

ŘEŠENÍ LEGISLATIVNÍCH PROBLÉMŮ DIGITALIZACE A ELEKTRONICKÝCH SLUŽEB V ODBORNÉM KONTEXTU ČINNOSTI KNIHOVEN

SOUHRN

TEMATICKÉ VYMEZENÍ

Tato kapitola se zabývá mnoha zásadními legislativními problémy, tzn.: ochranou dat a soukromí; šifrováním; elektronickým obchodem, ověřováním pravosti a elektronickým podpisem; využitím filtrovacího softwaru; a zákonem o duševním vlastnictví /IPR/ ve vztahu k metadatům,

POLITICKÉ SOUVISLOSTI

- V těchto oblastech je naléhavá potřeba vzdělávání a publicity. Zvláště to platí pro některé oblasti, jako je například filtrovací software (kdy se knihovny nevyhnutelně ocitnou ve střetu zájmů těch, kteří chtějí cenzurovat a těch, kteří zastávají tezi o svobodném toku informací) nebo přístup k šifrování (kde se stává kritickým napětí mezi státem prosazujícím legalizaci práva dešifrovat šifrované materiály a zastánci práva na soukromí). Tyto oblasti jsou čistě politické, a proto by knihovny měly vytvořit takovou strategii, která by rozhodně hájila jejich zájmy.
- Je nutno využít situace na trhu a vyplnit vakuum, které je v této oblasti evidenční a stát se „důvěryhodnou třetí stranou“ vystupující ve prospěch těch, kteří šifrované materiály používají
- Elektronický obchod a další pokrok v oblasti využívání elektronického podpisu se zřejmě brzy dočknou také veřejných knihoven, které budou nuceny zrychlit rozvoj a přizpůsobit se technickým a komerčním aplikacím těchto nových trendů.

DOPORUČENÍ PRO ÚSPĚŠNOU PRAXI

Dosud bylo zjištěno v oblasti evropských veřejných knihoven velmi málo iniciativ nebo užitečných příkladů z praxe. USA, Kanada a Austrálie nabízejí některé modelové příklady a zásady pro úspěšnou praxi, ale s ohledem na rozdílnost zákonodárství a kultury by musely být, pokud by měly sloužit v evropském kontextu, přizpůsobeny a upraveny.

ÚKOLY PRO BUDOUCNOST

- Je třeba školit pracovníky knihoven, zejména v oblastech ochrany dat, šifrovací technologie a strategie, ověřování pravosti, digitálních podpisů, směrnic o elektronickém obchodu a jejich aspektech, alternativách k filtrování softwaru a práv na intelektuální vlastnictví /IPR/ v metadatech
- Je také třeba lobovat na úrovni státních orgánů a zajistit takové změny v legislativě, které budou odpovídat potřebám knihoven
- Vedoucí pracovníci knihoven by si měli být více vědomi otázek zvýšené odpovědnosti, která souvisí s používáním nových technologií zaměstnanci a uživateli
- Knihovníci veřejných knihoven musí být seznámeni se všemi iniciativami, které se vztahují k ochraně menšin a jiných rizikových skupin obyvatel před nevhodným obsahem některých internetových stránek
- Knihovny by měly vzít v úvahu množící se příležitosti trhu způsobené tímto rozvojem a vystupovat například jako již zmíněné důvěryhodné třetí strany
- Je třeba propracovat vzorové smlouvy spolupráce mezi knihovnami i dalšími institucemi, které se budou vztahovat i na tvorbu metadat
- Veřejné knihovny by si měly vyměňovat nejlepší praktické zkušenosti ve všech těchto oblastech, zejména však v oblasti filtrovacího softwaru
- Učební plány knihovnických škol by se měly věnovat všem otázkám uvedeným v této kapitole
- EBLIDA a jiné odpovědné organizace by měly pořádát konference a semináře, publikovat příklady nejlepších praktických zkušeností z Evropy a ze zbytku světa a měly by také poskytovat referenční a aktualizaci služby týkající se nejnovějšího vývoje
- Veřejné knihovny, které iniciativně vyvinuly svůj vlastní fungující systém týkající se ochrany dat, by jej měly v co nejširším měřítku popularizovat a sdílet s ostatními knihovnami.

TEMATICKÉ VYMEZENÍ

Otázky, kterými se tato kapitola zabývá, zahrnují:

Strategii EU

Ochrana dat a soukromí

Šifrování a ověřování pravosti

Filtrovací software

Právo na intelektuální vlastnictví /IPR/ v metadatech

POLITICKÉ SOUVISLOSTI

Čtenáři by si měli všimnout, že v těchto oblastech neexistují žádné vhodné praktické příklady a to i přesto, že se této otázce věnuje zvýšená pozornost. Tato skutečnost je komentována také ke konci této kapitoly.

Evropská unie přijala celou řadu směrnic, které slouží k podpoře rozvoje informační společnosti. Mimo to také publikovala dokumenty, v nichž se na toto téma vedou diskuse a zorganizovala celou řadu příslušných jednání a konferencí.

Důležitost iniciativ EU nesmí být podceňována. V mnoha ohledech EU vede svět v rozvoji regulačního schématu informační společnosti a mnohé z těchto iniciativ mají pro veřejné knihovny obrovský význam.

Směrnice o elektronickém obchodu

Směrnice o elektronickém obchodu 00/31/EC (The E-Commerce Directive 00/31/EC)

http://europa.eu.int/eur-lex/prl/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf uvádí, že členské státy mají zaručit prostřednictvím svých zákonodárných systémů uzavírání obchodních smluv elektronickým cestou. Směrnice také omezuje za určitých podmínek zodpovědnost poskytovatelů internetových služeb (*Internet Service Providers - ISP*), například v případě, funguje-li ISP pouze jako prostředník a nemá tudíž nad obsahem odeslané zprávy kontrolu.

Tato směrnice je aplikovatelná ve všech typech elektronického obchodu, a proto je také relevantní všude tam, kde veřejná knihovna provozuje komerční aktivity s třetí stranou elektronickou cestou. To se bude například týkat i zajištění služeb elektronického dodávání dokumentů a přijímání objednávek dokumentů a jiných materiálů e-mailem. Pravidla upravující odpovědnost poskytovatelů těchto služeb na Internetu budou zásadní pro ty veřejné knihovny, které provozují své vlastní webové stránky. Směrnice ovlivní mnoho veřejných knihoven, avšak povědomí o ní není dosud dostatečně rozšířeno. Směrnice měla v členských zemích vstoupit v platnost v lednu 2002. Mnoho členských států se touto směrnicí již také řídí.

Důležitá politická otázka – příslušné orgány státu mají prosadit další legislativní opatření a vyvinout iniciativu k podpoře elektronického obchodu (e-commerce).

Směrnice o elektronických podpisech

Směrnice o elektronických podpisech (The Directive for E-signatures /1999/93/EC/)

http://216.239.51.100/search?q=cache:b_hy_cTjNHQC:europa.eu.int/comm/internal_market/en/media/sign/Dir99-93-ecEN.pdf+e-signatures+directive&hl=en&ie=UTF-8

vešla v platnost v lednu 2000. Všechny členské státy měly tuto směrnici uvést do praxe nejpozději do 19. července 2001. Cílem této směrnice je umožnit využití elektronických podpisů a přispět k jejich legislativnímu uznávání. Před legislativním uznáním stanovila směrnice určitou minimální autorizační normu. Elektronický podpis musí tedy být:

- jedinečně spjat s autorem;
- schopen identifikovat autora;
- vytvořen tak, aby byla autorovi samému umožněna kontrola a
- aby byl propojen s daty takovým způsobem, že všechny případné následné změny budou vyhledatelné.

V praxi lze splnění všech těchto požadavků dosáhnout s použitím Veřejného kódovacího klíče. V současné době tuto metodu používá však jen zlomek veřejných knihoven. Je proto nepravděpodobné, že by směrnice o elektronických podpisech měla na veřejné knihovny okamžitý dopad.

V členských státech mají podle této směrnice elektronické podpisy stejnou legislativní platnost jako tradiční ručně psané. Bezpečnost zůstává jednou z největších obav všech druhů podnikání, ale experti se shodují na tom, že elektronické podpisy se padělají mnohem hůře než tradiční. Viz také kapitola Poskytování služeb přizpůsobených individuálním potřebám uživatelům

Důležitá politická otázka – orgány státní správy jsou přesvědčeny, že by elektronické podpisy měly mít stejný statut jako ty ručně psané.

Ochrana dat

Ve všeobecném povědomí kolují informace, ať už oprávněně nebo ne, že stát a mnoho soukromých komerčních organizací postupně sbírají data o soukromých osobách, která pak slouží jejich zájmům. Mnohé z těchto informací jsou přitom jednoduše shromažďovány právě elektronickými prostředky. Legislativa ochrany dat se dotýká manipulování s informacemi o jednotlivcích. Manipulace s těmito informacemi může být v počítačové podobě nebo v jiné formě jako jsou například manuální registrační systémy, audiokazety, videokazety a podobně.

Zákon o ochraně dat se týká informací o jednotlivcích, které jsou naprosto neškodné, jako záznamy o autorech v katalogích knihoven, poměrně citlivé jako adresa či telefonní číslo, či velmi citlivé jako kriminální, zdravotní či sexuální minulost. Směrnice EU o ochraně dat podrobuje citlivé osobní údaje zvláště striktním pravidlům.

Legislativa týkající se ochrany dat vyžaduje, aby organizace kontrolovaly záznamy obsahující osobní údaje o žijících identifikovatelných osobách. Legislativa také většinou dává osobám uvedeným v databázích právo vědět, jaké záznamy jsou o nich uvedeny a co je jejich obsahem. Budou ale stanoveny výjimky, kdy vlády a některé příbuzné orgány budou mít povoleno zpracovávání dat pro účely prevence zločinnosti, národní bezpečnosti, vybírání daní apod., aniž by o tom příslušnou osobu informovaly.

Na rozdíl od aktivity EU, která přijala směrnici /EU Directive 95/46/EC/ prosazující ochranu dat, stojí za zmínku USA, které mají pouze omezenou ochranu na federální úrovni. Směrnice EU vyžaduje následující:

- uživatelé se, pokud chtějí užít osobní data, musejí zaregistrovat
- dotyčné osoby mají právo vědět, že jsou o nich pořízeny záznamy a přesvědčit se o jejich obsahu
- dotyčné osoby mají v případě újmy způsobené nepravdivými daty právo příslušný subjekt zažalovat
- uživatelé dat se musí řídit určitými obecnými zásadami a principy
- musí existovat výjimky v záležitostech národní bezpečnosti, prevence zločinnosti apod.
- musí fungovat systém znemožňující neautorizovaný přístup, vymazání či změnu záznamů
- uživatelé si musí před používáním osobních dat vyžádat příslušné povolení
- dotyčné osoby mají právo kdykoliv požádat, aby jejich osobní data byla z databáze odstraněna
- musí být pokryty jak manuální tak počítačové systémy
- dotyčné osoby mají právo vědět, komu byly osobní informace o nich poskytnuty
- pouze na základě obdržerých osobních informací nesmí být o dotyčných osobách učiněno žádné rozhodnutí

Směrnice Evropské unie měla v členských státech vstoupit v platnost do 24. října 1998, některé členské státy toto však nedodržely.

Směrnice zakazuje přesun osobních dat do těch zemí mimo Evropskou ekonomickou oblast /EEA/, které nemají "adekvátní úroveň ochrany". V důsledku toho směrnice naléhavě žádá tyto země, aby přijaly normy podobné těm evropským. To se týká zejména USA, kde ochrana dat prakticky neexistuje. Proto jsou na místě dvě otázky: co je "převod" a co zaručuje "adekvátní ochrana dat"?

"Převod" znamená buď exportování dat nebo povolení k zpřístupnění dat občanům v zahraničí. Umístění osobních dat na Internet zpřístupňuje data občanům mimo EEA. Služební cestování z Velké Británie do zemí mimo evropskou ekonomickou oblast nebo intranety společností, které umožňují přístup k datům i uživatelům mimo oblast EEA, jsou zrovna tak problematické jako některé evidentnější formy převodu.

Tři základní znaky nám mohou spolehlivě naznačit, zda existuje přiměřená úroveň ochrany dat:

- existence zákona o ochraně dat
- právo dotyčných osob na kontrolu záznamů týkajících se jejich osoby, jejich revize a možnost žaloby v případě újmy způsobené nepravdivými údaji
- existence dozorčího orgánu

Je stále nejasné, jak úzce či široce bude tato přiměřenost definována kromě těchto základních principů. Hodnocení bude s největší pravděpodobností záviset na specifických okolnostech přesunů dat.

V USA v současné době neexistuje federální zákon o ochraně dat. Aby se tento problém vyřešil, je pro země mimo evropskou ekonomickou oblast /a zvláště pak pro USA/ rozvíjena myšlenka "bezpečných přístavů". Jde o společnosti, které jsou vázány souborem zásad ochrany soukromí. Jakákoliv převedená data jsou v bezpečném přístavu uložena a nemohou být v rámci té země převedena jinam. Bezpečné přístavy dobrovolně dohlíží

na dodržování principů ochrany dat přijatých EU. Personální data nemohou být z těchto bezpečných přístavů převedena bez odsouhlasených a přijatých bezpečnostních opatření a dohledu.

Kvůli tomuto problému by veřejné knihovny měly věnovat zvýšenou pozornost zasilání různých dokumentů prostřednictvím Internetu.

Důležitá politická otázka - rozpor mezi USA a Evropskou unií naznačuje, že veřejné knihovny prezentované na Internetu musí být opatrné ve výběru uvedených osobních dat.

Šifrování a ověřování pravosti

Při současném trendu provádění každodenních transakcí elektronickou cestou by lidé měli mít jistotu, že jejich soukromá komunikace není během cesty globálními sítěmi zachycována či měněna. Jestliže se lidé na důvěrnost a autentičnost elektronických informací nemohou spolehnout, mohli by se vrátit k tradičnějším způsobům komunikace, čímž by obchodní jednání značně ovlivnili. Potenciál informační společnosti by tak nebyl plně využit.

Na tomto pozadí jsou nové a rozvíjející se kódovací techniky velmi rozšířené. Kódování je používáno ke skrytí či ověření obsahu elektronických dokumentů a k ochraně souborů před neautorizovaným přístupem, změnami a zcizením. Šifrování zahrnuje kódování textu tak, aby se nedal, pokud je příslušně označený, číst. Je používán v případech, kdy si lidé přejí, aby informace zůstaly důvěrné. Avšak kódování může být také zneužito pro nezákonné účely. Toto zjištění posílilo tlak na zákonodárné orgány přijmout omezení nerozluštitelného šifrování. Soukromí advokáti a obchodní skupiny se jakýmkoliv snahám omezit kódování brání argumentující přitom, že takový zásah by nežádoucím způsobem ohrozil soukromí osob a tím i rozvoj informační společnosti. Viz také [služby na míru](#).

Spojené státy americké tradičně odmítly export kódovacích softwarů a usilují o to, aby měly federální agentury přístup ke klíčům nezbytným pro dekódování dokumentů. Přístup USA ke kódování je po teroristických útocích na New York a Washington z 11. září 2001 ještě zatvrzelejší.

Ověření pravosti je elektronické potvrzení, že právě vy jste osoba, za kterou se prohlašujete. Pravost je potvrzení, že obdržená zpráva nebyla na cestě od odesílatele k příjemci nijak změněna. Občané si dnes potřebují být jisti, že se mohou účastnit elektronických transakcí se stejnou mírou důvěry jako transakci "papírových".

Veřejný kódovací klíč (Public Key Cryptography, nebo též PKC) využívá dvou klíčů - jeden z nich je široce přístupný a druhý je soukromý, známý pouze určitým osobám či službě, která klíč vlastní. Veřejný klíč může být nezajištěnými linkami přenášen nekódovaný, zatímco soukromý klíč musí být uchovávan v tajnosti. Proto je veřejný klíč velice zjednodušen.

Hlavním problémem státu je tedy otázka týkající se jeho práva na vyžádání klíčů od jejich majitelů k dekódování zpráv, ustanovení důvěryhodných třetích stran k využití klíčů ve prospěch třetí osoby a jejich zákonodárná úloha. Obecný profil otázek šifrování: <http://www.cyber-rights.net>

Ověřování pravosti nemusí nutně zahrnovat kódování. Velmi úspěšný systém ATHENS vyvinutý ve Velké Británii je založen na uživatelském znaku (ID) a heslu (password). Tento systém by měl být v nejbližší době modernizován, aby jej mohla využívat kterákoliv veřejná knihovna.

Důležitá politická otázka - napětí mezi státem a zastánci civilních práv kvůli dekódování zpráv. Na čí straně budou veřejné knihovny?

Filtrovací software

Hlavním problémem veřejných knihoven je obava, že uživatelé buď získávají, nebo zasílají z internetových stanic dokumenty, které jsou považovány za nevyhovující. Většinou jde o pornografické materiály, ale jisté obavy vyvolávají také dokumenty s rasově nesnášenlivým obsahem, násilnostmi, propagací drog, proteroristickou propagací atd. EU přijala řadu opatření týkajících se ochrany menšin a jiných ohrožených skupin občanů před nechráněným vstupem na Internet. K popisu tohoto problému existuje řada metod, ale jediná, která vyvolala pozornost a ohlas je právě metoda filtrovacího softwaru. Takový software /a na trhu je jich k dispozici celá řada/ znemožňuje pokusy otevřít webovou stránku, která obsahuje neslušná slova a v některých případech i určité obrázky /záleží na počtu barevných odstínů/.

Řada knihoven takový software instalovala jako pokus zaměřit se na tlak, pod který se dostala ve snaze zamezit uživatelům přístup k nevhodným materiálům. Některé studie /mnohé z nich financované EU/ bohužel ukazují, že všechny současné software nejsou natolik propracované, aby zamezily přístupu ke všem nevhodným internetovým stránkám. Ve světě existuje řada soudních případů a neformálních rozhodnutí týkajících se způsobu zpřístupnění Internetu ve veřejných knihovnách. Skupiny uživatelů i jednotlivci buď zažalovali nebo vyvíjeli na veřejné knihovny nátlak v souvislosti se zpřístupněním všech internetových stránek včetně těch s nevhodným obsahem široké veřejnosti. V některých případech bylo proto vyvinuto úsilí buď omezit přístup jako takový, nebo použít odpovídající filtrování softwaru. Zejména Americká knihovnická asociace /ALA/ vystupuje velmi výrazně na obranu veřejných knihoven v USA proti těmto tlakům a v zásadě byla úspěšná. Viz také multimedia.

Legislativní pozice veřejných knihoven závisí na tradicích jednotlivých zemí a vůli knihovníků odolávat vnější cenzuře. EU vyvíjí v tomto ohledu politiku bezpečného používání Internetu a je důležité, aby se veřejné knihovny do rozvoje a aplikace těchto postojů zapojily. Toto téma je zvláště problematické a veřejné knihovny by se měly snažit v rozvoji těchto postupů navzájem spolupracovat.

Důležitá politická otázka- napětí mezi těmi, kteří si cenzuru přejí a těmi, kteří se přiklánějí k názoru o svobodném toku informací. Veřejné knihovny se nacházejí v bojové linii.

Práva na intelektuální vlastnictví /IPR/ a metadata

Obecné problémy IPR jsou diskutovány na jiném místě. V zásadě jsou metadata chráněna Evropskou unií v rámci databáze autorských či jiných práv. V rámci směrnice o databázích jsou v databázi systematicky shromažďována data či jiné materiály, přičemž každý z nich je individuálně přístupný elektronickým či jiným způsobem. Každá sbírka metadat se bezesporu označuje jako databáze. Ochrana těchto databází závisí na míře intelektuální či tvůrčí činnosti spojené s jejich vytvářením.

Existuje také silný argument, že použil-li odborník k aplikaci metadat tvůrčích schopností a znalostí, měla by být tato data chráněna autorskými právy. A to i v případě, že by soud uznal, že se na ně tato ochrana nevztahuje, protože vzhledem k lidským a finančním investicím vloženým do jejich tvorby tato činnost bezesporu požívá výhod ochrany vyplývajících z autorského zákona. Tvorba metadat by tudíž měla být veřejnými knihovnami respektována jako každá jiná činnost chráněná autorskými právy, a pokud si knihovny vytvoří svá vlastní metadata, mají v případě, že by třetí strana bez dovození zkopírovala jejich podstatnou část, právo na podání žaloby. Viz také kapitola Identifikace zdrojů a vyhledávání informací.

IPR a metadata se stávají ožehavou otázkou zejména v případě, jedná-li se o jakoukoliv formu spolupráce či přidávání metadat do společné databáze. Nejsou-li otázky IPR předem dostatečně vyjasněny, nastává potenciální vážný problém když se strany například rozhodnou dohodu zrušit nebo pokud hrozí nebezpečí komerčního zneužití sbírky dat.

Důležitá politická otázka- tento problém bývá často přehlížen, ale může se stát potenciálním zdrojem vážných problémů, zvláště pokud se tato otázka při společných projektech nevyřeší předem.

DOPORUČENÍ PRO ÚSPĚŠNOU PRAXI

Hlavní aktivity veřejných knihoven, o kterých kapitola pojednává, jsou:

Ochrana dat a soukromí

Problémy vznikají zejména s ohledem na nedostatečnou podporu a využívání záznamů o čtenářích a výpůjčkách a sledování využití elektronických zdrojů. Jsou to často citlivé záležitosti a stala se řada případů, kdy policie sledovala a identifikovala návyky určitých čtenářů místních veřejných knihoven. Další potíže se objevují v souvislosti s postupováním informací o čtenářích komerčním organizacím. Další, již méně ožehavé komplikace se týkají udržování záznamů o autorech v knihovnických katalogích a publikování podrobností o zaměstnancích knihovny na webových stránkách. V případě problémů by měly veřejné knihovny při poučení zaměstnanců vycházet z etického kodexu či z praxe. Nutné jsou také rady týkající se legislativní odpovědnosti a ochrany dat.

Šifrování

V současné době nejsou veřejné knihovny příliš zapojeny do předávání či získávání zašifrovaných zpráv. Ovšem se vzrůstající pravděpodobností, že dříve či později budou finanční jednání knihovny, jako objednávání knih,

využívat metod elektronického obchodu, budou muset veřejné knihovny v této oblasti přidat. Je důležité vědět, že zákon poskytuje pouze základní regulační rámec pro šifrování a volba nejspolehlivější a nejzavedenější techniky je individuální záležitostí každé knihovny.

Šifrování se týká typu jednání firmy se zákazníkem /B2C/, zákazníka se zákazníkem /C2C/, firmy s firmou /C2C/ a na tyto různé druhy komunikace se také vztahují různá pravidla. B2C je pro veřejné knihovny nejdůležitější, protože komunikace s uživateli elektronickou cestou je stále běžnější. Je důležité si všimnout, že šifrování má důležitý politický podtext a knihovny se mohou ocitnout ve zněti argumentů pokud jde o povolení k používání šifrování. Evropské knihovny nemají v současné době stejné politické tradice v lobování jako má například Americká knihovnická asociace. To by se mělo v budoucnu změnit. Viz také [služby na míru](#).

Projednávání protiprávních činů

Mnoho uživatelů Internetu ignoruje autorské či jiné relevantní zákony. Záleží zde hlavně na jednotlivých případech, ale obecně platí, že pokud měly zodpovědné osoby o těchto činech povědomí nebo dobrý důvod věřit, že se takováto činnost odehrává, mohou za ni být zodpovědné.

Obecně jsou zaměstnavatelé zodpovědní za nelegální činy svých zaměstnanců, a to i v případě, že se děly bez jejich vědomí. Také knihovny by si tedy měly být vědomy toho, jak jejich zaměstnanci Internet využívají. Ovšem to se vztahuje pouze na úkony, které se od zaměstnance v jeho každodenní práci očekávají. Takže v případě, že je pracovník například zodpovědný za každodenní zaslání e-mailu v knihovně, je zodpovědnost za případné nelegální e-maily dělena mezi knihovnu a zaměstnance. Podobně pokud používá zaměstnanec software a použije například pirátský software na počítači, který patří jeho zaměstnavateli, jsou zaměstnanec a zaměstnavatel taktéž odpovědní rovným dílem. Zaměstnavatele je však obvykle snazší identifikovat a měl by disponovat finančními prostředky, a tak se poškozená strana obrací často pouze přímo na něj.

Knihovny by proto měly dbát na to, aby zajistily příslušné vzdělávání a školení zaměstnanců. Měly by také mít jasno ve firemní strategii v případě protiprávních činů a stanovit příslušné postupy. Taková strategie by například měla zaměstnancům a uživatelům knihovny zakazovat posílat či prohlížet dokumenty podléhající trestnímu stíhání. Zaměstnanci a uživatelé by také měli být poučeni o nutnosti posílat dokumenty pouze předpokládaným příjemcům a také o postupech v případě, že obdrží jakoukoliv nezákonnou či nevyžádanou zprávu.

Všechny výše zmíněné skutečnosti naznačují, že vedoucí pracovníci knihoven musí v případě obdržení formální stížnosti třetí osoby na nezákonnost jednat rychle. Dříve, než na takovou stížnost odpoví, měli by co nejrychleji shromáždit dostupná fakta a vyhledat radu právníka. Jestliže se stížnost ukáže jakkoliv opodstatněnou, měla by knihovna podniknout okamžité kroky k vyřešení problému, například vymazat nevhodné materiály či omezit přístup zaměstnanců a uživatelů k některým zařízením. Pokud to neudělá, může to výrazně otřást důvěrou uživatelů v knihovnu. Všechny podklady by se měly kopírovat a ukládat na bezpečném místě.

Směrnice EU o elektronickém obchodu uvádí, že by členské státy měly zaručit, aby v případě, že služba slouží k ukládání informací poskytnutých třetí stranou, NEBYL poskytovatel služby za obsah informací uložených touto třetí stranou zodpovědný, a to za podmínky, že:

- nemá poskytovatel o protiprávní aktivitě povědomí
- v případě stížnosti na obsah, nemá k dispozici fakta ani podrobnosti k identifikaci tohoto protiprávního obsahu
- jakmile obdrží nezbytná fakta, okamžitě nevhodné informace vymaže či k nim zamezí přístup

Ověřování pravosti a elektronické podpisy

Je jasné, že se knihovníci budou muset poučit o využití kódování a jeho aspektech. V současné době má s jeho využitím zkušenosti pouze malý počet veřejných knihoven, avšak je velice pravděpodobné, že se jeho použití stane v členských státech v nejbližších letech povinné. Veřejné knihovny se musí seznámit se základními technickými, manažerskými a legislativními otázkami, které jsou s tím spojeny. Veřejné knihovny se těší u veřejnosti značné důvěře a přízni, mohou se tak stát „důvěryhodnou třetí stranou“ (Trusted Third Parties – TTP). V zájmu toho, aby byly šifrovací klíče neporušené, měly by vlády jednotlivých zemí rozhodnout o tom, že klíče musí být před použitím uloženy v TTP. Toto je ojedinělý případ, kdy mají knihovny šanci těžit z mezery v trhu, která vznikla změnou klasického prostředí aplikací informačních technologií. Viz také [služby na míru](#).

Ověřování pravosti je pro veřejné knihovny velmi důležité, protože mnoho vydavatelů elektronických zdrojů neudělí knihovně k jejich používání licenci, aniž by se ujistilo, že k nim budou mít přístup pouze oprávnění uživatelé. Tito vydavatelé se zdají být spokojeni s úrovní ochrany poskytované programem ATHENS <http://www.athens.ac.uk>, ale mnozí z nich budou v nejbližší době vyžadovat vyšší standard. Tento problém je aktuální zejména pro vzdálené uživatele, kteří se chtějí na systém napojit a musejí mít nejprve řádné oprávnění. Jedním z důvodů, proč vydavatelé elektronických zdrojů v současné době váhají dovolit vzdáleným uživatelům přístup, je právě strach z nedostatečné autorizace; vyšší úroveň ochrany napomůže zpřístupnění rozsáhlých digitálních zdrojů v knihovnách.

Filtrovací software

I když se většina diskusí mezi knihovnami a veřejností o využívání či nevyužívání filtrování softwaru odehrává v USA, můžeme podobné případy najít i v Evropě. Je důležité, že veřejné knihovny nejsou ovlivněny krátkozrakými názory jen proto, aby vyhověly nejhlasitější se projevující menšině. V současné době neexistuje žádný filtrovaný software, který by byl schopen poskytnout ochranu vyžadovanou zainteresovanými občany, aniž by přitom nevyloučil také neškodné dokumenty. Veřejné knihovny mají ale v každém případě povinnost poskytnout občanům k vyžadovaným materiálům volný přístup a volání po cenzuře odmítají. Kromě filtrování softwaru existuje i řada jiných strategií:

Metoda přijatelného využívání: uživatelům může být zakázáno využívání určitých zařízení, pokud nedodržují daná pravidla. Viz také kapitola Poskytování služeb přizpůsobených individuálním potřebám uživatelů.

Požadavek, aby všichni rodiče podepsali prohlášení, že jsou si vědomi rizika přístupu dětí k nevhodným dokumentům při využívání zařízení knihovny. Pokud rodiče odmítnou podepsat, nebude dětem použití těchto přístrojů dovoleno. Použití automatizovaných hodnotících systémů, jako například dobře známého systému PICS <http://www.w3.org>, knihovnám pomůže rozhodnout, které materiály jsou vhodné ke zpřístupnění a které nikoliv. Ale pozor, uživatelé u nichž bude využívání Internetu monitorováno si tohoto musí být vědomi a musí souhlasit /jak je vyžadováno zákonem o ochraně dat/.

Práva na intelektuální vlastnictví /IPR/ v metadatech viz také popis zdrojů

Hlavní otázkou je zde školení pracovníků knihovny o zákonech o autorských právech a o právech souvisejících s databázemi, aby plně porozuměli svým právům a povinnostem v rámci těchto zákonů. Existuje zde zvláště ožehavý problém v souvislosti s tvorbou metadat v případě společného projektu několika knihoven. Tato forma spolupráce je čím dál rozšířenější, ovšem často začíná bez znalosti základních principů. Vlastnictví takto společně vytvářené sbírky je rozděleno mezi více organizací, což znamená, že žádná jednotlivá knihovna nesmí s informacemi v databázi pracovat bez souhlasu všech ostatních subjektů. V takovýchto případech je před začátkem spolupráce nejlepší uzavřít smlouvu o spolupráci. Toto je také otázkou školení, v tomto případě však manažerů projektů.

Dalším problémem je ochrana práv k metadatům vytvořených knihovnou samotnou. V závislosti na důležitosti a hodnotě sbírky metadat to vyžaduje aktivní postoj a přístup ke správě Internetu. Řada komerčních organizací nabízí tyto služby za poplatek. Ve většině případů nemají metadata takový význam a důležitost, aby musela být takto přísně střežena, ale musíme vzít v úvahu, že umístěním metadat do některé z veřejně přístupných částí webové stránky knihovny riskují využití těchto metadat třetí stranou pro její vlastní prospěch.

Zatím je k dispozici jen málo modelových smluv týkajících se práv na intelektuální vlastnictví /IPR/ v souvislosti s metadaty, ačkoli výzkum v této oblasti však stále pokračuje. V současné době však stále není zpracována žádná jasná strategie, která by mohla být veřejným knihovnám poskytnuta. Viz [metadata](#).

ÚKOLY PRO BUDOUCNOST

Je jasné, že zmíněné problémy je třeba chápat v celé jejich rozmanitosti. Mohou být shrnuty takto:

- Je třeba vzdělávat pracovníky knihoven, zvláště pak v oblasti ochrany dat, kódování a strategie, ověřování pravosti a digitálních podpisů, směrnic týkajících se elektronického obchodu a jejich aplikace, alternativ k filtrování softwaru a ochrany intelektuálního vlastnictví pokud se týká metadat. Vzdělávání by se mělo týkat jak technické stránky (stručné seznámení se současnými možnostmi), stránky sociální (tedy co je či by mohlo být oblíbené), ale také právní stránky (co se smí a nesmí a jaká jsou práva a povinnosti zaměstnanců knihovny).

- Je třeba lobovat na úrovni státu, aby zajistil prosazování změn v legislativě s ohledem na potřeby veřejných knihoven
- Vedoucí pracovníci knihoven si musejí být více vědomi odpovědnosti knihovny za využívání nových technologií jak zaměstnanci, tak uživatelé
- Veřejné knihovny musí být průběžně informovány o všech odpovídajících způsobech ochrany menšin a jiných rizikových skupin občanů před nevhodným Internetovým obsahem. Tyto iniciativy se mohou týkat nově vytvářeného software, legislativy, nového kodexu pravidel a zásad pro činnost a funkce vznikající v rámci inovované praxe a nových klasifikačních systémů
- Veřejné knihovny by měly využít důvěry, které se těší u vlád i občanů, vzít v úvahu možnosti vzniklé na trhu a vystupovat například v roli důvěryhodné třetí strany.
- Americká knihovnická asociace vyvinula užitečné rady týkající se filtrovacího softwaru a postupů, které by mohly být upraveny pro využití v evropských veřejných knihovnách.
- Je třeba propracovat vzorové smlouvy pro spolupráci, jež se budou vztahovat i na tvorbu metadat
- V mnohých z těchto oblastí je třeba zpracovat soubor zásad pro úspěšnou praxi. Paul Sturges vyvíjí soubor takových zásad pro veřejné knihovny za podpory Rady Evropy. Ten se stane výborným odrazovým můstkem.
- Veřejné knihovny by si měly vyměňovat nejlepší praktické zkušenosti ve všech těchto oblastech, především však v otázce filtrování softwaru.
- Učební plány knihovnických škol by se měly zabývat všemi otázkami zmíněnými v této kapitole
- EBLIDA a další zodpovědné organizace by měly pokračovat v organizaci konferencí a seminářů týkajících se této problematiky a publikovat příklady nejlepší praxe z Evropy a celého světa. Tímto způsobem budou veřejné knihovny EU moci využívat i nejlepších zkušeností z ostatních zemí. Předpokládá se však, že nejlepší inovační koncepce přijdou právě ze zemí Evropské unie a že zbytek světa bude kopírovat praxi z EU a ne naopak
- EBLIDA a další zodpovědné organizace by měly pokračovat v poskytování referenční a informační služby o nových poznatcích v této problematice.

Nejdůležitější věcí, na kterou je třeba také poukázat, je velmi rychlý rozvoj techniky a obchodu, který by měl být průběžně sledován.

Nejlepší cestou pro EBLIDu či další knihovnické asociace je vývoj důležitých pravidel a zásad úspěšné praktické činnosti v nových podmínkách a podle potřeby lobování na úrovni státních orgánů. V některých oblastech je stále třeba organizovat výzkum a měli by být osloveni sponzoři a grantové agentury, ale ve většině případů je to otázka vývoje a poučení se z nejlepších praktických zkušeností. Výzkum provedený k této zprávě ukázal, že knihovny zatím nepublikovaly nic, co by vypovídalo o nejlepších praktických zkušenostech, jež se vztahují k této otázce. *Možná nejdůležitějším poselstvím je tedy podpořit iniciativu veřejných knihoven, které těchto zkušeností dosáhnou a rozšíří je mezi ostatní.*

ODKAZY NA WEBOVÉ STRÁNKY

Mezinárodní

Electronic Privacy Information Centre /EPIC/

/Elektronické centrum soukromých informací/

Kódování a svoboda 2000: mezinárodní průzkum strategie kódování v roce 2000. Odhad národních a mezinárodních strategií kódování z hlediska občanských svobod.

<http://www2.epic.org/reports/crypto2000/>

International Federation of Library Associations and Institutions /IFLA/

/Mezinárodní federace knihovnických asociací a institucí/

Prohlášení o knihovnách a intelektuální svobodě. Mezinárodní prohlášení zaměřené na celou knihovnickou profesi uvádějící principy intelektuální svobody. Návrhy Deklarace Organizace spojených národů pro podporu lidských práv.

<http://www.ifla.org/V/press/pr/990326.htm>

International Federation of Library Associations and Institutions /IFLA/

/Mezinárodní federace knihovnických asociací a institucí/

Postoj IFLA k problematice autorských práv v digitálním prostředí. Srpen 2000. Specifičtější usnesení poskytující informaci o postoji IFLA k autorským právům v digitálním prostředí. Webová stránka přináší také soubor principů jako rukověť pro řešení této problematiky v knihovnách.

<http://www.ifla.org/V/press/copydig.htm>

OECD

Směrnice týkající se ochrany uživatelů v kontextu s elektronickým obchodem

(*e-commerce*). Příklad mezinárodních směrnic zpracovaný společně zástupci resortu obchodu a skupinami uživatelů. V některých zemích použito jako základ pro zpracování národních směrnic/viz nahoře/. Dokument je k dispozici ve formátu pdf v různých jazycích.

<http://www.oecd.org>

Strategie ochrany soukromí OECD,

kteřá vychází z prognóz v oblasti obchodu

<http://www.oecd.org/oece/pages/document/displaywithoutnav/0,3376,EN-document-589-17-no-21-17091-0,00.html>

Strategie kódování: Směrnice a problémy

Jeden ze starších /1997/ přístupů k mezinárodní strategii kódování zaměřený na nadnárodní organizace. Směrnice doporučené OECD, které by mohly vytvořit užitečný základ pro tvorbu strategie.

<http://www.epic.org/crypto/OECD/>

UNICTRAL

/Komise Spojených národů pro mezinárodní obchodní právo/

Vzorový zákon o elektronickém obchodu s průvodcem a výkladem. Průvodce legislativou Spojených národů týkající se elektronického obchodu. Zajímavý příklad celosvětové strategie. Zákon je jasný a srozumitelný a může sloužit jako model pro ostatní státy.

<http://www.unictr.org/english/texts/electrom/ml-ec.htm>

Vzorový zákon o elektronických podpisech. 2001.

Jako v předchozím odkazu, tentokrát však o elektronických podpisech.

http://www.kisa.or.kr/policy/sub3/data/pdf/PD_00_01_UNICTRAL.pdf

Evropa

Rada Evropy

Hlavní zásady týkající se veřejného přístupu a svobody vyjádření v informacích poskytovaných elektronickou cestou: Směrnice pro evropskou kulturní politiku. Jeden z nejdůležitějších dokumentů k tomuto tématu. Příklad mezinárodní směrnice zaměřené na instituce, jakými jsou knihovny, muzea a archívy.

<http://www.coe.int/T/E/CulturalCo-operation/Culture/Resources/Referencetexts/Guidelines/freedomexpression.asp>

Rada Evropy/EBLIDA

Rukověť evropské legislativy a strategie knihoven. Listopad 1998. Příspěvky z mnoha zemí včetně Velké Británie, Francie, Maďarska, Nizozemí a Norska. Zaměření na svobodu vyjádření, přístupu a autorský zákon.

http://www.coe.int/T/E/CulturalCo-operation/Culture/Resources/ReferenceTexts/Guidelines/ecubook_R3.asp

INDECS /Mezinárodní operabilita dat v systémech elektronického obchodu (e-commerce)/

Závěrečná zpráva. Srpen 2000. Dobrý příklad projektu metadat financovaného Evropskou komisí. Jeho cílem bylo podpořit rozvoj metadat způsoby, které umožňují automatizaci elektronického obchodu (*B-Commerce Systems*) na poli intelektuálního vlastnictví v síťovém prostředí.

<http://www.indecs.org/project.htm#finalDocs>

Úplný koncept managementu knihovny /TOLIMAC/

Upravená závěrečná zpráva. Dobrý příklad současného výzkumu zabezpečení knihovních systémů. TOLIMAC byl projekt sponzorovaný EU, který měl za cíl rozvoj manažerských systémů umožňujících bezpečnou výměnu elektronických informací mezi uživateli knihoven a poskytovateli informací přes Internet.

<http://www.tolimac.ulb.ac.be/>

Irsko

Irská knihovnická asociace

Autorský zákon a související právní normy 1999. Zpráva o strategii v oblasti autorského zákona /na stránce jsou k dispozici nejnovější informace/ týkající se legislativních iniciativ v Irsku a Evropské unii.

<http://www.libraryassociation.ie/policy/copyright.htm>

Velká Británie

Knihovnická asociace /VB/

Poradenská služba profesní organizace zaměřená na problémy elektronického obchodu (E-Commerce) v knihovnách. Poskytuje užitečné obecné informace o problému, ale nikoliv skutečné zásady .

http://www.la-hq.org.uk/directory/prof_issues/ity2525.html

Knihovnická asociace /VB/

Hlavní poznámky k použití filtrování (maskování) softwaru v knihovnách. Stručná doporučení zaměřená na povinnosti a zodpovědnost knihoven při používání filtrování softwaru. Webová stránka informuje o legislativní situaci ve Velké Británii, důvěrných informacích a soukromí, vzdělávání dospělých uživatelů i dětí a schopnosti aplikovat poznatky z využívání filtrace softwaru.

http://www.la-hq.org.uk/directory/prof_issues/filter2.html

Knihovnická asociace /VB/

Použití filtrování (maskování) softwaru v knihovnách. Rámcová informace o strategii přístupu Knihovnické asociace k využití filtrace softwaru.

http://www.la-hq.org.uk/directory/prof_issues/filter.html

Knihovnická asociace /VB/

Intelektuální svoboda a cenzura, 1998. Rozsáhlé vyjádření týkající se nezávislosti knihovníků na určitém fondu knihovny a přístupu k informacím prostřednictvím služeb knihovny. Užitečné jako pohled britských knihovníků na tuto otázku.

http://www.la-hq.org.uk/directory/prof_issues/ifac.html

Sdružení knihovnických asociací pro autorská práva /LACA/

Postoj LACA k problematice autorských práv v digitálním prostředí. Hlavní orgán Velké Británie lobující pro knihovní, informační a archivní profese a jejich uživatele v oblasti korektních praktik týkajících se autorských práv. V otázce autorských práv v digitálním prostředí citelně napadá pozici IFLA.

<http://www.cilip.org.uk/committees/laca/laca.html>

Národní rada zákazníků

Ochrana soukromí - zásady sběru a použití osobních dat. Červen 2001. Přehled poskytnutý skupinou zákazníků ve Velké Británii se zaměřením na všechny ty, kteří "sbírají, zpracovávají a využívají" osobní data - od firem, přes útvary vlády k marketingovým organizacím. Čtivé a užitečné.

http://www.ncc.org.uk/pubs/personal_privacy.htm

Velšská národní knihovna

Opatření na ochranu dat. Detailní a propracovaná strategie ochrany dat týkající se této malé národní knihovny se zaměřením na harmonizaci se Zákonem o ochraně dat ve Velké Británii z roku 1998. Může sloužit jako vhodný model pro mnoho typů knihoven.

http://www.llgc.org.uk/gwyb/data/dp_policy.pdf

Kancelář e-vyslanců

E-státní správa: Systém ověřování pravosti. Prosinec 2000. Součást strategie vlády v informačním věku ve Velké Británii. Tento dokument stanovuje rámec pro ověřování pravosti on-line operací při jednáních s poskytovateli služeb veřejnému sektoru.

<http://www.e-envoy.gov.uk/publications/frameworks/authentication/authentication.htm>

Tribe, A

Prezentace UKOLN: Webové stránky veřejných knihoven týkající se Zákonu o ochraně dat z roku 1998. Prezentace zaměřená na otázky nejlepších praktických zkušeností, které musí být akceptovány "web-manažery" knihoven v zájmu zajištění souladu se zákonem.

<http://www.ukoln.ac.uk/public/events/managing/tribe/plwmw2000/>

Univerzita v Leicesteru, univerzitní knihovna

Vyjádření k ochraně dat. 20. únor 2001. Příklad přístupu odborné knihovny k ochraně dat při respektování Zákona o ochraně dat z roku 1998. Spíše stručné, ale dobrý odrazový můstek pro vytvoření modelu.

<http://www.le.ac.uk/li/libservices/dataprot.html>