Usnesení

Rady vlády pro lidská práva
ze dne 28. listopadu 2008

k využívání kamerových a dalších sledovacích systémů

Rada vlády pro lidská práva

I. s c h v a l u j e podnět Výboru pro občanská a politická práva s úpravami podle připomínek Rady vlády pro lidská práva,

II. d o p o r u č u j e vládě, aby přijala komplexní právní úpravu problematiky provozování kamerových a dalších sledovacích systémů a

II. žádá předsedu Rady vlády pro lidská práva, aby v souladu s čl. 2 odst. 4 statutu Rady vlády pro lidská práva předložil prostřednictvím ministryně pro lidská práva návrh usnesení vlády.

N á v r h

U S N E S E N Í
vlády ze dne …… 2008 č. ……

k využívání kamerových a dalších sledovacích systémů

V l á d a

I. s c h v a l u j e podnět Rady vlády pro lidská práva k využívání kamerových a dalších sledovacích systémů;

II. u k l á d á ministru vnitra, aby

ve spolupráci s předsedou Úřadu pro ochranu osobních údajů vypracoval a vládě nejdéle do jednoho roku od přijetí tohoto usnesení předložil návrh komplexní právní úpravy využívání kamerových a dalších sledovacích systémů, zpracovávajících osobní údaje.
Návrh by měl obsahovat zejména:

1. oprávnění provozovat kamerové a další sledovací systémy výhradně buď k ochraně majetku a osob (soukromý a veřejný sektor), anebo na základě zvláštního zákona k definovaným účelům ve veřejném zájmu (veřejný sektor),

2. oprávnění veřejného sektoru provozovat kamerové a další sledovací systémy na základě zvláštního zákona jen na základě odůvodnění zvýšenou potřebou v místě a čase vyhodnotit získané informace pro plnění úkolů, s přesným vymezením místa, účelu a forem zpracování formou obecně závazného právního předpisu (vyhláškou),

3. povinnost provozovatelů kamerových a dalších sledovacích systémů zajistit, aby se co nejméně zpracovávaly osobní údaje bez výběru

4. povinnost provozovatelů kamerových systémů poskytnout jednoznačné informace o provozu kamerových systémů přímo na místě, které je sledováno prostřednictvím kamer, včetně hlubokého odkazu na informaci na Internetu s dalšími informacemi o zpracování osobních údajů (například okruhu příjemců, práva na přístup k vlastním údajům ad.)

5. omezení možnosti uchovávání záznamů získaných kamerovými systémy z míst veřejně přístupných maximálně po dobu, která odpovídá požadavkům § 5 odst. 1 písm. e) zákona o ochraně osobních údajů a která bude zveřejněna v rámci informací o systému, pro Policii ČR a městské policie a přísnou regulaci uchovávání záznamů kamerových systémů umožňujících identifikaci osob pro ostatní uživatele,

6. povinnost, aby při každé instalaci konkrétního kamerového systému bezpečnostním sborem byl vysvětlen a písemně zdokumentován účel instalace kamerového systému a na žádost zpřístupněn,

a to tak, aby tyto návrhy respektovaly i pravidla mezinárodních dokumentů uvedených v podnětu a

III. d o p o r u č u j e ministru vnitra, aby pravidelně předkládal Poslanecké sněmovně zprávu

o tom, kdy a jak konkrétně využití kamerového systému prokazatelně pomohlo v potírání kriminality.

Provede:
ministr vnitra

Na vědomí:
předseda Úřadu pro ochranu osobních údajů

Podnět Rady vlády pro lidská práva k využívání kamerových a jiných sledovacích systémů

1. Úvod

V posledních desetiletích došlo v Evropě, včetně České republiky, k prudkém rozvoji využívání kamerových systémů (mj. *Closed-Circuit Television*, CCTV) na veřejných místech i v místech, které veřejnosti nejsou běžně přístupné.

Současné sledovací systémy zvládají i pokročilé operace:

1. posílat záznamy do kontrolního centra z terminálů
2. nahrávat záznamy, které byly viditelné pouze prostřednictvím CCTV
3. získat záznamy s vysokým rozlišením a barevně je reprodukovat
4. sdružovat obrazové záznamy a zvuk
5. zvýšit zorné pole až na 360°
6. používat pevné či mobilní a rotační kamery
7. jsou schopny přibližovat objekty až do velmi podrobných detailů.

Mezi možnosti použití (resp. příklady praxe) kamerových systémů patří mimo jiné výměna záznamů mezi supermarkety navzájem, a to záznamů s „podezřelými" zákazníky či se zloději přímo chycenými. Nejnovější dnešní systémy umí identifikovat hlas nebo i konverzaci filmovaných osob a dokonce i porovnávat hlasový záznam s jiným, uloženým a indexovaným s identifikačními údaji původce. Již systémy z roku 1998 například dokázaly pracovat s prohledávací rychlostí 1000 záznamů za sekundu a obsahují i funkci rozpoznání obličeje osoby – při porovnání s databází (*face recognition*), noční vidění apod.

2. Právní úprava

Velmi podstatně se v jednotlivých zemích liší právní úpravy tohoto problému. Často jednotlivé právní úpravy rozlišují, zda systém využívá správní úřad (např. policie), nebo soukromá osoba, která ani nevykonává jakoukoli veřejnou moc (banky, čerpací stanice, obchody, atd.). Některé státy mají zřízeny pro zavádění kamerových systémů povolovací řízení či dozorové úřady, jiné ne. Rozlišováno také bývá tzv. užití pro dozor a užití pro prevenci.

V České republice chybí jasná a závazná pravidla, podle kterých by se měl řídit každý, kdo chce kamerové systémy užívat. Obecně se dá říci, že na ty záznamy z kamerových sledovacích systémů, které obsahují tváře či jiné identifikační znaky osob, lze v současné době vztáhnout režim zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů. Při ochraně soukromí lze také vycházet z pravidel obsažených v Listině základních práv a svobod, vyhlášené pod č. 2/1993 Sb., a dále např. z § 14 odst. 1 zákona č. 262/2006 Sb., nového zákoníku práce, ve znění pozdějších předpisů, podle něhož nesmí být, mimo jiné, zásah do oprávnění zaměstnanců v rozporu s dobrými mravy, z § 316 odst. 2 téhož zákona, který zakazuje zaměstnavateli narušovat soukromí zaměstnance na pracovišti bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele, a z §§ 11 až 13 zákona č. 40/1964 Sb., občanského zákoníku, ve znění pozdějších předpisů, tj. že obrazové a zvukové záznamy týkající se fysické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením nebo k účelům úředním na základě zákona. O mezinárodních instrumentech bude pojednáno v další kapitole.

Mimořádnými zmocněními ohledně zpracovávání osobních údajů získaných prostřednictvím kamerových systémů disponují Policie České republiky a obecní policie podle zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, a podle zákona č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů. Policie může pořizovat záznamy z míst veřejně přístupných a z průběhu služebních zásahů a úkonů. Na základě výjimky podle § 3 odst. 6 zákona o ochraně osobních údajů se na policii nevztahuje informační povinnost podle

tohoto zákona, avšak policie musí na základě § 42f odst. 2 zákona o policii o stálém umístění kamerových systémů vhodným způsobem informovat a zákon o Policii České republiky jí nařizuje, aby nejméně každé 3 roky prověřovala, zda uchovávané osobní údaje stále potřebuje pro plnění svých povinností.

Jiné osoby potřebují pro zpracovávání osobních údajů získaných prostřednictvím kamerových systémů právní titul, neboť se ve většině případů jedná o zpracování osobních údajů bez souhlasu subjektů údajů (vizte občanský zákoník) a musí subjekty údajů řádně informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny. Používání takového kamerového systému rovněž musí být podle zákona o ochraně osobních údajů řádně registrováno na Úřadu pro ochranu osobních údajů, pokud není naplněna některá z výjimek podle § 18 zákona o ochraně osobních údajů (např. kasina podle zákona č. 202/1990 Sb., o loteriích a jiných podobných hrách).

3. Mezinárodní právo

Na tomto poli existuje řada mezinárodních dokumentů, které mohou sloužit jako vodítko pro budoucí právní úpravu. Především jde o instrumenty Rady Evropy, které vychází ze základní premisy, že „veřejnost jako celek nesmí být zatížena nadměrnými zásahy zdůvodněnými potřebou předcházet nežádoucímu chování menšiny společnosti“.[1]

Ochranu při pořizování obrazových záznamů obsahuje především **Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat (CETS 108)**, jíž je Česká republika smluvní stranou. Zpracování osobních údajů ve formě záznamů z kamerových systémů spadá do požadavků čl. 5 (požadavky na kvalitu osobních údajů), čl. 7 (bezpečnost uchovávaných osobních údajů), čl. 8 (právo přístupu subjektu údajů ke „svým“ údajům), čl. 10 (sankce a náhrady za porušení povinností správce osobních údajů) a čl. 12 (přeshraniční pohyb osobních údajů), který je rozveden v **dodatkovému protokolu týkajícího se dozorových úřadů a přeshraničního toku údajů (CETS 181)** ze dne 8. listopadu 2001, který president republiky rovněž ratifikoval.

Na Úmluvu o ochraně jednotlivců se zřetelem na automatické zpracovávání osobních údajů navazují **doporučení Výboru ministrů Rady Evropy** k jednotlivým sférám, jde zejména o:

a) Doporučení č. R(87) 15 o nakládání s osobními údaji v policejním sektoru
b) Doporučení č. R(89) 2 o ochraně osobních údajů pro účely zaměstnávání
c) Doporučení č. R(95) 4 o ochraně osobních údajů i sektoru telekomunikací
d) různá další doporučení, výslovně sledování prostřednictvím kamer nezmiňující, která však obsahují záruky ochrany osobních údajů včetně těch souvisejících s používáním kamerových systémů.

Významným a pro účely navrhovaných legislativních změn klíčovým dokumentem jsou v rámci Rady Evropy vypracované **Principy pro ochranu jednotlivců ve vztahu k shromažďování a zpracovávání osobních údajů prostřednictvím kamerových systémů** (*Guiding principles for the protection of individuals with regard to the collection and processing of personal data by means of video surveillance*; dále jen „Vodítka pro kamery“).[2]

[1] Giovanni Buttareli: *Protection of personal data with regard to surveillance and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance*. Rada Evropy 2000

[2] http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/reports_and_studies_of_data_protection_committees/Q-Report_videosurveillance_2003.asp

Obsah Vodítek pro kamery – jakékoli sledování a záznam prostřednictvím kamer musí splňovat tyto podmínky:

1. Ověřit zda a do jaké míry je provoz kamery oprávněný, na explicitních právních základech a řádně provozovaný.
2. Přijmout taková opatření, aby byly dodrženy všechny principy a povinnosti v ochraně osobních údajů.
3. Používat kamerová zařízení pouze, pokud nelze využít jiné, k ochraně soukromí šetrnější, praktiky.
4. Dodržet vždy zásady výběrovosti a proporcionality ve vztahu k účelu sledování v každém jednotlivém případě, a to v zájmu ochrany svobody jednotlivce (souhlas subjektu údajů, minimálně konkludentně vyjádřený), zejména svobody pohybu a práva na informační sebeurčení (tj. oprávnění rozhodnout jaké osobní údaje budou poskytnuty jinému) a konečně i práva na rozumně očekávanou míru soukromí i na veřejných místech.
5. Dodržet princip, že osobní údaje musí být relevantní k danému účelu a nesmí tento účel překračovat s ohledem na shromažďovaný obrazový záznam, zvuk i biometrická data (rozsah zorného pole kamery, možnosti přibližování atd.) a zamezit odcizení, indexování (především sdružování) či dlouhodobému uchovávání osobních údajů (pokud nejde o specifické účely, kde je to nutné).
6. Zamezit kamerovému sledování pokud může vést k jakékoli formě diskriminace, anebo bylo zřízeno pro sledování určité skupiny osob výhradně definované jejich názory, vyznáním či sexuálním životem.
7. Dodržet princip transparentnosti, tj. zveřejňováním určitých kamerových systémů (nejlépe veřejně přístupným oznámením a nejlépe nezávislému dozorovému úřadu) a informováním subjektů údajů (pomocí viditelné a srozumitelné informace nebo piktogramu informujícího o umístění kamer). Omezení této transparentnosti je možné pouze z rozumných a přiměřených důvodů spočívajících v ochraně práv a svobod či účelů dle čl. 9 Úmluvy o ochraně jednotlivců se zřetelem na automatické zpracovávání osobních údajů.
8. Zajistit zesílenou ochranu soukromí v případě specifických rizik pro subjekty údajů či u invazivnějších technik, např.:
   a) sdružování obrazových záznamů a biometrických údajů,
   b) používání inteligentních analytických a intervenčních systémů,
   c) software pro automatické obnovování záznamů a pro rozpoznávání obličeje,
   d) různé další zpracovávání sbíraných údajů,
   e) profilování subjektů údajů, nebo
   f) kamery zřízené za účelem ovlivňování chování osob.
9. Zakázat sdělování osobních údajů třetím stranám jako obecné pravidlo, specifické případy výjimek musí být relevantní a zdůvodněné ve vztahu k účelu výjimky.
10. V případě uchování osobních údajů policií prostřednictvím automatických prostředků, které jsou výsledkem kamerového dozoru, mají být dále vztahy do úvahy zásady doporučení č. R (87) 15 o použití osobních údajů v policejním sektoru.
11. Připravit opatření pro zajištění oprávnění na přístup subjektů údajů ke svým zaznamenaným osobním údajům, s výjimkami jen pokud slouží k účelům čl. 9 Úmluvy o ochraně jednotlivců se zřetelem na automatické zpracovávání osobních údajů či ochraně práv a svobod.
12. Zamezit používání systémů určených k záměrnému sledování kvality a kvantity práce na pracovišti resp. pokud jsou provozovány z důvodů hodných zvláštního zřetele, plně informovat zaměstnance – přitom musí být vždy zachována lidská důstojnost zaměstnanců, včetně možnosti navazovat sociální a osobní vztahy na pracovišti. V případě chodu kamer musí mít zaměstnanci přístup k záznamům za účelem hájení svých oprávnění a nejlépe by měla být sjednána s odborovou organisací dohoda o používání kamer.

4. Nedostatky současného stavu a problémy možného řešení

1. Podmínky provozování kamerových systémů bez souhlasu, forma souhlasu subjektu údajů, rozsah povinně poskytovaných informací o účelu a rozsahu zpracovávaných informací nejsou pro oblast kamerových systémů používaných soukromoprávním osobami jasně stanoveny. V žádném případě neobstojí názor, že subjekt údajů dává vstupem do prostor označených jako sledované kamerami, souhlas s pořízením a uchováváním jeho osobních údajů (podoba, hlas). Podmínky na právní úkon, včetně jednostranného úkonu typu souhlasu, dává právní řád jasné: mj. svobodnou vůli. Svoboda volit zde zcela zřejmě dána není, neboť záznam na kameru je dnes již nedílnou podmínkou celé řady rutinních úkonů prakticky všech provozovatelů – návštěva banky, prodejny, MHD apod. Tudíž je třeba hledat právní titul pro možné zpracování osobních údajů bez souhlasu subjektů údajů: např. ochrana majetku (galerie).
2. Nedostatečné zohlednění *soft law* Rady Evropy, zejména Vodítek pro kamery.
3. Porušování zákona v této oblasti není řádně stíháno, protože o většině kamerových systémů se veřejné úřady nedozví.
4. Zákon o Policii České republiky a zákon o obecní policii mají závažné nedostatky, mezi něž patří především:
   a) Chybí garance proti nadužívání kamerových systémů.
   b) nedefinují dostatečně přesně rozsah a způsob, jakým mají být jednotlivci informováni o využívání kamerových systémů, a o právech a povinnostech využívání záznamů z těchto systémů jako důkazy v civilních sporech a jiných oblastech.
   c) Tříletá lhůta určená policistům i strážníkům zákonem pro prověřování potřebnosti uchovávaných osobních údajů je zřejmě příliš dlouhá.

Specifikum kamerového sledování oproti jinému běžnému zpracování osobních údajů spočívá v tom, že v případě obrazových informací na záznamu zpravidla nejde o fysické osoby správcem určené, ale pouze všeobecně na základě podoby nebo jiných prvků určitelné. Nic na tom nemění, že se v řadě případů jedná i o fysické osoby týmž správcem určené v jiném zpracování (zaměstnanci v personální agendě zaměstnavatele, obyvatelé domu v evidencích vedených v souvislosti se správou domu). Pro fysické osoby určené v jiném zpracování stejného správce se ovšem nebezpečí pro jejich soukromí ze sledování vyplývající výrazně zvyšuje. To však neznamená, že by měly mít při posuzování kamerového systému větší nebo jiná práva než fysické osoby pouze určitelné. V obou případech jde o subjekty údajů, jejichž práva musejí být rovná.

Popírání nebo bagatelizování významu kamerových systémů při potírání kriminality je neobjektivní. Tak jako řada jiných vynálezů či technologií, jsou i kamerové systémy jak využitelné, tak zneužitelné. Principem ochrany musí být, aby záznamy nedokumentující protiprávní jednání byly co nejrychleji smazány, aniž by je kdokoliv sledoval, ne aby pod záminkou realizace práva na přístup subjektu údajů, jímž je kdokoliv, kdo do sledovaného prostoru vstoupil nebo to jen prohlašuje, mohlo docházet k jinak nedůvodnému sledování záznamu provozovatelem kamerového systému.

Je třeba hledat cesty k tomu, aby kamery mohly být všeobecně vyžívány pro legitimní účely prevence kriminality a současně důsledným prosazením legislativních a technických opatření vyloučit nebo na minimum omezit možnosti jejich zneužití k indiskrétnímu sledování lidí.

Je zřejmé, že je nutné prosazovat zcela nové přístupy, při kterých se nelze jen opírat o směrnici 95/46/ES, o ochraně fysických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, která je v tomto případě nedostatečná. Oprávnění subjektu údajů na přístup je v případě informací o osobách určitelných kontraproduktivní, protože nutně vede k určování nejen subjektu údajů, ale i dalších osob na záznamu zobrazených s nevyhnutelným následkem zjištění údajů na záznamu o nich uchovaných.

Problematické je i ustanovení o výjimce pro zpracování výlučně pro osobní potřebu. Právě sousedské indiskrétní sledování kamerou je závažným problémem ochrany soukromí a tvoří podstatnou část stížností. Tyto skutečnosti (z hlediska § 12 a § 3 odst. 3 zákona č. 101/2000 Sb.) ukazují na nedostatečnost řešení problému kamerového sledování na základě zákona č. 101/2000 Sb., respektive směrnice 95/46/ES. Podle jednoho právního názoru se na základě čl. 3 směrnice nevztahuje na zpracování osobních údajů pro výkon výlučně osobních či domácích činností, tedy ani na kamery. Podle druhého právního názoru nelze považovat indiskrétní sledování za výlučně osobní či domáckou činnost ve smyslu směrnice, je třeba i takovéto obecné pojmy vyložit v souladu se smyslem směrnice, kterým určitě nebylo umožnit zásahy do soukromí tohoto typu na základě právě tohoto ustanovení. Postih právnických osob a podnikatelů za sledování kamerovými systémy je za této výjimky v každém případě jen polovičatým řešením, když každý *voyeur* může pro svou osobní a domácí potřebu indiskrétně sledovat kamerou své okolí a pořízené záběry o soukromí sousedů sobě a svým přátelům promítat, jak dlouho bude chtít. Je otázkou, zda pevnější půdu pro komplexní řešení nedává § 12 občanského zákoníku, jehož striktní výklad by už dnes mohl v některých případech vést k zákazu provozování kamerového systému rozhodnutím soudu. Při monitorování vymezeného prostoru kamerovým systémem sice nemusí docházet k cílenému pořizování obrazového záznamu konkrétní fysické osoby, současně však určité fysické osoby, které se většinou protiprávního jednání nedopouštějí, v některých případech nevyhnutelně musejí vstupovat do sledovaného prostoru, zejména v místě bydliště nebo v zaměstnání. Při monitorování se záznamem tedy nevyhnutelně dochází k pořizování obrazového záznamu těchto osob. Občanský zákoník přitom nerozlišuje mezi pořízením záznamu v soukromí nebo na veřejnosti. Je tedy v takovém zákonem nestanoveném případě pořízení takto získaného obrazového záznamu fysické osoby bez jejího svolení v souladu s občanským zákoníkem? Žádná judikatura v tomto ohledu není známa. Zákon o monitorování kamerovými systémy by se proto musel vztahovat na používání kamerových systémů jak právnickými, tak fysickými osobami, bez ohledu na to, zda jde o potřebu podnikatelskou nebo výlučně osobní, přičemž zvláštní důraz by měl být kladen na napevno instalované kamery.

Do budoucna se pro důsledné řešení problematiky kamerových systémů jako závažného fenoménu zasahujícího do soukromí lidí jeví jako možná pouze cesta kombinace legislativních a technických opatření (logování) blokovat nejen používání, ale i jakýkoliv přístup k pořízenému záznamu i pro samotného správce a přístup a použití záznamu omezit na zákonem výslovně stanovené situace – dokumentování jiným způsobem zjištěného protiprávního jednání ve sledovaném prostoru s přesně stanoveným omezením zdůvodnitelné doby pro uchovávání záznamu. Legislativní základ pro takové řešení by bylo možné nacházet v zákoně č. 101/2000 Sb. Neposuzuje Úřad pro ochranu osobních údajů provozování kamerového systému se záznamem jako automatizované zpracování osobních údajů? Nestanoví § 13 odst. 4 písm. c) zákona č. 101/2000 Sb., že v oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel povinen pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány?

V každém případě by šlo o opatření, která by zasáhla do dosud nijak neomezovaného trhu s kamerami a nutně by tedy vyvolala silné lobbyistické tlaky. Mnoho stávajících kamerových systémů by zřejmě přísnější zákonem stanovené parametry nesplňovalo a muselo by být odstraněno. Na druhou strany by to mohlo znamenat nový *boom* pro výrobce „*privacy safe cameras*“. Pouze „české řešení“ by však pravděpodobně nemělo naději na úspěch. Zřejmě by přitom byla nutná zcela nová koordinovaná celoevropská strategie, pokud je ovšem zájem tento závažný problém ochrany soukromí opravdu důsledně řešit, např. v rámci pracovní skupiny TWG.

5. Závěr

Informační společnost bude přinášet nové a nové technologie zasahující do soukromí lidí. Ochránci osobních údajů přitom budou vždy v menšině a defenzivě. Naději na úspěch má jen

umožnit využití nových technologií pro legitimní účely, kýmkoliv a kdekoliv, a znemožňovat jejich zneužití pro účely nelegitimní, kýmkoliv a kdekoliv.

V souvislosti se stále rozšířenějším využíváním kamer pro soukromé účely a rostoucímu počtu kontroversí ohledně jejich je třeba říci, že záběr kamery, která je využívána k ochraně soukromého majetku, by měla být využíván pouze k ochraně tohoto soukromého majetku, tudíž by neměla:

a) monitorovat veřejné prostranství, jak je definováno v § 34 zákona č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů, tj. „všechna náměstí, ulice, tržiště, chodníky, veřejná zeleň, parky a další prostory přístupné každému bez omezení, tedy sloužící obecnému užívání, a to bez ohledu na vlastnictví k tomuto prostoru“ a

b) monitorovat soukromý majetek jiné osoby.

Při dodržení těchto podmínek by bylo možné odbřemenit Úřad pro ochranu osobních údajů tak, že by takový kamerový systém nepodléhal oznamovací povinnosti. Jedině legálně získaný důkaz může být použit jako důkaz. Legislativní úprava v podobě komplexní úpravy kamer, která se bude vztahovat též na bezpečnostní sbory, se tak jeví jako nezbytná; její nedostatek v jasné podobě způsobuje právní nejistotu a roztříštěnou praxi dozorových úřadů. To by mělo být uspokojivě zajištěno přijetím doporučovaných legislativních a z nich vyplývajících rozpočtových opatření.