

## **Doporučení Výboru pro občanská a politická práva ohledně provozu kamerových systémů**

Konkrétní doporučení na změnu legislativy a praxe v oblasti provozu kamer jak státními složkami, tak soukromými subjekty. Dnes je velká většina z nich používána bez zákonné opory, přičemž jde o technologii velmi zneužitelnou. Cílem doporučení připraveného IuRe je vnést do používání kamer jasná pravidla a záruky ochrany osobních údajů a práva na soukromí.

usnesení Výboru pro občanská a politická práva k využívání kamerových systémů

I.Návrh usnesení Rady pro lidská práva

**1/RLP doporučuje vládě, aby uložila ministerstvu vnitra, Úřadu pro ochranu osobních údajů *ev. dalším resortům* připravit novelizaci zákonů o Policii ČR, zákona o obecní policii a zákona o ochraně osobních údajů s ohledem na tato doporučení:**

**2/Novelizovat zákon č. 283/1991 Sb., o Policii ČR a zákon č. 553/1991 Sb., o obecní policii, tak, aby tyto zákony obsahovaly povinnost poskytnout o provozu kamerových systémů jasnou informace na místě, které je sledováno**

**3/Novelizovat zákon č. 283/1991 Sb., o Policii ČR zákon č. 553/1991 Sb., o obecní policii, tak, aby tyto zákony stanovily, že uchovávání záznamů získaných kamerovými systémy z míst veřejně přístupných je možné pouze 1 týden**

**4/Přijmout níže uvedenou legislativní úpravu – variantní řešení, přičemž na varianty volí zpracovatel úpravy.**

**Varianta A:**

**Novelizovat zákon č. 101/2000 Sb., o ochraně osobních údajů tak, aby zákon stanovil, že informace o využívání kamerových systémů (rozsahu, účelu, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny) musí být jasně umístěna na místě sledovaném příslušným systémem. Případné záznamy z těchto systémů mohou být uchovávány maximálně 1 týden.**

#### **Varianta B:**

**Novelizovat zákon č. 101/2000 Sb., o ochraně osobních údajů, tak, aby zakazoval všem subjektům mimo policejních uchovávat a zpracovávat záznamy umožňující identifikaci osob**

**5/Zajistit implementaci dalších požadavků Směrnice Rady Evropy 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) do právních předpisů.**

**Umožnit kapacitně posílit Úřad na ochranu osobních údajů pro účely dozoru nad dodržováním zákona v oblasti sledování kamerami.**

**2RLP vyjadřuje svou podporu rozšíření kapacit Úřadu na ochranu osobních údajů tak, aby byl schopen vypořádat se s nárůstem agendy spojené s kontrolní činností v oblasti využívání kamerových systémů**

4)dodržet vždy zásady výběrovosti a proporcionality ve vztahu k účelu sledování v každém jednotlivém případě a to v zájmu ochrany svobody jednotlivce (kde je to možné, svoboda zahrnuje souhlas subjektu údajů, minimálně konkludentně vyjádřený), zejména svobody pohybu a práva na informační sebeurčení (tj. práva rozhodnout jaké osobní údaje budou poskytnuty jiné osobě či instituci) 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)

## II. Odůvodnění

V posledních desetiletích došlo v Evropě i v České republice k prudkému rozvoji využívání kamerových systémů (mj. Closed-Circuit Television – CCTV) na veřejných místech i v místech, které veřejnosti nejsou běžně přístupné. V průměru v Evropě používá tyto systémy 29 procent veřejně přístupných institucí. [1](#)

Velmi podstatně se v jednotlivých zemích liší právní úpravy tohoto problému. Často jednotlivé právní úpravy rozlišují, zda systém využívá státní orgán (např. policie), či fyzická či právnická osoba (banky, čerpací stanice, obchodní domy). Některé země mají zřízeny pro zavádění kamerových systémů povolovací řízení, či dohledové orgány, jiné ne.

Rozlišováno také bývá tzv. užití pro kontrolu a užití pro prevenci.

V České republice chybí jasné ustanovení, 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 o ochraně osobních údajů. Při ochraně soukromí lze také vycházet z Listiny základních práv a svobod čl. 10 o zachování lidské důstojnosti a ochraně před neoprávněným zasahováním do soukromého a osobního života, z ustanovení zákoníku práce § 7 odst. 2, podle něhož nesmí být mimo jiné zásah do práv zaměstnanců v rozporu s dobrými mravy, a z občanského zákoníku § 11 až 13.

Mimořádnými zmocněními ohledně zpracovávání osobních údajů získaných prostřednictvím kamerových systémů disponují Policie ČR a městské či obecní policie. Policie může pořizovat záznamy z míst veřejně přístupných a z průběhu služebních zásahů. Musí ale o stálém umístění kamerových systémů vhodným způsobem informovat a zákon jí nařizuje, aby nejméně každé tři roky prověřovala, zda uchovávané osobní informace stále potřebuje pro plnění svých povinností.

Jiné právnické a fyzické subjekty pro zpracovávání osobních údajů získaných prostřednictvím kamerových systémů potřebují souhlas subjektu údajů a musí jej

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 řádně registrováno na Úřadu pro ochranu osobních údajů.

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

Ochranu při pořizování obrazových záznamů obsahuje především **Úmluva č. 108 (Úmluva o ochraně jednotlivců se zřetelem na automatické zpracovávání osobních údajů)**.

Zpracování osobních údajů ve formě záznamů z kamerových systémů spadá do požadavků článku 5 (požadavky na kvalitu osobních údajů), článku 7 (bezpečnost uchovávaných osobních údajů), článku 8 (právo přístupu subjektu údajů ke „svým“ údajům), článku 10 (sankce a náhrady za porušení povinností správce osobních údajů) a článku 12 (přeshraniční pohyb osobních údajů).

Na Úmluvu č. 108 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 **Směrnice 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 Směrnice o kamerových systémech.

### **Obsah směrnice:**

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. Kamerové systémy pro policejní účely mohou být provozovány pouze pro účely prevence reálného nebezpečí nebo potlačování specifických trestných činů.

2) přijmout taková opatření, aby byly dodrženy všechny principy a povinnosti na úseku ochrany osobních údajů

3) používat kamerová zařízení pouze pokud nelze využít jiné, k ochraně soukromí šetrnější praktiky

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 nejlépe nezávislému dozorovému orgánu) a informováním subjektů údajů (pomocí viditelné a srozumitelné informace nebo piktogramu informujících 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 č. 108.

8) zajistit **zesílenou ochranu** soukromí v případě specifických rizik pro subjekty údajů či u invazivnějších technik, např.:

- **sdužování obrazových záznamů a biometrických údajů;**
- **používání inteligentních analytických a intervenčních systémů;**
- **software pro automatické obnovování záznamů a pro rozpoznávání obličejů;**
- **různé další zpracovávání sbíraných údajů;**
- **profilování subjektů údajů;**
- **možnost přijímání automatických rozhodnutí na základě získaných údajů ohledně profesionálních schopností, výkonu, spolehlivosti či etnického původu;**

**- 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) připravit opatření pro **zajištění výkonu práva na přístup subjektů údajů** ke svým osobním zaznamenaným údajům, s výjimkami jen pokud slouží k účelům čl. 9 Úmluvy č. 108 či ochraně práva a svobod.

11) **zamezit používání systémů určených k záměrnému sledování kvality a kvantitativní práce na pracovišti** resp. pokud jsou provozovány, 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 nároků a nejlépe by měla být dohoda o používání kamer sjednána s odborovým orgánem.

Nedostatky současného stavu

1/Zákony o Policii ČR a obecní policii nedefinují dostatečně přesně rozsah a způsob, jakým mají být občané informováni o využívání kamerových systémů, a o právech a povinnostech využívání záznamů z těchto systémů jako důkazy v civilních sporech a jiných oblastech.

2/Tříletá lhůta nařízená Policii ČR i obecní policii zákonem pro prověřování potřebnosti uchovávaných osobních údajů je příliš dlouhá.

3/Forma povinného souhlasu subjektu údajů, rozsah povinně poskytovaných informací o účelu a rozsahu zpracovávaných informací nejsou pro oblast kamerových systémů používaných právnických a fyzických subjektů 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). Nároky na právní úkon, včetně jednostranného úkonu typu souhlasu, dává právní řád jasně: 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.

4/Nedostatečné zohlednění soft-law Rady Evropy, zejména Směrnice o kamerových systémech.

5/Porušování zákona v této oblasti není řádně stíháno.

Návrh řešení

Nezbytná je zde legislativní úprava; její nedostatek v jasné podobě způsobuje právní nejistotu, roztržitou praxi a nemožnost efektivních zásahů kontrolních orgánů.

Pokud bude v návrhu nového trestního zákona přijata skutková podstata § 158 kriminalizující zneužívání záznamů a písemností uchovávaných v soukromí, bude částečně neoprávněné použití záznamů z kamerových systémů trestněprávní koncovku, což je žádoucí, nicméně hlavní je stanovit jasná pravidla pro provozování kamerových systémů.

To by mělo být uspokojivě zajištěno přijetím doporučovaných legislativních a rozpočtových opatření.