

AI “pomáhá a chrání”. Jste sledováni a vyhodnocováni

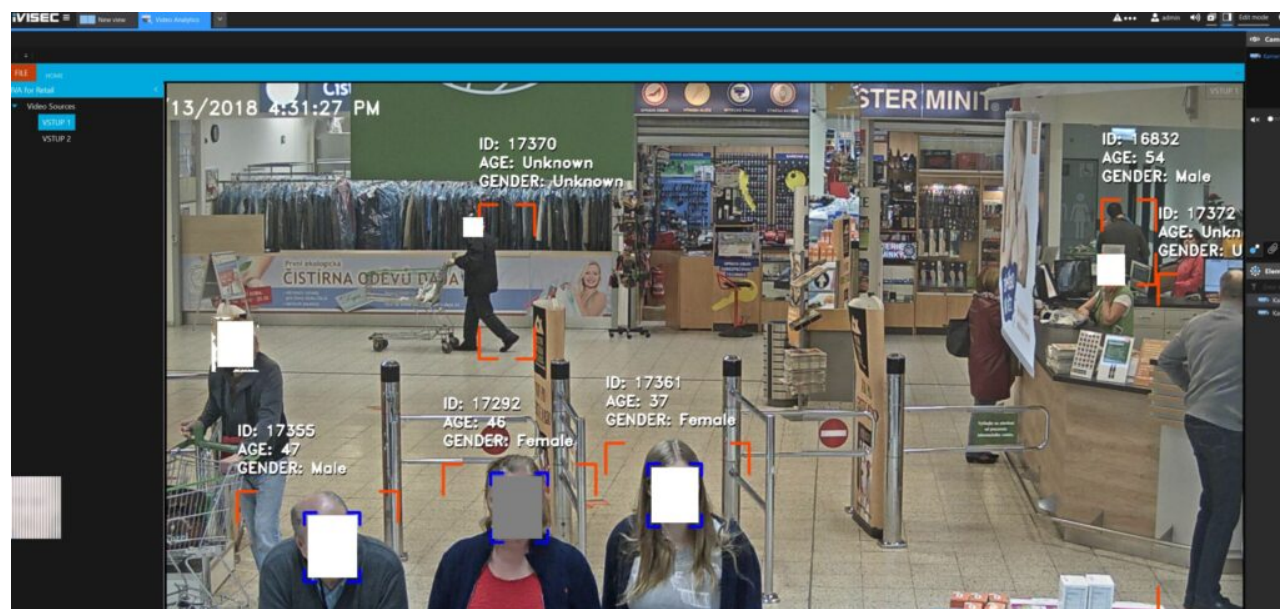
- CZ24 News | 4. března 2024

ČESKO / SVĚT: Jste sledováni a vyhodnocováni. Ne pořád, ale stále častěji. Při jízdě autem, dívají se kde parkujeme, jak dlouho, sledují, co kde nakupujeme, jak se chováme při sezení v kavárně, dívají se, zda jsme na ulici nenechali podezřelý balíček, prověří si nás proti databázi hledaných teroristů a zločinců při vstupu na koncert.

Jde jim to pěkně od ruky, v ČR jsou na oblast sledování lidí specializované desítky firem, jež nabízí AI řešení pro výše popsané disciplíny. Kamery s jejich softwarem sledují 7×24 provoz v pražských tunelech, pohyb osob po Praze a Brně, a kromě veřejných zakázek na monitoring veřejného prostoru umí sledovat i obchody, firmy a její pracovníky. Počítají návštěvníky, zjistí jejich věk a pohlaví (muž, žena, další to neumí).

K dispozici jsou ale i fajnové funkce jako spouštět poplach na základě události, kterou systém sám rozpozná. např. výskyt neznámé osoby (bez RFID čipu nebo jiného identifikátoru) ve sledovaném prostoru, rozliší chování jakékoli osoby – zda se chová „normálně“, zda nevykazuje „nekoherentní pohyby“, nebo zda je aktuálně v pozici „střelec“, což by se výjimečně bylo bývalo hodilo pro spuštění automatizovaného alarmu na FF UK.

Sledují zda osoba opustila monitorovaný prostor a zanechala v něm např. tašku. Systémy umí identifikovat hledanou osobu z fotky v HD videa z městské kamery na náměstí, nebo z kamery u silnice, která sleduje posádky projíždějících aut. Nejde jen o neškodné počítání kolik lidí v jaké věkové struktuře a s jakou náladou přišlo do obchodu a s jakou náladou odcházeli. Viz fotka – je stará, dnes jsou řešení již mnohem dál, toto je taková hračka, proti aktuálním komerčním řešením.



Firmy elegantně obešly GDPR, neskladují vaše fotky, ale jen váš digitální otisk z fotky odvozený. Fotky resp. videozáznamy, využijí k vytvoření vašeho digitálního dvojčete, vektoru hodnot který vás dostatečně jednoznačně popisuje. Tento digitální otisk může porovnat s dalšími otisky záznamů osob a s vysokou mírou pravděpodobnosti vás umí opět nalézt někde v davu na ulici. Původní obrázek již není zapotřebí, může se smazat. Tím je vyhověno zákonům. Pokud vás stejný systém zachytí na jiném místě, opět si zapamatuje pouze váš specifický vektor a data si uloží. Systém ví, na kterých místech

jste kdy byli a tato lokalizační data moc místa nezaberou, lze je skladovat velice dlouho a velice levně.

Zajímavé u zpracování obrazových dat je, že některé AI systémy umí zpětně ukázat na zdrojovém obrázku (zviditelnit) podle čeho určily unikátnost objektu (osoby, auta apod.) a ty mohou být pokaždé jiné, například u auta může jít o body na jeho střeše, okraj zrcátka, a další body, které my jako lidé vůbec nevnímáme jako podstatné. Vlastně to člověk vůbec nerozlišuje. Stroj nás vidí jinak.

Vytvoření tohoto digitálního otisku je jednosměrné, nelze z něj zpětně rekonstruovat vaši podobu. Je to obdoba „hashování“ hesla, které je také jednosměrné. Váš digitální otisk zatím není osobní údaj. Je to metoda efektivně mimo zákon. Nikdo není schopen, bez znalosti algoritmu říci, že se jedná vlastně o „biometrický“ údaj. Systémy jsou zatím roztržštěné, každý má jiný algoritmus a pokud si vás nastuduje umělá inteligence při nákupu v COOPu, není možné aby se tato data využila při analýze dat například z městské kamery provozované pod jiným systémem. Zatím neproběhla standardizace biometrických dat a formátů pro jejich sdílení.

Dnes má k vašim datům přístup kdekdo a přístup k nim se mnohdy vůbec neeviduje a taktéž se nijak nesleduje účel přístupu k datům. Zákon to neukládá a tak se to neřeší. V ČR je třeba dořešit skladování a skartování primárních obrazových materiálů. Pokud systém evidující vaše záznamy podléhá zákonu o spisové službě, jsou zde nastaveny skartační lhůty, ale většinou jsou tyto systémy zcela mimo režim „spisovek“ takže mohou být data uložena kdekoli a kdokoli je bez kontroly může zneužívat. Důvod pro smazání fotek a videí bývá spíše než ochrana práv lidí to, že došlo místo na disku.

Maloobchodní řetězce rostou na AI samoobsluze na bázi 7×24. Jako uživatel беру na vědomí, že mne kamera a možná i operátor sledují. Některé obchody využívají AI skrytě a návštěvníka nevarují.

Vnitro onehdy pořádalo soutěž a algoritmy firem vyhledávaly co nejrychleji osobu ze záznamů podle zadané fotky. Identifikace osoby trvala vteřiny a to bez false-positive. Začíná být jasné, proč Bartošova DIA tlačí na digitalizaci občanek. Nejde jim o naše pohodlí, abychom nemuseli nosit plastovou kartičku v kapse. Ani jim nejde o úsporu práce úředníků. Chtějí získat průběžně aktualizovanou bázi osob, jejich fotek, telefonních čísel a údajů o našem pohybu. Smartpohonek vše poctivě nabonzuje, pokud mu to povolíme (a možná i pokud mu to zakážeme). MVČR se rozhýbalo a začalo „to“ implementovat celoplošně. Nejde jim to rychle, ale jsou vytrvalí a mají téměř neomezené prostředky.

Snad se to státnímu aparátů nepodaří hnedtak zprovoznit. Hlásí se nějaký zákonodárce, kdo se o to postará? Pokud je zdržíte o pár let, máte můj hlas.

ZDROJ: dfens-cz.com

AUTOR: Architekt