoritmu a pomocí svého soukromého klíče. Získaný výsledek "V" je přiložen k původní zprávě. Takto upravená zpráva je tzv. elektronicky podepsána. Jak postupujeme při ověření? K otevřenému textu vypočteme hash, označme jej "H1". Odšifrujeme "V" pomocí veřejného klíče podepsané osoby a dostaneme jím spočtený hash "H2". Nyní porovnáme "H1" a "H2". Pokud jsou tyto hodnoty shodné, pak nebyl dokument cestou změněn (hashe jsou shodné) a dokument podepsala osoba, které přísluší veřejný klíč (jen ta mohla "H2" zašifrovat pomocí svého soukromého klíče).

V praxi celý systém vyžaduje ještě třetí důvěryhodnou stranu. Tato třetí strana eviduje veřejné klíče a stvrzuje identitu jejich majitelů. Takováto strana se nazývá certifikační autorita. Používání elektronických podpisů však potřebuje zákonnou úpravu. Velice zhruba řečeno, musí být elektronický podpis (a jeho jednotlivé bezpečnostní varianty) přesně definován, je potřeba uznat rovnost elektronického podpisu s podpisem normálním, zajistit neodmítnutí elektronického podpisu z důvodu, že je proveden elektronicky a musí být stanovena pravidla chování certifikačních autorit a podmínky, které musí tyto instituce splňovat, případně musí být stanoven určitý režim a dohled nad službami certifikačních autorit. Koncem roku 1999 přijala evropská komise Směrnici o elektronických podpisech (1999/93/EC) v rámci Evropské unie. Tento dokument je pro členy EU závazný a své zákony musí s tímto dokumentem postupně harmonizovat. Zároveň probíhal proces schvalování zákona o elektronickém podpisu i v České republice. Do tohoto zákona se podařilo včlenit většinu požadavků Směrnice. Po schválení v parlamentu a senátu podepsal 11. 7. 2000 tento důležitý zákon i prezident české republiky. Tento zákon nabývá účinnosti od 1.10.2000. Téměř současně proběhl podobný akt i v USA; prezident Bill Clinton podepsal americký zákon o elektronickém podpisu (Electronic Signatures in Global and National Commerce Act) a to na stejném místě, kde byl před 224 lety podepsán nejdůležitější akt v dějinách USA - Declartion of Independence. Bill Clinton symbolicky zákon podepsal elektronicky pomocí svého soukromého klíče.

V České republice dohled nad certifikačními autoritami a další úkony vyplývající z tohoto zákona byly svěřeny nově vzniklému Úřadu pro ochranu osobních údajů. Dne 10.8.2000 navrhl senát prezidentovi, aby jmenoval Karla Neuwirta předsedou tohoto úřadu. Prováděcí vyhlášky úřadu zajistí vytvoření vhodných podmínek k uskutečnění elektronického styku občan - stát a rozvinutí elektronické komerce v naší republice.

Poznámka (vloženo 10/2003):

Prováděcí vyhláška (366/2001 Sb., O upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu) nabyla účinnosti 3.10.2001.

Od 1.1.2003 převzalo všechny kompetence k zákonu o elektronickém podpisu na základě zákona č. 517/2002 Sb. nově vzniklé Ministerstvo informatiky (http://www.micr.cz/).

C. K oprávnění zaměstnavatele kontrolovat práci zaměstnance pomocí moderních technologií

Ján Matejka
(*Ústav státu a práva AV ČR, Praha,* Právnická fakulta ZČU, Plzeň, jan@matejka.us)

1. Úvod

V poslední době jsme stále častěji svědky zajímavé skutečnosti. Vědecko-technický pokrok stále častěji „předbíhá“ platnou právní úpravu. Kupodivu tomu tak není vždy z důvodu nedbalosti či neznalosti zákonodárce, ale zejména proto, že technika a věda vůbec jsou fenoménem, který sám o sobě musí být vždy dynamičtější. Jednou z oblastí, která je, v důsledku, v minulosti zcela nevídaného, rozvoje odposlouchávacích, kamerových a jiných podobných zařízená, stále častěji veřejností v tomto smyslu přetřásána, je vyjma obecné problematiky ochrany soukromí člověka, také ochrana soukromí zaměstnance při výkonu práce pro zaměstnavatele. Zatímco stávající právní úprava ochrany soukromí nedoznala za posledních padesát let žádných výrazných změn, informační a komunikační technologie, které umožňují toto právo narušit, naopak prošly změnami zcela zásadními, a to včetně jejich (zejména cenové) dostupnosti. V řadě právních oborů je tedy třeba zvážit zda právní předpisy stále více nezaostávají za reálným ekonomickým životem a praktickými potřebami ekonomických subjektů, pracovní právo nevyjímaje. Jedním z problémových okruhů je zde bezpochyby **otázka rozsahu oprávnění zaměstnavatele kontrolovat využívání pracovní doby zaměstnance**, a to včetně prostředků, které zaměstnanec v pracovní době používá. Na tyto a jim podobné otázky se pokusí nalézt odpověď tento článek.

2. Právní úprava ochrany soukromí

Zjevně nejvýznamnějším dokumentem, který poskytuje ochranu soukromí člověka, je Úmluva o ochraně lidských práv a základních svobod (dále jen Úmluva), která ve svém čl.8 mimo jiné stanoví, že „***každý má právo na respektování svého soukromého života, obydlí a korespondence**, přičemž státní orgán nemůže do výkonu tohoto práva zasahovat kromě zákonem stanovených případů, a i to pouze v nezbytném rozsahu a okruhu případů“* (např. zájem národní či veřejné bezpečnosti, apod.). Podle čl. 12 Všeobecné deklarace lidských práv[1] nesmí být nikdo vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má rovněž právo na zákonnou ochranu proti takovým zásahům nebo útokům.

Tuto ochranu rovněž poskytuje i Listina základních práv a svobod (dále jen Listina), a to zejména v čl. 7, 10 a 13. Článek 7 stanoví obecné pravidlo, že „***nedotknutelnost osoby a jejího soukromí je zaručena**, omezena může být jen v případech stanovených zákonem*“. O poznání komplexnější úpravu stanoví čl. 10, který praví, že „*Každý občan má právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno*“. Stejně tak se zde uvádí, že „***každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života a na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě***. Listina v tomto ohledu dále rovněž ve svém čl.13 uvádí, „*že nikdo nesmí porušit listovní tajemství ani tajemství jiných*

[1] Všeobecná deklarace lidských práv Valného shromáždění OSN ze dne 10.12.1948

písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon".

Vzhledem k tomu, že jde o ustanovení poměrně obecná, nemusí být vždy zřejmé, jak velkému okruhu údajů a skutečností, resp. písemností a záznamů, je toto ochrana poskytována. V tomto ohledu lze ale vycházet z dosavadní soudní praxe[2], podle které toto ustanovení chrání **nejenom vlastní obsah veškerých** zpráv a záznamů (lhostejno zda jde o zprávy či záznamy telefonické, elektronické, či jiné), **ale také veškeré související údaje** (např. údaje o volaných číslech, datu a čase hovoru, době jeho trvání, informace o lokalizaci prostředku zajišťujících hovor, apod.), které lze považovat za nedílnou součást tohoto obsahu.

Jak ale vyplývá z výše zmíněných předpisů, **právní řád výslovně dovoluje zákonné výjimky z této ochrany**, a to především z důvodu nezbytného veřejného zájmu (např. tedy zájmu na ochraně společnosti před trestnými činy a na tom, aby takové činy byly náležitě zjištěny) nebo v případě konfliktu s jinými právními instituty (ochrana osobnosti, činnost statistická, evidenční, apod.). Přípustný je však pouze takový zásah, který lze považovat za nezbytný (zákonný), a to ve výše uvedeném smyslu. K tomu, aby nebyly překročeny meze této nezbytnosti, existuje v některých případech systém účinných a fungujících pravidel a záruk, včetně efektivní kontroly jejich dodržování (např. dohled Parlamentu ČR nad prostředky operativní techniky Policie ČR, apod.). V návaznosti na výše zmíněné předpisy, bývá tato problematika stále častěji promítána i do různých, převážně stavovských, předpisů, které zásadně mývají oporů v zákonných normách. Za zmínku stojí např. ***Prohlášení o knihovnách a intelektuální svobodě*** Výkonné rady Mezinárodní federace knihovnických spolků a institucí[3] (IFLA/FAIFE), které bylo přijato dne 25. března 1999 v Haagu Podlé tohoto prohlášení mají uživatelé knihovny právo na soukromí a anonymitu své osoby. Knihovníci a další pracovníci knihovny nesmí sdělit třetí osobě totožnost uživatelů ani informace o jimi užívaných materiálech".[4] U nás lze pak zmínit např. ***Etický kodex Práva pacientů*** Centrální etické komise Ministerstva zdravotnictví ČR, který byl přijat dne 25. února 1992*, a* podle kterého má nemocný právo na to, aby byly v průběhu ambulantního i nemocničního vyšetření, ošetření a léčby, v souvislosti s programem léčby, brány maximální ohledy na jeho soukromí a stud.

3. Ochrana osobnosti a práva na soukromí v pracovněprávních vztazích

3.1 Obecné aspekty

Pracovněprávní předpisy problematiku ochrany osobnosti zaměstnanců v pracovněprávních vztazích neřeší buď vůbec, anebo pouze okrajově, a to dokonce i v těch případech, jejichž výslovnou úpravu lze bezesporu považovat za velmi potřebnou. Zákoník práce se práv na ochranu osobnosti dotýká pouze výjimečně. Jde zejména o ustanovení §7 odst.2, jež poskytuje ochranu před ponižováním lidské důstojnosti účastníka pracovněprávního vztahu, dále pak §22 odst.2, jež upravuje určité aspekty ochrany osobnosti zaměstnance při provádění kontroly odborovými orgány, případně ustanovení §60 odst.2 a 4, jež se týkají písemností osobní povahy při skončení pracovního poměru a pracovních posudků na zaměstnance.Samostatnou kapitolou je zde úprava ve zvláštních souvisejících předpisech (např. v zákoně o ochraně osobních údajů, apod.) jiné otázky ochrany osobnosti zákoník práce neupravuje.

[2] Viz. např. nález Ústavního soudu ze dne 22. ledna 2001 sp. zn. II. ÚS 502/2000
[3] http://ifla.inist.fr/
[4] Plný text tohoto prohlášení lze nalézt na adrese http://www.faife.dk/policy/iflastat/iflastat.htm

V tomto ohledu lze nepochybně zcela souhlasit s názorem[5], že v těch případech, které nejsou ošetřeny právní úpravou zákoníku práce ani speciálních předpisů, je namístě využití ***analogie iuris*** a aplikovat ustanovení občanského zákoníku §11 a násl. o ochraně osobnosti, a to za podmínky, že to vyžaduje integrita obecných zásad právních a pracovněprávních.

Obecná právní úprava ochrany osobnosti je pak zakotvena zejména v již výše citovaném čl.10 Listiny. Na toto ustanovení pak přímo navazuje §11 občanského zákoníku, podle něhož ***má fyzická osoba právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy***. Dle §12 se ***písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením***. Výjimky lze připustit pouze na základě úředních účelů (§12 odst. 2) a zpravodajských (§12 odst. 3) Podle těchto ustanovení náleží právo na ochranu osobnosti **každé fyzické osobě bez rozdílu,** tedy i zaměstnancům**.** V případě fyzických osob toto právo představuje zejména možnost rozhodovat o zpřístupnění soukromých skutečností fyzické osoby jiným subjektům, jakož i právo na ochranu před vnějším neoprávněným zasahováním jiných subjektů do soukromí fyzické osoby[6]. Do této oblasti je rovněž nutno zahrnovat rozsáhlý okruh minulých a přítomných osobních požitků a zážitků fyzické osoby, její soukromou komunikaci, včetně korespondence a jiných osobních kontaktů.[7] Právo na ochranu osobnosti tak zahrnuje rovněž **právo na projevy osobní povahy**, tedy slovní a jiné projevy jakožto jedny z výrazů osobnosti každého člověka. Právo na projevy osobní povahy obsahuje právo na zachycení lidského projevu i právo k záznamům takového projevu jak ve formě písemné či jiné. Pro úspěšné uplatnění práva na ochranu osobnosti se v zásadě nevyžaduje vyvolání následků, ale stačí, že neoprávněný zásah byl objektivně způsobilý narušit nebo ohrozit práva chráněná ustanovením §11 ObčZ[8]. Ustanovení §12 ObčZ pak chrání před neoprávněným pořízením a použitím kromě jiných také písemnosti osobní povahy týkající se fyzické osoby nebo jejích projevů osobní povahy. Uvedené písemnosti osobní povahy mohou být pořízeny a nebo použity pouze se svolením dotčené fyzické osoby. Písemností osobní povahy se rozumí osobní (soukromá) korespondence či jiné zápisky nebo další písemnosti, které ze své povahy a s ohledem na jejich charakter nejsou určeny k veřejné prezentaci. Tyto písemnosti však nemusí mít vždy důvěrný obsah. Osobní povaha takovýchto písemností může mít osobní charakter pro autora či adresáta, resp. může tuto osobní povahu mít i ve vztahu ke třetí osobě, které se daný text týká.[9]

Je však zcela zřejmé, že ochrana osobnosti není a ani nemůže být záležitostí pouze občanskoprávních vztahů, ale že fyzická osoba může být poškozena na svých osobnostních právech i v řadě dalších společenských vztahů, např. tedy i ve vztazích pracovněprávních. Takováto výslovná právní úprava v pracovněprávních předpisech však chybí, a to navzdory skutečnosti, že je tato skutečnost relativně často předmětem kritiky ze strany právní teorie i praxe. Koncepce samotný přístup k ochraně osobnostních práv v pracovněprávních vztazích by však nepochybně musela odrážet řadu specifik těchto vztahů, a tedy nejen ochranu života. a zdraví zaměstnanců, ale také jejich jména, občanské cti, lidské důstojnost a veškeré projevy osobní povahy. Vedle ochrany života a zdraví zaměstnanců a vybraných aspektů lidské důstojnosti, které jsou v zásadě v předpisech pracovního práva již zakotveny, má v pracovněprávních vztazích zásadní význam ochrana projevů osobni povahy, zejména pak písemnosti a jiných záznamů, které bohužel v pracovněprávních předpisech výslovně zakotveny nejsou. [10]

[5] Matyášek, P. in Galvas, M. a kol, Pracovní právo, Masarykova univerzita, Brno 2001, s.73
[6] Jehlička, O., Švestka, J., Škárová, M., a kol., Občanský zákoník, Komentář, 6. vydání, C.H.Beck, Praha, 2001, str. 89
[7] Holub, J., a kol., Občanský zákoník komentář, 1. svazek § 1 – 487, Linde Praha a.s., Praha, 2002, str. 73
[8] Jehlička, O., Švestka, J., Škárová, M., a kol., Občanský zákoník, Komentář, 6. vydání, C.H.Beck, Praha, 2001, str. 109
[9] Mezi tyto písemnosti však nepatří obchodní korespondence, která, ač důvěrného charakteru, nemůže být zařazena pod pojem chráněné ustanovením §12 ObčZ (k tomu však srovnej judikaturu Evropského soudu pro lidská práva – viz dále)
[10] K tomu více Píchová, I., K ochraně osobních údajů v pracovněprávních vztazích, Právo a zaměstnání č.12/2001, s.5-7

3.2 Realizace právo na soukromí a ochrany osobnosti v pracovněprávních vztazích

Jak vyplývá z výše uvedeného, problematika ochrany osobnosti v pracovněprávní vztazích je poměrně problematická a vzhledem k roztříštěnosti a zčásti i absenci (výslovné) právní úpravy, i relativně složitá. Samotné meze práva na soukromí v pracovněprávních vztazích jsou tedy dána řadou zákonných norem (zejména pak občanským zákoníkem a zákonem o ochraně osobních údajů), přičemž hlavní rámec je zde poskytován Listinou, případně Úmluvou. Z pohledu realizace konkrétních práv a povinnosti při kontrole práce je však za klíčový předpis třeba považovat zejména občanský zákoník, jehož aplikace je formou ***analogie iuris*** *nezbytná, a dále pak* obecné pracovněprávní zásady uvedené v zákoníku práce (viz dále). Za velmi významný je třeba rovněž považovat zákon o ochraně osobních údajů, který však bohužel neodstranil existující aplikační problémy (viz výše), a z části rovněž přinesl řadu dalších pochybnost než jistot. V oblasti ochrany osobních údajů však je třeba tento zákon přednostně aplikovat i v rámci pracovněprávních vztahů. Klíčovým pojmem tohoto zákona je pojem osobní údaj, který je zákonem definován v §4 tohoto zákona jako „*jakýkoliv údaj týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze na základě jednoho či více osobních údajů přímo či nepřímo zjistit jeho identitu, přičemž o osobní údaj se nejedná, pokud je třeba ke zjištění identity subjektu údajů nepřiměřené množství času, úsilí či materiálních prostředků*“. Citlivým údajem je pak dle tohoto zákona „*osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, trestné činnosti, zdravotním stavu a sexuálním životě subjektu údajů*“. Správcem je poté „*každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj*“ a zpracovatelem „*každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona*“. Subjektem těchto údajů je „*fyzická osoba, k níž se osobní údaje vztahují“. Zveřejněným osobním údajem je pak „osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu*“.

Mezi základní povinnosti správce (v našem případě zaměstnavatele) o nichž je třeba se v tomto kontextu zmínit, patří zejména povinnost:

- ***shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu,***
- *uchovávat osobní údaje* ***pouze po dobu, která je nezbytná k účelu jejich zpracování****. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely statistické, vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů,*
- ***zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny****, pokud zvláštní zákon nestanoví jinak. Zpracovávat k jinému účelu lze osobní údaj, jen pokud k tomu dal subjekt údajů souhlas.*

Jak ostatně vyplývá z §5 odst.2, správce může zásadně zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Zákon však připouští výjimky (§ 5 odst. 2 písm. a – f)) Provádí-li správce zpracování osobních údajů na základě zvláštního zákona, je povinen dbát práva na ochranu soukromého a osobního života subjektu údajů. Bez souhlasu subjektu údajů lze osobní údaje zpracovávat pro účely statistické nebo vědecké. Pro tyto účely zpracování je nutno osobní údaje anonymizovat, jakmile je to možné. Při zpracování osobních údajů pro tyto účely je však nutno zajistit požadovanou úroveň jejich zabezpečení podle § 13 zákona.

Jedním z dalších předpisů, které rovněž stanoví meze práva na soukromí v pracovněprávních vztazích je nepochybně zákon **č. 106/1999 Sb., o svobodném přístupu**

k informacím, který upravuje podmínky přístupu k informacím některých správních orgánů a stanoví základní podmínky, za nichž jsou informace poskytovány. V souvislosti s touto zákonnou úpravou se v minulosti požadavek na sdělení konkrétní částky (zejména odměny), která byla vyplacena vedoucím pracovníkům v rámci jejich pracovního poměru. Jak ale vyplývá z §2 odst. 3, nevztahuje se tento zákon na poskytování osobních údajů a informací podle zvláštního právního předpisu, přičemž je v poznámce pod čarou uveden právě zákon o ochraně osobních údajů. V tomto ohledu je třeba vždy zkoumat na které z požadovaných údajů týkajících se pracovněprávního vztahu se vztahují omezení uložená zákonem o ochraně osobních údajů, a tím i vymezit vztah tohoto zákona k zákonu o svobodném přístupu k informacím. V § 10 zákona o ochraně osobních údajů je uvedeno, že při zpracování osobních údajů dbá správce nebo zpracovatel (v tomto konkrétním případě zaměstnavatel), na ochranu před neoprávněným zasahováním do soukromého a rodinného života subjektu údajů (v tomto případě zaměstnance). Znamená to, že zaměstnavatel má pro plnění svých úkolů právo, a pokud jde o sdělení informací podle zvláštního zákona (např. č. 106/1999 Sb.), používat a případně i jiným osobám **sdělovat ty osobní údaje zaměstnance, které se týkají výlučně jeho pracovních aktivit a zjevně nevypovídají o jeho soukromém životě**, za podmínky, že zaměstnavatel dodrží všechny povinnosti, uložené mu tímto zvláštním zákonem (např. zákoník práce). **Zaměstnavatel tak může, pokud je to potřebné k plnění jeho úkolů a zvláštní zákon nestanoví jinak, bez souhlasu zaměstnance sdělit jeho jméno a příjmení, akademický titul, funkční zařazení, kontaktní údaje zaměstnance na jeho pracoviště (číslo telefonu, faxu, adresu elektronické pošty).** Jinak je tomu však, pokud jde o přesnou **výši platu, mzdy případně odměny**. Finanční částka, kterou zaměstnanec při výplatě obdrží, je osobním údajem, jehož zveřejnění je třeba plně **podřídit režimu zákona o ochraně osobních údajů**. Vzhledem k tomu, že se na zveřejnění tohoto údaje nevztahuje žádná z výjimek podle § 5 odst. 2 písm. a – f) zákona o ochraně osobních údajů, může zaměstnavatel zveřejnit výši platu, mzdy nebo odměny pouze se souhlasem zaměstnance. Může však bez souhlasu jednotlivých zaměstnanců zveřejnit např. informaci o celkové výši odměn vyplacených v organizaci nebo jejím úseku. Pokud z této informace není určitelné, jaké konkrétní částky byly vyplaceny jednotlivým pracovníkům, není tento údaj údajem osobním a zákon o ochraně osobních údajů se tak na něj samozřejmě nevztahuje. Zaměstnavatel jako správce osobních údajů zaměstnance je tedy povinen **chránit údaje týkající se jeho soukromí**, nemůže však nesprávným výkladem zákona o ochraně osobních údajů zakrývat svoji neochotu poskytnout údaje, na které má veřejnost právo.[11]

3.3 Právo na soukromí na pracovišti ve světle judikátů Evropského soudu pro lidská práva

Jedním z nejvýznamnějších souvisejících rozhodnutí je **rozsudek Evropského soudu pro lidská práva ve věci Niemietz versus Německo**[12], kde se soud zabýval výkladem výše uvedeného čl.8 Úmluvy. V této věci bylo jednou ze stran, německým advokátem Niemitzem, namítáno že prohlídkou jeho advokátní kanceláře došlo k porušení článku 8 Úmluvy, a to zejména tím, že prohlídkou jeho advokátní kanceláře (pracoviště) došlo k zásahu do jeho „soukromého života" a „obydlí". Druhá strana ve věci však namítala, že článek 8 neposkytuje ochranu proti prohlídce pracoviště, ale naopak jasně rozlišuje mezi soukromým životem a obydlím na jedné straně a profesním a obchodním životem a místnostmi na straně druhé.

[11] Viz stanovisko Úřadu pro ochranu osobních údajů č. 6/2002, uveřejněné ve věstníku úřadu č. 18/2002 (K problémům z praxe - Poskytování osobních údajů o zaměstnancích)
[12] Rozsudek Evropského soudu pro lidská práva ze dne 16. prosince 1992 ve věci Věc Niemietz (Rozsudek ve věci Niemietz versus Německo)

Evropský soud pro lidská práva v této věci dovodil, že respektování soukromého života musí do určité míry zahrnovat právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi. Dále se pak soud rovněž uvedl, že **neexistuje důvod pro to, aby způsob chápání pojmu „soukromý život" vylučoval aktivitu profesní nebo obchodní povahy, protože právě během své pracovní činnosti má většina lidé značnou, ne-li největší příležitost rozvíjet vztahy s vnějším světem**. Soud dále rovněž uvedl, že tento názor lze podepřít také skutečností, že není vždy možné jasně rozlišit, které činnosti jednotlivce tvoří část jeho profesního nebo obchodního života a které nikoli. Takže zejména v případě osoby provozující svobodné povolání může být její práce v tomto kontextu tak významnou součástí jejího života, že se stává nemožným zjistit, v jakém postavení jedná v určitém okamžiku. Odepírat ochranu poskytovanou článkem 8 s odůvodněním, že napadené opatření se týkalo pouze profesní činnosti by navíc mohlo vést k nerovnému zacházení, a to v tom smyslu, že takováto ochrana by byla dosažitelná pro jednotlivce, jehož profesionální a neprofesionální činnosti jsou vzájemně natolik provázány, že neexistuje cesta, jak je vzájemně rozlišit. Celkově vzato, výše uvedené důvody přivedly soud k závěru, že **prohlídka stěžovatelovy kanceláře byla zásahem do jeho práv podle článku 8 Úmluvy**.

Takovéto klíčové rozlišení Evropský soud dosud neučinil a lze jej tedy nepochybně považovat za precedentní. V minulosti však již tento soud konstatoval[13], že k zásahu do soukromého života může dojít i tam, kde se telefonický odposlech na pracovišti týkal jak obchodních, tak i soukromých hovorů. Dále v minulosti[14] rovněž uvedl, že ani tam, kde prohlídka směřovala pouze proti obchodní aktivitě, se nelze spoléhat na vyloučení aplikace článku 8 Úmluvy.

Jedním z dalších souvisejících rozhodnutí Evropského soudu pro lidská práva je **rozhodnutí Halford v. Spojené království**[15].V této věci bylo jednou ze stran, žadatelkou Halford (asistentka policejního ředitele), namítáno, že hovory vedené z jejího domova i z její kanceláře byly odposlouchávány, a to za účelem získání a použití informací proti ní v probíhajícím pracovněprávním sporu se zaměstnavatelem. Paní Halford byla poskytnuta vlastní kancelář a dvě telefonní linky, z nichž jedna byla určena pro soukromé užívání. Tyto linky byly součástí interní telefonní sítě policie v Marseyside., telekomunikačního systému mimo veřejnou síť. Soud v této věci jasně konstatoval, že **telefonní hovory vedené z pracoviště stejně jako ty vedené z domova mohou spadat pod pojmy „soukromý život" a „korespondence" ve smyslu článku 8 Úmluvy.** V tomto ohledu Soud rovněž konstatoval, že **neexistuje žádný důkaz o tom, že by paní Halford byla jako uživatel interního telekomunikačního systému užívaného na Policejním ústředí v Merseyside upozorněna, že hovory vedené v tomto systému podléhají odposlouchávání. Soud shledal, že paní Halford oprávněně a důvodně očekávala při takových hovorech soukromí**[16]**.**

[13] Rozsudek Evropského soudu pro lidská práva ve věci Huvig versus Francie ze dne 24. dubna 1990, Série A č. 176 - B, str. 41, § 8 a str. 52, § 25

[14] Rozsudek Evropského soudu pro lidská práva ve věci Chappell versus Spojené království ze dne 30. března 1989, Série A č. 152 - A, str. 12 až 13, § 26 a str. 21 až 22, § 51).

[15] Rozsudek Evropského soudu pro lidská práva ze dne 25. června 1997 ve věci Halfordová (Rozsudek ve věci Halfordová versus Spojené království), Reports of Judgments and Decisions 1997 - III, str. 1016, § 44

[16] Soud se zde o přel o svá předchozí rozhodnutí ve věci Klass a další, tamtéž, Malone v. Spojené království ze dne 2. srpna 1985, Série A č. 82, s. 30, § 64, výše uvedený rozsudek případu Huvig, tamtéž, a mutatis mutandis výše uvedený rozsudek případu Niemietz, s. 33 - 35, §§ 29 - 33

4. Výkon kontroly práce zaměstnavatelem

4.1 Malá poznámka k rozsah oprávnění zaměstnance využívat prostředky zaměstnavatele k jiným (než pracovním) účelům

K posouzení konkrétních otázek oprávněnosti kontroly zaměstnavatele je zapotřebí nejprve zmínit rozsah oprávnění zaměstnance využívat prostředky zaměstnavatele k soukromým účelům.V tomto ohledu asi nemá význam připomínat, že každý zaměstnanec má vůči svému zaměstnavateli určité povinnosti. Obecně bývají stanoveny v zákoníku práce, konkrétněji pak ve vnitřních předpisech zaměstnavatele (např. v pracovním řádu) nebo v pracovní smlouvě. Zákoník práce ve svých ustanoveních neobsahuje výslovný zákaz zaměstnancům využívat prostředky zaměstnavatele k jiným (než pracovním) účelům. Z povahy věci a z řady dalších ustanovení (např. § 73 odst. 1 písm. d) však vyplývá, že **pokud zaměstnavatel neprojeví svůj souhlas k využívání těchto prostředků, není zaměstnanec k jejich využívání výše uvedeným způsobem oprávněn.** Samotné neoprávněné využívání prostředků zaměstnavatele (např. ve formě napsání a odeslání několika soukromých emailů) pak může představovat **méně závažné porušování pracovní kázně** (což může vést i k výpovědi, jestliže byl tento zaměstnanec v době posledních šesti měsíců v souvislosti s porušením pracovní kázně již písemně upozorněn na možnost výpovědi).

Souhlas zaměstnavatele pak může být projeven nejen prostřednictvím vnitřního předpisu nebo pracovní smlouvy, ale také ústně, případně konkludentně (což může vystavovat zaměstnance zbytečnému riziku důkazní nouze).

K této otázce je však třeba ještě dodat, že pokud byl zaměstnanci udělen souhlas s využíváním prostředků zaměstnavatele k jiným než pracovním účelům a zaměstnanec těchto prostředků také takto užívá, půjde bezesporu o zvláštní nepeněžité plnění v podobě daru nebo výhod poskytované zaměstnavatelem se všemi daňovými důsledky.

4.2 K obecnému oprávnění zaměstnavatele kontrolovat zaměstnance

Jak vyplývá z výše uvedeného, oprávnění zaměstnance využívat prostředky zaměstnavatele k jiným (než pracovním) účelům je plně závislé na rozhodnutí zaměstnavatele. V tomto ohledu lze říci, že jde o nepřímý projev. dispozičních práv zaměstnavatele, kde dochází k projevu tzv. nerovného postavení subjektů po vzniku pracovního poměru (jde o jakýsi výraz veřejnoprávní metody regulace, která je typická pro pracovní právo). Za účelem efektivní vymahatelnosti těchto práv zaměstnavatele, resp. povinností zaměstnance, stanoví zákoník páce další právo zaměstnavatele a to **kontrolovat práci zaměstnanců** a dávat jim k tomu účelu závazné pokyny (§ 9 odst. 3 ZP). Zákon však toto právo blíže nekonkretizuje a je tedy třeba vycházet z dalších souvisejících právních institutů (zejména pak práva na soukromí – viz výše).

Jedním z nejdůležitějších ustanovení zákoníku práce stanovící povinnost kontrolovat zaměstnance je §170 odst. 2, který uvádí, že „*zaměstnavatel je povinen soustavně kontrolovat, zda zaměstnanci plní své pracovní úkoly tak, aby nedocházelo ke škodám*“.

Je však zřejmé, že jak zaměstnavatel, tak i jiné orgány kontroly jsou při výkonu této kontroly omezení řadou zákonných ustanovení. Jde zejména o výše uvedenou ochranu soukromí, ochranu osobních údajů, listovní tajemství, apod.

4.3 K oprávnění zaměstnavatele kontrolovat příchozí zásilky (elektronickou poštu) v místo výkonu práce zaměstnance

Jedním z novodobých témat současnosti je posuzování otázky oprávnění zaměstnavatelé monitorovat na pracoviště zaměstnance příchozí korespondenci, zejména pak v podobě elektronické pošty. Uvedenou problematiku upravuje poměrně podrobně **zákon č. 29/2000 Sb., o poštovních službách**. K provedení některých ustanovení tohoto zákona (§6 odst. 6 a §22 odst. 4) pak byla přijata vyhláška Ministerstva dopravy a spojů č. 28/2001 Sb. Aniž bych se chtěl zabývat detailním rozborem těchto předpisů, podotýkám, že s ohledem na spory související s poštou elektronickou, obsahují tyto předpisy poměrně komplexní a rozporů relativně prostou právní úpravu, kde lze nalézt odpověď na většinu otázek souvisejících provozování poštovních služeb, jakož i práv a povinnosti, které při poskytování a provozování poštovních služeb vznikají.

Jednou z poměrně diskutovaných otázek je, alespoň v případě pošty elektronické, problematika určení skutečného adresáta, resp. určení, zda jde o korespondenci soukromou či firemní. Stávající platná právní úprava (resp. výše zmíněná vyhláška) zde vychází z předpokladu, že „*je-li v adrese uvedena na prvém místě právnická osoba a na druhém místě fyzická osoba, za adresáta se považuje právnická osoba. Je-li v adrese uvedeno na prvém místě jméno a příjmení fyzické osoby a na druhém místě označení právnické osoby, za adresáta se považuje fyzická osoba s tím, že poštovní zásilka nebo poštovní poukaz má být dodán prostřednictvím této právnické osoby. Je-li v adrese namísto jména a příjmení určité fyzické osoby uvedena pouze její funkce v právnické osobě, za adresáta se považuje právnická osoba. Je-li v adrese uvedeno několik fyzických osob svými jmény a příjmeními nebo společným označením (např. „manželé"), za adresáta může držitel poštovní licence považovat kohokoliv z nich*. Patrně netřeba dodávat, že v těchto případech je pak jasné, kdy jde o korespondenci osobní (kterou zaměstnavatel není oprávněn číst, ale pouze ji dále postoupí) a kdy jde o korespondenci firemní, tedy korespondenci určenou výhradně zaměstnavateli. Podobných (zpřesňujících) pravidel je zde však obsaženo podstatně více. Jinou otázkou je, zda bývají v praxi skutečně dodržována.

V tomto ohledu se však naskýtá otázka, zda vůbec a do jaké míry lze na elektronickou poštu (případně i na SMS zprávy) aplikovat **zákon o poštovních službách.** Vzhledem k poměrně volnému vymezení pojmu (např. §4 a násl.) lze dle mého soudu oprávněně tvrdit, že se na elektronickou poštu tento zákon vztahuje. Jak ale vyplývá z některých dalších ustanovení, nebude tomu tak vždy. Jak ostatně vyplývá z § 3 tohoto zákona, **písemné zprávy, které jsou dodávány bezúplatně jsou z jinak výlučné působnosti tohoto zákona vyloučeny.** Služby spočívající v bezúplatném dodávání těchto písemných zpráv tak lze tedy uskutečňovat i jinak než ve zvláštním režimu tohoto zákona.

Zákon však nikterak výslovně neuvádí, zda lze za písemnou zprávu považovat rovněž zprávu zasílanou elektronicky (datovou zprávu). Jak ale vyplývá z ustanovení § 3 odst. 2 tohoto zákona, „*...za dodání písemné zprávy se nepovažuje služba spočívající v přepravě sdělení v jiné než písemné podobě*". Vzhledem ke skutečnosti, že zpráva zasílaná elektronicky (datová zpráva) je bezpochyby přepravována ve formě elektronické a nikoli písemné (koneckonců jde pouze o řetězce nul a jedniček) lze konstatovat, že se toto ustanovení týká zejména telekomunikačních služeb, při nichž je sdělení transferováno (dodáváno) ve formě elektrických, resp. elektronických impulsů. Aplikace tohoto ustanovení tak připadá v úvahu nejenom v případě zpráv zasílaných elektronicky, ale též u telegramů, u nichž je sdělení přemísťováno telefonem, dálnopisem nebo faxem. Skutečnost, že v tomto případě sdělení

v určitou chvíli (bezprostředně před a po transferu) skutečně v písemné formě nemusí být v tomto případě právně významná. V tomto ohledu lze tedy vyslovit domněnku, že zákon o poštovních službách sice na jedné straně považuje zprávu zasílanou elektronickou poštou za zprávu písemnou, avšak přepravu takové elektronické zprávy za její dodání již nepovažuje. Z těchto důvodů lze učinit závěr, že přepravu elektronické poštu nelze považovat za její dodání, resp. dodávání ve smyslu zákona o poštovních službách. Ačkoliv tedy nelze tuto právní úpravu v plné rozsahu na elektronickou poštu aplikovat, jde bezesporu o významnou úpravu, kterou je třeba (alespoň dle mého soudu) na elektronickou poštu v některých případech přesto vztáhnout.

Dle nedávného stanoviska Úřadu pro ochranu osobních údajů[17], je však třeba mít na zřeteli, že i elektronická pošta je poštou a písemnosti v elektronické podobě a platí zde tedy i obdobná pravidla jako pro ostatní písemnosti. Dle tohoto stanoviska je při posuzování otázky monitorování elektronické pošty, nutno vzít v úvahu především výše zmíněný článek 13 Listiny a §12 ObčZ., které v tomto ohledu stanoví, že písemnosti osobní povahy smějí být pořízeny nebo použity jen se svolením fyzické osoby, jíž se týkají. Svolení není třeba tehdy, použijí-li se písemnosti osobní povahy k účelům úředním na základě zákona. Tzv. špionážní software, webové štěnice, skryté identifikátory a jiné podobné nástroje mohou pronikat do koncového zařízení uživatele bez jeho vědomí s cílem získat přístup k informacím, uchovávat skryté informace nebo sledovat činnost uživatele a mohou vážně narušit soukromí těchto uživatelů. Použití takových nástrojů by mělo být povoleno pouze k oprávněným účelům s vědomím uživatelů, kterých se dotýká. V tomto ohledu je však třeba rovněž vnímat i to, že zaměstnavatel má právo mimo jiné sledovat u svých zaměstnanců dodržování pracovní doby a jejího využití. Výkladem Úřad dále dovozuje, že zaměstnavatel by případně mohl pouze sledovat počet e-mailů došlých a odeslaných u svých zaměstnanců a požadovat, aby své soukromé záležitosti v pracovní době a na pracovišti vyřizovali v přiměřené a více méně v nezbytné míře, neboť, jak bylo výše uvedeno, ani pracovněprávní vztah neodstraňuje právo na přiměřené soukromí zaměstnanců. O svém záměru či praxi sledovat četnost přijímaných či odesílaných e-mailových zpráv by měl zaměstnavatel předem své zaměstnance uvědomit, a to nejlépe při navazování pracovního vztahu. K uvedenému účelu by měla existovat obecná pravidla pro zaměstnavatele a zaměstnance, z nichž by mělo být jasné, že obsah pošty je chráněn a že ve vztahu k němu se ctí listovní tajemství i ochrana osobních údajů. Úřad ve svém stanovisku dále doporučil následující zásady:

- *Zaměstnanec má právo na soukromí na pracovišti. Na tomto právu nic nemění skutečnost, že zaměstnanec používá komunikační či jiná zařízení zaměstnavatele. Lokalita a vlastnictví elektronického zařízení nemůže vyloučit právo na důvěrnost komunikací a korespondence stanovené v Ústavě a v dalších právních předpisech.*
- *Všeobecná zásada důvěrnosti korespondence zahrnuje komunikaci na pracovišti. Tato komunikace zahrnuje elektronickou poštu (e-mail) a k ní připojené soubory.*
- *Respektování soukromí také zahrnuje určitou míru práva vytvářet a rozvíjet vztahy mezi jedinci. Toto právo je, mimo jiné, nutno vzít v úvahu při posouzení oprávnění zaměstnavatele použít metody sledování zaměstnanců.*[18]

Z pohledu ochrany osobních údajů je však nutno mít na zřeteli ještě další otázku, a sice, zda vždy při monitorování e-mailové pošty dochází ke zpracování osobních údajů. K tomu by docházelo tehdy, když by zaměstnavatel svou činností systematicky monitoroval své zaměstnance a údaje získané z této činnosti by dále zpracovával. V takovém případě by na

[17] Viz stanovisko Úřadu pro ochranu osobních údajů, K problémům z praxe - č. 1/2003, Monitorování elektronické pošty a ochrana soukromí a osobních údajů zaměstnanců
[18] tamtéž

tuto činnost zaměstnavatele dopadal v plném rozsahu zákon o ochraně osobních údajů. Pokud však by zaměstnavatel e-mailovou poštu nesledoval systematicky, ale jen nahodile by ji prohlédl (např. proto, že jeho zaměstnanec je dlouhodoběji nepřítomen na pracovišti např. z důvodu nemoci), a to proto, že je třeba vyřídit pracovní korespondenci, pak by se zřejmě nejednalo o zpracování osobních údajů, a zákon o ochraně osobních údajů by tedy na tento postup nedopadal. Zaměstnavatel má tedy nepochybně právo pro naplňování své činnosti stanovit jednomu každému zaměstnanci formu a způsob komunikace s jinými subjekty, zejména když jsou zaměstnanci vzhledem ke své pracovní náplni pověřeni vykonávat činnosti zaměstnavatele, při nichž je třeba komunikovat i elektronickou formou.

Obecně lze dovodit, že předmětem ochrany čl.13 je především ochrana listovního tajemství zásadně neveřejné informace, která je určena konkrétnímu (a nikoli jinému) adresátovi. S ohledem na dikci tohoto ustanovení lze rovněž tvrdit, že je lhostejné na jakém médiu či nosiči záznamu je tato informace zaznamenána. Samotná trestněprávní ochrana je upravena zejména v § 239 trestního zákona, který vymezuje skutkovou podstatu trestného činu **porušování tajemství dopravovaných zpráv.** Podle tohoto ustanovení, bude potrestán **odnětím svobody až na šest měsíců** ten, *kdo úmyslně poruší tajemství*

- *uzavřeného listu nebo jiné písemnosti, při poskytování poštovní služby nebo jiným dopravním zařízením, nebo*
- *zprávy podávané telefonem, telegrafem nebo jiným takovým veřejným zařízením.*

Podle ustanovení § 240 trestního zákona pak bude potrestán odnětím svobody až na jeden rok ten*, kdo v úmyslu způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch*

- *prozradí tajemství, o němž se dozvěděl z písemnosti, telegramu nebo telefonního hovoru, které nebyly určeny jemu, nebo*
- *takového tajemství využije*

Zákon tak tedy rozlišuje samotné porušování listovního tajemství bez dalšího (§ 239) od případů, kdy toto porušování je zároveň prostředkem k dalšímu (ryze zištnému) cíli nebo ke způsobení škody (§ 240). Uvedenou trestněprávní úpravu lze bezesporu považovat za poměrně vyhovující. Jistou výhradu však lze vyslovit ke skutečnosti, že je zde chráněn pouze samotný obsah písemností a zpráv, a to bez ohledu na jejich hodnotu pro adresáta, odesílatele či pachatele.[19] V každém případě se zde vyžaduje úmysl pachatele, a tak zcela jistě nedojde k naplnění skutkovou podstaty např. v důsledku náhodného otevření soukromého email určenému zaměstnanci.

Právní úprava listovního tajemství zcela jistě spadá v plném rozsahu pod ochranu soukromí (viz výše) Za soukromí lze v tomto ohledu považovat sféra života člověka, do které v zásadě (až na zákonné výjimky) nelze bez jeho souhlasu zasahovat. Meze soukromí pak vymezuje to, co člověk podle zákona není povinen zpřístupnit nebo vyjevit někomu jinému. Opakem sféry soukromé je poté sféra věcí veřejných. Samotní soukromí tedy není jako takové nezadatelné resp. nezcizitelné, nýbrž se ho jeho subjekt může v určitém rozsahu ad hoc zříci.[20] V tomto ohledu je zřejmé, že samotný výkon práce není a ani nemůže spadat pod sféru soukromou. V některých specifických případech však mohou tyto sféry splývat (domáčtí zaměstnanci, teleworking, apod.). Takovým případem bude a stav, kdy zaměstnavatel umožní

[19] V některých dalších případech (§ 239 odst 2 a § 240 odst 2) pak může být pachatelem tohoto trestného činu **pouze pracovník poštovní nebo telekomunikační služby.**

[20] Viz též: Pavlíček V. a kol.: Ústava a ústavní řád České republiky, komentář, 2. díl, práva a svobody, 2. vydání, Linde, Praha 1999, str. 112 a113.

zaměstnanci užívat prostředky zaměstnavatele k soukromým účelům. V tomto ohledu lze pak zcela jistě tvrdit, že se na tuto soukromou korespondenci zaměstnance vztahuje ochrana listovního tajemství. Dle mého soudu však lze v takovém případě monitorovat řadu souvisejících (doprovodných) údajů, jako např. četnost a dobu strávenou zaměstnancem psaním soukromé korespondence a na základě takto zjištěných údajů pak žádat po zaměstnanci vysvětlení. V obecné rovině lze dále tvrdit, že zaměstnavatel má právo sledovat k jakým účelům a jakým způsobem a v jakém rozsahu je používáno jeho zařízení (telefonní linka, počítač, modem, apod.). Zaměstnavatel však oprávněn číst obsah těchto soukromých zásilek.

Režim ochrany soukromí zaměstnance však bude nepochybně jiný v případě, že zaměstnanec nebude oprávněn využívat související prostředky zaměstnavatele k soukromým účelům. I v takovém případě však nelze vyloučit, že pomocí prostředků zaměstnavatele (např. počítače) bude zaměstnanci doručena (nebo zaměstnancem neoprávněně odeslána) soukromá korespondence (obvykle email). Z výše uvedeného vyplývá, že zaměstnavatel nesmí zasahovat do soukromí zaměstnance. Pokud zaměstnavatel narazí na takovouto soukromou korespondenci, měl by od okamžiku zjištění této skutečnosti upustit od další manipulace s ní. Uvedené je praktické zejména z toho důvodu, že zaměstnavatel potřebuje přístup ke své poště (např. z důvodu nemoci zaměstnance) a v takovém případě skutečně může narazit na soukromou korespondenci. V tomto ohledu však je třeba vycházet z určitého prvku veřejnosti, a to zejména v těch případech, kdy dochází k užívání jedné emailové adresy (např. obchod@firma.cz) více zaměstnanci.

Elektronickou poštu, resp. právo ji užívat, lze nepochybně považovat za jakýsi výrobní prostředek svého druhu, který poskytuje zaměstnavatel zaměstnanci k výkonu práce. V tomto ohledu je navíc třeba říci, že ze samotné povahy (komerčního způsobu používání) elektronické pošty vyplývá, že jde navíc o nástroj komunikace mezi firmou a zákazníky (podobně jako např. telefonní číslo), a bylo by vskutku absurdní, aby zaměstnavatel, neměl přístup k informacím (např. v důsledku nemoci či dovelené zaměstnance), které pro něj mohou mít zásadní význam. V tomto ohledu je třeba navíc vycházet i ze toho, že elektronická pošta je ve většině případů zaměstnavatelem zřizována právě za komerčním (případně marketingovým) a nikoli soukromým účelem.

Jinými slovy, pokud není např. ve vnitřních předpisech stanoveno jinak, zaměstnavatel má právo číst a dále nakládat s elektronickou poštou zaměstnanců jen v těch případech, kdy lze důvodně předpokládat, že obsah zprávy je firemní. Uvedené však neznamená, že zaměstnavatel není povinen chránit další oprávněné zájmy zaměstnanců, zejména pak právo na **ochranu listovního tajemství, které musí být zajištěno u všech písemností** (§ 8 odst. 5 zákona o poštovních službách). Pro účely rozpoznání soukromé korespondence a firemní korespondence je v takových případech třeba analogicky postupovat podle pravidel pro poštovní zásilky ve smyslu výše uvedené vyhlášky Ministerstva dopravy a spojů.

Ani v těchto případech se však nelze vyhnout možnosti, že zaměstnavatel narazí na soukromou korespondenci zaměstnance. Otázku možné protiprávnosti takového jednání je pak třeba posuzovat vždy individuálně (v každém případě velmi podobně existujícím zvyklostem u papírové korespondence – viz výše).

4.4 K oprávnění zaměstnavatele kontrolovat výkonu práce prostřednictvím kamerových systémů

Platná právní úprava v tomto ohledu výslovně upravuje pouze odposlech a záznam telekomunikačního provozu, a to pouze pro potřeby orgánů státu. Jinak zde není žádná obecná právní úprava dovolující zasáhnout do soukromí zaměstnanců, a tudíž žádné omezení toho, a by bylo nejen obrazově, ale i zvukově sledováno a zaznamenáváno soukromí osob (zaměstnanců). Problém nastává podle okolností, až při dalším užití konkrétního záznamu, zejména pak zveřejnění. V každém případě je však zaměstnavatel povinen respektovat výše zmíněna ustanovení Listiny, Úmluvy a souvisejících zákonných norem, zejména pak občanského zákoníku. Z hlediska odpovědnosti toho, kdo sledování provádí, je třeba tedy učinit tyto dva rozhodující závěry:

- Zařízení, které sleduje situaci kamerovým systémem, by se vystavilo nebezpečí nějakých sankcí v případě, že by tento systém, resp. jeho výstupy, byl použit nějakým způsobem porušujícím článek 10 Listiny (lidská důstojnost, osobní čest, dobrá pověst. jméno, ochrana před neoprávněným zasahováním do soukromého a rodinného života, ochrana před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o osobě) nebo ustanovení § 11 a násl. občanského zákoníku. To je v zásadě představitelné jen tehdy, byl-li by pořízen a zneužit záznam, anebo byl-li by nějakým způsobem zřízen přístup neoprávněným osobám způsobem narušujícím tato ustanovení.

- Kdyby v zařízení došlo k události, které osoby odpovědné za chod zařízení jinak měly a mohly zabránit, odpovědnosti za tuto událost by se zařízení nebo jednotlivci nezprostili poukazem na to, že z důvodů občanských nebo jiných práv nemohly provozovat kamerový systém který by jinak byl účelný. Žádný právní předpis provozování takového systému nebrání, případná občanskoprávní nebo trestněprávní odpovědnost by se tedy posuzovala podle obecně platných hledisek, tzn. zejména zda bylo učiněno vše, co je možné a přiměřené tomu, aby k události nedošlo.

Z těchto důvodů by mělo být vždy velmi odpovědně zváženo, zda kamerový systém na pracoviště instalovat a jakém rozsahu a zda vůbec by měl pořizovat záznam.

5. Závěr

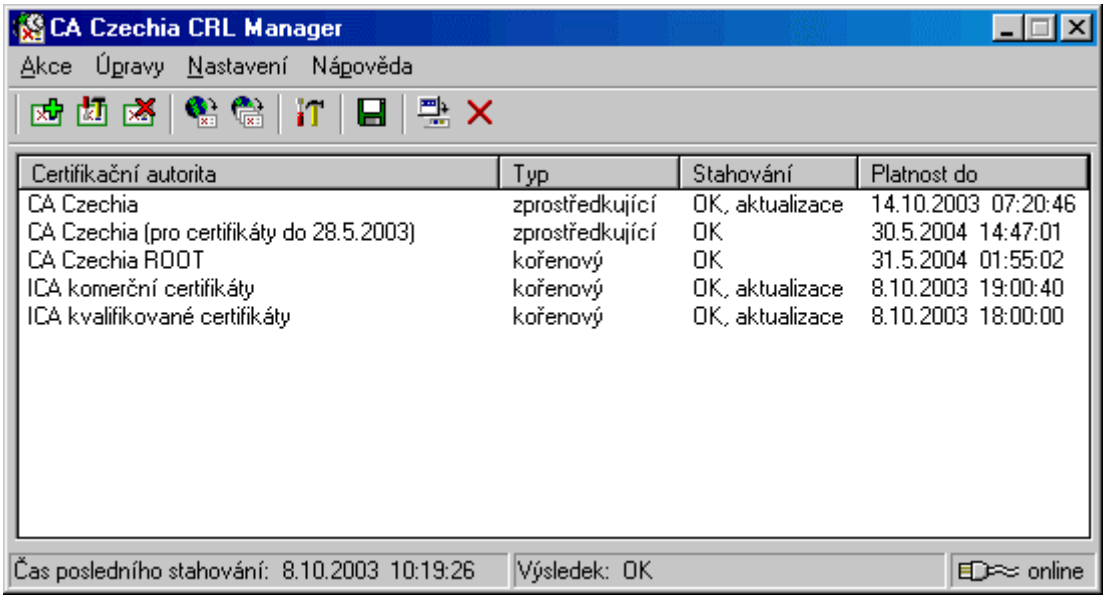
Jak vyplývá z výše uvedeného, právo na soukromí, ochranu osobnosti, listovní tajemství lze za určitých podmínek úspěšně realizovat i v rámci pracovněprávních vztahů. V tomto ohledu je třeba říci, že zaměstnavatel řadu poměrně efektivních prostředků k výkonu práva i povinnosti kontrolovat výkon práce svých zaměstnanců (ať již jde o výběr zaměstnanců, fyzická kontrola, apod.). V každém případě se zdá být vhodné doporučit konkrétní podrobnější vymezení vztahů výše zmíněné sféry soukromého života v místě výkonu práce ve vnitřních předpisech zaměstnavatele a předejít tak zbytečným sporům.. Osobně se domnívám, že i monitoring elektronické komunikace, který je opřen o platné vnitřní předpisy zaměstnavatele, se kterým zaměstnanec souhlasí a který splňuje některé další zákonné náležitosti (např. byl projednán s odborovou organizací (§18b odst. 2 písm g), lze považovat za oprávněný. To vše za předpokladů a podmínek uvedených výše.

D. Jednoduchá a automatická aktualizace CRL

Ing. Dušan Doležal, CA Czechia, dusan.dolezal@caczechia.cz

CRL Manager je malá aplikace, která v pravidelných intervalech stahuje a automaticky instaluje seznam zneplatněných certifikátů (CRL). Před samotných popisem programu uvedu nejprve důvody, které nás k jeho vývoji vedly.

Když jsme začali vyvíjet certifikační autoritu, narazili jsme při testování na poměrně závažný problém s instalací CRL. Operační systém Windows pracuje s CRL podobným způsobem jako s certifikáty, CRL se tedy nainstaluje do systémového úložiště certifikátu a je tak k dispozici pro všechny aplikace, které s ním potřebují pracovat. Pro instalaci je nutné kliknout pravým tlačítkem myši na soubor s CRL a v lokálním menu vybrat položku „Nainstalovat CRL“. Když pomineme fakt, že tento způsob je celkem nelogický (dalo by se očekávat, že po zobrazeni CRL bude v dialogu tlačítko „Nainstalovat“ podobně jako při zobrazení certifikátu), a hlavně nepohodlný (protože soubor je nutné nejprve uložit na disk a teprve poté může být nainstalován), narazíme záhy na mnohem závažnější problém. Instalace se totiž podaří pouze poprvé, kdy CRL v úložišti ještě není uloženo, při další instalaci stejného CRL (byť aktualizovaného) se instalace nezdaří a v úložišti zůstane původní CRL! Situace je o to horší, že systém zobrazí informaci o úspěšném dokončení instalace, takže uživatel vůbec netuší, že ve skutečnosti se instalace nezdařila, a používá tak vlastně neaktuální CRL!



Řešení uvedeného problému standardními prostředky systému je komplikované, resp. zcela nemožné. Ve Windows 2000 (a zřejmě i Windows NT) je možné použít MMC konzolu, otevřít snap-in modul „Certifikáty“, staré CRL z úložiště vymazat, a poté nainstalovat CRL nové. Ve Windows 9x bohužel podobná konzola není obsažena, takže zde prakticky neexistuje způsob (nebo mi alespoň není znám), jak tento problém obejít (pomocí Internet Exploreru je sice možné spravovat úložiště certifikátu, úložiště CRL zde ovšem nejsou dostupná). Protože jsme problém s instalací CRL, a tím de facto nemožnost jeho používání, považovali za zcela zásadní pro korektní využívání elektronického podpisu, rozhodli jsme se jej řešit vytvořením jednoúčelové utility, která by provedla instalaci CRL pomocí služeb rozhraní CryptoAPI (kde po nastavení příslušného příznaku kupodivu proběhne instalace CRL zcela korektně). A odsud už byl jenom krůček o doplnění dalších funkcí pro automatické

stahování a kontrolu verzí CRL, čímž vznikla současná podoba aplikace. Jenom pro úplnost bych dodal, že ve Windows XP se už uvedená chyba nevyskytuje a instalace CRL proběhne korektně, což ovšem samozřejmě neznamená, že zde není možné CRL Manager využít.

Nyní již k samotnému programu. Po jeho spuštění se do pravé části hlavního panelu Windows umístí malá ikona, pomocí které je možné otevřít hlavní okno programu. Vlastní program potom běží na pozadí a nastaveném intervalu stahuje CRL, pokud dojde k jeho aktualizaci, je CRL automaticky nainstalován do systémového úložiště. Při instalaci je zástupce programu umístěn do složky „Startup“ (resp. „Po spuštění“), takže je automaticky spuštěn při startu operačního systému (pokud uživatel při instalaci tuto možnost nezakáže). Prakticky jediné, co musí uživatel udělat, je nadefinování seznamu CRL, které budou stahovány. K tomu slouží průvodce, kde je možné CRL přidat několika způsoby. Abychom i tuto fázi uživatelům co nejvíce zjednodušili, obsahuje program seznam nejznámějších certifikačních autorit, kde stačí vybrat požadovanou certifikační autoritu a program si sám nastaví odpovídající adresy CRL. Seznam bude navíc průběžně aktualizován, pomocí tlačítka „Aktualizovat seznam“ je možné stáhnout aktuální seznam těchto předdefinovaných certifikačních autorit. Dalším způsobem, jak můžeme cestu k CRL zadat, je její zjištění z certifikátu odesilatele. Před použitím tohoto způsobu je nutné certifikát nejprve uložit na disk a poté zadat cestu k tomuto souboru. Pokud certifikát obsahuje položku CDP („CRL Distribution Point“), program z ní zjistí cestu k CRL. Zároveň se pokusí zjistit, zda je certifikát vystavitele zprostředkující či kořenový, pokud se mu to nepodaří (certifikát vystavitele není dostupný), je nutné typ certifikační autority vybrat ručně. Poslední možností je ruční zadání údajů, kdy cestu k CRL zjistíme např. na webových stránkách certifikační autority, z certifikační politiky, atp.

Tím je nastavení programu prakticky hotové a dále se již o jeho chod nemusíme starat. Samozřejmě je možné nastavit některé další vlastnosti, jako například interval, v jakém budou CRL stahovány (po instalaci je implicitně nastaven interval stahování po 1 hodině). Po otevření hlavního okna programu je možné zjistit podrobnější informace, například kdy byly CRL naposledy stahovány a s jakým výsledkem, zda došlo k jejich aktualizaci, atd. Dvojitým kliknutím na položku seznamu v hlavním okně se potom zobrazí příslušné CRL. Je také možné úplně zakázat automatické stahování a CRL „ručně“ stáhnout pomocí odpovídajícího menu či ikon. Pamatováno bylo také na uživatele, kteří se k internetu připojují pomocí modemu a většinu času jsou tedy ve stavu off-line. Pokud totiž v zadaném intervalu není uživatel připojen, program monitoruje stav linky a jakmile dojde k připojení, provede stažení CRL. Tolik tedy stručně k používaní programu, součástí programu je podrobná nápověda, kde se případně dozvíte další informace o jeho ovládání.

A na závěr dobrá zpráva, **program je šířen jako freeware**, za jeho používání tedy není třeba platit žádné poplatky. V současné době je k dispozici první verze programu, přičemž program si sám automaticky detekuje, zda není k dispozici novější verze a pokud ano, nabídne její stažení. Velikost instalačního souboru je pouhých 200kB, proto není problém jej stáhnout i v případě vytáčeného připojení. Ještě bychom rádi upozornili na skutečnost, že program není nijak vázán na používaní služeb Certifikační autority Czechia, mohou jej tedy zdarma používat jak klienti jiných certifikačních autorit, tak také osoby, které se spoléhají na jejich podpisy.

E. Recenze knihy „Řízení rizik“ autorů V. Smejkala a K. Raise

Doc. Ing. Arnošt Katolický, CSc.

Boj o vytváření a využívání podnikatelských příležitostí, je spojen se změnami, s inovacemi, s investicemi - přinášejícími riziko neúspěchu. Svět je stále více propojený, trhy jsou obsazeny, konkurence je stále dravější. V dynamických podmínkách hrají stále větší úlohu rychle se vyvíjející informace a znalosti. Dynamická stabilita je jedinou variantou ekonomické stability. Rozhodování managementu probíhá ve stále složitějších podmínkách - rostou nároky na jeho rychlost a na kvalitu komplexní analýzy o kterou se opírá. Absence rozhodnutí managementu ve chvíli kdy rozhodovací situace reálně vznikla, je rovněž rozhodnutím - většinou velmi rizikové.

Vydání knihy Smejkala a Raise je proto dobrou zprávou! Autoři se v knize věnují:

- teorii rizika
- managementu rizika
- metodám snižování rizika v podnikatelském prostředí.

Kniha přibližuje následující základní druhy rizika:

- tržní, organizační a právní
- informační, investiční, personální a technologická.

Přednostní orientace knihy je na rizika podnikatelská, především na ta, která podnikatelské subjekty ohrožují nejčastěji. Kniha se zaměřuje na proces řízení změn strategie, změny struktury a na zvládnutí krizových situací. Část problematiky pokrývá souhrnně, část analyzuje ve speciálních oddílech knihy.

Mnohá rizika nemůžeme trvale odstranit. Můžeme je identifikovat, aktivně použít metody pro snížení rizika a připravit aktivity směřující k minimalizaci důsledků rizika. Zvládání rizika podnikání vyžaduje přípravu a to jak přípravu profesní a kvalifikační, tak přípravu informačního, organizačního a sociálně-psychologického zázemí práce manažérů.

To znamená naučit se především:

- identifikovat rizikové faktory v manažérské práci,
- posuzovat možné důsledky rozhodování v rizikových situacích,
- rozlišovat rizika, systematizovat je,
- hodnotit negativní důsledky reálného výskytu krizové situace,
- zhodnocovat vlastní a cizí zkušenosti v práci s rizikem.

Řízení rizika je velmi obsáhlá oblast. Její zvládnutí v jedné knize nebylo lehké ani pro dvojici zkušených autorů, jakými jsou V. Smejkal a K. Rais. Výsledek snahy v prvním vydání knihy lze hodnotit kladně. Téma řízení rizika není tématem novým. Vydáním knihy Smejkala a Raise se však na knižním trhu objevuje souborné dílo, které umožňuje orientaci v teorii s náznakem praktického využití. Kniha usiluje o logické opodstatnění zahrnutých tvrzení. Ilustrovat to lze výběrem několika částí knihy:

- kritické momenty v procesu budování úspěšného podniku,
- "7S faktorů" a jejich rozbor. Kritické faktory úspěchu firmy.
- Hlavní faktory prostředí ovlivňující firmu,
- základní pojmy analýzy rizik,
- vztahy v analýze rizik, vztahy při analýze rizik a vztahy při řízení rizik,
- volba strategie analýzy rizik,
- projektová rizika plynoucí ze špatného řízení projektu,
- proces řízení rizik IS/IT ve firmě.

Kniha obsahuje podrobný vyčerpávající přehled metod snižování podnikatelských rizik.

Samostatné kapitoly pokrývají podrobně následující dílčí témata:

- informační riziko, včetně budování informační bezpečnosti,
- investiční rozhodování a riziko,
- právní rizika a jejich prevence,
- základy krizového plánování.

Autoři ukazují na příkladech metody pro preventivní odstranění příčin vzniku rizikových situací a pro snížení jejich nepříznivých důsledků. Představují princip

prognózování jako nástroj ke snižování neurčitosti znalostí o budoucnosti a jako nástroj pro snižování hrozících rizik.

Přes náročnost tématu je kniha psána srozumitelným jazykem, přístupným pro teoretiky i pro praktiky. Skutečnost, že teoretická část celou problematiku velmi pečlivě strukturuje, vytváří předpoklady pro využití knihy i pro studenty vysokých škol. Kniha systematicky probírá vnitřní souvislosti tématu a naznačuje i vazby na témata, která se stávají stále významnější - jako například procesní management a management znalostí. Pozoruhodná je i část týkající se projektů řízení rizika a příčin jejich častého neúspěchu.

Řízení rizika stupňuje nároky i na nástroje řízení. Od tužky, přes Excel až po sofistikované nástroje v podobě expertních systémů a nástrojů z oblasti umělé inteligence. Výklad obsažený v kapitole věnované investičním ekonomickým rizikům podporují i 3 tabulky, které jsou ke stažení na portálu GRADY v zazipovaném souboru o velikosti 181 Kb (http://www.grada.cz/content/priklady.php):

- model investice vytvořený na bázi genetických algoritmů,
- příklad výpočtu NPV sledované investice,
- model návratnosti parkoviště vytvořený na bázi genetických algoritmů.

Podle autorů je kniha určena širokému okruhu subjektů: manažérům, podnikatelům, studentům, ale i specialistům na řízení rizik. Otázka rizika má velmi blízko k sociálně-psychologickým stránkám myšlení lidí. Jsou lidé, kteří si v rizikových situacích přímo libují, jiní se mu snaží vyhýbat. Poznání problematiky řízení rizika na základě studia knihy může být přínosem pro obě skupiny - každá si z ní může pro praxi vybrat to svoje. Poznat problematiku rizika prospěje všem, kdo chce být připraven snižovat riziko prevencí vzniku krizových situací i těm, kdo chce být připraven na minimalizaci důsledků výskytu krize.

Problematika řízení rizika je tématem, které se dotýká nejen podnikatelů. Zařazení problematiky rizika v rozhodování ve veřejné správě je reakcí především na události posledních let.

Rozhodnutí GRADY vydat knihu V. Smejkala a K. Raise považuji za velmi chvályhodné (http://www.grada.cz/content/katalog.php?kid=2408&hash). Nepochybuji o tom, že u tak náročného a rozsáhlého tématu jakým je Řízení rizika se najde dost příležitostí jak v dalším vydání knihu dále obohatit, jak dále prohloubit vazby dílčích témat, jak ještě více přiblížit čtenářům praktickou aplikaci teorie řízení rizik. Knihu vřele doporučuji. Neměla by chybět nejen v knihovně, ale přímo na stole žádného manažéra podnikajícího v rizikovém prostředí.

F. Letem šifrovým světem

ZNALOSTI 2004
2. výzva k podaní příspěvku, pozvaní k účasti
Jan Staudek, Fakulta informatiky, FI MU Brno, předseda

20.10.2003 - termín podání abstraktu návrhu příspěvků
27.10.2003 - termín podání plných verzi návrhů příspěvků

Srdečně Vás zveme k účasti na 3. ročníku interdisciplinární konference, věnované aktuálním problémům získávání, zpracování, zpřístupňování a využívání znalostí.

Termín konaní konference: 25.2. - 27. 2. 2004

Místo konaní konference: Hotel SANTON, Brno

Podrobné informace, pokyny pro autory a pro nabídky příspěvků , složení organizačního výboru jsou uvedeny na www strance konference http://www.fi.muni.cz/znalosti2004/

Tematické okruhy
Dobývání znalosti z databází, strojové učení
Získávání a reprezentace znalosti od experta
Vyhledávání informaci, textové i multimediální databáze, extrakce informaci z textu
Modelování podobnosti, extrakce vlastnosti z dat
Znalostní systémy
Multi-agentní technologie
Značkovací jazyky, znalostní anotace dokumentu, sémanticky web
Znalostní ontologie a další konceptuální modely
Zpracování přirozeného jazyka
Znalostní management, včetně aspektu firemní praxe a implicitních znalosti
Strojové jazyky
Sémantický web a webové služby

Kontaktní adresy
Organizační záležitosti: staudek@fi.muni.cz
Program: michal.kratky@vsb.cz

Organizují
Česká informatická společnost
Gerstnerova laboratoř, FEL CVUT Praha
Katedra informačního a znalostního inženýrství, VSE Praha
Katedra informatiky, VSB-TU Ostrava,
Katedra softwarového inženýrství, MFF UK, Praha
Fakulta informatiky, Masarykova universita, Brno

O čem jsme psali v říjnu 1999 - 2002

Crypto-World 10/1999

A.	Back Orifice 2000	2-3
B.	Šifrování disku pod Linuxem	3-5
C.	Microsoft Point-to-Point Tunneling Protocol (PPTP)	5-6
D.	Letem šifrovým světem	7-8
E.	E-mail spojení	8
Příloha : INRIA leads nearly 200 international scientists in cracking code following challenge by Canadian company Certicom"		9-10

Crypto-World 10/2000

A.	Soutěž ! Část II. - Jednoduchá záměna	2 - 4
B.	Král DES je mrtev - ať žije král AES ! (P.Vondruška)	5 - 9
C.	Kde si mohu koupit svůj elektronický podpis? (P.Vondruška)	10-12
D.	Kryptografie a normy II. (PKCS #3) (J.Pinkava)	13-15
E.	Prohlášení ÚOOÚ pro tisk	16-19
F.	Statistika návštěvnosti www stránky GCUCMP	20-22
G.	Letem šifrovým světem	23-24
H.	Závěrečné informace	24

Příloha : ZoEP.htm
(plné znění zákona č.227/2000 Sb.- "Zákon o elektronickém podpisu a o změně některých dalších zákonů (Zákon o elektronickém podpisu)", který nabyl účinnosti 1.10.2000)

Crypto-World 10/2001

A.	Soutěž 2001, II.část (Absolutně bezpečný systém) (P.Vondruška)	2 - 5
B.	E-komunikace začíná ! (?) (P.Vondruška)	7-11
C.	Digitální certifikáty, Část 2. (J.Pinkava)	12-14
D.	Šifrátor do vrecka (L.Cechlár)	15-16
E.	Interview s hackerem	17-19
F.	Mikolášská kryptobesídka	20-21
G.	Letem šifrovým světem	22-23
H.	Závěrečné informace	24

Příloha : Vyhláška 366/2001 Sb. (366_2001.pdf)
(prováděcí vyhláška ÚOOÚ k Zákonu o elektronickém podpisu č.227/2000 ve tvaru předaném k vyhlášení ve Sbírce zákonů)

Crypto-World 10/2002

A.	Úvodní komentář (P.Vondruška)	2 - 5
B.	Elektronický podpis (J.Hobza)	6 - 24
C.	Mikulášská kryptobesídka	25
D.	Letem šifrovým světem	26
E.	Závěrečné informace	27

G. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (Internet, noviny) nebo se jedná o původní články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Články neprocházejí jazykovou kontrolou!

Adresa URL, na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci **o zasílání** tohoto sešitu se mohou zaregistrovat pomocí e-mailu na adrese na e-mail pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci formulář na http://crypto-world.info . Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání sešitu.

Ke **zrušení registrace** stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu !). Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byl sešit zasílán. Ke zrušení registrace lze také opět použít formulář na http://crypto-world.info

3. Spojení

běžná komunikace, zasílání příspěvků k otištění , informace
pavel.vondruska@crypto-world.info
pavel.vondruska@post.cz
pavel.vondruska@ct.cz