Video nadzor z vidika varstva osebnih podatkov

Marko Potokar, Tatjana Welzer Družovec

Namen prispevka:
Prispevek obravnava področje video nadzornih sistemov in njihove uporabe v zasebnem in javnem sektorju v Sloveniji. Podan je pregled uporabe video nadzora in stanje z vidika Zakona o varstvu osebnih podatkov.

Metodologija:
Raziskava o uporabi video nadzora v Sloveniji je bila opravljena na podlagi analiz nadzornih ogledov ter poročil nadzornega organa za varstvo osebnih podatkov ter na podlagi lastnih izkušenj pri delu nadzornika za varstvo osebnih podatkov. Kot dodatni vir informacij za raziskavo so bili uporabljeni podatki o uravnavanju uporabe video nadzora na podlagi izdanih mnenj nadzornega organa za varstvo osebnih podatkov.

Ugotovitve:
Izsledki raziskave kažejo, da se video nadzor s časom povečuje, najpogosteje ugotovljene nepravilnosti v zvezi z njegovim izvajanjem pa ostajajo skoraj enake. V zadnjem obdobju je zaznati, da se video nadzor pojavlja tudi na območjih, kjer zakonsko ni dopusten.

Omejitve:
Zaradi občutljive narave tematike (morebitna nezakonita uporaba in izvajanje video nadzora, strah pred prijavo zlorab uradnim organom ipd.) je opravljanje raziskav na tem področju težje. Zelo malo je znanstvenih objav.

Praktična uporabnost:
Rezultati in interpretacije raziskave bodo podlaga za nadaljnje poglobljene raziskave na področju video in drugih nadzornih sistemov in sistemski regulaciji uporabe le-teh.

Izvirnost:
Raziskovanje področja uporabe video nadzornih sistemov in posledic le-te na zasebnost in druga področja, je v začetnih fazah oziroma ga sploh še ni. Zelo malo je o tej tematiki napisanega s stališča informacijske varnosti in zasebnosti.

Ključne besede: video nadzor, zasebnost, družba nadzora, ZVOP-1

1 Uvod

Uporaba moderne tehnologije nam je z avtomatizacijo procesov in tako prihranjenim časom, s hitro in krajevno neomejeno komunikacijo, neslutenimi možnostmi dostopa do informacij in zbiranja znanja, novimi načini sproščanja in zabave zelo olajšala življenje. Hkrati je v današnjem svetu vse težje zagotavljati varstvo osebnih podatkov in posameznike zaščititi pred pretiranim posegom v njihovo zasebnost. Nevarno je, da se tega mnogokrat niti ne zavedamo, niti se ne zavedamo posledic, ki jih taki posegi prinašajo. Mnogi so mnenja, da danes že živimo v družbi

nadzora, v kateri se zbirajo informacije o posamezniku, o njegovem gibanju in aktivnostih s strani vladnih in nevladnih organizacij. Za zbiranje in nadaljnjo obdelavo informacij se v modernih družbah uporabljajo nadzorne tehnologije, ki temeljijo na informacijski tehnologiji. Ena izmed takih tehnologij so video nadzorni sistemi, ki izhajajo iz najstarejšega načina odkrivanja in preprečevanja nezaželenega vedenja in dejanj, to je opazovanja.

2 Video nadzorni sistemi

Kljub razširjenosti in dolgoletni uporabi video nadzora obstajajo le opisne definicije pojma video nadzorni sistem oziroma sistem video nadzora. Ena izmed njih določa video nadzorni sistem kot funkcijsko povezana specialna tehnična sredstva, ki s sprejemanjem, prenašanjem, obdelavami, arhiviranji in prikazi sprejetih slik omogočajo vizualno opazovanje in nadzor ter kasnejše analize dogajanja v varovanih prostorih. Med specialna tehnična sredstva, ki sestavljajo video nadzorni sistem štejemo kamere t.j. naprave, ki sprejemajo video signale in jih pretvarjajo v električne ali elektromagnetne impulze ter le-te posredujejo v sredstva za prikazovanje ali shranjevanje, prenosne poti preko katerih prenašamo signale od kamer do drugih lokacij (npr. do varnostno nadzornih centrov), naprave za prikazovanje zajetih signalov med katere sodijo tudi preklopniki, delilniki slik in krmilni sistemi za premikanje kamer ter naprave za shranjevanje signalov (Golob, 1997).

Prvotni video nadzorni sistemi so bili sistemi z 'neumno' kamero (angl.: dumb camera), ki so potrebovali prisotnost človeka, ki je analiziral posnetke. To je bila t.i. prva generacija video nadzornih sistemov, ki so bili analogni. Sledila ji je druga generacija, pri kateri je bila kamera povezana z računalnikom, ki je sam 'ocenjeval' zajete posnetke (Surette, 2005). Video nadzorni sistemi so bili prvotno namenjeni kot pomoč organom oblasti pri preprečevanju in pregonu kriminalnih dejanj, sčasoma pa se je področje njihove uporabe močno razširilo. Z digitalizacijo in uvedbo računalniške tehnologije je postal video nadzor zanimiv tudi za komercialne namene, saj se lahko uporablja za analiziranje vedenja in kupnih navad posameznikov, ali v politiki, kjer se je npr. v obdobju volitev v Mehiki že leta 2000 in 2006 uporabljal sistem za prepoznavo obrazov, s katerim je vlada preprečevala večkratno oddajo glasov volilcev (Vacca, 2007). Poleg 'klasičnih' video nadzornih sistemov za prepoznavo obrazov, gibanja, pozicije, ki delujejo v vidnem področju elektromagnetnega spektra, se uspešno uporabljajo tudi video sistemi za termovizijo, ki temeljijo na zaznavi toplotnega sevanja. Tovrstni sistemi so sicer manj občutljivi na vremenske pogoje (vlaga, megla, rosenje leč, temperaturne spremembe, slaba osvetlitev, noč ipd.) kot video nadzorni sistemi, ki delujejo v vidnem območju, se pa pri termoviziji pojavljajo druge omejitve. Ena izmed njih je oddaljenost opazovanega objekta, saj jakost sevanja pada s kvadratom razdalje. Dodatno omejitev predstavljajo vrsta materiala in debelina ovire za katerimi se nahaja opazovani objekt ter opazovanje objektov z enako temperaturo kot je temperatura okolice.

Poleg naštetih tehničnih omejitev se v praksi zastavljajo tudi številna vprašanja o smiselnosti in učinkovitosti uporabe video nadzornih sistemov. Število kamer za učinkovit nadzor je dostikrat premajhno, njihova postavitev napačna in kvaliteta slike zaradi nepravilne izbire objektivov slaba (Ivanovič in Habbe, 1998). Namestitev in uporaba video nadzornih sistemov na urbanih področjih je javnost razdelila na dva tabora: pristaši prvega so prepričani, da video nadzor posega v zasebnost in tako omogoča kontrolo oblasti nad prebivalci, za druge pa je le-ta dobrodošel, saj naj bi povečeval stopnjo varnosti in zmanjševal družbeno nesprejemljivo vedenje (Davies in Velastin, 2005). Na eni strani vplivneži, politiki in mediji pritrjujejo mnenju, da je video nadzor učinkovit (z vidika varovanja) in k dokazovanju pozivajo kriminologe, na drugi strani pa se civilna družba osredotoča na nevarnosti, ki izhajajo iz nadzorovanja

(Groombridge, 2002). Osnovna uporaba video nadzora v mestnih središčih je odkrivanje kaznivih dejanj in prekrškov, takoj ko se zgodijo. Policija na podlagi posnetkov video nadzornega sistema zbira dokaze, ki lahko usmerijo kriminalistično preiskavo k hitremu odkritju kršitelja. Obstajajo številni dokazi, da se video nadzor večkrat uporablja za obravnavo družbeno nesprejemljivega in kaznivega vedenja (Mencinger in Meško, 2004). Poleg naštetega ima izvajanje video nadzora tudi preventivno funkcijo preprečevanja kriminalitete. Nameščanje tehničnih sredstev za nadzorovanje javnih prostorov kot so trgovski centri, banke in parkirišča, z namenom zmanjševanja možnosti tatvin in drugih kaznivih dejanj, sodi med t.i. situacijsko strategijo preprečevanja kriminalitete (Meško, 2000). Ne glede na mnenja javnosti in politike o video nadzoru z vidika zagotavljanja varnosti pa v praksi prihaja do neskladnosti in kršitev zakonodaje s področja varovanja osebnih podatkov.

3 Pravna regulacija video nadzora v Sloveniji

Po navedbah poročila informacijskega pooblaščenca iz leta 2006, je pregled slovenske zakonodaje pokazal, da je bilo takrat v Sloveniji veljavnih 1684 zakonov, ki urejajo obdelavo osebnih podatkov, od tega 213 takih, ki določajo zbirke osebnih podatkov (Letno poročilo Informacijskega pooblaščenca, 2006). Eden izmed načinov obdelave osebnih podatkov je tudi video nadzor. Ključni razlog za zakonsko ureditev izvajanja videonadzora je sodobni način življenja, zlasti razvoj tehnologije in potreba po varnosti posameznikov in premoženja. Uporabo video nadzora v Sloveniji ureja kar nekaj zakonov med drugim Kazenski zakonik (KZ-1, 2008), Zakon o policiji (ZPol-UPB7, 2009), Zakon o zasebnem varovanju (ZZasV-1, 2011), Zakon o igrah na srečo (ZIS-D, 2010) in seveda Zakon o varstvu osebnih podatkov (ZVOP-1, 2005). V nadaljevanju bomo podrobneje obravnavali Zakon o varstvu osebnih podatkov in njegova določila glede video nadzora.

3.1 Zakon o varstvu osebnih podatkov

Vsebina in namen Zakona o varstvu osebnih podatkov sta opredeljena v prvem členu tega zakona, ki določa, da se z njim določajo pravice, obveznosti, načela in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti in neupravičeni posegi v zasebnost in dostojanstvo posameznika oziroma posameznice pri obdelavi osebnih podatkov (ZVOP-1, 2005). Za razumevanje ZVOP-1 je eden glavnih pojmov obdelava osebnih podatkov, ki je določena kot kakršnokoli dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki, ki so avtomatizirano obdelani ali ki so pri ročni obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov, zlasti zbiranje, pridobivanje, vpis, urejanje, vpogled itd. Namen tako široke definicije je, da bi bilo področje uporabe ZVOP-1 zasnovano čim širše, saj taka definicija zajema praktično vsa ravnanja, ki jih je mogoče izvajati z osebnimi podatki. Določbe ZVOP-1 se namreč uporabljajo le, kadar gre za obdelavo osebnih podatkov (1. člen ZVOP-1). Osebni podatek je namreč po določbi prvega odstavka 6. člena ZVOP-1 katerikoli podatek, ki se nanaša na posameznika, ne glede na obliko, v kateri je izražen, posameznik pa je po določbi 2. točke istega člena določena ali določljiva fizična oseba, na katero se osebni podatek nanaša, pri čemer je fizična oseba določljiva, če se jo lahko neposredno ali posredno identificira. Nadalje je bistvenega pomena, da način identifikacije ne povzroča velikih stroškov, nesorazmerno velikega napora ali ne zahteva veliko časa. Iz navedenega izhaja, da je tudi videonadzor eden izmed načinov obdelave osebnih podatkov. Ključno za obstoj osebnega podatka pa je, da je to podatek na podlagi katerega je možna identifikacija posameznika. To pomeni, da posnetek, ki je tako slabe kakovosti, da se posameznika ne da identificirati, ne more biti osebni podatek. Tako posameznik, ki je le domnevno na posnetku in na podlagi njega ni določen ali določljiv, ne

more uživati pravnega varstva po predpisih o varstvu osebnih podatkov. Nadalje je potrebno upoštevati tudi splošna določila ZVOP-1, ki določajo, kdaj se ta zakon lahko uporabi in katere so izjeme, ko se ZVOP-1 ne uporablja. V 7. členu ZVOP-1 je določeno, da se ta zakon ne uporablja v primeru, ko posamezniki obdelujejo osebne podatke izključno za osebno uporabo, družinsko življenje ali za druge domače potrebe. Tako ZVOP-1 ni pravna podlaga za ukrepanje v primeru, ko npr. posameznik nadzoruje gibanje ljudi na ulici ali pa snema dogajanje v sosedovem stanovanju. To pa ne pomeni, da prizadeti posameznik nima pravnega varstva, če mu je bila kršena pravica do zasebnosti (Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem, 2006).

ZVOP-1 ureja videonadzor v 74. (splošne določbe), 75. (dostop v uradne službene oziroma poslovne prostore), 76. (večstanovanjske stavbe) in 77. členu (delovni prostori). V posameznih konkretnih primerih je potrebno upoštevati predvsem namene, ki jih je zakonodajalec določil kot dopustne za izvajanje videonadzora. Bistvena je določba prvega odstavka 75. člena ZVOP-1, v kateri je določeno, da lahko javni in zasebni sektor izvajata videonadzor dostopa v njihove uradne službene oziroma poslovne prostore, 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. S to določba je uveden video nadzor le pri dostopu v službene oziroma poslovne prostore. Video nadzor znotraj le-teh pa je urejen v 77. členu ZVOP-1 pod bistveno strožjimi kriteriji. Tako prvi odstavek 77. člena določa, da se izvajanje videonadzora znotraj delovnih prostorov lahko izvaja 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. Video nadzor v večstanovanjskih stavbah je določen v drugem odstavku 76. člena, ki določa, da se videonadzor v večstanovanjski stavbi uvede le, kadar je to potrebno za varnost ljudi in premoženja.

Podrobneje obrazložimo še načelo namenskosti. Načelo namembnosti ali načelo namenskosti (angl.: the finality principle) je temeljno načelo varstva osebnih podatkov. Določeno je v 16. členu ZVOP-1 (osebni podatki se lahko zbirajo le za določene in zakonite namene ter se ne smejo nadalje obdelovati tako, da bi bila njihova obdelava v neskladju s temi nameni, če zakon ne določa drugače). V primeru obdelave osebnih podatkov načelo namembnosti izhaja iz drugega odstavka 38. člena Ustave Republike Slovenije, po katerem mora biti med drugim v zakonu določen namen, za katerega se osebni podatki lahko obdelujejo. To ustavno določbo je treba razumeti tako, da morajo biti vse okoliščine v zvezi z obdelavo osebnih podatkov določene v zakonu, predvsem namen obdelave osebnih podatkov. V pravnem redu Republike Slovenije je uveljavljeno načelo stroge namembnosti. Nameni morajo namreč biti nedvoumni, določni ter določeni pred zbiranjem podatkov. Zato je povsem logično, da mora biti namen obdelave oziroma zbiranja osebnih podatkov predhodno, vnaprej določen v zakonu. Takšna ureditev je smiselna predvsem z vidika varstva pred morebitnimi zlorabami osebnih podatkov.

Odločanje oziroma natančno ocenjevanje nujnosti in potrebnosti uvedbe videonadzora mora torej slediti zgoraj navedenim namenom, upravičenost pa se mora vedno presojati od primera do primera, kar pomeni, da mora biti osnovno vodilo pri uvedbi videonadzora načelo, da se ta uvede, kadar ni na razpolago drugega milejšega ukrepa za zagotovitev teh ciljev (varnosti ljudi in premoženja).

3.2 Zakon o informacijskem pooblaščencu

Informacijski pooblaščenec je samostojen in neodvisen državni organ, ki je med drugim pristojen za inšpekcijski nadzor nad izvajanjem zakona in drugih predpisov, ki urejajo varstvo

ali obdelavo osebnih podatkov. Tako Informacijski pooblaščenec opravlja inšpekcijski nadzor po zakonu, ki ureja varstvo osebnih podatkov (Zakon o Informacijskem pooblaščencu (ZInfP), 2005). Pri Informacijskem pooblaščencu so poleg informacijskega pooblaščenca zaposleni državni nadzorniki za varstvo osebnih podatkov ali državne nadzornice za varstvo osebnih podatkov (v nadaljnjem besedilu: nadzornik) (1. odstavek 8. člena ZInfP). Nadzorniki so pri opravljanju nalog inšpekcijskega nadzora in drugih nalog po zakonu, ki ureja varstvo osebnih podatkov, v skladu s svojimi pooblastili samostojni ter jih opravljajo v okviru in na podlagi ustave in zakonov (5. odstavek 8. člena ZInfP). Zakon o informacijskem pooblaščencu in Zakon o inšpekcijskem nadzoru (ZIN-UPB1, 2007) sta pravna podlaga za nadzor in preiskovanje suma kršitev tudi s področja video nadzora, ki ga ureja ZVOP-1.

4 Uporaba video nadzora v Sloveniji z vidika ZVOP-1

Raziskava o uporabi video nadzora v Sloveniji je bila opravljena na podlagi analiz nadzornih ogledov ter poročil nadzornega organa za varstvo osebnih podatkov ter na podlagi lastnih izkušenj pri delu nadzornika za varstvo osebnih podatkov. Kot dodatni vir informacij za raziskavo so bili uporabljeni podatki o uravnavanju uporabe video nadzora na podlagi izdanih mnenj nadzornega organa za varstvo osebnih podatkov.

V letu 2006 se je 31 prijav in pritožb nanašalo na izvajanje videonadzora dostopov do službenih oziroma poslovnih prostorov, delovnih prostorov ter videonadzora v večstanovanjskih stavbah. Opravljeni inšpekcijski nadzori na tem področju so največkrat odkrili nepravilnosti v zvezi z vodenjem evidence posnetkov pri čemer upravljavci niso zagotovili kataloga zbirke osebnih podatkov in podatkov iz kataloga niso posredovali Informacijskemu pooblaščencu, obvestila o tem, da se izvaja videonadzor, so bila večinoma pomanjkljiva, saj niso vsebovala vseh informacij kot je to določeno v 74. členu ZVOP-1, bila so premajhna ali pa jih je bilo premalo, dostikrat pa so bila postavljena na neprimernih krajih. Inšpekcije so odkrile tudi primere izvajanja videonadzora v slačilnicah oziroma garderobah trgovskih in športnih objektov, predstojniki pred začetkom izvajanja videonadzora ali pozneje niso izdali pisne odločitve za izvajanje videonadzora oziroma v tej odločitvi niso pojasnili razlogov za njegovo uvedbo, zaposleni pred začetkom izvajanja videonadzora o tem niso bili pisno obveščeni, za izvajanje videonadzora v večstanovanjskih stavbah ni bila pridobljena pisna privolitev solastnikov, ki imajo v lasti več kot 70 odstotkov solastniških deležev, odkrito pa je bilo tudi izvajanje videonadzora v večstanovanjskih hišah pri katerem se je dogajanje, ki so ga spremljale kamere sproti predvajalo na posebnem kanalu interne kabelske televizije (Poročilo Informacijskega pooblaščenca, 2006).

V letu 2007 je bilo v inšpekcijskih postopkih odkritih 24 sumov kršitve določb ZVOP-1 v javnem in 38 v zasebnem sektorju. Med drugim je Informacijski pooblaščenec ukrepal tudi zaradi nezakonitega izvajanja video nadzora v večstanovanjskih stavbah, pri čemer je šlo za prenos slike videonadzora prek kabelske televizije (Poročilo Informacijskega pooblaščenca, 2007).

Poročilo iz leta 2008 ugotavlja, da je bilo področje kršenja določb ZVOP-1 z vidika video nadzora na tretjem mestu (prednjačile so kršitve s področja ZVOP-1, ki zadevajo obdelavo osebnih podatkov in zavarovanje osebnih podatkov), skupaj pa je bilo odkritih 14 sumov kršitve določb ZVOP-1 v javnem in 32 v zasebnem sektorju (Poročilo Informacijskega pooblaščenca, 2008).

V letu 2009 se je video nadzor po številu kršitev ZVOP-1 pomaknil na četrto mesto (uvrstil se je za kršitvami s področja obdelave osebnih podatkov, zavarovanje osebnih podatkov in

neposrednega trženja). Skupno je bilo odkritih 11 sumov kršitve določb ZVOP-1 v javnem in 46 v zasebnem sektorju (Poročilo Informacijskega pooblaščenca, 2009).

Naslednje leto se je video nadzor glede na število kršitev uvrstil na šesto mesto (za obdelavo in zavarovanjem osebnih podatkov, neposrednim trženjem, katalogi in registri ter kršitvijo namena obdelave osebnih podatkov), kar pa ne pomeni, da je bilo število kršitev s področja video nadzora manjše kot predhodna leta: v letu 2010 je bilo ugotovljenih 8 sumov kršitve določb ZVOP-1 v javnem in 51 v zasebnem sektorju (Poročilo Informacijskega pooblaščenca, 2010). Poročilo informacijskeg pooblaščenca iz leta 2010 med drugim navaja primer, da je »v postopku inšpekcijskega nadzora Informacijski pooblaščenec ugotovil, da občina kršitve v mirujočem prometu (napačno ustavljanje in parkiranje) ugotavlja tako, da pregleduje posnetke video nadzornega sistema. Občinskemu redarju tako ni bilo treba »na terenu« ugotavljati, da napačno parkirano ali ustavljeno vozilo predstavlja kršitev in oviro za mlade starše z vozički in invalide, ampak je preprosto v pisarni pregledal posnetke, izpisal registrske številke napačno parkiranih ali ustavljenih avtomobilov, vpogledal v evidenco motornih vozil, da je ugotovil identiteto voznika, in poslal plačilni nalog. Informacijski pooblaščenec je z odločbo odredil prenehanje pregledovanja videoposnetkov z namenom izrekanja sankcij zaradi napačnega parkiranja na javnih površinah. Občina je zoper izdano odločbo vložila tožbo na Upravno sodišče Republike Slovenije, to pa je v letu 2011 pritrdilo odločitvi Informacijskega pooblaščenca.«

V letnem poročilu za leto 2011 je navedeno, da »Informacijski pooblaščenec na področju izvajanja videonadzora ugotavlja, da se takšen nadzor še vedno nezadržno širi, in sicer tudi na območja, kjer takšen nadzor sploh ni dopusten. Takšni primeri so npr. savne, garderobe, dvigala ter nekatere javne površine (npr. sprehajalne poti). Kot najpogosteje ugotovljene nepravilnosti v zvezi z izvajanjem videonadzora se še vedno pojavlja neustrezno oziroma pomanjkljivo evidentiranje pregledovanja oziroma uporabe posnetkov, uporaba posnetkov za nezakonite namene (npr. kontrola zaposlenih), slabo vidna in nepopolna obvestila o izvajanju videonadzora, neobstoj pisne odločitve o uvedbi videonadzora, izvajanje videonadzora znotraj delovnih prostorov brez posvetovanja z reprezentativnim sindikatom ter neizdelani katalogi za zbirko posnetkov video nadzornega sistema.« Skupno je bilo odkritih 22 sumov kršitve določb ZVOP-1 v javnem in 67 v zasebnem sektorju (Poročilo Informacijskega pooblaščenca, 2011).

V zvezi z izvajanjem videonadzora je v letnem poročilu informacijskega pooblaščenca za leto 2012 v enem izmed inšpekcijskih postopkov »ugotovljeno, da zavezanec izvaja videonadzor delovnih prostorov (recepcija) in tistih delovnih prostorov izven delovnega mesta (garderoba), kjer je z določbo tretjega odstavka 77. člena ZVOP-1 izrecno prepovedan. Zavezanec je z eno kamero snemal celotno območje recepcije, ki se nahaja ob vhodu v prostore fitnes studia, dve kameri pa sta bili nameščeni v moški garderobi oziroma slačilnici. Glede na navedene določbe ZVOP-1 je Informacijski pooblaščenec zavezancu odredil, da mora prenehati izvajati videonadzor moške garderobe v prostorih fitnes studia ali pa obiskovalcem fitnes studia zagotoviti ločene prostore za preoblačenje, v katerih ne bo izvajalvideonadzora. Odredil mu je tudi, da mora prenehati izvajati videonadzor recepcije fitnes studia ali pa obstoječi videonadzor recepcije spremeniti, tako da bo videokamera snemala zgolj območje blagajne, ki se nahaja v tej recepciji. Informacijski pooblaščenec je zavezancu tako v obeh primerih izvajanja videonadzora prepustil odločitev, ali bo z njegovim izvajanjem v celoti prenehal ali pa ga bo prilagodil in spremenil tako, da bo v skladu z določbami ZVOP-1.« Skupaj je bilo podanih 16 sumov kršitve določb ZVOP-1 v javnem in 56 v zasebnem sektorju (Poročilo Informacijskega pooblaščenca, 2012).

Tabela 1: število sumov kršitev ZVOP-1, število izdanih prekrškovnih odločb in ugotovljene nepravilnosti ter število zaprosil za mnenje Informacijskega pooblaščenca s področja video nadzora.

	Sum kršitve določb ZVOP-1 (javni/zasebni sektor)	Prekrškovne odločbe	Ugotovljene nepravilnosti	Zaprosila za mnenja IP
2006	3/28	6	Bazen, dom starejših občanov, garderobe in slačilnice, otroška igrišča, mestni avtobus, večstanovanjske stavbe, gostinski lokali, vodenje evidence pregledovanja shranjenih videoposnetkov.	42
2007	24/38	12	večstanovanjske stavbe (interna TV), delovno mesto, obvestila, razlogi uvedbe, prijava zbirk OP, vodenje evidence pregledovanja shranjenih videoposnetkov.	105
2008	14/32	15	Obvestila, razlogi uvedbe, prijava zbirk OP, vodenje evidence pregledovanja shranjenih videoposnetkov, večstanovanjske stavbe (interna TV).	47
2009	11/46	11	Obvestila, razlogi uvedbe, vodenje evidence pregledovanja shranjenih videoposnetkov.	20
2010	8/51	20	Uporaba ni v skladu z namenom (primer uporabe VN posnetkov s strani občine za ugotavljanje napačnega parkiranja), obvestila, sledljivost...	2*objavljena na spletni strani IP
2011	22/67	39	Uporaba ni v skladu z namenom, sledljivost, prijava zbirk...	2*objavljena na spletni strani IP
2012	16/56	45	Uporaba ni v skladu z namenom, sledljivost, prijava zbirk...	2*objavljena na spletni strani IP

V Tabeli 1 je prikazano število sumov kršitev določb ZVOP-1 v javnem in zasebnem sektorju, število izdanih prekrškovnih odločb in ugotovljene nepravilnosti ter število zaprosil za mnenje Informacijskega pooblaščenca s področja video nadzora.

5 Zaključek

Izsledki raziskave kažejo, da se video nadzor s časom povečuje, najpogosteje ugotovljene nepravilnosti v zvezi z njegovim izvajanjem pa ostajajo skoraj enake. V zadnjem obdobju je zaznati, da se video nadzor pojavlja tudi na območjih, kjer zakonsko ni dopusten. Poseben izziv pa za zaščito pravic posameznikov do zasebnosti predstavljala vpeljava in uporaba t.i. inteligentne video analitike. Lahko bi trdili, da gre pri inteligentni video analitiki za novo (četrto) generacijo video nadzornih sistemov, ki so nadgrajeni z ustrezno strojno in programsko opremo. Napredni algoritmi omogočajo prepoznavo vzorcev na video posnetkih v realnem času, prepoznavo starosti, spola, obrazov, gibanja, nenavadnih situacij ipd. Pri uporabi inteligentne video analitike se tako hitro znajdemo na področju biometrije, ki jo ZVOP-1 še posebej pazljivo obravnava.

Zavedati se moramo, da je poleg hitrega razvoja informacijske tehnologije, zaradi občutljive narave tematike (morebitna nezakonita uporaba in izvajanje video nadzora, strah pred prijavo zlorab uradnim organom ipd.) opravljanje raziskav na tem področju težje. Raziskovanje področja uporabe video nadzornih sistemov in posledic le-te na zasebnost in druga področja, je v začetnih fazah oziroma ga sploh še ni. O tej tematiki ni veliko napisanega s stališča informacijske varnosti in zasebnosti. Tako ta prispevek predstavlja podlago za nadaljnje poglobljene raziskave na področju video in drugih nadzornih sistemov in sistemski regulaciji uporabe le-teh.

Uporaba video nadzornih sistemov in njena problematika je večplastna. Po eni strani je to tehnologija, ki pozitivno vpliva na stopnjo varnosti v okolju v katerem je nameščena oziroma uporabljana in pripomore k uspešnejšemu preiskovanju kriminalnih dejanj. Seveda pa se uporaba teh sistemov ni ustavila na področju varovanja ljudi in premoženja, ampak sega tudi v marketinške vode od sistemov za štetje kupcev in njihovega gibanja v prodajalnah, do sistemov za prepoznavo starosti in spola kupcev. Video nadzor sam po sebi ni nekaj negativnega, tako kot orodje še ni orožje. Lahko pa to hitro postane. Enako velja za (informacijsko) tehnologijo, ki nam je prinesla veliko dobrega in polno koristi. Prav tako nobena tehnologija ni posebej nevarna, če se uporablja sama zase, se pa nevarnost zlorabe lahko poveča, če pride do njihovih združevanj.

Literatura

Golob, R. (1997). *Sistemi zaščite in varovanja oseb in premoženja.* Ljubljana: Narodna in univerzitetna knjižnica.

Groombridge, N. (2002). Crime Control or Crime Culture TV. *Surveillance & Society,* 1(1), 30-46.

Ivanovič, Ž. in Habbe, J. (1998). *Kako preprečiti tatvine v prodajalnah*. Ljubljana: Lisac&Lisac.

Kazenski zakonik (KZ-1). (2008). *Uradni list RS*, *št. 55/2008.*

Letna poročila Informacijskega pooblaščenca. (2006-2012*). Poročilo informacijskega pooblaščenca*. Pridobljeno na https://www.ip-rs.si/publikacije/letna-porocila/

Mencinger, J. in Meško, G. (2004). Veliki brat in učinkovitost video nadzorovanja v Angliji. V T. Pavšič (ur.), *Zbornik prispevkov 5. slovenski dnevi varstvoslovja*, str. 862-872. Ljubljana: Fakulteta za varnostne vede.

Meško, G. (2000). Pogledi na preprečevanje kriminalitete v pozno modernih družbah. *Teorija in praksa*, *4*(37),716-727.

Smernice za izvajanje videonadzora. *Smernice informacijskega pooblaščenca*. Pridobljeno na https://www.ip-rs.si/publikacije/prirocniki-in-smernice/

Surette, R. (2006). The thinking eye: Pros and cons of second generation CCTV surveillance systems. *Policing: An International Journal of Police Strategies & Management*, *1*(28),152 – 173.

Vacca, J. R. (2007). *Biometric Technologies and Verification Systems*. Burlington: Elsevier.

Zakon o igrah na srečo *(*ZIS-D). (2010.) *Uradni list RS*, *št*. *106/10*.

Zakon o Informacijskem pooblaščencu (ZInfP). (2005). *Uradni list RS*, *št*. 5*1/2007*.

Zakon o inšpekcijskem nadzoru (ZIN-UPB1). (2007). *Uradni list RS*, *št*. 5*1/2007*.

Zakon o policiji (ZPol-UPB7). (2009). *Uradni list RS* št. 66/2009.

Zakon o varstvu osebnih podatkov (ZVOP-1). (2005). *Uradni list RS*, št. 94/2007.

Zakon o varstvu osebnih podatkov (ZVOP-1) s komentarjem. (2006). Ljubljana: Narodna in univerzitetna knjižnica.

Zakon o zasebnem varovanju (ZZasV-1). (2011). *Uradni list RS*, *št. 17/2011.*