Spolok pre ochranu osobných údajov

Kamery na všetkých školách s využitím umelej inteligencie

Stanovisko Spolku pre ochranu osobných údajov

Bratislava, 11. novembra 2024

Spolok pre ochranu osobných údajov vyjadril znepokojenie nad vládnym návrhom na plošné využitie kamerových systémov s umelou inteligenciou na základných a stredných školách. Podľa schváleného materiálu by mali kamery zabezpečiť rozpoznávanie osôb s cieľom zvýšiť bezpečnosť v školskom prostredí. Spolok však upozorňuje, že takéto riešenie prináša otázky súvisiace s ochranou osobných údajov, najmä pokiaľ ide o nevyhnutnosť, rozsah a bezpečnosť takéhoto spracúvania, ako požaduje legislatíva GDPR. Poukázal tiež na vysoké požiadavky, ktoré na systém tohto druhu kladie aj Nariadenie o umelej inteligencii (AI Act), pretože ide o vysoko rizikové operácie. Podľa Spolku nie sú dostatočne zdôvodnené riziká ani efektívnosť takého monitoringu, najmä s ohľadom na prevenciu špecifických hrozieb. Odborníci na ochranu osobných údajov navrhujú, aby sa zvážili aj menej invazívne alternatívy, ktoré by dokázali efektívne prispieť k vytýčeným cieľom bezpečnosti na školách.

Spolok pre ochranu osobných údajov vníma so znepokojením materiál „Systémové riešenie bezpečnosti osôb v objektoch základných a stredných škôl a v ostatných rizikových objektoch s prístupom verejnosti“ schválený vládou SR na svojom 48. zasadnutí, ktoré sa konalo dňa 11.9.2024 (ďalej aj ako „materiál“).

Podľa schváleného materiálu by mali byť na všetky školy na Slovensku umiestnené kamery na snímanie žiakov, učiteľského zboru a personálu na školách za pomoci umelej inteligencie tak, aby bolo možné včas odlíšiť osoby s príslušnosťou k danej školy od nepovolaných osôb (detekcia tváre s následnou identifikáciou základných tvárových charakteristík). Účelom má byť snaha zabrániť násiliu páchaného na školách, šíreniu drog a zabrániť e-mailovým útokom o výbušných látkach umiestnených na školách.

Takto popísaný účel a rozsah spracúvaných osobných údajov môže byť podľa názoru Spolku pre ochranu osobných údajov v rozpore so základnými zásadami spracúvania osobných údajov, ktoré od každého prevádzkovateľa vyžaduje GDPR. Ani predchádzanie trestnej činnosti by nemalo byť dôvodom na snímanie podobizní v takom veľkom rozsahu, pokiaľ nie je zrejmé, že prispeje k naplneniu stanoveného účelu. Už z vymedzeného účelu je pritom zrejmé, že kamerový záznam nemôže žiadnym spôsobom prispieť k nedoručeniu e-mailovej správy o umiestnených výbušných látkach na školách. Ak má kamera so zabudovanou umelou inteligenciou vedieť rozlišovať cudzie osoby od žiakov, rovnako zrejme nezabráni možným útokom, ktoré podľa medializovaných správ a vyššie uvedeného materiálu páchajú

najčastejšie práve žiaci, či bývalí študenti týchto škôl. Systém by podľa predloženého materiálu tieto osoby automaticky vyhodnotil ako známe osoby.

Z metodických usmernení a kontrolnej činnosti dozorujúcich orgánov naprieč celou Európskou úniou, slovenský Úrad na ochranu osobných údajov nevynímajúc, vyplýva, že kamerové záznamy sa považujú za masívny zásah do práv občanov, a preto by sa mala pri takom spracúvaní zachovať zásada minimalizácie spracúvania osobných údajov a ich uchovávania a najmä nevyhnutnosť spracúvania. Za minimalizáciu sa považuje umiestnenie kamier naozaj len na tie objekty, kde preukázateľne došlo k protiprávnej činnosti, ktorú je možné kamerovým systémom zachytiť. Kamery by nemali byť umiestnené len „preventívne", a to na akékoľvek typy útokov. Minimalizácia uchovávania znamená uchovanie na maximálne 72 hodín, v závažne odôvodnených prípadoch aj viac, čo však vyžaduje podrobné zdôvodnenie zo strany prevádzkovateľa systému. Z predloženého materiálu však nie je dostatočne zrejmé, kto a v akom rozsahu bude tieto záznamy vyhodnocovať, aby bolo možné včas zasiahnuť.

Spolok pre ochranu osobných údajov preto pri tak zásadnom materiáli očakával, že z neho bude vyplývať:

- Kto bude prevádzkovateľom pri spracovaní osobných údajov;
- Odôvodnenie legitimity a legality účelu pre spracúvanie osobných údajov;
- Právny základ spracúvania osobných údajov;
- Posúdenie vplyvu pri spracúvaní osobných údajov (riziková analýza).

Spolok pre ochranu osobných údajov si dovoľuje v tomto bode zdôrazniť, že v prípade vysokej rizikovosti je povinná predchádzajúca konzultácia s Úradom na ochranu osobných údajov. Riziková analýza je pritom povinná ešte pred samotným zamýšľaním začatia spracúvania osobných údajov, t.j. podľa názoru Spolku mala byť vykonaná ešte predtým, ako bol materiál predložený na rokovanie vlády.

Pritom nasadenie kamerových systémov pre systematické monitorovanie osôb v školách (žiakov, učiteľov, rodičov) so sebou prináša nasledovné riziká spojené zo zásahom do ich súkromia:

- Z predloženého materiálu vyplýva, že hovoríme o systematickom monitorovaní a zaznamenávaní podobizní s tvárovou biometriou všetkých detí navštevujúcich základné a stredné školy na Slovensku, vrátane pedagógov a ostatných zamestnancov škôl.
- Kamerové systémy sú prevádzkované v prostredí počítačových sietí a kybernetický priestor čelí narastajúcemu počtu útokov, v rámci čoho možno usudzovať, že uložené a spracúvané dáta môžu čeliť možnej kompromitácii v kybernetickom priestore.
- Spracúvanie osobitnej kategórie osobných údajov (detekcia tváre s následnou identifikáciou základných tvárových charakteristík) v spojení s využitím umelej inteligencie predstavuje riziko, že tieto osobné údaje budú v prípade nedostatočnej ochrany zneužité s nepriaznivým dopadom pre dotknuté osoby, a to kedykoľvek v budúcnosti.
- Podľa materiálu by sa malo jednať o systémy umožňujúce automatickú detekciu, bez zásahu človeka, čo by mohlo byť kvalifikované ako profilovanie s automatickým rozhodovaním. Podľa GDPR by sa pritom automatizované rozhodovanie a profilovanie založené na osobitných kategóriách osobných údajov malo umožniť len za osobitných podmienok.

- S ohľadom na predošlé medializované bezpečnostné incidenty na školách, kedy páchateľmi násilia boli žiaci, alebo bývali žiaci škôl, je otázne, či by kamerový systém pomocou umelej inteligencie včas rozpoznal blížiacu sa hrozbu. Z toho dôvodu je otázna nevyhnutnosť takejto spracovateľskej operácie.

V neposlednom rade materiál žiadnym spôsobom neuvádza, ako sa vysporiadal s Nariadením č. 2024/1689 Aktom o umelej inteligencii (AI Act), ktorý kamerové záznamy s využitím umelej inteligencie zaradzuje k vysoko rizikovým operáciám s prísnymi požiadavkami kladenými na poskytovateľa a nasadzovateľa riešenia. Nakoľko v materiáli nie sú uvedené všetky očakávané informácie súvisiace so spracúvaním osobných údajov, nemožno vylúčiť, že spracúvanie bude predstavovať zakázanú operáciu podľa Aktu o umelej inteligencii. Spolok pre ochranu osobných údajov v žiadnom z bodov materiálu predloženého do vlády nevidí odôvodnenie zaznamenávania podobizní všetkých detí na Slovensku, vrátane nadväzujúceho rozpoznávania identity (učenia sa umelej inteligencie).

Medzinárodné výskumy[1] pritom naznačujú, že kamerové sledovanie má iba zanedbateľný, alebo žiadny pozitívny dopad na úroveň trestnej činnosti. Štúdia nezistila významný dopad na kriminalitu v žiadnom zo skúmaných fyzických priestorov. Násilné trestné činnosti sa v týchto priestoroch znížili, ale zníženie bolo kompenzované celkovým zvýšením kriminality v okolí monitorovaných priestorov. Ergo: kriminalita sa presunula do nemonitorovaných oblastí. O to skôr je problémom, že v slovenskom prípade ide o fiktívne útoky vo forme poplašných správ šírených elektronickými prostriedkami. Voči takýmto vektorom útoku majú kamerové systémy nulový preventívny účinok a páchateľa od úmyslu zaslať poplašnú správu neodradia.

„Umiestnenie kamerových systémov s umelou inteligenciou na všetky školy v krajine predstavuje rozsiahly zásah do súkromia žiakov, učiteľov a zamestnancov," uviedla Lucia Semančínová, predsedníčka Spolku pre ochranu osobných údajov. „Zásady ochrany osobných údajov, najmä minimalizácia ich spracúvania a nevyhnutnosť, sú v prípade takto navrhnutého monitoringu vážne ohrozené. Pokiaľ chceme skutočne posilniť bezpečnosť na školách, mali by sme sa zamerať na riešenia, ktoré sú efektívne, no zároveň primerané a šetrné voči právam jednotlivcov, špeciálne detí," dodala s tým, že Spolok je pripravený spolupracovať na hľadaní alternatívnych prístupov k tejto problematike.

Spolok pre ochranu osobných údajov je otvorený diskusii s prekladateľmi materiálu v tejto téme, a to v snahe nájsť účinné a menej invazívne riešenia na dosiahnutie vymedzeného účelu.

Kto sme

Spolok pre ochranu osobných údajov je združenie profesionálov zaoberajúcich sa otázkami ochrany a spracúvania osobných údajov, ktorá združuje záujemcov o túto problematiku a profesionálov v tomto odbore v súkromnom podnikaní, samospráve a verejnej správe.
Spolok je jediná profesijná organizácia združujúca zodpovedné osoby menované k naplneniu povinností podľa článku 37 Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679 (GDPR).
Spolok v tomto roku oslávil svoje 5. výročie a každoročne vyhlasuje aj ocenenie Zodpovedná osoba roka, v rámci ktorého oceňuje zodpovedné osoby, ktoré nielen že vo svojich

[1] Napr. What Criminologists and Others Studying Cameras Have Found (Noam Biale, Advocacy Coordinator, ACLU Technology and Liberty Program)

organizáciách prispievajú k riadnemu, spravodlivému a transparentnému spracovaniu osobných údajov, ale sa tak isto zúčastňujú odbornej diskusie, delia sa o svoje skúsenosti a prispievajú ku zvyšovaniu ochrany osobných údajov a ochrany súkromia.