



Inteligentna video analitika in varstvo osebnih podatkov

»» Smernice informacijskega pooblaščenca

Namen dokumenta:	Namen smernic je pojasniti značilnosti inteligentne video analitike, razjasniti dileme glede njenega odnosa z videonadzorom, kot ga ureja ZVOP-1, ter podati usmeritve in praktične odgovore, kako zakonito in transparentno uporabljati zmogljivosti inteligentne video analitike.
Ciljne javnosti:	Ponudniki sistemov video analitike, oglaševalci, trgovci, organizacije, ki razmišljajo o nadgradnji obstoječih videonadzornih sistemov ali uvedbi inteligentnih video analitičnih sistemov
Status:	Javno
Verzija:	1.0
Datum izdaje:	22.4.2013
Avtorji:	Informacijski pooblaščenec
Ključne besede:	Smernice, inteligentna video analitika, videonadzor, klubi zvestobe, neposredno trženje, obdelava osebnih podatkov, določljivost posameznika, informiranost posameznikov, zunajdomno oglaševanje.

Kazalo vsebine



UVOD	4
KAJ JE INTELIGENTNA VIDEO ANALITIKA, KAKO DELUJE IN KAJ OMOGOČA?	4
Spekter varovanja zasebnosti - od štetja obiskovalcev.....	6
...do oglaševanja ali kdo bo koga gledal?	7
SMERNICE ZA ZAGOTAVLJANJE VARSTVA OSEBNIH PODATKOV PRI INTELIGENTNI VIDEO ANALITIKI.....	9
Razvrstitev aplikacij inteligentne video analitike glede na določljivost posameznikov	10
Ali štejemo inteligentno video analitiko za videonadzor?	11
Inteligentna video analitika in upoštevanje temeljnih načel varstva osebnih podatkov	13
PRIMERI IMPLEMENTACIJE INTELIGENTNE VIDEO ANALITIKE	19
P R I M E R 1 - Nadgradnja obstoječega videonadzornega sistema z zmožnostmi inteligentne video analitike	19
P R I M E R 2 - Uvedba inteligentne video analitike v objektu zgodovinskega pomena	20
P R I M E R 3 - Uporaba video analitike za avtomatsko prepoznavo tablic na bencinskih servisih	21
.....	21
P R I M E R 4 - Uporaba video analitike za izvajanje zunajdomnega oglaševanja v prostorih trgovskega centra	21
Uporaba inteligentne video analitike v javnem sektorju in na javnih prostorih..	22
ZAKLJUČEK	23



O SMERNICAH INFORMACIJSKEGA POOBLAŠČENCA

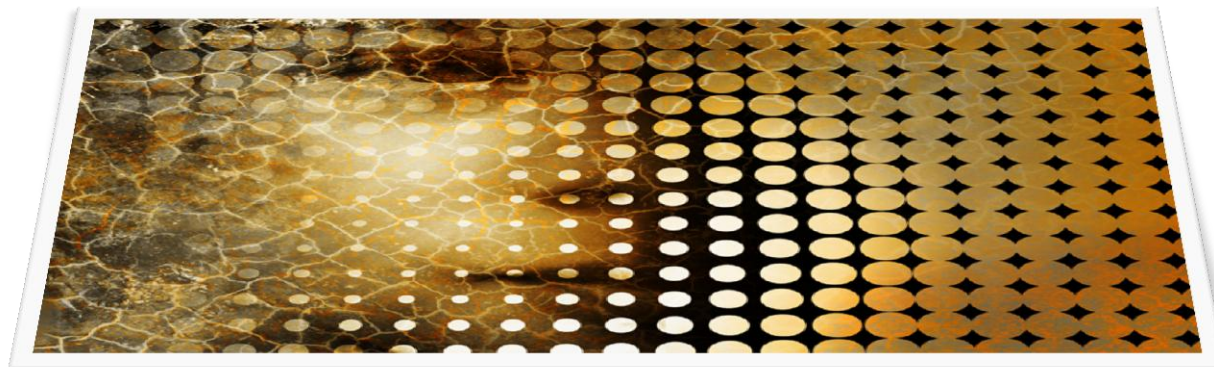
Namen smernic IP je podati skupne praktične napotke za upravljavce zbirk osebnih podatkov (OP) na jasen, razumljiv in uporaben način in s tem odgovoriti na najpogostejše zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci zbirk OP. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 - uradno prečiščeno besedilo; v nadaljevanju ZVOP-1).

Pravno podlago za izdajo smernic Pooblaščenca daje 49. člen ZVOP-1, ki med drugim določa, da Pooblaščenec daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način ter pripravlja in daje neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju.

Oglejte si tudi:

- Mnenja IP: <http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/>
- Brošure IP: <http://www.ip-rs.si/publikacije/prirocniki/>

Smernice IP so objavljene na spletni strani: <http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/>



U V O D

Po internetu, kjer je vedenjsko in personalizirano oglaševanje na podlagi natančnih metrik postalo povsem vsakdanje, postaja tudi oglaševanje izven našega doma bolj informirano in bolj segmentirano. A zmogljiva video analitika obljublja več kot le nove priložnosti za oglaševalce - obljublja večjo varnost in boljše upravljanje s človeškimi in drugimi viri; nove in kakovostnejše storitve so priložnosti, ki ženejo razvoj video analitike. Trendov razvoja video analitike najbrž ni ne smiselno ne možno ustaviti, lahko pa zahtevamo uporabo tehnologije na transparenten način in s takšno zasnovo, ki upošteva koncept vgrajene zasebnosti.

Namen pričujočih smernic je pojasniti značilnosti inteligentne video analitike, razjasniti dileme glede odnosa z videonadzorom, kot ga ureja ZVOP-1, ter podati usmeritve in praktične odgovore, kako zakonito in transparentno uporabljati zmogljivosti inteligentne video analitike.

KAJ JE INTELIGENTNA VIDEO ANALITIKA, KAKO DELUJE IN KAJ OMOGOČA?

Inteligentna video analitika temelji na algoritmih, ki omogočajo prepoznavo vzorcev na video posnetkih v resničnem času. Programska oprema »preiskuje« živo sliko in poskuša iz nje izluščiti določene vzorce, ki naj bi ustrezali ljudem, obrazom ali drugim objektom. Odvisno od sofisticiranosti sistema lahko zazna, ali se pred kamero nahaja človek ali predmet, z določeno natančnostjo ugotavlja starost in spol posameznika, sledi pojavu, mirovanju in gibanju posameznika ali predmeta. Za delovanje sistema ni potrebno shranjevanje posnetkov, saj tovrstna video analitika deluje v realnem času, prav tako nihče ne gleda »žive slike«, ker za to ni nobene potrebe.

Skupna značilnost modalnosti inteligentne video analitike, ki so v centru pozornosti teh smernic, je, da posameznika in predmete obravnavajo kot objekte in da posameznikov in predmetov ne identificirajo na individualni ravni.

Z drugimi besedami, inteligentna video analitika je sposobna ugotoviti oziroma zaznati, ali se pred kamero nahaja človek, obraz ali objekt, ne omogoča pa ugotoviti, kdo to je. Inteligentna video analitika deluje na metapodatkih (tip objekta, smer gibanja in hitrost gibanja objekta) in omogoča zaznavo, ne pa prepoznave v smislu identifikacije.

Rešitve, ki gredo dlje in ki omogočajo prepoznavo posameznika oz. njegovo identifikacijo ali avtentikacijo, npr. z uporabo biometrije (npr. z biometrijsko prepoznavo obraza), v večji meri niso predmet teh smernic, prav tako te smernice *primarno* ne naslavlajo rešitev, ki omogočajo posamezno prepoznavo predmetov, kot je npr. avtomatska prepoznavna registrskih tablic in drugih aplikacij v domeni inteligentnih transportnih

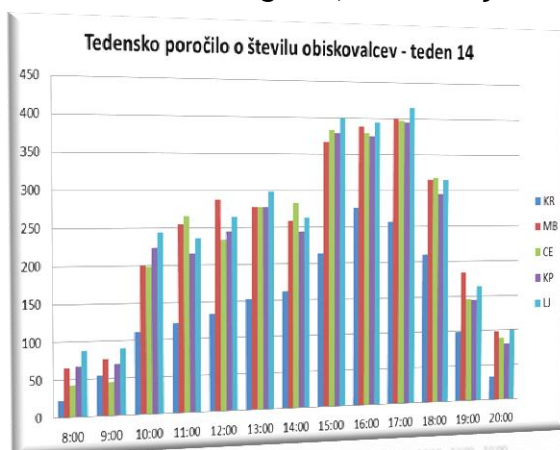


sistemov. Pooblaščenec te teme obravnava v drugih smernicah¹ in mnenjih, v teh smernicah pa jih obdelamo do te mere, da je vidna razlika glede na sisteme, kjer cilj ni identifikacija ali razločevanje posameznikov.

Nekateri uporabljajo tudi pojem anonimna video analitika (ang. anonymous video analytics - AVA), a smo se zaradi relativnosti pri določljivosti posameznika v velikih zbirkah podatkov², zaradi katere težko (in vnaprej) z gotovostjo trdimo, da gre za anonimne podatke³, odločili, da uporabljamo termin Inteligentna video analitika.

S pomočjo inteligentne video analitike lahko upravljalci bolje spoznajo kategorije svojih obiskovalcev in jim prilagajajo svojo ponudbo. Zaradi širokega spektra možnosti, ki jih ponuja inteligentna video analitika, se zanjo zanimajo večji trgovci, kulturne ustanove, oglaševalci, ponudniki elektronskih in poštnih komunikacij - pametni elektronski oglasni prikazovalniki in video analitični sistemi si utirajo pot na letališča, muzeje, trgovske centre. Prihaja do zanimivih situacij, ko podjetja dobivajo konkurenco, kjer je sploh ne bi pričakovali - pošta, naftni trgovci, operaterji elektronskih komunikacij in elektrodistributerji - vsi vidijo svoje priložnosti in primerjalne prednosti.

Za praktičen prikaz delovanja obravnavane tehnologije si pogledjmo praktični primer. Vzemimo trgovca, ki razmišlja o uvedbi takšne rešitve v svoje poslovalnice. Ko posameznik



prečka virtualno črto pred kamero v trgovskem centru, sistem z določeno stopnjo napake oceni njegovo starost in spol ter si zabeleži čas in datum prečkanja ali čas, ko je oseba stala v dometu kamere. Kamere zaznavajo pretok prometa v določenem prostoru in te podatke nato prikažejo na vizualni način, kot so "toplotne slike" oziroma grafični prikaz frekventnih poti ali območij. Oprema prav tako lahko izmeri točen čas, ki ga je oseba porabila za gledanje direktno v kamero (ali za opazovanje proizvoda, branje oglasa, ipd.) ali za gledanje v smeri kamere - v tem primeru je sistem zmožen točno določiti, kaj je oseba v danem trenutku opazovala (angl. audience measurement). Tovrstni sistemi naj ne bi omogočali

prepoznave osebe v smislu ali se je ta konkretna oseba že (in kdaj) pojavila v določeni poslovalnici, temveč se v aplikacijo zabeležijo podatki, kot so npr.:

- čas in datum vstopa: 12. 5. 2010, 12:03, zaznan obraz, moški, starost: 35, čas pred kamero: 3s, levi vhod v poslovalnico.

¹ Več o uporabi biometrijskih ukrepov in zakonskih pogojev za njihovo uvedbo si lahko preberete v smernicah o biometriji: <http://bit.ly/lagBLV>.

² Glej npr. Paul Ohm. *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, August 2009. Dostopno na: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

³ S tem pa naj bi bile zahteve glede varstva osebnih podatkov in zasebnosti manjše.



Takšen sistem bi trgovcu omogočal različne grafične in analitične prikaze podatkov glede na zajeti nabor podatkov, npr. štetje obiskovalcev moškega spola ali čas, ki so ga ženske v starosti 30-40 let prebile pred določenim oglasom.

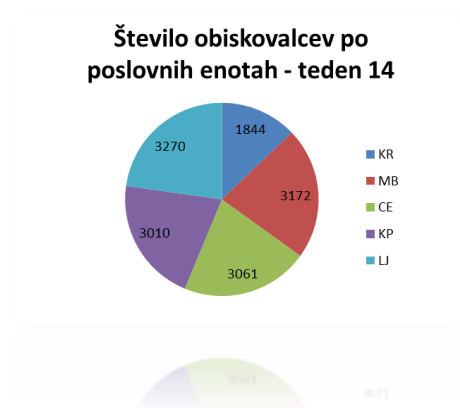
Če se pred kamero (npr. vgrajeno v digitalni zaslon) nahaja moški, bi se lahko prikazal oglas za brivsko peno oziroma oglas za barvo za lase, če bi sistem zaznal žensko.

Spekter varovanja zasebnosti - od štetja obiskovalcev...

Inteligentna video analitika lahko nudi številne možnosti uporabe, ki sodijo v domeno **upravljanja, oglaševanja, varnosti** in drugih področij. Naštejmo nekaj primerov oziroma namenov uporabe:

UPRAVLJANJE

- štetje obiskovalcev,
- ugotavljanje in optimizacija frekventnih poti,
- izdelava različnih analiz in statistik
 - časovni prikaz najštevilnejših in najslabših obiskov,
 - število obiskovalcev ženskega/moškega spola, časovni prikaz najboljšega in najslabšega obiska,
 - razporeditev vseh obiskovalcev v starostne skupine,
 - statistike posameznega območja glede na uro dneva in število obiskovalcev ...
- zaznavanje vrst na blagajnah
- optimizacija razporeditve delovne sile (npr. glede na čakalne vrste).



OGLAŠEVANJE

- čas gledanja oglasa glede na spol in starost
- prilagajanje vsebin in oglasnih sporočil
- oblikovanje cen za trženje na osnovi statistik in analiz
- povezovanje s socialnimi omrežji, klubi zvestobe ...

VARNOST

- ugotavljanje pozabljenih objektov (npr. kovčkov)
- proženje alarma ob pozabljenih, odtujenih, premaknjenih objektih ...



...do oglaševanja ali kdo bo koga gledal?

Inteligentna video analitika omogoča nove priložnosti tudi za oglaševalce, ki upravljajo z digitalnimi zasloni. Oglasna sporočila in vsebine je namreč možno dinamično prilagajati ciljnim skupinam (angl. Dynamic Content Provisioning) glede na značilnosti posameznika, ki se nahaja pred zaslonom. V bližnji prihodnosti lahko pričakujemo, da bo inteligentna video analitika zmožna prepoznati tudi blagovne znamke (»tri vzporedne črte«, »krokodilčka« in ...) ter različne objekte (npr. kolesa, vozičke ipd.). Glede na navedeno lahko pričakujemo porast t.i. **zunajdomnega digitalnega oglaševanja** (DOOH, angl. Digital Out Of Home)⁴. Zunajdomno oglaševanje išče svoje priložnosti tudi v povezavi z mobilnimi napravami, klubi zvestobe in družabnimi omrežji - uporabniki so lahko o novih ponudbah obveščeni prek SMS, bluetootha, prek pametnih oglasnih prikazovalnikov lahko dobijo različne kupone z ugodnostmi, si sestavijo nakupovalni listek in ga shranijo na pametni mobilnik, sodelujejo v nagradnih igrah itd. **Zunajdomno oglaševanje se tako zliva s trendi kot so mobilnost, interaktivnost, družabnost, računalništvo v oblaku in internet stvari, ki že oblikujejo našo sedanost.**



Industrija zunajdomnega oglaševanja se približuje vedenjskemu oglaševanju, ki je vseprisotno na spletu in ki na podlagi obnašanja uporabnikov na spletu uporabnikom dostavlja prilagojene oglasne vsebine. Kjer koli lahko in je dopustno postaviti velik digitalni zaslon, tam je tudi možnost za zunajdomno digitalno oglaševanje: športni stadioni, letališča, trgovski centri, zabavišni centri...

Pričakovati je, da bodo obstoječi »neumni« oglasni panoji prej ko slej stvar preteklosti, saj oglaševalcem ne zmorejo nuditi toliko, kot njihovi »vrstniki« na internetu in drugih medijih - kakšen je dejanski doseg oglasa in ostale metrike, ki so ključne za oglaševalce in njihove naročnike. Oglasi, ki so lahko povezani v mreže in upravljani na daljavo, nudijo povsem

⁴ Drugi pojmi, ki se v povezavi s tem uveljavljajo v angleškem jeziku, so: »digital signage«, narrowcasting", "screen media", "place-based media", "digital merchandising", "digital media networks", "captive audience networks" (vir: Wikipedija).



nove možnosti. Oziroma, kot naj bi skoraj sto let nazaj rekel starosta modernega oglaševanja, John Wanamaker: »Polovica denarja, ki ga namenim za oglaševanje, je zapravljenega. Problem je v tem, ker ne vem, katera polovica je katera⁵.«

Dobičkonosnost kakovostnih oglaševalskih metrik se je na spletu zelo jasno pokazala in pričakovati je, da bo tudi v »off-line« svetu učinek podoben. Z eno pomembno razliko, saj se, kot kaže, vedenjskega oglaševanja v realnem svetu precej bolje zavedamo kot tistega na spletu. Bi vas motil oglas za določeno motorno olje na digitalnem prikazovalniku ob cesti (prilagojen vašemu vozilu na podlagi avtomatske prepoznave registrske tablice in povezave z registrom motornih vozil⁶)?

Ja? Kaj pa podobna stvar na internetu?

Po drugi strani pa je treba pri posamezniku prilagojenemu oglaševanju upoštevati tudi to, da oglas vidi zunaj cel svet in če je prilagojen enemu posamezniku, je lahko to zelo nerodno. Reklamni pano z reklamo za nekaj, kar načeloma v javnosti ni njegov slog ali temelji na podatkih, ki drugim niso znani ali vidni... Na spletu namreč posamezniku prilagojeni oglas vidi samo posameznik, oz. še kdo, ki je ravno takrat z njim ob računalniku.



⁵ https://en.wikipedia.org/wiki/John_Wanamaker

⁶ <http://www.dailymail.co.uk/news/article-1216414/Now-driversdetails-sold-DVLA-used-bizarre-roadside-adverts-Castrol.html>



SMERNICE ZA ZAGOTAVLJANJE VARSTVA OSEBNIH PODATKOV PRI INTELIGENTNI VIDEO ANALITIKI

Različna združenja⁷ in varuhi zasebnosti^{8,9} opozarjajo, da je ustrezen pristop k obravnavi vprašanj **varstva zasebnosti in osebnih podatkov** ter **transparentnosti** bistven za doseganje zaupanja pri uporabnikih, kar pa je temeljni pogoj na nadaljnjo rast in uveljavitev zunajdomnega digitalnega oglaševanja, kot trenutno vodilnega področja uveljavljanja video analitike¹⁰. V študiji¹¹ iz leta 2009 so ugotovili, da 90% mladih odraslih v ZDA zavrača oglaševanje, ki temelji na njihovih »off-line« aktivnostih. Različna združenja ponudnikov, predvsem na področju ZDA, so tako že pristopila k samoregulaciji s sprejemom kodeksov¹² in smernic¹³ za upoštevanje zasebnosti pri zunajdomnem oglaševanju¹⁴. Hkrati pa je pomembno opozoriti na to, da morajo v prostoru Evropske unije ponudniki takega oglaševanja in analitike predvsem upoštevati zahteve zakonodaje s področja varstva osebnih podatkov. Morebitni kodeksi za samoregulacijo pa so dobrodošlo dodatno orodje, namenjeno večji transparentnosti in zaščiti pravic posameznikov.

Večina ljudi se je hočeš-nočeš že navadila na varnostne kamere, njihova dejanska učinkovitost pa je seveda drugo vprašanje. Prav gotovo pa trenutno običajni posameznik še ne pričakuje, da video zaslon, ki si ga ogleduje in kamere pred katerimi se sprehaja, ocenjujejo njegov spol in starost, ugotavljajo, kako dolgo gleda kakšen oglas in temu prilagajajo oglaševanje in storitve¹⁵. Inteligentno video analitiko nekateri že vidijo kot nadaljnji korak k uresničitvi scenarijev iz filma Posebno poročilo (Minority Report) - sveta, v katerem oglasi gledajo ljudi in jim svetujejo, kje in kaj naj kupijo.

Bi morali biti zaskrbljeni ali je strah pretiran? Odgovor leži - kot običajno - nekje vmes.

V nadaljevanju pojasnjujemo, kako v okvir zakonodaje s področja varstva osebnih podatkov umeščamo inteligentno video analitiko. V kolikšni meri in pod katerimi pogoji gre za obdelavo osebnih podatkov in kako upravljavci takih sistemov lahko zadostijo pogojem zakonodaje.

⁷ Glej npr.: Center for Democracy and Technology (CDT). A Framework for Digital Signage Privacy, 2010. Dostopno na: https://www.cdt.org/files/pdfs/A_Framework_for_Digital_Signage_Privacy-Center_for_Democracy_and_Technology-March_2010.pdf

⁸ Glej npr. Information and Privacy Commissioner, Ontario. White Paper: Anonymous Video Analytics (AVA) technology and privacy, 2011. Dostopno na: <http://www.ipc.on.ca/images/Resources/AVAwWhite6.pdf>

⁹ Podobna stališča zastopa tudi Federal Trade Commission (FTC) v poročilu Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers. Dostopno na: <http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>

¹⁰ <http://www.digitalsignageconnection.com/how-emerging-privacy-issues-could-impact-digital-signage-success>

¹¹ Americans Reject Tailored Advertising. Dostopno na: https://www.nytimes.com/packages/pdf/business/20090929-Tailored_Advertising.pdf

¹² Glej npr.: POPAI - THEE GLOBAL ASSOCIATION FOR MARKETING AT RETAIL, Digital Signage Group. Best Practices: Recommended Code of Conduct for Consumer Tracking Research, 2010. Dostopno na: <http://www.popai.com/docs/DS/2010dsc.pdf>

¹³ Glej npr. Digital Signage Federation Privacy Standards: www.DigitalSignageFederation.org

¹⁴ Manj tovrstnih samoregulativnih aktivnosti pa je - pričakovano - moč zaslediti na področju inteligentne video analitike, ki ne zasleduje oglaševalskih ciljev (npr. pri ponudnikih števec obiskovalcev, ipd.)

¹⁵ Glej: Pam Dixon: The One-Way Mirror-Society. Privacy Implications of the new Digital Signage Networks, 2010. Dostopno na: <http://www.worldprivacyforum.org/pdf/onewaymirrorsocietyfs.pdf>



Razvrstitev aplikacij inteligentne video analitike glede na določljivost posameznikov

Delovanje inteligentne video analitike po eni strani predstavlja določen poseg v zasebnost posameznika, obenem pa deluje na način, ki bi ga lahko obravnavali kot obdelavo statističnih in ne osebnih podatkov. Glede na konkretne primere funkcionalnosti in stopnjo posega v zasebnost posameznika lahko v splošnem razvrstimo¹⁶ aplikacije inteligentne video analitike v tri sklope¹⁷.



RAVEN 1 - Zaznavanje prisotnosti

Sem sodijo rešitve, kjer se posameznika obravnava kot zaznani objekt, ne ugotavlja pa se njegovih socio-demografskih značilnosti, kot so spol ali starost. Rešitve se ne uporabljajo za vedenjsko trženje, posnetki se ne hranijo, podatki se sproti agregirajo.

Primer: rešitve, pri katerih se šteje obiskovalce, zaznava čakalne vrste, prožijo določeni alarmi ob odsotnosti, premikanju ipd.



RAVEN 2 - Segmentiranje

Zbirajo in obdelujejo se podatki o posamezniku, kot so spol, starost, podatki o vedenju (npr. dolžina gledanja oglasa), iz katerih pa posameznik ni določljiv. Podatki se uporabljajo za prilagojeno oglaševanje, ne omogočajo pa določljivosti posameznika in se ne povezujejo z drugimi podatki, ki to omogočajo.

Primer: pametni digitalni prikazovalniki, ki omogočajo ugotavljanje spola in starosti in prikazujejo ustrezne oglase.

Posebej velja opozoriti, da se z zbiranjem drugih dodatnih atributov (npr. podatkov o stopnji potenja, telesni temperaturi, nosečnosti, specifičnih vedenjskih vzorcih ipd.) oz. s kombiniranjem atributov lahko zgodi, da gre pri takšni aplikaciji za aplikacijo ravni 3, saj se s tem povečuje možnost razlikovanja med posamezniki ali določljivosti posameznika, takšne aplikacije zato potem že sodijo v raven 3.



RAVEN 3 - Identifikacija in profiliranje

Namen zbiranja in obdelave podatkov je identifikacija ali razločevanje posameznika od posameznika in posredovanje oglasov ali drugih storitev, ki so prilagojeni (konkretnemu) posamezniku. Zajeti podatki se nanašajo na določljive posameznike oziroma skupaj z drugimi podatki omogočajo določljivost posameznika.

Primer: pametni digitalni prikazovalniki, ki omogočajo povezovanje z uporabniškimi profili na družabnih omrežjih ali s podatki iz klubov zvestobe ali drugih zbirk osebnih podatkov, biometrijska prepoznavna obraza, uporaba RFID oznak, avtomatska prepoznavna registrskih tablic.

¹⁶ Glej npr. Information and Privacy Commissioner, Ontario, Canada. White Paper: Anonymous Video Analyti



Ali oziroma kdaj gre pri inteligentni video analitiki za obdelavo osebnih podatkov?

Pri delovanju video analitike gre za **avtomatsko obdelavo podatkov**, kjer pa se s tem, ko se ne hrani posnetek posameznika, izvaja **sprotna anonimizacija**. Anonimizacija je po določbi 18. točke 6. člena ZVOP-1 **takšna sprememba oblike osebnih podatkov, da jih ni več mogoče povezati s posameznikom ali je to mogoče le z nesorazmerno velikimi napori, stroški ali porabo časa**.

Pri video analitiki tipa 1 in 2 se v nobeni fazi ne ugotavlja niti ne razločuje med posamezniki na osebni, določljivem nivoju, zato so pogosto imenuje tudi »anonimna video analitika¹⁸«. Takšne statistične podatke je tako treba šteti za anonimizirane podatke, za katere ne veljajo določbe ZVOP-1. Glede na anonimizirano obdelovanje osebnih podatkov kot tudi glede na anonimizirano objavo rezultatov raziskave je izključeno, da bi se lahko objava rezultatov raziskave uporabila za sprejem kakršnihkoli odločitev, ki bi bile usmerjene k posamezniku. To pomeni tudi to, da posameznik praktično ne more uveljavljati pravice do seznanitve s temi podatki, saj je iz podatkov nemogoče razbrati tiste, ki bi se nanašali na točno določenega posameznika.

Kljub temu pa Pooblaščenec poudarja, da je za pridobitev takšnih statističnih podatkov v določeni fazi, pa čeprav je ta faza lahko neskončno kratka, treba obdelovati osebne podatke posameznikov, v konkretnem primeru primarno podobo obraza, čas vstopa ali zadrževanja pred kamero in druge podatke, odvisno od funkcionalnosti sistema. Brez obdelave teh podatkov, pri čemer oprema za posameznika ugotavlja njegovo starost in spol na podlagi njegove podobe obraza, tudi do statističnih podatkov ne bi mogli priti. V delovanju konkretne opreme torej prihaja do - sicer praktično neskončno kratke - toda z vsebinskega vidika pomembne faze, v kateri se obdelujejo osebni podatki. Da je treba omenjeno obdelavo šteti za obdelavo osebnih podatkov, bi bilo zelo jasno v primeru, ko bi shranili posnetek posameznika, kateremu smo ugotavljali spol in starost, vendar pa gre tudi v konkretnem primeru, ko se posnetek obraza ne hrani, za obdelavo osebnih podatkov v času zajema podatkov, nato pa se praktično v realnem času osebni podatki anonimizirajo. **S sprotnim zavrženjem slike praktično v realnem času pa se zagotavlja učinkovitejše varstvo pravice posameznika do zasebnosti in varstva osebnih podatkov, saj se obdelujejo le anonimizirani podatki, ki jih ni več mogoče povezati z določenim ali določljivim posameznikom.**

Ali štejemo inteligentno video analitiko za videonadzor?

Inteligentne video analitike in video nadzora ne bi smeli mešati in obravnavati enako. Samo zato, ker se uporablja tehnologijo, ki temelji na videu oziroma sliki, še ne pomeni, da gre za videonadzor in to še ne pomeni, da gre za enakovredne posege v zasebnost.

¹⁸ Glej npr. Information and Privacy Commissioner, Ontario, Canada. White Paper: Anonymous Video Analytics (AVA) technology and privacy, 2011. Dostopno na: <http://www.ipc.on.ca/images/Resources/AVAwwhite6.pdf>



Pomislino na krmiljenje zabavnih igrice s pomočjo video konzol, ali interaktivne zaslone, kjer se lahko zabavamo, pridobivamo informacije in družimo. Vsako uporabo tehnologije je treba trezno presojati glede na posege v zasebnost in pri tem paziti na tehnološko nevtralnost, sicer lahko povzročimo oviro razvoju brez sorazmernih koristi za varstvo zasebnosti.

Pri uvajanju inteligentne video analitike v povezavi z videonadzorom za varovanje premoženja in ljudi lahko v grobem ločimo tri **scenarije**:

1. upravljavec ne uporablja klasičnega videonadzora in uvaja inteligentno video analitiko;
2. upravljavec želi nadgraditi obstoječi videonadzorni sistem z zmožnostmi inteligentne video analitike;
3. upravljavec želi hkrati uvesti videonadzor z zmožnostmi inteligentne video analitike.

Videonadzor, ki ga ureja ZVOP-1, se lahko uporablja za namene, ki jih dopušča ZVOP-1:

- če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz službenih oziroma poslovnih prostorov ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih (dostop v uradne službene oziroma poslovne prostore, 75. člen ZVOP-1);
- kadar je to potrebno za varnost ljudi in premoženja (večstanovanjske stavbe, 76. člen ZVOP-1);
- le v izjemnih primerih, kadar je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi (delovna mesta, 77. člen ZVOP-1).

Pri video analitiki nobena oseba ne gleda ne posnetkov niti žive slike (kot je recimo slednje primer pri videonadzoru za varovanje, kjer varnostnik opazuje živo sliko) - to ni ne smiselno ne uporabno, temveč strojna in programska oprema izvaja analizo v realnem času brez udeležbe človeka. Pri video analitiki lahko ugotovimo, da se obdelujejo podatki o posameznikih (podoba obraza, starost, spol...), da pa se podatki ne hranijo v obliki, ki bi bila povezana s posameznikom, temveč se podatki naprej **(praktično v realnem času) obdelujejo le še v statistični oziroma agregirani obliki**. 17. člen ZVOP-1 dopušča, da se lahko ne glede na prvotni namen zbiranja osebni podatki nadalje obdelujejo za zgodovinsko, statistično in znanstveno-raziskovalne namene, vendar pa je treba **statistične podatke, ki jih izdelava video analitika, voditi ločeno od zbirke podatkov videonadzornega sistema**, saj je vsebina zbirke videonadzornega sistema za varovanje ljudi in premoženja predpisana in omejena in vanjo ni dopustno vnašati drugih podatkov, kot npr. podatkov o starosti in spolu posameznika. Po določbi 4. odstavka 75. člena namreč ta zbirka vsebuje posnetek posameznika, datum in čas vstopa in izstopa iz prostora, lahko pa tudi osebno ime posnetega posameznika, naslov njegovega stalnega ali začasnega prebivališča, zaposlitev, številko in podatke o vrsti njegovega osebnega dokumenta ter razlogu vstopa, če se navedeni osebni podatki zbirajo poleg ali s posnetkom



videonadzornega sistema. Povezovanje zbirke osebnih podatkov videonadzornega sistema in zbirke podatkov, ki jih ustvari video analitika, bi predstavljajo kršitev določb ZVOP-1.

Glede na vse navedeno inteligentne video analitike ni smiselno obravnavati kot videonadzor in tudi obstoječa literatura in dokumenti tega ne obravnavajo na ta način. Video analitika pa glede na zgornja pojasnila nedvomno pomeni avtomatsko obdelavo osebnih podatkov posameznikov, katerih podoba je na določeni točki uporabljena za analitiko.

Inteligentna video analitika in upoštevanje temeljnih načel varstva osebnih podatkov

Glede na navedene sklope je treba zagotoviti spoštovanje temeljnih načel varstva osebnih podatkov¹⁹, ki so v Sloveniji zajeta v ZVOP-1:

- zakonitost (8., 9. in 10. člen ZVOP-1),
- poštenost in transparentnost, (18. člen ZVOP-1),
- namenskost (16. člen ZVOP-1),
- sorazmernost (3. člen ZVOP-1),
- kakovost (točnost, ažurnost, celovitost) (18. člen ZVOP-1),
- zavarovanje in odgovornost (24. in 25. člen ZVOP-1).

Z a k o n i t o s t

Pogoji, pod katerimi je dopustno uporabljati inteligentno video analitiko, bi morali biti sorazmerni glede na poseg v zasebnost, ki ga uporaba tehnologije prinaša. Kot smo že pojasnili, moramo tudi **inteligentno video analitiko šteti za avtomatsko obdelavo osebnih podatkov**, ne pa tudi za videonadzor.

Glede na značilnosti video analitike ravni 1 in ravni 2, kjer so posegi v zasebnost posameznikov minimalni, je za uvedbo tovrstnih video analitik treba poskrbeti za poštenost in transparentnost, predvsem z ustreznimi obvestili. Tudi v obstoječih sprejetih okvirih se klasifikacija video analitike osredotoča na zgoraj omenjene tri ravni, katerim ustrezajo naslednji pogoji, pod katerimi je mogoče zagotoviti zakonitost.

¹⁹ Obstajajo različne klasifikacije, v evropskem prostoru se manifestirajo kot temeljna načela direktive o varstvu osebnih podatkov in nacionalnih zakonov, v drugih državah, zlasti v ZDA in Kanadi se uveljavljajo t.i. prakse poštene rabe podatkov (Fair Information Practice - FIP). Kljub občutnim razlikam v ameriškem in evropskem pristopu k varovanju zasebnosti, so omenjena temeljna načela presenetljivo - ali pa tudi ne - podobna.



RAVEN 1 - Zaznavanje prisotnosti	Zakoniti interesi, ki prevladujejo nad interesi posameznika
	+
RAVEN 2 - Segmentiranje	Obvestila
RAVEN 3 - Identifikacija in profiliranje	Izrecna privolitev posameznika ali podlaga v zakonu
	+
	Obvestila

Pri ravni 1 in ravni 2 je treba v vsakem konkretnem primeru pretehtati, ali legitimni interesi zasebnega sektorja prevladujejo nad interesi posameznika oz. ali so za varstvo pravic posameznika zagotovljeni zadostni ukrepi, da bi lahko uporabili pravno podlago iz 3. odstavka 10. člena ZVOP-1. Nekaj konkretnih primerov iz prakse je obdelanih v poglavju »Primeri implementacije inteligentne video analitike«. Kot smo že opozorili, se namreč lahko s povečevanjem števila zajetih kategorij podatkov oziroma atributov, ali pa s povezovanjem teh, lahko zgodi, da postane posameznik določljiv, zato gre lahko v konkretnem primeru že za aplikacijo ravni 3, kjer se zahteva izrecna privolitev posameznika ali podlaga v zakonu.

Za implementacije inteligentne video analitike, ki sodijo v raven 1 ali raven 2, morate posameznike **jasno in izčrpno obvestiti o obdelavi osebnih podatkov**. Več o tem, kaj naj bi bila vsebina obvestila, kje morajo biti nameščena in kako naj bi bila oblikovana, si lahko preberete v naslednjem poglavju.

V primeru, da bi sistem video analitike za vas zagotavljal zunanji izvajalec, ne pozabite na ustrezno ureditev pogodbene obdelave osebnih podatkov, skladno z določbami 11. člena ZVOP-1.

Za implementacije inteligentne video analitike, ki sodi v **raven 3 potrebujete pravno podlago v izrecni privolitvi posameznika ali v zakonu**. Za določene obdelave osebnih podatkov lahko veljajo tudi posebni, strožji režimi. Takšen recimo obstaja za uvedbo biometrijskih ukrepov, kot je npr. **biometrijska prepoznavna obrazov**, ki jih posebej ureja ZVOP-1²⁰, ki **taksativno omejuje dopustne namene uvedbe biometrijskih ukrepov** in zahteva predhodno **odobritev** nadzornega organa za varstvo osebnih podatkov (angl. prior checking). Takšno ureditev npr. pozna Francija na področju pametnih digitalnih oglasov. Francoski nadzorni organ za varstvo osebnih podatkov (CNIL) je s sprejetjem zakona (št. 2010-788 iz 12. julija 2010, poznanega kot "Grenelle II") namreč dobil tudi pristojnost nadzora nad napravami za merjenje "gledanosti" (elektronskih) oglasov na javnih mestih, kot so nakupovalna središča, železniške postaje, letališča ipd. Vsak sistem, ki samodejno meri "občinstvo" oglaševalskih naprav z analiziranjem tipologije ali vedenja posameznikov,



ki se gibljejo v bližini takšnih naprav, odslej potrebuje predhodno privolitev CNIL. Utemeljeno je pričakovati, da bo v prihodnjih letih uporaba tovrstnih naprav in sistemov zakonsko urejena tudi v drugih državah EU. Ob spremembah ZVOP-1 obstaja možnost, da se konkretna problematika natančneje uredi tudi v našem pravnem redu.

Poštenost in transparentnost

Pri uporabi inteligentne video analitike prihaja do določenega posega v zasebnost posameznika in do obdelave osebnih podatkov posameznika in je zato treba poskrbeti za **transparentnost** delovanja takšne opreme in **ustrezno obveščenost posameznika v smislu zagotavljanja pravice posameznika do nadzora nad obdelavo njegovih osebnih podatkov**. Obvestilo o obdelavi osebnih podatkov je temelj zakonite implementacije video analitike. Z veliko verjetnostjo lahko namreč ugotovimo, da bi posameznik želel vedeti, ali v določenem trgovskem centru kamere ugotavljajo njegov spol, starost, gibanje po trgovskem prostoru in zadrževanje pred določenimi oglasnimi prostori in da se lahko tudi prostovoljno odloči, ali ga takšen sistem moti ali ne. Gre za upoštevanje temeljnih načel varstva zasebnosti in osebnih podatkov, zlasti načela poštenosti in informiranosti o obdelavi osebnih podatkov, po katerem naj bi posameznik vedel, kdaj se podatki o njem obdelujejo, kdo to počne in s kakšnimi nameni. Načelo informiranosti in poštenosti obdelave osebnih podatkov bo v prihodnje še bolj pomembno, saj si lahko predstavljamo, da se bodo podatkom o spolu in starosti obiskovalcev v bližnji prihodnosti pridružili (oziroma povezali) še ostali podatki, kot so pogostost nakupovanja v določeni trgovini, nakupne navade ipd., kar je že raven, kjer bo oglaševanje in oblikovanje ponudbe prilagojeno točno določenemu posamezniku. Takšne ravni obdelave osebnih podatkov bodo terjale tudi strožje pogoje.

Kot smo že omenili različna združenja²¹ in varuhi zasebnosti²² opozarjajo, da je ustrezen pristop k obravnavi vprašanj **varstva zasebnosti in osebnih podatkov ter transparentnosti** bistven za doseganje zaupanja pri uporabnikih, kar pa je temeljni pogoj za nadaljnjo rast in uveljavitev inteligentne video analitike, zlasti pa zunajdomnega digitalnega oglaševanja²³.

Pooblaščenec je glede na navedeno mnenja, da je treba zagotoviti transparentnost delovanja tovrstne opreme z ustrezno **obveščenostjo posameznikov** in je mnenja, da bi morala biti postavljena **jasna in razločna obvestila na (vseh) mestih, kjer se takšna oprema uporablja**.

²¹ Glej npr.: Center for Democracy and Technology (CDT). A Framework for Digital Signage Privacy, 2010. Dostopno na: https://www.cdt.org/files/pdfs/A_Framework_for_Digital_Signage_Privacy-Center_for_Democracy_and_Technology-March_2010.pdf

²² Glej npr. Information and Privacy Commissioner, Ontario, Canada. White Paper: Anonymous Video Analytics (AVA) technology and privacy, 2011. Dostopno na: <http://www.ipc.on.ca/images/Resources/AVAwite6.pdf>

²³ <http://www.digitalsignageconnection.com/how-emerging-privacy-issues-could-impact-digital-signage-success>



Koristno je, da so obvestila zasnovana na **treh nivojih**:

»» 1. OZNAKA NA SAMI NAPRAVI

Prva raven se nanaša na označevanje samih senzorjev oziroma naprav, kjer posameznik pride v stik s sistemom inteligentne video analitike. Oznaka bi morala nuditi osnovne informacije, s pomočjo katerih lahko posameznik izve, da gre za tovrstne naprave. Upoštevajte naslednje smernice:

- Označena bi morala biti **vsaka** naprava (senzor), ki uporablja video analitiko.
- Pri postavitvi obvestil upoštevajte specifične prostora in izhajajte iz izhodišča, da mora biti obvestilo na **vidnem** in na takšnem mestu, da se posameznik lahko seznani z njegovo vsebino, **preden pride v domet senzorjev video analitike**²⁴.
- **Ni dovolj, da se namesti zgolj eno obvestilo na vhodu v poslovalnico.**
- Obstoječa obvestila o videonadzoru za varovanje ljudi/premoženja niso primerna niti zadostna; priporočamo, da obvestila o napredni video analitiki ločite od obvestil o izvajanju videonadzora.
- Uporaba **neoznačenih** ali **prikritih** naprav z inteligentno video analitiko ni dopustna.

V prihodnosti je možno pričakovati razvoj enotnih piktografskih standardov, zlasti na področju zunajdomnega oglaševanja, ki lahko omogočijo boljše in enostavnejšo prepoznavnost s strani uporabnikov.

»» 2. VEČ INFORMACIJ OB NAPRAVI

Na drugi ravni bi morali ob napravi imeti **podrobnejše obvestilo z bistvenimi informacijami o sami napravi**, ki naj vsebuje:

- **pojasnilo o namenu delovanja naprave,**
- **podatke o identiteti upravljavca** (t.j. naročnika) sistema,
- **obseg podatkov**, ki se zbirajo,
- **komu(vse) se posredujejo osebni podatki,**
- **s katerimi drugimi podatki se povezujejo zbrani podatki,**
- **naslov spletne strani ali drugega mesta**, kjer lahko posameznik pridobi **več informacij**,
- **druge informacije** (koristne so tudi informacije, ki posamezniku pojasnjujejo, česa naprava NE počne, npr. glede hrambe posnetkov, povezovanja z drugimi zbirkami ipd.).

²⁴ V primeru števec obiskovalcev bo torej takšno obvestilo moralo biti na takšnem mestu, da se lahko posameznik z njim seznani še pred vstopom.



PRIMER OBVESTILA

SISTEM INTELIGENTNE VIDEOANALITIKE ali NAZIV SISTEMA

- Sistem omogoča **šteje obiskovalcev, ugotavljanje starosti in spola obiskovalcev z določeno verjetnostjo**, čas **zadrževanja v bližini kamere** ter prilagajanje digitalnih oglasov demografskim skupinam.
- **Sistem ni povezan z obstoječimi varnostnimi videonadzornimi sistemi in ne hrani videoposnetkov.** Vse obdelave video slike se izvajajo v realnem času.
- **Sistem ne omogoča prepoznave posameznih oseb**, ampak s pomočjo algoritmov ocenjuje le splošne demografske podatke (spol, starostna kategorija) in statistične podatke o izbranih aktivnostih (npr. mimohod, pogled v kamero, zadrževanje v bližini kamere).
- S sistemom upravlja _____.
- Namen uporabe sistema je:
 - spremljanje nakupovalnih navad po spolu in ocenjeni starosti strank,
 - _____,
 - _____.
- Več informacij je na voljo na spletnem naslovu _____.
- Osebni podatki se sproti anonimizirajo. Anonimizirani podatki se hranijo _____.
- Osebni podatki se ne posredujejo tretjim osebam. Upravljavcu trgovskega centra se posredujejo le brezosebni statistični podatki o ocenjeni starosti, spolu, času obiska, _____.

Če si resnično želimo transparentnosti in razumemo, da je transparentnost do naših strank tudi nam v prid, potem bomo posamezniku dali kratke, jasne in razumljive informacije - postavite se v kožo posameznika!

»» 3. PODROBNEJŠE INFORMACIJE (npr. na spletu)

Na tretji ravni bi upravljavec sistema moral objaviti **izčrpne**, a še vedno **jasne in jedrnat**e informacije o delovanju sistema, npr. v obvestilu na svoji spletni strani, prek telefona v kontaktnem centru ali v živo pri okencu z informacijami. Neprimerno bi bilo informacije o delovanju tovrstnega sistema »zakopati« globoko v dolg tekst politike zasebnosti ali pogojev uporabe storitev.



Namenskost

Upoštevanje načela namenskosti lahko zagotovite z ustreznimi obvestili, s katerimi posamezniku omogočite informiranost o tem, za katere namene boste uporabili zbrane podatke. Uporaba osebnih podatkov v nasprotju z namenom, za katere so bili zbrani, ni dopustna. Če boste podatke posredovali tretjim osebam, je o tem treba obvestiti posameznika.

Sorazmernost

Sorazmernost se nanaša tako na obseg kot na roke hrambe osebnih podatkov. Upoštevajte koncept **vgrajene zasebnosti**²⁵ in sledite načelu **minimizacije podatkov**.

V začetnih fazah projekta (ko določamo/preučujemo želene funkcionalnosti) morate določiti minimalni zadostni nabor osebnih podatkov, s katerim lahko dosežemo namen obdelave:

- če določeni osebni podatki niso potrebni, potem naj se jih ne zbira (pogosto za izpolnitev zadanega cilja zadostujejo že anonimizirani ali statistični podatki),
- če brez osebnih podatkov ne gre, potem upoštevamo načelo sorazmernosti.

Kakovost (točnost, ažurnost)

Načelo točnosti in ažurnosti je - tako kot ostala temeljna načela - bolj pomembno pri implementacijah video analitike ravni 3, katere namen je razločevanje med posamezniki: osebni podatki, ki se zbirajo morajo biti ažurni in točni.

Zavarovanje

Podatki morajo biti ustrezno zavarovani s tehničnimi in organizacijskimi ukrepi, s katerimi se zagotavlja zaupnost, celovitost in razpoložljivost podatkov. Preprečena mora biti nepooblaščen seznanitev, brisanje, spreminjanje, posredovanje, objavljanje ali uničevanje podatkov, pristop k varovanju informacij pa mora biti celovit in proaktiven - upravljavci bi morali izkazati zavezanost k proaktivnemu in odgovornemu ravnanju z osebnimi podatki (angl. accountability).

²⁵ Glej smernice pooblaščenca: »Skrb za zasebnost? Pri nas je vgrajena!« Dostopne so na: http://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_za_razvoj_informacijskih_resitev.pdf



PRIMERI IMPLEMENTACIJE INTELIGENTNE VIDEO ANALITIKE

P R I M E R 1 - Nadgradnja obstoječega videonadzornega sistema z zmožnostmi inteligentne video analitike

Trgovec želi nadgraditi obstoječi videonadzorni sistem z zmožnostmi inteligentne video analitike, da bi lahko ugotovil obiskanost svojih poslovalnic po urah, dnevih in tednih ter deleže obiskovalcev po starosti in spolu. V svojih poslovalnicah bi obstoječi videonadzorni sistem, ki ga uporablja za namen varovanja premoženja, in ki shranjuje posnetke 30 dni, nadgradil s programsko opremo, ki omogoča štetje obiskovalcev ter ugotavljanje starosti in spola obiskovalcev. Podatki o obiskovalcih bi se v podatkovno bazo, ki je ločena od arhiva posnetkov, zapisovali na naslednji način:

- čas in datum vstopa: 12. 5. 2010, 12:03, zaznan nov obraz, moški, starost: 35, čas pred kamero: 3s, levi vhod v poslovalnico.

*Omenjen primer sodi v **raven 2**, saj se zbirajo in obdelujejo podatki, kot so spol, starost in podatki o vedenju, iz katerih pa posameznik ni določljiv. Podatki se uporabljajo za prilagojeno oglaševanje, ne omogočajo pa določljivosti posameznika in se ne povezujejo z drugimi podatki, ki to omogočajo, npr. s podatki, ki se shranjujejo v okviru delovanje videonadzornih kamer.*

*Trgovec mora zagotoviti transparentnost in sicer mora na vidno mesto namestiti obvestilo **na vsaki napravi**, ki uporablja inteligentno video analitiko, ne potrebuje pa privolitve posameznikov. **Obstoječa obvestila o videonadzoru za namen video analitike niso zadostna**. Obvestila naj bodo v več **nivojih** (oznaka naprave, informacije ob sami napravi, podrobnejše informacije na spletnem ali drugem mestu). **Podatkov, ki jih zbirka inteligentna video analitika, ni dovoljeno vnašati v zbirko podatkov videonadzornega sistema za varovanje ljudi in premoženja, prav tako ni dovoljeno povezovati omenjenih zbirk podatkov**. Če bi sistem zbiral več kategorij podatkov, potem je treba posebej pozorno preveriti, ali sistem omogoča določljivost posameznika in tako sodi v raven 3.*



PRIMER 2 - Uvedba inteligentne video analitike v objektu zgodovinskega pomena

Javni zavod, ki upravlja z objektom zgodovinskega pomena, želi s partnerjem vzpostaviti inteligentni video sistem, ki bo omogočal:

- štetje obiskovalcev na posameznih vhidih in glavnem vhodu,
- štetje obiskovalcev v čakalni vrsti,
- merjenje časa čakanja v čakalni vrsti,
- prikaz gibanja obiskovalcev (t.i. heat map),
- povprečen čas zadrževanja v posamezni coni merjenja,
- obveščanje o vstopu obiskovalca v virtualno varovano območje.

Navedeni podatki se bodo hranili ločeno od posnetkov. Sistem bo deloval tudi kot običajni videonadzor za varovanje premoženja in ljudi. Posnetki se bodo hranili 7 dni pri pogodbenem partnerju.

Primer vključuje klasični videonadzor in video analitiko ravni 1.

Javni zavod mora za postavitev videonadzora upoštevati določbe 74. člena (splošne določbe glede videonadzora) in 75. člena ZVOP-1 (videonadzor dostopa v uradne službene oziroma poslovne prostore), v primeru, da bi videokamere snemale tudi delovne prostore, pa tudi pogoje iz 76. člena ZVOP-1 (videonadzor v delovnih prostorih) in upoštevati ostala temeljna načela varstva osebnih podatkov.

Poleg navedenega mora javni zavod upoštevati smernice glede upoštevanja varstva osebnih podatkov pri delovanju video analitike ravni 1. To pomeni, da mora zagotoviti ustrezno obveščenost o delovanju video analitike skladno s temi smernicami (glej poglavje »Poštenost in transparentnost«).

Priporočamo, da sta **obvestili glede videonadzora in video analitike ločeni**.

Glede na to, da bo storitve izvajal pogodbeni obdelovalec, mora z njim skleniti pisno pogodbo, ki mora vključevati konkretiziran dogovor o postopkih in ukrepih za zavarovanje osebnih podatkov, skladno z zahtevami 11. člena ZVOP-1. Iz pogodbe mora biti jasno, da pogodbeni obdelovalec v imenu in za račun naročnika izvaja storitev videonadzora z namenom varovanja premoženja in ljudi ter storitev video analitike ter da podatkov ne sme uporabljati za svoje namene.



P R I M E R 3 - Uporaba video analitike za avtomatsko prepoznavo tablic na bencinskih servisih

Ponudnik bencinskih servisov želi nadgraditi obstoječi sistem videonadzora, ki ga uporablja za varovanje premoženja in ljudi z zmogljivostmi inteligentne video analitike, ki bi omogočala prepoznavo registrskih tablic ter proženje alarma ob pojavu določne registrske tablice (npr. takšne, ki je uvrščena na seznam tablic, pri katerih je bil v preteklosti izvedeno točenje goriva brez plačila -pobeg).

V tem primeru gre za **implementacijo video analitike ravni 3**, saj je namen zbiranja in obdelave podatkov identifikacija oz. razločevanje posameznika od posameznika. Zajeti podatki se namreč nanašajo na določljive posameznike oziroma skupaj z drugimi podatki omogočajo določljivost posameznika. Glede na navedeno bi moral ponudnik bencinskih servisov za uporabo takšne videoanalitike izkazati pravno podlago za obdelavo osebnih podatkov v smislu 10. člena ZVOP-1 (pravne podlage za obdelavo osebnih podatkov v zasebnem sektorju).

P R I M E R 4 - Uporaba video analitike za izvajanje zunajdomnega oglaševanja v prostorih trgovskega centra

Ponudnik zunajdomnega digitalnega oglaševanja uvaja sistem, s katerim je s pomočjo inteligentne video analitike mogoče prilagajati vsebino oglasnega prostora na digitalnih zaslonih glede na starost in spol posameznika, ki se nahaja pred digitalnim zaslonom. Sistem omogoča ocenjevanje spola, starosti in razdalje posameznika od digitalnega zaslona ter podatek o tem, ali je posameznik obrnjen k zaslonu (pozoren) ali ne. Posnetki se ne hranijo. Podatki se uporabljajo za prilagojeno oglaševanje različnim demografskim skupinam in merjenje učinkovitosti oglasov, ne omogočajo pa določljivosti posameznika in se ne povezujejo z drugimi podatki, ki to omogočajo.

Glede na to, da se zbirajo in obdelujejo podatki o posamezniku, kot so spol, starost ter podatki o vedenju, iz katerih pa posameznik ni določljiv, gre za video analitiko ravni 2, zato mora ponudnik poskrbeti za ustrezno obveščenost (glej poglavje »Poštenost in transparentnost«). Posebno pozornost je treba nameniti morebitnemu zbiranju dodatnih podatkov, saj gre z določljivostjo posameznika za raven 3.



Uporaba inteligentne video analitike v javnem sektorju in na javnih prostorih

Treba je poudariti, da kljub temu, da se zdijo posegi v zasebnost na prvi pogled minimalni, določene funkcionalnosti in določeni načini uporabe lahko predstavljajo tudi tveganja za večje posege v zasebnost posameznika. Takšno je recimo zaznavanje nenavadnega obnašanja, torej takšnega, ki statistično odstopa od ustaljenega, oz. ki ustreza vnaprej nastavljenim vzorcem. To lahko vključuje nahajanje na neobičajnih mestih, predolgo postopanje na določenem mestu, opotekajoče gibanje ipd. **Takšna vedenja lahko vodijo v proženje alarmov, začetek snemanja in zelo verjetno vodijo v identifikacijo posameznika z različnimi nameni.** Tovrstne funkcionalnosti porajajo različna etična in moralna vprašanja - kakšno je normalno in kakšno deviantno vedenje, bom sprožil alarm, če se bom tako obnašal? Ob nepoznavanju delovanja tehnologije s strani posameznika se navedeno lahko odrazi v strahu pred določenim obnašanjem in posegom v svoboščine in pravice posameznika. Prav tako so povsem verjetni argumenti, da gre za prve korake k nadaljnjemu nadzoru posameznika, ki bo olajšal uveljavitev tehnologije in metod za enolično biometrijsko identifikacijo posameznika. **Zmožnosti inteligentne video analitike tako ne gre podcenjevati in se pri tem sklicevati, da je za varovanje pravic posameznika vedno in v vsakem primeru poskrbljeno s sprotno obdelavo posnetkov in usmerjenostjo k objektu in ne posamezniku.**



Glede na navedeno je zlasti pri uporabi tovrstnih tehnologij v javnih prostorih in na javnih površinah, posebej, ko so uporabniki tehnologije organi pregona, nujno opraviti javno in strokovno debato, v okviru katere je treba opraviti teste nujnosti in sorazmernosti s posegom v človekove pravice.



ZAKLJUČEK

Inteligentna video analitika obljublja številne nove možnosti za upravljanje virov, oglaševanje, varnosti in druge pomembne vidike poslovanja. Prinaša nam nove storitve, omogoča razvoj in nova delovna mesta. Kot pri vsaki drugi tehnologiji, ki temelji na obdelavi podatkov, ki se tako ali drugače nanašajo na posameznike, pa je zelo pomembno, da je njena uporaba izvedena na način, ki upošteva koncept vgrajene zasebnosti. Zakonite in legitimne cilje je namreč pogosto možno doseči ne »na račun zasebnosti«, temveč tako, da jo s pravočasnim premislekom in ukrepi ohranimo; pri tem morajo biti večja tveganja povezana z večjimi varovalkami. Inteligentna video analitika je le eden od primerov, kjer tehnologija prehiteva zakonodajo. Da bo zakonska regulacija vendarle neizbežna, ni več vprašanje, v prehodnem obdobju pa je najmanj, kar moramo zahtevati, upoštevanje temeljnih načel varstva zasebnosti in osebnih podatkov s posebnim poudarkom na ustrezni informiranosti posameznikov.

