05. január 2012 07:56

Autor:  [Ondrej Zimen](http://www.penonline.sk/autor/ondrej-zimen)

**Neoprávnené zásahy kamerového systému do súkromia fyzickej osoby**

Zamysleli ste sa už niekedy nad tým, ako je to s monitorovaním vašej osoby prostredníctvom kamerových systémov?! Ako sa na túto problematiku pozerá slovenský právny poriadok?

Každého z nás sa viac či menej dotýka využívanie kamerových systémov rôznymi subjektmi a na rôzne účely. Pomocou kamier nás monitorujú, zaznamenávajú a vyhotovujú obrazové resp. audiovizuálne záznamy, ktorých imanentnou súčasťou sú rôzne údaje, ktorých povaha je predurčená oscilovať okolo čl. 19 ods. 2 a ods. 3 Ústavy Slovenskej republiky, kde sú zakotvené základné práva týkajúce sa ochrany súkromia občana.[[1]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftn1)

Problematika právnej úpravy použitia kamerového systému je popretkávaná ako vlákna pavučiny cez rôzne právne odvetvia do siete, v ktorej uviazli rôzne proti sebe stojace právom chránené záujmy. V nasledujúcom článku sa preto pokúsim systematizovať a charakterizovať súvisiace časti nášho právneho poriadku v rámci dotknutých právnych odvetví.

**Správne právo**

Kľúčovou právnou normou z hľadiska aplikácie spomenutých ústavných článkov je zákon na ochranu osobných údajov č.428/2002 Z.z. v znení neskorších predpisov (ďalej len „zákon č. 428/2002 Z.z.“). V kontexte využívania kamerového systému zákon č. 428/2002 Z.z. stanovuje striktné pravidlá pre prevádzkovateľa takéhoto informačného systému brániace potenciálnemu zneužitiu vyhotoveného záznamu.

Z dikcie zákona č.428/2002 Z.z. vyplýva, že *priestor prístupný verejnosti, je možné monitorovať pomocou videozáznamu alebo audiozáznamu, ale len na účely zabezpečovania verejného poriadku a bezpečnosti, odhaľovania kriminality alebo narušenia bezpečnosti štátu, a to len vtedy, ak je snímaný priestor zreteľne označený ako monitorovaný.*[[2]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftn2)  Označenie o monitorovaní priestoru kamerovým systémom nie je potrebné ak tak určuje osobitný zákon. (napr. zákon č.483/2001 Z.z. o bankách a o zmene a doplnení niektorých zákonov).

Vyhotovený záznam možno využiť len na účely trestného konania alebo konania o priestupkoch, ak osobitný zákon neustanovuje inak. Ak takto vyhotovený záznam nie je využitý na vyššie uvedené účely je nevyhnutné ho zlikvidovať v lehote siedmich dní odo dňa nasledujúceho po dni, v ktorom bol záznam vyhotovený.

Takže v podstate každé použitie kamerového systému na miestach prístupných verejnosti subjektmi rôznej povahy[[3]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftn3) (napr. najčastejšie podnikatelia, obce či správcovia bytových družstiev) spadá pod úpravu zákona č. 428/2002 Z.z. Tieto subjekty, ktoré kamerové systémy z rôznych dôvodov využívajú na monitorovanie verejne prístupných miest majú postavenie prevádzkovateľa informačného systému v zmysle § 4 ods. 2 zákona č. 428/2002 Z.z. Dozor pri ochrane súkromia fyzických osôb nad takýmito prevádzkovateľmi, s výnimkou spravodajských služieb, vykonáva Úrad na ochranu osobných údajov SR, ktorý vykonáva aj osobitnú registráciu týchto subjektov a môže za rôzne porušenia zákona č. 428/2002 Z.z. udeliť pokutu vo výške od 10 000 Sk (331,93 EUR) do 10 000 000 Sk (33.193,91 EUR).

**Trestné právo**

V rámci trestného práva má použitie kamerového systému povahu tzv. ITP, t.j. informačno-technického prostriedku (ďalej len „ITP“). ITP môžu používať iba Policajný zbor, Slovenská informačná služba, Vojenské spravodajstvo, Zbor väzenskej a justičnej stráže a Colná správa v rozsahu podľa osobitných predpisov, ktorými sú jednotlivé osobitné zákony (ďalej len „oprávnené štátne orgány“), ktorými je upravená pôsobnosť a činnosť týchto štátnych orgánov a zároveň v intenciách zákona č. 166/2003 Z.z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním).

Využitie ITP je možné iba vtedy, ak je to *v demokratickej spoločnosti nevyhnutné na zabezpečenie bezpečnosti štátu, obranu štátu, predchádzanie a objasňovanie trestnej činnosti alebo na ochranu práv a slobôd iných. Použitím informačno-technického prostriedku sa môže základné právo alebo sloboda obmedziť len v nevyhnutnom rozsahu a nie dlhšie, ako je to nevyhnutné na dosiahnutie zákonom uznaného cieľa, na ktorý slúži.*[[4]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftn4) To znamená, že aj údaje získané prostredníctvom ITP možno použiť výhradne v súlade s uvedeným účelom. Strážcom ústavy a zákona je v prípadoch použitia ITP zákonný sudca udeľujúci oprávneným orgánom štátu písomný súhlas na ich použitie a preverujúci účel a dôvody aplikácie ITP počas celej doby, v ktorej ich oprávnené orgány štátu používajú. Bez takéhoto súhlasu resp. dodatočného písomného súhlasu[[5]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftn5) nesmú byť informácie získané prostredníctvom ITP použité a musia byť bezodkladne zničené. Tiež nie je možné takéto informácie použiť ako dôkaz v trestnom konaní, keďže trestné právo explicitne vyžaduje, aby sa použitý dôkaz získal zákonným spôsobom.

Takže typické využitie kamerového systému v podmienkach relevantných pre odvetvie trestného práva, čiže vyhotovovanie záznamov utajovaným spôsobom oprávnenými štátnymi orgánmi na zisťovanie, odhaľovanie a dokumentovanie trestnej činnosti, si pochopiteľne nevyžaduje žiadne zreteľné označenie monitorovaného priestoru ako pri využívaní kamier prevádzkovateľmi podľa § 4 ods. 2 zákona č. 428/2002 Z.z. či súhlas dotknutých osôb.

Popri zákonnom sudcovi dozerá na dodržiavanie práva na súkromie aj Úrad na ochranu osobných údajov SR, ktorý vo vzťahu k oprávneným štátnym orgánom (s výnimkou SIS, VOS a VSS)[[6]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftn6) vykonáva svoju pôsobnosť, avšak z ohľadom na výrazné obmedzenia vyplývajúce z § 2 zákona č. 428/2002 Z.z.

Z hľadiska vzniku trestnej zodpovednosti v kontexte s neoprávneným zásahom kamerového systému do súkromia fyzickej osoby prichádzajú do úvahy najmä trestné činy podľa § 194a Ochrana súkromia v obydlí, § 374 Neoprávnené nakladanie s osobnými údajmi a tiež § 377 Porušenie dôvernosti ústneho prejavu a iného prejavu osobnej povahy zákona č. 300/2005 Z.z. Trestný zákon v znení neskorších predpisov.

**Pracovné právo**

Využívanie kamerového systému v rámci pracovnoprávnych vzťahov zamestnávateľom na monitorovanie pracoviska a diania na ňom je často diskutovanou témou, ktorá vždy značne polarizuje diskutujúce strany. Hodnotenie argumentov jednotlivých strán z dôvodu vecnosti preskočím a uspokojím sa s konštatovaním, že je vždy vecou zamestnávateľa či sa pre takýto krok rozhodne.

Avšak v prípade, že zamestnávateľ na pracovisku nainštaluje kamerový systém je povinný mať na zreteli znenie čl. 11 zákona č. 311/2001 Z.z. Zákonník práce v znení neskorších predpisov (ďalej len „ZP“), ktorý vo vzťahu k zákonu č. 428/2002 Z.z. predstavuje pre tento prípad lex specialis avo vzťahu k pracovnoprávnym vzťahom jednu zo základných zásad.

*Zamestnávateľ môže o zamestnancovi zhromažďovať len osobné údaje súvisiace s kvalifikáciou a profesionálnymi skúsenosťami zamestnanca a údaje, ktoré môžu byť významné z hľadiska práce, ktorú zamestnanec má vykonávať, vykonáva alebo vykonával. Zamestnávateľ nesmie bez vážnych dôvodov spočívajúcich v osobitnej povahe činností zamestnávateľa narúšať súkromie zamestnanca na pracovisku a v spoločných priestoroch zamestnávateľa tým, že ho sleduje bez toho, aby bol na to upozornený, alebo kontroluje listové zásielky adresované zamestnancovi ako súkromnej osobe. Ak je u zamestnávateľa zavedený kontrolný mechanizmus, je zamestnávateľ povinný informovať zamestnanca o rozsahu kontroly a spôsoboch jej uskutočňovania.*[[7]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftn7)

Pri aplikácii kamerového systému v súlade s čl. 11 ZP nepotrebuje zamestnávateľ súhlas dotknutých osôb, t.j. zamestnancov a tento informačný systém taktiež v zmysle § 25 ods.2 písm. e) zákona č. 428/2002 Z.z. nepodlieha registrácii.

V prípade, že sa zamestnávateľ rozhodne monitorovať pracovný proces takýmto spôsobom mal by si určite zapracovať do svojich interných právnych aktov ustanovenie o využívaní kamerového systému, s ktorým by preukázateľne oboznámil svojich zamestnancov a nemal by kamery inštalovať na toaletách, šatniach, sprchách a podobných miestach, kde by mohlo dôjsť k neprimeraným a neodôvodnením zásahom do súkromia zamestnancov. Kontrolný mechanizmus na sledovanie zamestnanca je legitímny za podmienky, že zamestnanca o kontrole zamestnávateľ informuje a súčasne ho informuje aj o rozsahu takejto kontroly a spôsobe jej uskutočňovania.[[8]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftn8)

Ako problematický bod z hľadiska ochrany osobných údajov sa môže javiť na prvý pohľad fakt, že obrazový záznam vyhotovený kamerovým systémom má povahu osobitnej kategórie osobného údaju, keďže o identifikovaných resp. identifikovateľných fyzických osobách odhaľuje dodatočnú informáciu v zmysle § 8 ods. 1 zákona č. 428/2002 Z.z.. Evidentne do úvahy prichádza najmä rasový alebo etnický pôvod, ktorý je z obrazového záznamu zrejmý na prvý pohľad. Avšak v prípade vyhotovovania obrazových záznamov zamestnávateľom v súlade s článkom 11 ZP možno konštatovať, že pôjde o výnimku z obmedzenia pri spracúvaní osobitných kategórií osobných údajov v zmysle § 9 ods. 1 písm. a) zákona č. 428/2002 Z.z., a teda takéto spracúvanie osobných údajov nebude zakázané

**Občianske právo**

Použitie kamerového systému má relevanciu v rámci občianskoprávnych vzťahov hlavne z pohľadu zásahu do integrity osobnosti človeka. Predmetom ochrany ľudskej osobnosti je v našom právnom poriadku podľa ustanovenia § 11 zákona č.40/1964 Zb. v znení neskorších predpisov (ďalej len „OZ“)najmä život a zdravie, občianska česť a ľudská dôstojnosť, súkromie, meno a prejavy osobnej povahy.

OZ v. § 12 ods. 1 upravuje aj právo na ochranu písomností osobnej povahy, podobizní, obrazových snímkov, ale hlavne právo na ochranu pred vyhotovením alebo použitím obrazových a zvukových záznamov týkajúcich sa fyzickej osoby alebo jej prejavov osobnej povahy bez súhlasu tejto osoby. Práve toto právo je kľúčové z hľadiska použitia kamerového systému v zmysle neoprávneného zásahu do osobnosti človeka, keďže právnu ochranu požívajú práve imateriálne stránky ľudskej osobnosti, ktoré sú zachytené na určitom hmotnom substráte, teda v tomto prípade na pamäťovom disku prípadne na VHS páske.

Podmienkou poskytnutia občianskoprávnej ochrany osobnosti je neoprávnený zásah do jej osobnostných práv (§ 11 a nasl. OZ). Neoprávnený zásah musí byť spôsobilý privodiť ujmu osobnosti človeka. Porušením práva na ochranu súkromia pritom nie je len neoprávnené získavanie vedomostí a poznatkov o súkromí fyzickej osoby, ale aj neoprávnené rozširovanie týchto poznatkov a vedomostí. Dôsledkom neoprávneného zásahu do práva na súkromie môže byť zníženie dôstojnosti alebo vážnosti v spoločnosti v značnej miere, pritom však tento dôsledok nie je jediným právom požadovaným prejavom závažnosti ujmy spôsobenej fyzickej osobe.[[9]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftn9) Za neoprávnený zásah nemožno považovať: a) existenciu tzv. zákonných licencií podľa § 12 ods. 2 až 3 OZ, b) okolnosti vylučujúce protiprávnosť, c) súhlas dotknutej osoby daný nad rámec zákonnej licencie.

Občanovi, ktorému neoprávnený zásah kamerového systému do osobnostných práv spôsobil ujmu má k dispozícii klasický triumvirát občianskoprávnych žalôb prostredníctvom, ktorých môže uplatniť svoje právo na súdnu ochranu. Poškodený občan môže podať na príslušný všeobecný súd: a) negatórnu žalobu (návrh na upustenie od neoprávneného zásahu), b) reštitučnú žalobu (návrh na odstránenie následkov zásahu), c) satisfakčnú žalobu (návrh na poskytnutie primeraného zadosťučinenia).

Ochrana osobnosti je v občianskom práve konštituovaná na princípe objektívnej zodpovednosti, takže na vznik zodpovednosti nie je potrebné zavinenie subjektu neoprávneného zásahu. Dokonca podľa judikatúry Ústavného súdu Slovenskej republiky (sp. zn. I. US 155/07 zo dňa 3.12.2008) je možné aby bola v prípade medializácie informácie za určitých kumulatívne naplnených okolností spoluzodpovedná aj iná osoba, ktorá ju médiám poskytla.

**Záver**

Možno konštatovať, že vytvorená legislatíva upravujúca využívanie kamerového systému sa javí z pohľadu ochrany súkromia fyzickej osoby ako dostatočná. Primerane zohľadňuje váhu proti sebe stojaceho práva na súkromie fyzických osôb ako aj verejný záujem na ochrane spoločnosti pred rôznymi nežiaducimi javmi. Dostatočné možnosti právnej ochrany či existujúce kontrolné mechanizmy však nikdy nebudú automaticky znamenať, že naše práva nebudú porušované neoprávnenými zásahmi. Je len na každom z nás či dovolí „veľkému bratovi“, nad nevyhnutný zákonom umožnený rámec, bez následkov nazerať do svojho súkromia a osobných údajov.

[[1]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftnref1) právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života, právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe
[[2]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftnref2) § 10 ods. 7 zákona na ochranu osobných údajov č.428/2002 Z.z. v znení neskorších predpisov
[[3]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftnref3) Bližšie pozri § 4 ods. 2 zákona č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov
[[4]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftnref4) § 3 ods. 1 zákona č. 166/2003 Z.z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním)
[[5]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftnref5) § 5 ods. 2 zákona č. 166/2003 Z.z. o ochrane súkromia pred neoprávneným použitím informačno-technických prostriedkov a o zmene a doplnení niektorých zákonov (zákon o ochrane pred odpočúvaním)
[[6]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftnref6) SIS – Slovenská informačná služba, VOS – Vojenské obranné spravodajstvo, VSS – Vojenská spravodajská služba
[[7]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftnref7) Čl. 11 zákona č. 311/2001 Z.z. v znení neskorších predpisov (Zákonník práce)
[[8]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftnref8) Barancová H., Schronk R. Pracovné právo. Sprint. Bratislava 2007. S 141
[[9]](http://www.penonline.sk/pravne-oblasti/spravne-pravo/analyzy-a-studie/neopravnene-zasahy-kameroveho-systemu-do-sukromia-fyzickej-osoby#_ftnref9) ULC Čarnogurský. Ochrana osobnosti. PRO BONO 11