IZVORNI ZNANSTVENI ČLANAK

UDK: 351.74
Primljeno: studeni 2020.

ŽELJKO KARAS*

Snimanje policijskih službenika kao povreda europskog prava o zaštiti osobnih podataka

Sažetak

Autor u radu analizira europske propise i sudske odluke o zaštiti osobnih podataka u slučajevima videosnimanja osoba na javnome mjestu bez njihova pristanka. Analiza obuhvaća europske propise (GDPR i dr.), presude Europskog suda, Europskog suda za ljudska prava i smjernice mjerodavnih tijela. Na temelju pravnih izvora analizirao je tumačenje definicije osobnih podataka, obrade podataka videosnimanjem ili objavljivanjem, ulogu pristanka osobe koju se snima, obilježja javnoga mjesta, status službenika, iznimke koje mogu isključiti povredu (novinarska iznimka i iznimka kućne uporabe) te uporabu snimaka u kaznenome postupku.

Rezultati analize pokazuju da europski standardi štite sve vrste osobnih podataka i da ne postoje iznimke u odnosu na državne ili javne službenike. Videosnimanje ili objavljivanje izgleda ili drugih tjelesnih obilježja na temelju kojih je moguće odrediti identitet policijskih službenika - predstavlja obradu njihovih osobnih podataka kao i ostalih građana na javnome mjestu. Snimanje policijskih službenika dopušteno je samo uz njihov prethodni pristanak ili na temelju zakonskih osnova (prema presudi Europskog suda u slučaju Buivids). Povreda može predstavljati kažnjivu radnju ovisno o uređenju u domaćem pravnom sustavu, a prema počiniteljima moguće je pokretati odgovarajuće postupke. Ovakav model ima korijene u pravu na samoodređenje prema kojem pojedinac može odlučivati o pojedinim aspektima vlastite privatnosti, a to se pravo zadržava i na radnome mjestu.

Ključne riječi: *videosnimanje, policijski službenici, zaštita osobnih podataka, Europski sud, Europski sud za ljudska prava, GDPR.*

* izv. prof. dr. sc. Željko Karas, Visoka policijska škola, Zagreb, Hrvatska.

1. UVOD

Širenje mobilnih elektroničkih uređaja u protekla dva desetljeća znatno je utjecalo na sve aspekte ljudskih aktivnosti. Digitalne kamere i mobiteli postali su jednome dijelu populacije najvažnije sredstvo prenošenja dojmova i događaja. U takvim okolnostima javljaju se novi izazovi u definiranju privatnosti koja tradicionalno nije bila izložena velikom broju nepoznatih subjekata koji mogu prikupljati i prosljeđivati podatke poznatim i nepoznatim osobama (*Doyle*, 2013). Privatne stvari obuhvaćene snimkom mogu vrlo jednostavno postati dostupne širokoj javnosti uz brojne negativne posljedice (*Zittrain*, 2008: 112). Takve promjene u obuhvaćanju privatnosti traže prilagođavanje propisa tehnološkim izazovima i zaštitu privatnosti pred novim oblicima ugrožavanja.

Uređenje mogućnosti videosnimanja osoba na javnome mjestu nije jednostavno razmatrati u poredbenome pravu jer u državama Europske unije (dalje: EU) postoje različiti pristupi u pravnom reguliranju ovoga područja. U nekim su državama pojedini oblici ograničenja propisani u policijskom, prekršajnom ili kaznenom zakonodavstvu, a u nekim je sustavima zaštita slike osobe propisana u području autorskog prava. U ovome je radu analiza usmjerena na zaštitu osobnih podataka kao području na kojem su na europskoj razini već dulje vrijeme postavljeni osnovni zajednički standardi koji se mogu primjenjivati na situacije snimanja drugih osoba na javnome mjestu. Ovakvo je uređenje općenitije od drugih područja prava i moguće ga je primjenjivati neovisno o tome jesu li ispunjeni dodatni uvjeti iz nekih posebnih propisa koji mogu ograničavati snimanje u pojedinom pravnom sustavu (npr. zaštita tajnosti podataka, zaštita u okviru kaznenog prava itd.).

Iako je zaštita osobnih podataka već dugo predmet zajedničkog razmatranja na europskoj razini uz brojna detaljna tumačenja, u raspravama o definicijama i o opsegu zaštite javljaju se nova pitanja ili ponavljaju neka stara. Jedno od takvih pitanja odnosi se na dopuštenost videosnimanja policijskih službenika. S ciljem razmatranja toga pitanja, ovaj je rad usmjeren na analiziranje pravila o zaštiti osobnih podataka te na primjenjivost takvih pravila na snimanje policijskih službenika na javnome mjestu. Obuhvaćen je razvoj europskog prava zaštite osobnih podataka kroz konvencije, direktive, uredbe i neobvezujuće smjernice nadležnih tijela. S ciljem analiziranja relevantnih presuda, pretraživane su odluke Europskog suda (ES)[1] i Europskog suda za ljudska prava (ESLJP).[2] Ukratko je prikazan povijesni razvoj s ciljem pronalaženja začetaka pojedinih pravnih rješenja. Prikazan je odnos kaznenog postupovnog prava prema dopustivosti snimaka za dokazivanje u postupku.

O primjenjivosti općih pravila o zaštiti osobnih podataka na policijske službenike (odnosno na državne ili javne službenike) nema objavljenih znanstvenih ni stručnih radova. O nekim općenitim aspektima ovih pravila pisali su razni autori. Videonadzor na radnome mjestu razmatrali su *Gumzej i Dragičević* (2019), a razvoj europskih propisa prikazali su Čizmić i Boban (2018). Status privatnih snimaka u kaznenom pravu i kaznenom postupku detaljno su opisali *Martinović i Tripalo* (2017).

[1] Europski sud (službeni prijevod engl. *Court of Justice*), Luksemburg. Kolokvijalni naziv - Europski sud pravde.

[2] Europski sud za ljudska prava, Strasbourg, Francuska.

2. OSNOVNO O EUROPSKIM PROPISIMA

Zaštita osobnih podataka jedno je od prava koje je u razvoju europskih integracija imalo vrlo važnu poziciju, što podrazumijeva potrebu njegova potpunog afirmiranja i u onim članicama EU-a koje zbog povijesnog razvoja do potkraj 20. stoljeća možda nisu imale naglasak na takvim osobnim pravima građana. Tranzicijski su sustavi do početka demokratskih tendencija bili u većoj mjeri usmjereni na drugačije vrste prava građana. Intencija isticanja specifične uloge ovog prava pokazana je njegovim izričitim navođenjem u čl. 8. Povelje Europske unije o temeljnim pravima (dalje: Povelja).[3] Odredba načelno određuje zaštitu osobnih podataka (st. 1.), uz mogućnost obrade samo na pravičan (pošten) način za legitimne zakonske svrhe ili uz pristanak osobe (st. 2.). Ako ne postoji suglasnost osobe ili ako nije utemeljeno na zakonskim osnovama, prikupljanje osobnih podataka predstavlja povredu. Povreda može biti propisana u pojedinoj državi članici kao kazneno djelo, slično kao što je većinom propisano za povrede iste razine prava kao što je privatnost ili povreda osobne slobode. Za praćenje poštovanja pravila predviđeno je nadzorno tijelo koje se treba brinuti za neovisnu kontrolu nad provođenjem ovih pravila (st. 3.). S obzirom na to da je zaštita osobnih podataka jedno od temeljnih prava na razini Povelje, to znači da je potrebno vrlo usko tumačiti svako ograničenje tog prava. U odnosu na pravo privatnosti, u čl. 7. Povelje propisana je i općenita zaštita osobnog i obiteljskog života, doma i komunikacije.

Osnovni dokument koji uređuje zaštitu osobnih podataka u Europskoj uniji jest Opća uredba o zaštiti osobnih podataka (dalje: Uredba) koja je stupila na snagu 2018. godine.[4] Veći dio sadržaja Uredbe (engl. *General Data Protection Regulation - GDPR*) istovjetan je sadržaju prijašnje Direktive koju je naslijedila.[5] Na temelju Direktive donesena su brojna tumačenja i nastala je opširna sudska praksa koja se primjenjuje i putem nove Uredbe. Za provedbu pojedinih odredaba Uredbe u hrvatskom je pravu donesen odgovarajući zakon.[6]

Osim u okvirima EU-a, uređenje je zaštite osobnih podataka prije započeto i u djelokrugu Vijeća Europe koje je o zaštiti osobnih podataka 1981. godine donijelo Konvenciju o zaštiti pojedinaca vezanoj uz automatsku obradu osobnih podataka (dalje: Konvencija).[7] U toj Konvenciji uređena su osnovna načela koja su preuzeta i u druge dokumente u kojima su unapređivana i razvijana. Njezin utjecaj na pravnu regulaciju EU-a vidljiv je i kroz definicije pojedinih pojmova kao što su osobni podaci ili njihova obrada (čl. 2.) u kojima se može pratiti slijed preko Direktive do trenutačno vrijedeće Uredbe.

---

[3] Povelja Europske unije o temeljnim pravima, Službeni list EU, C 202/389, 7. lipnja 2016.

[4] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), Službeni list EU-a, L 119/1, 4. svibnja 2016.

[5] Direktiva 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka, Službeni list EU-a, 281/31, 23. studenoga 1995.

[6] Zakon o provedbi Opće uredbe o zaštiti podataka, Narodne novine br. 42/18.

[7] Konvencija 108 Vijeća Europe o zaštiti pojedinaca vezanoj uz automatsku obradu osobnih podataka; Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i dodatnog protokola uz konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi s nadzornim tijelima i međunarodnom razmjenom podataka, Narodne novine – međunarodni ugovori, br. 04/05.; Zakon o potvrđivanju izmjena i dopuna Konvencije 108, Narodne novine – međunarodni ugovori, 12/05.

Od drugih izvora Vijeća Europe potrebno je naglasiti Europsku konvenciju za ljudska prava (dalje: EKLJP)[8] koja nema zasebnu odredbu o zaštiti osobnih podataka kakvu ima Povelja, ali prema tumačenjima u judikaturi, osobni podaci potpadaju u područje zaštite privatnoga života. Za razliku od Europskog suda, EKLJP ne poznaje zasebno pravo na zaštitu osobnih podataka nego to promatra kao dio poštovanja osobnog i obiteljskog života iz čl. 8. EKLJP-a; te ga smatra konkretizacijom prava na privatnost u vezi s obradom osobnih podataka (*Satakunnan pr. Finske*, para. 8-28). Europski sud za ljudska prava zaključio je da pohranjivanje podataka koji se odnose na privatni život potpada pod primjenu zaštite privatnosti iz čl. 8. st. 1. EKLJP-a (*Amann*, para. 65); tako da se i u okviru Vijeća Europe u suštini ostvaruje podjednaka zaštita kao i putem Povelje odnosno Uredbe.

3. DEFINIRANJE VRSTE OSOBNIH PODATAKA NA SNIMCI

3.1. Izgled osobe kao osobni podatak

Pojam osobnih podataka definiran je u čl. 4. t. 1. Uredbe kao bilo koji podatak koji se odnosi na pojedinca koji je identificiran ili kojeg je moguće identificirati (engl. *identified or identifiable*).[9] Definicija obuhvaća izravni i neizravni oblik određivanja identiteta. Time je opseg primjene vrlo širok jer nije neophodno da je identitet naveden u trenutku obrade - već je dovoljno da su prikazana obilježja na temelju kojih osoba može biti posredno identificirana. Uredba navodi pojedine vrste podataka na koje se odnosi identitet: identifikacijski broj ili bilo koje drugo obilježje značajno za tjelesni, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet. U primjeni takve definicije nema poteškoća s izravnim ili očiglednim osobnim podacima (pravni identitet) koji mogu poslužiti u identificiranju, kao kada je Europski sud utvrdio da po prirodi stvari u ovu skupinu pripadaju podaci o imenu i prezimenu, telefonskim brojevima, zaposlenju i slični (*Lindqvist*, t. 24.). Takvi osobni podaci vode se u raznim evidencijama i registrima pojedinih ustanova. Rasprava se više vodila o pitanju može li se zaštita odnositi i na neka druga obilježja poput izgleda lica ili tijela osobe što ne predstavlja pravni identitet, ali je dio tjelesnih obilježja.

Primjer je stajalište jedne članice navedeno u mišljenju nezavisnog odvjetnika Suda u predmetu *Buivids*.[10] Jedna je članica EU-a smatrala da se ne radi o osobnim podacima ako se osobu ne može izravno identificirati iz fizičkog pojavljivanja na određenoj snimci, odnosno ako bi trebalo naknadno provesti značajne dodatne napore da bi se odredilo ime i prezime snimljene osobe. Na toj je snimci bilo više osoba, ali nisu bila navedena njihova imena, pa

[8] Konvencija za zaštitu ljudskih prava i temeljnih sloboda, Narodne novine - međunarodni ugovori, br. 18/97., 6/99., 14/02., 13/03., 9/05., 1/06., 2/10.

[9] U prijevodu dokumenta korišten je pojam utvrđenog identiteta što je međutim u kriminalističkom stručnom jeziku poseban postupak prema policijskom zakonodavstvu korištenjem prirodoznanstvenih ili tehničkih metoda (daktiloskopija, DNK itd.).

[10] Predmet *Buivids* odnosi se na građanina koji je pozvan u policijske prostorije radi upravnog predmeta. Tijekom kratkog vremena boravka u policijskoj postaji, kamerom je snimio policijskog službenika koji je radio na njegovu predmetu, te druge policijske službenike koji su odlazili na teren.

pretraživanjem interneta ne bi bilo moguće njihovo pronalaženje po imenu kao bitnome dijelu identiteta (za razliku od slučaja *Lindqvist* u kojem su imena bila navedena).[11]

Međutim, definicija iz Uredbe šira je od takvih stajališta o izravnom navođenju imena kao samo jednog oblika identificiranja, te je dovoljno da postoji hipotetička vjerojatnost određivanja identiteta na temelju tjelesnih obilježja osobe. Za fizičko su identificiranje dovoljna obilježja po kojima je osobu moguće individualizirati, a u tu skupinu svakako pripadaju obilježja lica, tijela, glasa i slična obilježja. Prema odlukama ES-a, izgled osobe snimljen kamerom sadržava osobne podatke (engl. *personal data*), ukoliko je iz nje moguće otkriti identitet dotične osobe (*Ryneš*, t. 22.).[12] Sud je u slučaju *Buivids* zaključio da je snimatelj napravio kratku videosnimku na kojoj je obuhvaćeno lice i glas pojedinih policijskih službenika, te zaključuje da takva obilježja predstavljaju njihove osobne podatke (*Buivids*, t. 28.). To znači da obilježja na temelju kojih je moguće identificirati osobu nisu samo njihovi izravno navedeni podaci koji čine pravni identitet, nego to mogu biti tjelesna obilježja kao što je izgled lica, tijela, glas, način kretanja i druga obilježja osobe koja mogu neizravno poslužiti identifikaciji (npr. oznaka pripadnosti policijskoj jedinici, broj službene značke). Ovakav je pristup sličan metodama utvrđivanja identiteta u kriminalistici koje su usmjerene na pojedina obilježja koja predstavljaju fizički identitet. Pojam osobnih podataka vrlo je širok te obuhvaća bilo koji podatak objektivne ili subjektivne prirode koji se može povezati s određenom osobom, što je i bila intencija tijekom donošenja europskog zakonodavstva (*Demetzou*, 2020: 130). U definiciji Uredbe navedena su i razna druga obilježja poput ekonomskih, kulturnih ili socijalnih - što upućuje na vrlo široke mogućnosti primjene.

Smjernica Europskog nadzornika za zaštitu podataka (engl. *European Data Protection Supervisor - EDPS*) na temelju sudske prakse istaknula je da osobni podatak obuhvaća prikaze lica koje je moguće prepoznati (engl. *recognisable facial images*). Za definiciju osobnih podataka nije bitno zna li snimatelj točan pravni identitet osobe, niti je bitno ima li hipotetičke tehničke mogućnosti ili suradnju s odgovarajućim ustanovama za provedbu takve identifikacije. Dovoljno je da se radi o sadržaju na temelju kojeg je moguće prepoznati osobu (*EDPS*, 2010: 8); odnosno da podaci potpomažu određivanje identiteta nekog pojedinca (*Bygrave*, 2002). U odnosu na kvalitetu snimke ili cjelovitost obuhvaćanja izgleda lica ili tijela osobe ili njezinih drugih osobnih obilježja, nije nužno da se radi o cjelovitim slikama, nego se može raditi i o manje jasno vidljivom licu ili kojem drugom dijelu tijela, ali takav materijal može predstavljati osobni podatak ako se iz njega može neizravno odrediti identitet. Nije nužno da se radi o obilježjima koja se rabe za biometrijsko identificiranje za koje Uredba u čl. 4. t. 14. kao primjer navodi računalne sustave prepoznavanja lica ili otisaka prstiju.[13] Primjer neizravnog određivanja identiteta jest snimka niske rezolucije, ali se iz odijevanja, stasa, kretanja, vrste prostora, predmeta koje nosi i sličnih obilježja može zaključiti o kojoj se osobi radi, osobito

[11] Predmet *Lindqvist* odnosi se na internetske stranice župe na kojima su bili objavljeni osobni podaci zaposlenika kao što su ime, prezime, adrese, pojedini telefonski brojevi, obiteljski status pojedinih osoba, uz pojedine šaljive dodatke poput ozljede ili bolovanja. Podaci su objavljeni bez njihova znanja i suglasnosti.

[12] Predmet *Ryneš* odnosi se na videonadzor kojim je sniman dio javnog prostora, prometnica ispred kuće te susjedni ulaz. Snimka je kontinuirano zapisivana preko starijih snimaka, a uređaj nije imao zaslon te nije bilo moguće bez drugih komponenti pregledavati što se snima.

[13] „osobni podaci dobiveni posebnom tehničkom obradom u vezi s tjelesnim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci“, čl. 4. t. 14. Uredbe.

uz pomoć onih kojima je poznata navedena lokacija i službenici koji se tamo učestalo kreću (*EDPS*, 2010: 8). Ovakvo tumačenje obuhvaća i razne objekte ili predmete na temelju kojih se mogu izvoditi zaključci o identitetu policijskog službenika (npr. registarske oznake vozila, kućni broj ili izgled zgrade koju čuva itd.).

Osobni podaci mogu biti anonimizirani (t. 26. uvodne izjave Uredbe) uklanjanjem navedenih osobnih obilježja sa snimke (npr. izmjena glasa, zamućivanje lica, zamućivanje registarskih oznaka). Ako su na snimci netočno navedeni neki podaci o pravnom identitetu, primjerice pseudonimi ili lažna imena, ali je i nadalje vidljiv pravi tjelesni izgled osobe, to ne znači da su uklonjeni osobni podaci na temelju kojih je osobi moguće odrediti pravi identitet. Razina složenosti identificiranja osobe nije kriterij definicije. Definicija može biti ispunjena i ako se radi samo o hipotetičkoj mogućnosti identificiranja, neovisno o tome je li ju netko konkretno iskoristio u određenome roku nakon snimanja.

3.2. Tumačenja ESLJP-a o osobnim podacima na snimkama

Istovjetno tumačenje o tjelesnom izgledu kao osobnom podatku odavno je zastupljeno i u gledištima ESLJP-a. Taj je sud također zaključio da slika (fotografija) ili snimka izgleda osobe predstavlja podatak koji je zaštićen u okviru privatnosti osobe. Izgled osobe (engl. *person's image*) predstavlja jedan od glavnih atributa osobnosti prema kojem se osoba razlikuje od drugih i radi toga je takvo obilježje sastavni dio koji se štiti u okviru privatnog života. Slijedom toga, slike (ili snimke) također potpadaju u zaštitu privatnosti po čl. 8. EKLJP-a (*Reklos i Davourlis pr. Grčke*, para. 40).

U Konvenciji je osobni podatak definiran od 1981. godine kao svaka obavijest koja se odnosi na određenog ili odredivog pojedinca (čl. 2.). Nadležno je radno tijelo po toj Konvenciji (*CJ-PD*, 2003) promatralo aktivnost videosnimanja kao primjer obuhvaćanja osobnih podataka, radi čega je izdalo načela o videonadzoru koja bi se trebala primjenjivati neovisno o tome radi li se o javnom ili privatnom prostoru. Jedno od tih načela (t. 4.) preporučuje da snimljena osoba ne bude prepoznatljiva na objavljenoj snimci.

4. DEFINIRANJE OBRADE PODATAKA SNIMANJEM

4.1. Snimanje kao obrada podataka

Iz prethodno navedenih definicija proizlazi da lice osobe, njezin izgled i slične individualne tjelesne karakteristike predstavljaju osobne podatke, ali je potrebno razjasniti sljedeći uvjet o postojanju aktivnosti obrade tih podataka (*Tzanou*, 2020: 21). Prema čl. 4. t. 2. Uredbe, obrada je definirana vrlo široko te obuhvaća bilo koji pojedinačni postupak ili skup postupaka koji se provode na automatiziran ili neautomatiziran način. Kao primjeri navedeni su prikupljanje, snimanje, organiziranje, pohranjivanje, prilagođavanje, pronalaženje, korištenje, objavljivanje, kombiniranje, brisanje i druge radnje. Dakle, među ovim brojnim aktivnostima navedeno je prikupljanje, bilježenje i pohrana podataka (engl. *collection, recording, storage*), što su aktivnosti koje se provode snimanjem ili fotografiranjem. I prema

Konvenciji, automatska obrada podataka obuhvaća cjelovito ili djelomično automatizirane djelatnosti pohrane, unosa, širenja i druge djelatnosti (čl. 2. t. c. Konvencije).

Europski je sud zaključio da snimanje videozapisa na uređaj za snimanje, odnosno na tvrdi disk elektroničkog uređaja, predstavlja automatiziranu obradu podataka (*Ryneš*, t. 25.). Načela zaštite odnose se na bilo koju informaciju, neovisno o kojem se načinu obrade ili mediju radi. Kao što je navedeno u uvodnim izjavama Uredbe, obrada se odnosi na sva sredstva kojima se može odrediti neka osoba (t. 26. recitala Uredbe) što po prirodi stvari znači da obuhvaća i digitalno snimanje (*DPWP*, 2004: 6). Obrada zvuka i slike upravo je bio jedan od glavnih ciljeva donošenja prijašnje Direktive, što je i naglašeno u t. 14. uvodnih izjava Direktive o razvoju suvremenih tehnika kojima se mogu obuhvaćati osobni podaci.[14]

Nadovezujući se na aktivnost snimanja, postavljalo se pitanje je li za pojam obrade podataka dovoljno samo videosnimanje (odnosno fotografiranje) ili je potrebno poduzimati i druge računalne aktivnosti da bi bio zadovoljen uvjet obrade podataka, primjerice analiziranje i povezivanje snimke s nekim drugim evidencijama koje sadrže pravne podatke o identitetu. Smjernice su preporučivale široko tumačenje prema kojem se pojam obrade podataka primjenjuje i kada se provodi samo aktivnost snimanja ili fotografiranja neovisno o tome povezuje li se odmah taj podatak u sustavu s određenom osobom, odnosno s njezinim drugim podacima. Za obradu podataka nije neophodno računalno prepoznavanje lica ni bilo kakva slična aktivnost određivanja identiteta (*DPWP*, 2004: 15). Iz navedenog slijedi da definicija obrade podataka može biti ispunjena bez obzira na to radi li se o postupcima klasificiranja snimki, računalnog prepoznavanja osoba, biometrije, unošenja u baze podataka i slično. Nevažan je pravni status entiteta koji provodi obradu podataka i razina tehnološke opremljenosti, odnosno radi li se o velikoj ustanovi ili o nekom subjektu koji nema složenu tehničku opremu (*Voigt*, 2017: 17).

Videosnimanje potpada pod definiciju obrade podataka neovisno o tehničkim karakteristikama sustava. Nebitno je provodi li sustav permanentno snimanje ili samo kod reagiranja određenih senzora, je li sustav fiksni ili prijenosni, na koji način dostavlja snimke i drugo (*DPWP*, 2004: 15). Ovo je značajno za primjenu pojedinih ovlasti u trenutku snimanja jer se zaštita ne odnosi samo na posljednju fazu objavljivanja na određenim medijima. Već se i u fazi snimanja podaci prikupljaju na samome mjestu događaja i time može biti ostvarena povreda. U slučaju *Ryneš* (t. 59.) nezavisni odvjetnik Suda iznio je dvojbu o pitanju da li je ograničenje prava na poštovanje privatnog života moguće tek objavljivanjem drugim osobama, ili je dovoljna i sama radnja snimanja te pohranjivanja snimke. Dovoljno je ako je provedeno snimanje ili pohranjivanje kao obrada podatka, neovisno o tome je li taj podatak javno prikazan (*Digital Rights Ireland i Seitlinger*, t. 34.). Kazneno djelo nedozvoljene uporabe osobnih podataka u našem zakonodavstvu također se sastoji od aktivnosti prikupljanja, obrade ili korištenja (čl. 146. st. 1. Kaznenog zakona, dalje: KZ).[15]

4.2. Razlike između stalnog videonadzora i jednokratnog snimanja

Sustavi stalnog videonadzora koji su ugrađeni u pojedinim objektima radi povećavanja sigurnosti mogu prikupljati veliku količinu podataka o pojedinim osobama, poput njihovih

[14] „snimanje, pohranjivanje ili komuniciranje zvučnih ili slikovnih podataka".

[15] Kazneni zakon, Narodne novine br. 125/11., 144/12., 56/15., 61/15., 101/17., 118/18., 126/19.

navika, druženja i sličnih. Videonadzor je definiran kao stalna i sustavna radnja, neovisno o trajanju pohrane, i nedvojbeno je bio obuhvaćen prijašnjom Direktivom kao što slijedi iz njezine uvodne izjave (recital) br. 16.[16] Europski je sud utvrdio da snimanje osoba na uređaju za kontinuirano snimanje potpada u automatsku obradu osobnih podatka (*Ryneš*, 25). Zbog ovih je razloga u nekim europskim državama čak ograničeno i snimanje prometa kamerom (engl. *dashcam*) iz vozila (*Balzer, Nugel*, 2014).

O razlikama obrade podataka u sustavima stalnog nadzora i jednokratnog snimanja izražavana su različita gledišta. Nezavisni odvjetnik Suda u predmetu *Ryneš* smatrao je da pojam automatske obrade podataka može obuhvaćati samo stalni videonadzor. Naveo je da su pravna pitanja vezana uz uporabu mobilnih uređaja poput digitalnih fotoaparata, mobilnih telefona ili digitalnih kamera sasvim drugačije pravne prirode (*Ryneš*, Mišljenje, t. 30.). U odnosu na primjedbu da jednokratno snimanje ne predstavlja obradu podataka, nezavisni odvjetnik Suda u slučaju *Buivids* bio je na posve suprotnom stajalištu od nezavisnog odvjetnika Suda u slučaju *Ryneš*, te je izrazio gledište da je definicija obrade strukturirana alternativno, odnosno ne mora biti ispunjen uvjet unošenja snimki u složeniji sustav (*Buivids*, Mišljenje, t. 34.). Takvo je stajalište Sud prihvatio. Pojedine su države smatrale da jednokratno snimanje ne bi trebalo ulaziti u pojam obrade podataka (*Buivids*, Mišljenje, t. 32.), jer se kod permanentnog snimanja podaci unose u neki oblik sustava; dok je za razliku od toga situacija drugačija kada neka osoba snima samo jednu snimku. Za takve su aktivnosti smatrali da se ne bi mogle tumačiti kao da se radi o organiziranim aktivnostima, odnosno strukturiranoj formi unošenja podataka. Sud nije preuzeo takva mišljenja.

Za problem razlikovanja sustava stalnog nadzora od jednokratnih ili povremenih oblika snimanja, mjerodavno je tijelo preporučilo da se ista mjerila kakva se odnose na složene mreže povezanih kamera, također odnose i na bilo koji drugi manji uređaj ili sustav, neovisno o tome je li fiksni ili mobilni, ako ima mogućnost obuhvaćati neke slikovne podatke (*EDPS*, 2010: 7). Kao primjer uređaja koji također ispunjava definiciju obrade osobnih podataka eksplicitno se navode mobilne kamere, prijenosne videokamere, fotoaparati, *web*-kamere i slični uređaji potrošačke elektronike. U tom značenju, obrada se ne odnosi samo na permanentno snimanje, nego i na *ad hoc* snimanje. Ako se za snimanja rabe bespilotne letjelice, također potpadaju pod ovakva pravila (*O'Malley*, 2015).

Razlika između dugotrajnih ili jednokratnih snimki može biti u količini podataka koji se obrađuju, ali za primjenu europskih pravnih standarda zaštite nije bitno koliko su opsežni podaci, nego je dovoljno da je obuhvaćena minimalna razina. Osim toga, ponekad i na vrlo kratkoj snimci može biti sadržana znatno veća količina osobnih podataka - ovisno o vrsti događaja i namjeni snimke. Prikazana argumentacija opravdava zaključak da za pojam obrade osobnih podataka nije potrebno sustavno ili višekratno prikupljanje velike količine podataka. Europski sud i u predmetu snimanja policijskih službenika *Buivids* navodi odredbu o definiciji obrade podataka iz čijeg teksta proizlazi da se pravila o zaštiti osobnih podataka odnose na bilo koju operaciju, odnosno bilo koju djelatnost koja predstavlja obradu osobnih podataka (*Buivids*, t. 36.).

Pojam obrade podataka Sud je u predmetu *Ryneš* smatrao ispunjenim time što je videosnimka pohranjena na uređaju kontinuiranog snimanja (engl. *continuous recording device*), odnosno na tvrdom disku tog sustava, što prema definiciji predstavlja automatsku

[16] „obrada zvučnih i slikovnih podataka, kao u slučajevima videonadzora".

obradu osobnih podataka (*Ryneš*, t. 23., 25.). U slučaju *Buivids* Europski je sud utvrdio da je građanin koristio prijenosnu digitalnu videokameru, što je Europski sud po definiciji također smatrao uređajem za kontinuirano snimanje, neovisno o trajanju snimke. Kontinuirano snimanje znači da se snimka po prirodi stvari sastoji od većeg broja sličica u sekundi, a ne da se snimanje provodi kroz dulje razdoblje. Dakle, takvo snimanje prema odluci Europskog suda predstavlja proces obrade osobnih podataka - automatskim načinom u smislu definicije obrade i potpada pod primjenu europskih pravila o zaštiti osobnih podataka.

5. OBRADA PODATAKA OBJAVLJIVANJEM SNIMKE

5.1. Postavljanje snimke na internetske stranice

Aktivnost postavljanja snimke na internet potrebno je promatrati odvojeno od aktivnosti snimanja jer ih mogu provoditi nepovezani subjekti. Ponekad su snimke nastale kao rezultat djelatnosti subjekata koji ih nisu namjeravali objavljivati, ali ih je objavio neki drugi subjekt kojem je snimka u međuvremenu postala dostupna. Za postojanje odgovornosti subjekta koji je objavio snimku bitno je definirati potpada li njegova zasebna aktivnost objavljivanja također u pojam obrađivanja podataka, ili je aktivnost obrade samo ono što je napravio snimatelj.

O ovome pitanju također su izražena razna stajališta, poput onih prikazanih u slučaju *Lindqvist.* Jedno je od stajališta da sama aktivnost postavljanja na internetsku stranicu ne bi trebala predstavljati automatsku obradu podataka, nego da automatska obrada takvih podataka započinje tek kada internetske tražilice indeksiraju sadržaj na svoje popise. Kada bi neki korisnik pretraživao po tim ključnim riječima, rezultat bi bila poveznica na osobne podatke na toj stranici. Prema takvu stajalištu koje je zastupao *Lindqvist*, slijedilo bi da obradu podataka na internetu ustvari provode pojedini sustavi pretraživanja, a ne fizičke osobe koje postavljanju neke podatke na internet.

Prema navodima u mišljenju nezavisnog odvjetnika Suda, Vlada je u slučaju *Lindqvist* smatrala prihvatljivom širu definiciju, odnosno da svaka računalna obrada podataka predstavlja automatsku obradu podataka. Podaci koji se snimaju na računalu prolaze kroz interne procese raščlanjivanja u binarne oblike da bi ih mogle obrađivati hardverske komponente. Dio tih procesa sastavni je dio rada računala i ne provodi ih korisnik, niti mu je poznato kako se to obavlja u dijelovima računala. Prema ovakvom obliku tumačenja, obrada podataka postoji svaki put kada računalo radi svojih unutarnjih procesa pretvara podatke. Čini se da bi onda obrada podataka postojala čim je neka slika presnimljena na neku memorijsku jedinicu jer je tada računalo moralo provesti pojedine procese prijenosa. Ovakvo je tumačenje preširoko jer se radi o obradi koja nije namijenjena poboljšavanju identificiranja, nego o uobičajenoj obradi za potrebe djelovanja računalnog sustava.

Vlasti su smatrale da svaki proces poput unošenja podataka u neki računalni program također predstavlja obradu podataka (*Lindqvist*, t. 21.). Čini se da prema ovakvu tumačenju nije ključno da su podaci obrađeni s ciljem njihova unošenja u pojedine baze podataka, odnosno računalne programe s ciljem pretraživanja ili klasificiranja. Učitavanje na internetske stranice traži korištenje najmanje jednog računala na kojem su podaci uneseni, i drugog računala koje predstavlja poslužitelj povezan s internetom. Europska je komisija također

smatrala da stavljanje na internetske stranice po prirodi stvari podrazumijeva automatsku obradu (*Lindqvist*, t. 22.).

Europski se sud nije očitovao o najširoj definiciji prema kojoj bi već i hardverska obrada predstavljala automatsku obradu, nego je aktivnost stavljanja na internetsku stranicu smatrao dovoljnim da bi se radilo o pojmu obrade (*Lindqvist*, t. 25.). Za to pitanje Sud je zaključio da učitavanje stranica obuhvaća pojedine računalne procedure i druge operacije pristupačnosti ostalim korisnicima interneta, i da se barem u nekome dijelu tih aktivnosti radnje provode automatski (*Lindqvist*, t. 26.). Sud smatra opravdanim zaključiti i u slučaju *Buivids* da aktivnost objavljivanja videosnimke koja sadržava osobne podatke policijskih službenika, na stranicu na kojoj će korisnici moći gledati, dijeliti ili poslati videosnimku - predstavlja obradu podataka u cjelini ili djelomično provedenoj na automatski način u značenju definicije (*Buivids*, t. 39.). Uključivanjem internetskih portala koji mogu dodatno obrađivati snimke, može biti proširen skup subjekata koji provode obradu osobnih podataka, neovisno o tome što nisu uključeni u nastanak ili postavljanje snimke. To je posljedica neodređenosti Uredbe zbog koje može biti upitna i njihova odgovornost (*Mahieu*, 2019).

5.2. Prijenos uživo bez snimanja

Prenošenje snimke uživo bez pohranjivanja na određeni medij specifična je situacija u kojoj je također potrebno analizirati primjenu definicije o obradi podataka. U takvim slučajevima ne radi se o pohranjivanju snimke na računalnome sustavu snimatelja, nego se snimka uživo prosljeđuje preko videoveze (engl. *live video-monitoring*) – a što je moguće izravnim prijenosom na pojedine internetske stranice koristeći razne programe koji su namijenjeni prijenosima. Ovisno o načinu postavljanja prijenosa, može ih gledati neograničeni broj osoba ili pak snimke mogu biti namijenjene samo užem krugu registriranih osoba. Ilustrativan primjer može biti uživo prenošenje nekog događaja u kojem postupaju policijski službenici.

Ovakvo djelovanje također ulazi u pojam obrade podataka. Primjer kojeg navodi *EDPS* odnosi se na opciju kada bi pojedini događaj bio nadziran uređajima, ali snimka ne bi bila pohranjena na određeni medij (*EDPS*, 2010: 9), nego bi samo bio prenošen do osoba koje bi mogle pratiti događaje. To je također protumačeno kao aktivnost koja obuhvaća osobne podatke i potpada pod primjenu definicija. Obrada podataka prema gledištu nezavisnog odvjetnika Suda odnosi se i na otkrivanje podataka trećoj strani iako to otkrivanje nije bilo predviđeno u trenutku njihova prikupljanja (*Smaranda Bara*, Mišljenje, t. 57.).

6. PRISTANAK NA SNIMANJE NA JAVNOME MJESTU

6.1. Obilježja pristanka na snimanje

Pravo na zaštitu osobnih podataka povrijeđeno je ako snimljena osoba nije dala privolu na snimanje (pristanak, engl. *consent*). Preostalih pet zakonskih osnova navedenih u čl. 6. st. 1. Uredbe odnosi se na oblike snimanja koje ne provode građani (ugovorne obveze, javni interes itd.). Pristanak je uvjet snimanja i prema čl. 8. st. 2. Povelje. Obilježja pristanka detaljno su

protumačena u pravnim izvorima koji su prethodili Uredbi, kao i u pratećim smjernicama za tumačenje. Prema definiciji u čl. 4. st. 11. Uredbe, pristanak znači slobodno odabrano, specificirano, informirano i nedvosmisleno izražavanje namjera kojima subjekt kroz izjavu ili jasno izraženom reakcijom (potvrdnom radnjom) pokazuje suglasnost da mogu biti obrađeni njegovi osobni podaci. Takva je definicija neznatno proširena u odnosu na stariju definiciju iz čl. 7. t. a. Direktive dodavanjem izričaja da pristanak može biti dan izjavom ili izražavanjem na drugi način; dok su ostali elementi uvedeni i protumačeni znatno prije (*WP*, 2011). Traženje pristanka treba biti podložno strogim zahtjevima s obzirom na to da se odnosi na temeljna prava iz Povelje (*EDPB*, 2020: 5).

Pristanak može biti valjana osnova samo ako je subjekt bio slobodan odlučivati, odnosno ako je doista imao mogućnost prihvatiti ili odbiti obradu podataka. Pristanak nije dobrovoljan ako postoji nerazmjer između moći subjekta koji traži pristanak i subjekta koji bi trebao davati pristanak (*Gawronski*, 2019). Pristanak je slobodan ako osoba neće imati negativnih posljedica u slučaju odbijanja, ako se ne osjeća prisiljenom i ako doista ima mogućnost izbora (*EDPB*, 2020: 7; *WP*, 2018: 5). Uvjet specifičnosti odnosi se na poznavanje konkretne svrhe radi koje se podaci obrađuju. Subjekt koji prikuplja podatke trebao bi transparentno prikazati radi čega se podaci prikupljaju. Nije dopušteno naknadno određivanje svrhe na koju osoba nije pristala. Trebalo bi konkretno definirati na što se odnosi, izbjegavajući općenite pojmove poput „multimedijalne obrade". Potrebno je naznačiti o čemu se radi, npr. objavljivanje na konkretnom internetskom portalu, uključivanje u određeni dokumentarni film i slično (*EDPB*, 2020: 14).

Povrede su osobnih podataka česte upravo u području naknadne promjene svrhe snimanja. Ako snimke potječu iz sustava koji je postavljen na nekom objektu s ciljem zaštite imovine i osobe su pristale biti snimljene za tu svrhu, bilo bi neobično kada bi snimke izlazile u javnost radi prikazivanja nekih neugodnih događanja koji služe zabavi ili ismijavanju. Takvo objavljivanje predstavlja povredu svrhe prikupljanja i moguće je pokretanje odgovarajućeg postupka prema nadležnim subjektima. Slično vrijedi i za snimke policijskih službenika koji su snimljeni u nekoj javnoj prigodi, a potom mediji ponavljaju iste slike ili snimke kod sasvim drugačije vrste događaja čime ih se stavlja u izmijenjen kontekst. Takav urednički rad osim povrede osobnih podataka može predstavljati i kazneno djelo protiv časti i ugleda, ovisno o razini netočnog prikazivanja činjenica.[17]

Prema EDPB-u, uvjet informiranosti znači potrebu poznavanja identiteta subjekta koji provodi obradu, svrhu radnje obrade podatka, vrstu i oblik podataka koji će biti obrađeni, pravo povlačenja pristanka i druge okolnosti za specifične situacije. Uz identitet subjekta koji provodi obradu mora biti poznat i identitet svih ostalih subjekata kojima će podaci biti proslijeđeni na obradu. Ovakvi se podaci traže radi toga da bi davatelj suglasnosti bio upoznat kome daje pristanak i da podaci kasnije ne bi bili prebačeni nekom drugom subjektu koji bi ih koristio za neke drugačije ciljeve. Navedeni minimum obavještavanja može biti napisan, izrečen, poslan porukom ili dostavljen na drugi način. Osoba koja je dala pristanak, naknadno ga može povući (*EDPB*, 2020: 15).

[17] Npr. kod vijesti o određenom kaznenom djelu (npr. korupcija, zlouporaba položaja u policiji itd.) neki mediji ponavljaju dostupne snimke sasvim drugih policijskih službenika te gledatelji ili čitatelji stječu dojam da su upravo to okrivljeni policijski službenici.

6.2. Prethodnost pristanka

Pristanak na obradu osobnih podataka mora biti izražen prije početka obrade podataka, što bi u ovdje promatranim slučajevima značilo da snimatelj mora prije početka snimanja zatražiti pristanak osobe koju će snimati. Iako taj uvjet prethodnosti nije izričito naveden u odredbama važeće Uredbe kao što nije bio ni u prethodnoj Direktivi, otprije je sastavni dio tumačenja (*WP*, 2018: 17). Uvjet prethodnosti jasno proizlazi iz izričaja odredbe u kojoj je pojam gramatički izražen u prošlome vremenu, što znači da pristanak mora biti dan prije početka obrade. Takvo je tumačenje preuzeo i odbor koji donosi smjernice tumačenja prema novoj Uredbi (*EDPB*, 2020: 20). Prema njihovim smjernicama, osoba koja namjerava snimati druge osobe trebala bi zatražiti pristanak prije snimanja i također navesti minimalne činjenice.

Način izražavanja pristanka može biti potpisivanjem određene izjave, iako su moguća i usmena dopuštenja koja bi, prema smjernicama EDPB-a, trebala biti snimljena jer bi kasnije moglo biti poteškoća u dokazivanju. Preporuke o snimanju pristanka bile su sastavni dio tumačenja prethodne Direktive (*WP*, 2018: 17), a i prije toga mjerodavna radna skupina detaljno je opisala način uvođenja ovih pravila (*WP*, 2011: 5). Teret dokazivanja postojanja pristanka jest na subjektu koji obrađuje podatke prema čl. 7. st. 1. Uredbe. U slučaju dvojbe o tome je li osoba dala pristanak na obradu podataka, snimatelj će morati dokazivati da je pristala (*EDPB*, 2020: 22).

U slučaju *Buivids* osoba je snimala policijske službenike digitalnom kamerom. Neki od službenika uočili su kameru jer nije bila prikrivena. Međutim, možda nisu znali je li kamera uključena niti ih je zanimalo zbog čega ju osoba drži. Neovisno o tome, njihovo uočavanje kamere nije oblik izražavanja pristanka na snimanje. Tijekom sudske rasprave *Buivids* je potvrdio da nije imao privolu niti za snimanje niti za objavljivanje snimaka policijskih službenika (*Buivids*, Mišljenje, t. 64.). Već i početak snimanja bez traženja suglasnosti po ovim odredbama dovodio bi do povrede. Zaštita osobnih podataka ne bi bila potrebna ako se radi o javnom događanju u kojem sudjeluju pojedini viši policijski službenici ako su na događaj pozvani i mediji, primjerice na neke javne svečanosti, obljetnice, pokazne vježbe ili slične događaje namijenjene pokazivanju u javnosti.

Sloboda pristanka policijskog službenika na davanje pojedinih osobnih podataka nije narušena zakonskom obvezom pokazivanja službene značke i iskaznice tijekom primjene pojedinih policijskih ovlasti na zahtjev građana (čl. 17. st. 2. ZPPO-a).[18] Ta je obveza oblik kojim se službenik predstavlja u smislu pripadnosti tijelu vlasti, a ne u smislu dužnosti iznošenja svojih osobnih podataka ili nekih aspekata privatnosti. Pokazivanje iskaznice ili značke ne podrazumijeva pravo građana na registriranje pojedinih osobnih podataka naznačenih na iskaznici poput imena ili prezimena, broja iskaznice, broja značke i sličnih obilježja. Takva obilježja također mogu poslužiti određivanju identiteta te potpadaju u osobne podatke i zaštićena su Uredbom. To međutim ne sprječava mogućnost korištenja takvih obilježja s ciljem prijave policijskog službenika nadležnim tijelima u slučaju sumnje na neku nezakonitost, ali se onda podrazumijeva korištenje u mjerodavnim postupcima, a ne za javno prikazivanje takvih podataka. Načelo javnosti u postupanju policije (čl. 9. ZPPO-a) ne obuhvaća obvezu uvida u sve osobne podatke ili privatna obilježja policijskih službenika, nego općenito upoznavanje javnosti s postupcima, rezultatima, načinom donošenja pojedinih pravila, nadzorom zakonitosti i sličnim okolnostima.

[18] Zakon o policijskim poslovima i ovlastima, Narodne novine br. 76/09., 92/14., 70/19.

6.3. Utjecaj pristanka na primjerke snimaka prema praksi ESLJP-a

Prema presudama ESLJP-a, pravo privatnosti iz čl. 8. EKLJP-a obuhvaća i pravo osobe na kontrolu daljnjeg korištenja slike osobe (*Bogomolova pr. Rusije*, para. 52;[19] *Reklos i Davourlis pr. Gr*čke, para. 40).[20] To znači da osoba osim što ima pravo pristati ili odbiti aktivnosti snimanja, ima i pravo odbijanja objavljivanja ili publiciranja (engl. *the right to refuse publication*). Uz to, ovo pravo obuhvaća i pravo pojedinca na prigovor snimanju, prigovor načinu pohranjivanja i kasnijoj reprodukciji slike. Učinkovita zaštita podrazumijeva traženje pristanka osobe prije slikanja, a ne tek kasnije kada se slika objavljuje.[21] Stoga ESLJP smatra da bi u protivnom ključni atribut osobnosti bio u rukama drugih osoba, a osoba koja je snimljena ne bi imala kontrolu nad svojom slikom (*Reklos i Davourlis pr. Grčke*, para. 40-42).

Tako ESLJP ima vrlo opsežnu judikaturu o aktivnostima pravnih ili fizičkih osoba u objavljivanju raznih vrsta snimaka.[22] Osobni podaci prikupljeni bez suglasnosti osobe ne mogu postati vlasništvo snimatelja kojim bi on dalje raspolagao (*Lynskey*, 2015: 231). Primjer povrede naknadnom uporabom snimaka mogu biti razne vrste snimaka koje su izvorno nastale uz suglasnost osobe (npr. u odnosima unutar obitelji, intimnoj vezi, prijateljstvu, radnom mjestu, školi, sportskom klubu itd.), a nakon narušavanja međusobnih odnosa, netko od sudionika javno objavljuje snimke bez pristanka snimljenih osoba. U opisu kaznenog djela nedozvoljene uporabe osobnih podataka iz čl. 146. st. 1. KZ-a, obuhvaćeno je i korištenje podataka.

Nadalje, ESLJP traži uvjet pristanka prije snimanja (engl. *prior consent*), ali i naknadno ostvarivanje kontrole nad svim ostalim oblicima slike što bi obuhvaćalo i primjerke koji se nalaze kod snimatelja (engl. *retention by the photographer, Reklos i Davourlis pr. Grčke*, para. 43). Kod klasičnog snimanja to obuhvaća i negative, a kod digitalnih oblika snimanja to bi moglo obuhvaćati ostale primjerke koje snimatelj pohranjuje na svojim memorijskim karticama u kameri, na mobitelu ili na drugim uređajima. To je u skladu s definiranom ulogom pristanka prema Uredbi i tumačenjima Europskog suda u odnosu na daljnju obradu podataka, iako ES nije donio odluku u kojoj bi izričito odlučivao o ovakvoj situaciji. Pitanje je vrlo značajno za postupke policijskih službenika prema snimkama koje se nalaze na uređajima kojima su građani snimali druge osobe bez njihova pristanka. Ako je uređaj sredstvo kojim je počinjeno kazneno djelo i na njemu se nalaze sporne snimke, moguće je primijeniti pojedine policijske ovlasti ne samo prema osobi, nego i u odnosu na uređaj i snimku.

Agencija za zaštitu osobnih podataka (dalje: AZOP; 2016 i 2017) također se bazira na promatranju pristanka osobe koju se snima u tumačenju pravila o zaštiti osobnih podataka policijskih službenika, te zaključuje da bez pristanka policijskog službenika ne nalazi zakoniti

---

[19] Slučaj *Bogomolova* odnosi se na objavljivanje fotografije osobe na naslovnici brošure iako nije zatražena suglasnost snimljene osobe, a dodatna je okolnost to što je izdanje bilo o specifičnoj grupi osoba među koje slikana osoba ne pripada (siročad).

[20] Slučaj *Reklos* odnosi se na uslugu snimanja novorođenčadi u privatnoj klinici bez suglasnosti roditelja.

[21] „obtaining the consent of the person concerned at the time the picture is taken and not simply if and when it is published", *Reklos i Davourlis pr. Grčke*, para. 40.

[22] Od ostalih značajnijih povreda čl. 8. EKLJP-a veznih uz objavljivanje snimaka u medijima moguće je izdvojiti slučaj *Bremner pr. Turske* o televizijskoj emisiji skrivene kamere; *Peck pr. Ujedinjenog Kraljevstva* o snimke pokušaja samoubojstva na javnome mjestu što je slučajno snimila nadzorna kamera; *Hachette pr. Francuske* o objavljivanju neprikladna snimka žrtve na mjestu događaja.

temelj ni svrhu za snimanje policijskih službenika. Slično je mišljenje izrazilo i istovrsno slovensko tijelo zaduženo za zaštitu osobnih podataka (*Kraljić,* Ünver, 2019: 117). *Westin* (1967) je definirao informacijsku privatnost kao zahtjev pojedinca, skupine ili ustanove u određivanju kada će, kako i koji njihovi podaci biti komunicirani prema drugim subjektima. Posebnost takvog europeiziranog pristupa jest u tome što se pravu privatnosti pristupa intrizično kao samostalnoj odluci pojedinca. Pristanak i odlučivanje osobe u središtu je provođenja prava privatnosti. *Fried* (1968) je privatnost opisao kao kontrolu koju osoba može imati nad informacijama o sebi. Pojedinac bi trebao imati mogućnost odlučivati koji će dio njegova privatnog života biti javan (*Kühn*, 2018: 243).

6.4. Utjecaj javnog mjesta na tumačenje pristanka

6.4.1. Obilježja javnog mjesta

Kada se osoba nalazi na javnome mjestu, mogu je zapažati druge nazočne osobe, ali to još ne znači da je dala pristanak na invazivnije načine registriranja osobnih podataka. Niti iz prije prikazanih definicija kao niti iz drugih odredbi Uredbe ne proizlazi mogućnost gubitka statusa osobnih podataka na pojedinim prostorima na kojima se osoba nalazi. Osobni podatak zadržava takvo svojstvo bez obzira na djelomičnu izloženost drugim osobama na javnome mjestu. Kretanjem na javnome mjestu osoba se odriče jednog dijela privatnosti vezanog uz dom, ali radi toga ne bi trebala biti u potpunosti izuzeta od svih ostalih prava iz svoje privatne sfere (*DPWP*, 2004: 5).[23]

Na primjer, ako je osoba izašla iz stana na javni prostor gdje će se susresti s drugom osobom i predati joj neki predmet, okolnost da se susret događa na javnome mjestu ne znači da svaka osoba na javnome mjestu ima pravo uvida u njezin mobitel, uvid u sadržaj njezine torbe ili u sadržaj njezina razgovora. Slično takvim pravima privatnosti u odnosu na predmete, osobe nazočne na javnome mjestu imaju pravo na zaštitu svojih osobnih podataka. Očekivana razina socijalnog kontakta na javnome mjestu jest zapažanje dostupnih obilježja druge osobe, ali svaka intenzivnija aktivnost poput snimanja ili registriranja predstavlja zahvat u osobne podatke. Osnovni je kriterij aktivnost obrade podataka, a ne vrsta prostora. U tumačenjima EKLJP-a, promatranje drugih osoba ne predstavlja ograničenje njihove privatnosti (*Herbecq i dr. pr. Belgije*), ali snimanje jest teža razina i predstavlja ograničenje prava privatnosti (*Amann pr. Švicarske*).

Nazočnost na javnome mjestu nije okolnost koja bi predstavljala pravnu osnovu za uvid u tuđe osobne podatke. Drugačije je stanje ako u nekim situacijama javno mjesto ima posebna obilježja, primjerice na javnom okupljanju ili na koncertu na kojem se može očekivati veliki broj osoba i podrazumijeva se aktivnost snimanja. Svaka osoba koja dolazi na takvo događanje pristaje na takvu razinu zahvata u privatnost (*Buchmann*, 2019). Primjer je vjenčanje javno poznate osobe na turistički posjećenom jezeru na kojem je u otvorenom čamcu došla do otočića na kojem je bio muški zbor, radi čega je i prema procjeni ESLJP-a bila svjesna da će to privući veliki interes nazočnih osoba koje tu lokaciju i inače često snimaju.[24]

---

[23] „Such an individual in transit may well expect a lesser degree of privacy, but not expect to be deprived in full of his rights and freedoms as also related to his own private sphere and image“, (*DPWP*, 2004: 5).

[24] „wedding was organised in a very unusual way, for example with the arrival of the bride in an open boat

U predmetu *Buivids* - građanin koji je snimao policijske službenike tvrdio je da nije povrijedio nikakva pravila nego je samo snimao javne službenike na javno dostupnome mjestu (*Buivids*, t. 24.). U dijelu tog prigovora sadržana je pretpostavka da se svaku osobu na javnome mjestu može snimati, odnosno da se podrazumijeva pristanak na snimanje ili da na javnome mjestu ne postoje prava privatnosti. Međutim, sud nije smatrao da takva obilježja imaju ikakav utjecaj na pravna pitanja o osobnim podacima (*Buivids*, t. 25.). Nazočnost na javnome mjestu nije oblik izražavanja pristanka na snimanje. Štoviše, upravo na javnome mjestu prema pravilima zaštite podataka ES-a postoje dodatna ograničenja zbog velikih mogućnosti obuhvaćanja drugih osoba novijim tehnologijama. Na primjer, snimanje nije dopušteno za kućne potrebe ako se postavlja sustav videonadzora koji obuhvaća javni prostor poput ulice i ulaza u drugu kuću (*Ryneš*, t. 33.).[25] Privatne kamere ne bi trebale biti usmjerene na susjedstvo ni na javni prostor (*EDPB*, 2019, 11).

Ako su neka osobna obilježja bila dostupna na nekom javnom mjestu, to znači da su bila dostupna u određeno vrijeme, na određenom prostoru, pred nazočnim osobama i da su podložna njihovu pamćenju. To ne znači da bi sadržaj trebao biti dostupan svima i u svakome trenutku. Generativna karakteristika interneta omogućuje brzo širenje sadržaja, pa kao što jedan isječak snimke s koncerta može obići cijeli svijet, tako i privatnost neke osobe može biti nepopravljivo narušena jednom neugodnom snimkom (*Zittrain*, 2008: 99); a da ne bi bilo jasno radi kojih društvenih ciljeva bi to trebalo pravno potpomagati. Prije interneta privatnost je bila drugačija i po kvalitativnim i kvantitativnim ograničenjima. Radi se o velikoj količini raznih sadržaja koje netko može učiniti dostupnim neodređenome broju osoba (*Kühn*, 2018: 244).

To su razlozi koji su doprinijeli tome da je u čl. 35. st. 3. t. c. Uredbe izričito uvedena obligatorna provjera opravdanosti videonadzora javnih mjesta (*EDPB*, 2019: 7).[26] Očevidno je da je EDPS (2010: 27) i prije preporučio da se za nadzor javnog prostora mora provoditi procjena opravdanosti, neovisno o tome što tadašnja Direktiva nije sadržavala odredbu o obligatornoj provjeri. Na nekim javnim prostorima namijenjenima odmaranju, sportu, druženju, zdravstvenim i sličnim potrebama - u velikoj su mjeri izraženi interesi zaštite podataka (npr. plaža, čekaonica u bolnici, sauna itd.), neovisno o tome što se radi o javno dostupnim mjestima (*EDPB*, 2019: 13). U okviru primjene Konvencije iz 1981. godine, mjerodavna su tijela također uvidjela velike mogućnosti prikupljanja podataka na javnome mjestu, radi čega se nastojalo videosnimanje regulirati (*CJPD*, 2003: 3).[27] U slučaju iz 2004. godine ESLJP je također utvrdio da određena zona interakcije osoba na javnom mjestu može potpadati u zaštitu privatnosti.[28]

---

and the presence of a men's choir singing a hymn on the islet. Moreover, since the ceremony took place in an area that was accessible to the public, easily visible, and a popular holiday location", *Lillo-Stenberg i Sæther pr. Norveške*, para. 43.

[25] „U mjeri u kojoj videonadzor, poput onoga u glavnom predmetu, obuhvaća, *iako djelomično, javni prostor*, te je zbog te činjenice usmjeren prema eksterijeru privatne sfere onoga tko provodi obradu podataka tim sredstvom, ta se obrada ne može smatrati isključivo 'osobnom ili domaćom' aktivnošću", *Ryneš*, t. 33. (dodano označavanje).

[26] „Procjena učinka na zaštitu podataka iz stavka 1. obvezna je osobito u slučaju: sustavnog praćenja javno dostupnog područja u velikoj mjeri", čl. 35. st. 3. t. c. Uredbe.

[27] „in order to avoid any unintentional and unjustified infringement of the data subject's rights and fundamental freedoms, for example, the freedom of movement, and to ensure in particular respect of his *privacy*, even *in public places*", *CJPD* (2003: 3), dodano označavanje.

[28] „There is therefore a zone of interaction of a person with others, even in a *public context*, which may fall

Osim osobnih podataka, iz snimaka se mogu protumačiti i razni drugi aspekti privatnosti poput toga kakve je aktivnosti netko provodio na određenome mjestu, koga je možda posjećivao, kakve ima navike, kakve predmete posjeduje i slično. Rizici za privatnost povećani su na javnome mjestu jer postoji veća mogućnost za prikupljanja podataka.[29] Stanje nije kao u starija vremena u manjim mjestima kada je osoba otprilike mogla znati tko ju može uočiti u javnosti (*Lippert, Wood*, 2012). Zapažanje i prenošenje podataka o privatnim aktivnostima drugih osoba pripada u dio usmenih djelovanja koja su ponekad nepristojna (npr. ogovaranje, glasina, trač, njem. *Tratsch*), ali nisu pravno zabranjena - sve dok ne narušavaju ugled ili ne dovode do posljedica za tuđa prava. Pravni sustav nema legitimni interes ograničavanja temeljnih prava iz Povelje samo zato da bi netko mogao prikupljati materijal za glasine, da bi mogao pikantnije komentirati tuđi život ili se zabavljati na tuđim nezgodama. U pravnom uređenju ne postoji pravo snimanja drugih (svojevrsno pravo „zabadanja nosa u tuđe stvari") niti bi pravni sustav trebao podupirati takav koncept. Primjerice, u slučaju *Lindqvist* uz ime i prezime zaposlenika bili su objavljeni podaci u šaljivom tonu o obiteljskom stanju, hobijima, dužini bolovanja ili ozlijeđenom dijelu tijela (*Morgan*, 2012: 213); a nije jasno koji bi bili legitimni interesi pravnog podupiranja javnog objavljivanja takvih podataka.
Videosnimke uz komentare na društvenim mrežama postaju suvremene inačice glasina ili ogovaranja, ali uz znatno pojačani učinak jer su se tradicionalno prenosile samo poznatim osobama, a sada objave mogu biti dostupne nepoznatim osobama. Zbog brzog prelaska na nove medije neki se još nisu naviknuli na potrebu postojanja pojedinih ograničenja. Nije jasno koje bi koristi ostvario pravni sustav ako bi svima bio dopušten uvid u takav segment privatnosti drugih građana. Uloga ogovaranja u psihološkim procesima predstavlja način nadmetanja pojedinaca u prikazivanju svoje društvene uloge (*McAndrew*, 2007). U odnosu na policijske službenike, nesporno je da uloga javnosti u nadzoru zakonitosti tijela vlasti predstavlja važan čimbenik. Ali ako je svrha određenih snimaka povećati pozornost javnosti prema određenom problemu zakonitosti, to je društveno prihvatljiv cilj prenošenja podataka (*Feinberg*, 2012) i moguće ga je provoditi fokusiranjem na problem bez uključivanja razine osobnih podataka.

6.4.2. Povijesni razvoj privatnosti na javnome mjestu u europskom pravu

Primjedbe koje se temelje na tezi da se podrazumijeva da se osoba odriče privatnosti kada je na javnome mjestu, potječu iz povijesnog razvoja američkog ustavnog prava. Američki je model privatnosti rezultat tumačenja nastalog u 19. stoljeću o ometanju privatnog posjeda. Polazište je teorija *Warrena* i *Brandeisa* iz 1860. godine koji su definirali da privatnost postoji na onome mjestu gdje osoba može biti sama u svojem prostoru. Takva teorija podrazumijeva zonu odvojenosti u kojoj je privatni posjed vrlo strogo zaštićen (engl. *trespass*) za razliku od javnog mjesta. Na javnome mjestu osoba nema pravo biti sama, a iz toga se izvodi zaključak da na javnome mjestu osoba nema pravo na dio privatnosti. Ovakva je teorija privatnosti uvelike kritizirana kao i njezin ključni pobornik u drugoj polovici 20. stoljeća, utjecajni američki pravnik *Prosser* - uglavnom zbog zastarjelosti i neuvažavanja novih izazova u području

within the scope of 'private life' ", *Von Hannover pr. Njemačke*, para. 50, dodano označavanje.

[29] „A considerable portion of the information collected by means of video surveillance concerns identified and/or identifiable persons, who have been filmed as they moved in *public and/or publicly accessible* premises", (*DPWP*, 2004: 5), dodano označavanje.

privatnosti (*Richards, Solove*, 2010). Brojni američki pravnici predlagali su preuzimanje njemačkog modela zaštite osobnih prava jer su smatrali da napretkom televizije određena razina zaštite privatnosti mora postojati i pred kamerama na javnome mjestu gdje se povećavaju mogućnosti ne samo za promatranje, nego i za snimanje te prenošenje snimaka (*Krause*, 1965: 484).

Načelna suprotnost američkom modelu privatnosti jest europski pristup koji se uvelike bazira na modelu koji ima korijene u njemačkom pravu u kojem pojam osobnih prava nije bio vezan uz privatnost na posjedu, nego uz samu osobu, neovisno o tome gdje se nalazi. Takva prava u njemačkom sustavu potpadaju u prava osobnosti (njem. *Persönlichkeitsrecht*) koja su nešto šira od pojma privatnosti. Začetke prava moguće je pronaći u idejama *Kantove* metafizike ćudoređa prema kojoj čovjek postoji zato da bi mogao provoditi svoje namjere, a ne da bi bio sredstvo iskorištavanja u tuđim rukama. Europski pristup uvažava vrijednosti pojedinca (integriteta i dostojanstva) te daje prednost njegovu individualnom stavu, a ne općim karakteristikama prostora.[30] Začetke pravnog uređenja postavio je *Von Gierke* u knjizi o privatnom pravu iz 1895. godine (*Krause*, 1965: 485). Iz tog je razdoblja najpoznatiji slučaj zaštite osobnih materijala filozofa *Friedricha Nietzschea* čija se obitelj usprotivila posthumnom objavljivanju njegovih pisama u novinama. S obzirom na to da u to vrijeme još nije bilo izričito zakonski normirano pravo na samoodređenje osobe, carski je sud 1908. godine iskoristio autorsko pravo da bi ostvario zaštitu osobnih podataka i slika.[31] Takvo je tumačenje desetljećima korišteno u sudskoj praksi i raširilo se po Europi, a brojne europske države i danas u zakonodavstvu o autorskim pravima imaju razvijena prava na zaštitu slike druge osobe, uz vrlo visoke odštete ako nije postojala suglasnost (franc. *droit à l'image*, njem. *Recht am eigenen Bild,* nizoz. *portretrecht*).[32] Sljedeću razinu razvoja započeo je njemački Savezni vrhovni sud 1954. godine presudom u kojoj je zaključio da zaštita izgleda može postojati i kada nema autorskog prava, čime je u sudskoj praksi nastalo zasebno pravo osobnosti tumačenjem ustavnih odredbi (*Krause*, 1965: 488),[33] a par godina kasnije je uvedeno i na zakonskoj razini (od 1959. godine).

Brojni su američki pravnici takvo uređenje privatnosti smatrali poželjnim uzorom. *Westin* (1967) je isticao da privatnost na osnovnoj razini obuhvaća pravo na individualno samoodređenje, a na sljedećoj razini kontrolu nad dijeljenjem osobnih informacija. Privatnost može obuhvaćati obilježja odvojenosti (od uplitanja drugih), intimnosti (krug prijatelja i bliskih osoba), anonimnosti (čuvanje identiteta od drugih) i rezerviranosti (prekid neželjenih komunikacija). To su sve svojstva koja bi se trebala koristiti kako na privatnim tako i na javnim mjestima, ovisno o odabiru pojedinca. Velike razlike američkih i europskih pogleda na nastanak koncepta osobnih prava ponekad se opisuju većim pokušajem udaljavanja europskih država od totalitarnih sustava i naglašavanjem slobodne odluke pojedinca (*Whitman*, 2004).

Površan dojam da u američkom sustavu postoji efektivno pravo snimanja drugih na javnome mjestu temelji se samo na promatranju američkog ustavnog uređenja privatnosti (*Mishra*, 2007). Međutim, postoje velika ograničenja koja nisu uvedena kroz pravo privatnosti

---

[30] Opširnije o razvoju ovog područja u *Schwartz* i *Peifer* (2010: 1947).

[31] *Fall Nietzsche*, Entscheidungen des Reichsgerichts in Zivilsachen, vol. 69, 404., prema *Krause* (1965).

[32] Npr. odšteta za objavljivanje slike osobe bez njezina pristanka, prema njemačkoj sudskoj praksi u pravilu iznosi više od deset tisuća eura. To je jedan od razloga zbog kojeg na društvenim mrežama ili portalima nema snimaka policijskih službenika u većini starijih članica EU-a.

[33] Entscheidungen des Bundesgerichtshofes in Zivilsachen, 1954, 334., prema *Krause* (1965).

na ustavnoj razini, nego kroz nižu zakonsku razinu propisa o nezakonitom nadziranju osoba (engl. *wiretapping statutes*). Gotovo sve američke savezne države zabranile su snimanje ili objavljivanje snimaka policijskih službenika uz propisane visoke kazne (*Alderman*, 2010: 489).

7. OSOBNI PODACI U PROVOĐENJU SLUŽBE

7.1. Snimanje na radnome mjestu

Za odgovor na pitanje odnosi li se europska zaštita osobnih podataka i na građane zaposlene u javnim ili državnim službama koji provode pojedine ovlasti, potrebno je najprije razmotriti pravila o osobnim podacima na radnome mjestu. Niz dokumenata na europskoj razini nastojao je pružiti smjernice za tumačenje zaštite osobnih podataka na radnome mjestu s ciljem pojačavanja prava, slobode i digniteta u kontekstu zapošljavanja. U smjernicama za jedinstvenu primjenu mjera prema ranijoj Direktivi, naznačeno je da se građani ne odriču svojih prava u trenutku dolaska na radno mjesto, odnosno da kao zaposlenici i dalje imaju legitimno očekivanje određenog stupnja privatnosti, ali je to njihovo pravo potrebno uvažavati u odnosu na druge interese radnog mjesta. Osnovno je načelo da razina nadzora mora biti transparentna zaposlenicima, da može biti primjenjivana samo ona razina koja je nužna, te mora biti razmjerna u odnosu na legitimne ciljeve (*DPWP*, 2002: 4).

Sud je utvrdio da osobni podaci građana ne gube to svojstvo u profesionalnoj dužnosti (Österreichischer *Rundfunk*, t. 64.; *Bavarian Lager*, t. 66.-70.; *Worten*, t. 19.-22.). To bi značilo da građani zapošljavanjem u određenoj pravnoj osobi zadržavaju svoja prava na osobne podatke, slično kao što zadržavaju i primjerice pravo privatnosti u odnosu na sadržaj svojih privatnih predmeta koje nose na posao (npr. torba, mobitel, e-pošta i slično). U odluci *ClientEarth* Sud ponavlja zaključak da okolnost što se neka osobna informacija nalazi u djelokrugu profesionalne aktivnosti, nije takve prirode da bi joj prestajalo svojstvo osobnog podatka. Namjera takvog tumačenja jest u isticanju osobnosti pojedinca i razlikovanje osobnog segmenta od službenih zadaća koje mogu biti drugačije pravno regulirane. Okolnost da se osoba bavi određenim zanimanjem ne znači da se odrekla svojih osobnih prava. Osobne je sadržaje potrebno razlikovati od službenih poslova ili podataka čija zaštita i tajnost ovisi o stajalištu zakonodavca te mogu biti obuhvaćeni ako nisu klasificirani ili na drugi način zakonski zaštićeni. Određen dio osobnih podataka vezan uz radno mjesto skuplja poslodavac, primjerice za kadrovske potrebe. Kao primjere obrade osobnih podataka na radnome mjestu *DPWP* (2001) navodi podatke o plaćama, porezima, godišnjim odmorima, bolovanjima, disciplinskim mjerama, obrazovnim aktivnostima, nesrećama na radu i sličnima (*DPWP*, 2001: 7).

Europski je sud u slučaju iz 2012. godine također izrazio stajalište da se osobni podaci ne odnose samo na navedene podatke vezane uz poslodavca, nego i na druge podatke koji su na radnome mjestu povezani s pojedinom osobom (*Worten*, t. 19.). Ne radi se o novijem pravilu, nego je spomenuto već dulje vrijeme zastupljeno u tumačenjima pred Europskim sudom, primjerice 2008. godine u odnosu na podatke o sudionicima sastanaka u okviru poslovnih aktivnosti. Dio sudionika sastanka nije pristao da budu zabilježeni njihovi osobni podaci vezani uz nazočnost na sastanku (*Bavarian Lager*, t. 68.). Pojam privatnog života ne može biti takav da bi se isključivao u aktivnostima profesionalne prirode (*Schecke i Eifert*, t. 59.). Europski je sud u predmetu *Schecke* utvrdio da zaštita koju pruža Direktiva ne ovisi o

aktivnostima koje su poslovne naravi (*Schecke i Eifert*, t. 59.). To bi značilo da se primjenjuje pravilo o zaštiti osobnih podataka i tijekom provođenja radnih zadaća jednako kao i u privatnim okolnostima građana nakon radnoga vremena.

7.2. Privatnost tijekom poslovnih aktivnosti prema tumačenju ESLJP-a

Europski sud za ljudska prava također je utvrdio da pojam privatnog života ne može biti tumačen restriktivno; već da nema razloga za izdvajanjem aktivnosti profesionalne prirode iz pojma privatnog života (*Amann pr. Švicarske*, para. 65; *Rotaru pr. Rumunjske*, para. 43). Tako je ESLJP u predmetu *Amann* utvrdio da privatnost ne može biti interpretirana restriktivno i da nema razloga koji bi opravdavali izdvajanje aktivnosti profesionalne ili poslovne prirode iz pojma privatnosti građana (para. 65). Odluka *Rotaru* ponavlja stajalište o nemogućnosti izdvajanja privatnosti iz profesionalnih ili poslovnih aktivnosti (para. 43). I u slučaju *Niemitz pr. Njemačke* - ESLJP je utvrdio da nema načela koje bi smatralo da bi privatni život trebao biti izuzet iz aktivnosti koje su profesionalne ili poslovne prirode.[34] Prema ESLJP-u, zaštita privatnog života nije ograničena samo na dom osobe jer svaka zaposlena osoba ne može biti cijelo vrijeme kod kuće, nego mora obavljati razne druge aktivnosti. U tijeku radnog vremena većina ljudi u najvećoj mjeri dolazi u prigodu razvijanja poznanstava i odnosa s ostalim građanima, te je čak ponekad teško odvojiti ili razlikovati privatne i poslovne sadržaje u nekim aktivnostima (*DPWP*, 2002: 7).

7.3. Status službenika

Javne i državne službe imaju specifičan položaj jer građani koji su njihovi zaposlenici postupaju prema drugima u svojstvu službenika te su radi toga pod posebnim nadzorom zakonitosti s ciljem smanjivanja zlouporaba i povećanja transparentnosti. Radi toga se ponekad javljaju neutemeljena mišljenja da se građani zaposleni kao policijski službenici odriču svojih osobnih prava te da u jednakoj mjeri mogu biti snimani službeni i osobni podaci. Takva stajališta prije svega zanemaruju činjenicu da građani zaposleni kao policijski službenici ne postupaju kao privatne osobe, nego prema pravilima službe i smjernicama rukovoditelja. Europski sud smatra da i građani koji su javni službenici imaju osobna prava i prema njima traži jednaku zaštitu osobnih podataka. Time se ne ograničava mogućnost nadzora zakonitosti rada policije ni bilo kojeg drugog tijela vlasti, kao niti uporaba snimaka u pravnim postupcima prema pojedinim službenicima; ali se nastoji utjecati na zaštitu osobnih podataka tijekom objavljivanja. Osim toga, ako su snimkom uz osobne podatke obuhvaćeni i neki službeni podaci koji su zakonski zaštićeni i klasificirani raznim razinama tajnosti, takva radnja može predstavljati kazneno djelo.

Različita gledišta o podacima zaposlenika u javnom sektoru predočena su u jednom mišljenju nezavisnog odvjetnika Suda. Tijekom analiziranja stanja u državama EU-a, jedno od izraženih stajališta bilo je da službenici provode javne dužnosti i radi toga moraju prihvatiti

[34] „There appears, furthermore, to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature", *Niemitz pr. Njemačke*, para. 29.

opciju da se radi o postupanju u javnom interesu i u javnom okruženju - te da njihove ovlasti mogu biti podvrgnute javnim provjerama i nadzoru (*Buivids*, Mišljenje, t. 27.). Takvu su argumentaciju pojedine vlade smatrale razlogom izuzimanja od primjene pravila o zaštiti osobnih podataka za snimanje javnih službenika. Međutim, te se dvije okolnosti ne isključuju, odnosno moguće je provjeravati i nadzirati zakonitost postupanja, ali bez javnog razglašavanja nečijih osobnih podataka ili povrede tajnosti službenih podataka, a osobito bez insinuiranja nezakonitosti dok to ne provjeri nadležno tijelo.

Nezavisni odvjetnik Suda za vrednovanje takvog gledišta konzultirao je recital prijašnje Direktive i mjerodavne odredbe, među kojima nema ni jedne naznake da postoje bilo kakve iznimke od zaštite u odnosu na državne ili javne službe kao ni bilo koja druga tijela vlasti (*O'Boyle*, 2020: 67). Pravila su konstruirana upravo tako da podržavaju temeljna prava svake osobe kao pojedinca, a građani zaposleni kao javni službenici u suštini bi trebali imati jednaku zaštitu temeljnih prava privatnosti (čl. 7. Povelje) i osobnih podataka (čl. 8. Povelje). Osim što suprotna stajališta nisu utemeljena na pravnim izvorima, dovodila bi do stajališta da bi građani koji su javni službenici trebali biti u većoj mjeri izloženi ograničenjima svojih osobnih prava, što bi dovodilo do brojnih negativnih posljedica (*Buivids*, Mišljenje, t. 30.). Građani koji su zaposleni kao policijski službenici ne odriču se svoje privatnosti ni osobnih podataka ulaskom u službu, ali podrazumijeva se da pojedini službeni postupci mogu biti podvrgnuti nadzoru zakonitosti. Takva tumačenja ničime ne utječu na pravo građana u podnošenju raznih vrsta predstavki ili prijava na rad policijskih službenika, nego samo limitiraju aktivnosti koje narušavaju osobne ili privatne podatke te posredno doprinose omalovažavanju, ismijavanju ili ugrožavanju institucija.

Kao što je nezavisni odvjetnik Suda naznačio u svojemu mišljenju, nema odredbe koja bi davala izričitu iznimku da obrada osobnih podataka javnih službenika ne bi bila obuhvaćena europskim propisima. Slijedom takve prakse, ES navodi činjenicu da okolnost što je neki podatak prikupljen u okviru profesionalne aktivnosti, ne znači da ne može imati svojstvo osobnog podatka (*ClientEarth*, t. 30.). Europski je sud zaključio da snimanje i objavljivanje snimaka službenika pripada u primjenu zaštite osobnih podataka. Također je i u smjernicama za tumačenje navedeno da se pravila odnose i na privatni i na javni sektor (*DPWP*, 2002: 6). Konvencija također sadržava odredbu o tome da se zaštita podataka odnosi i na privatni i na javni sektor (čl. 3. t. 1. Konvencije).

Zaštita je osobnih podataka na radnome mjestu jednaka neovisno o tome odnosi li se na podatke koje prikupljaju poslodavci ili na podatke koje prikupljaju drugi subjekti s kojima se zaposlenik susreće tijekom radnog vremena. U predmetu *Buivids* Sud je zaključio da snimanje policijskih službenika u provođenju njihovih dužnosti, bez njihove suglasnosti, ne znači da je potrebno isključiti primjenu pravila o zaštiti osobnih podataka (*Buivids*, t. 42.). Potrebno je razlikovati koji je dio podataka moguće javno prikazivati, a koji dio predstavlja osobne podatke građana ili službene podatke koji su klasificirani i zabranjeno ih je pokazivati javnosti.

AZOP (2016) navodi da uporaba uređaja za snimanje predstavlja naročito invazivnu metodu prikupljanja osobnih podataka s obzirom na to da policijski službenik pri obavljanju radnih dužnosti uživa zaštitu privatnosti i osobnih podataka. Nezavisni odvjetnik Suda smatra da je čisti voajerizam kada bi se snimalo zbog pogrešnog uvjerenja nekih građana da se službenike može snimati kao neko neotuđivo pravo građana (*Buivids*, Mišljenje, t. 59.). Takvo pravo ne postoji ni u Povelji, ni u Konvenciji ni u EKLJP-a, te bi pobornici njegove primjene u bilo kojoj članici EU-a imali poteškoća u pokazivanju domaćih ili europskih pravnih propisa iz kojih bi to pravo proizlazilo.

7.4. Razlike u statusu političara i službenika

U opravdavanju potrebe pružanja zaštite službenicima na jednakoj razini kao i zaposlenicima drugih tijela ili pravnih subjekata, Europski se sud referirao i na praksu ESLJP-a. Razlog za to su pojedini prigovori stranaka da je prema praksi ESLJP-a neke subjekte dopušteno kontrolirati na pojačanoj razini slično kao i političare, te da radi toga i javni službenici mogu očekivati manju razinu zaštite osobnih podataka. Političari se dobrovoljno uključuju u političke funkcije za koje je uobičajeno da podrazumijevaju manju razinu zaštite privatnosti (*ClientEarth*, t. 30.). Pojedini od prigovora pozivali su se na izdvojeno mišljenje nekoliko sudaca u predmetu *Pedersen i Baadsgaard pr. Danske* prema kojem bi javni službenici jednako kao i političari trebali biti podložni većim razinama prihvatljive kritike, jer njihove osjetljive dužnosti, koje su često ključne za sigurnost i dobrobit zajednice, stavljaju policiju u središte društvenog nadzora (izdvojeno mišljenje, t. 9.).[35]

Međutim, za političare su limiti prihvatljive kritike puno širi nego za državne ili javne službenike, jer su političari podložni provjeri svake riječi i djela ne samo od novinara, nego i od javnosti općenito. Političari su se neizbježno i svjesno stavili na otvoreni prostor i moraju pokazati veći stupanj tolerancije na kritiku. To ne znači da političari nemaju pravo na zaštitu ugleda, ali razina zaštite mora biti razmjerna u odnosu na interese otvorene diskusije o političkim pitanjima (*Oberschlick pr. Austrije*, para. 59). Značajna posebnost političara i javnih osoba jest to što oni donose odluke koje su izraz njihovih privatnih stajališta i njima mogu oblikovati život cijele zajednice. Za razliku od toga, građani zaposleni kao policijski službenici ne nastupaju kao privatne osobe, nego postupaju na temelju službenih pravila i naredbe rukovoditelja te predstavljaju tijelo vlasti. Prema praksi ESLJP-a, u kategoriju osoba koje je moguće slikati ili snimati bez pristanka pripadaju javne ili poznate osobe (engl. *public or newsworthy figure*) na temelju javnog interesa (*Reklos i Davourlis pr. Gr*čke, para. 41), a primjer su političari ili osobe koje su na drugi način ušle u javnu arenu i široko su poznate većem broju građana (*Krone pr. Austrije*, para. 37). U tu kategoriju mogli bi ulaziti samo neki viši policijski rukovoditelji koji su na radnim mjestima iz kojih proizlazi odgovornost za funkcioniranje cijelog sustava.

Veliko vijeće ESLJP-a u slučaju *Pedersen i Baadsgard* utvrdilo je da bi javni službenici u provođenju službenih poslova trebali biti podložni većim razinama prihvatljive kritike, ali da ne bi trebalo smatrati da javni službenici moraju sebe izlagati temeljitoj javnoj provjeri svake riječi i radnje kao što je to kod političara. Iako je policijski službenik voditelj istraživanja u tom slučaju bio podložan kritikama (kao načelnik i voditelj skupine za istraživanje), ne bi trebao biti tretiran na istoj razini kao političar u odnosu na objavljivanje osobnih podataka. Shodno tome, ESLJP smatra da naročito ne bi bilo opravdano prekoračiti granicu kritike i iznositi neutemeljene optužbe da je počinio kazneno djelo. To bi ne samo potkopalo javno povjerenje, nego bi i povrijedilo pretpostavku nedužnosti (*Pedersen i Baadsgaard pr. Danske*, para. 80). Ovakav zaključak može biti primijenjen i na razne druge snimke ili slike uz koje se prilikom objave prezentiraju netočni navodi i komentari u odnosu na policijske službenike, što u pravnom smislu predstavlja povredu njihovih prava.

---

[35] U tom slučaju je postupak vođen bio protiv dvojice producenata televizijske emisije iz 1990. o ubojstvu iz 1982. godine. U emisijama je kritiziran rad policije i nastupio je navodni svjedok koji je izjavio da je vidio osuđenika u vrijeme počinjenja na drugome mjestu. U emisiji je postavljen niz retoričkih pitanja uz pokazivanje slike jednog policijskog službenika, što je ostavilo dojam kao da je on odgovoran za navodne propuste. Producenti su osuđeni za klevetu. Vrhovni sud potvrdio je presudu i povećao odštetu.

8. KUĆNA IZNIMKA ZA PRIKUPLJANJE OSOBNIH PODATAKA

Uredba sadržava nekoliko iznimaka kojima se može isključiti protupravnost pojedinih oblika prikupljanja osobnih podataka (čl. 2. st. 2. Uredbe). Na fizičke osobe koje provode snimanje može se primijeniti iznimka ako su podaci bili isključivo namijenjeni za provođenje njihovih osobnih ili kućnih aktivnosti (čl. 2. st. 2. t. c. Uredbe). Osim te iznimke, uporaba podataka dopuštena je za novinarske aktivnosti, te za aktivnosti nekih državnih tijela u području sigurnosti i istraživanja kaznenih djela (točka d. iste odredbe), ali se na potonje ne mogu pozivati građani. S obzirom na to da je zaštita podataka jedno od temeljnih prava iz Povelje, iznimke od zaštite moraju se tumačiti vrlo usko.

Iznimka koja dopušta prikupljanje podataka za osobne ili kućne aktivnosti odnosi se na razne potrebe koje su uobičajene u svakodnevnome životu i komunikaciji s drugima. Primjer kućne uporabe osobnih podataka iz uvodnih izlaganja (recitala) Uredbe jest bilježenje telefonskih brojeva, imena i sličnih podataka u notesu (t. 18.). Cilj je takvih aktivnosti pregledniji popis i ubrzavanje mogućnosti kontaktiranja, što je osobna uporaba drugačija nego kad bi takve podatke namjeravali javno objaviti. Primjer prikupljanja podataka za kućnu uporabu može biti turist koji na odmoru snima okolinu s ciljem pokazivanja slika članovima obitelji ili prijateljima - te mu nije namjera stavljati snimke na medij dostupan neodređenom broju ljudi. Sličan je primjer i kada sportaš biciklist na kacigi nosi kameru kojom snima karakteristike staze za potrebe kućne zabave ili radi sportske pripreme, ili kada bi netko snimao svoj vrt i osobe koje se tamo zabavljaju (*EDPB*, 2019: 7).

Europski sud zaključuje da iznimka korištenja za osobne ili kućne svrhe ne može biti ispunjena ako se podaci čine dostupnima neodređenom broju osoba (*Satamedia*, t. 44.). Postavljanjem podataka na internetske stranice oni postaju dostupni velikom broju osoba i u takvim se slučajevima građani ne mogu pozivati na kućne potrebe (*Lindqvist*, t. 32.). Europski je sud zaključio da se očito ne radi o privatnom ili obiteljskom životu pojedinca ako su tuđi osobni podaci publicirani na internetu i dostupni drugima (*Lindqvist*, t. 47.). Sagledavajući sadržaj snimke policijskih službenika u slučaju *Buivids*, ES je zaključio da ne proizlazi da bi snimljeni sadržaji policije potpadali u neku od navedenih iznimaka (*Buivids*, t. 42.).

U odnosu na prigovor da se u slučaju *Buivids* možda radilo o kućnoj uporabi, odnosno obiteljskim potrebama za snimanje policijskih službenika, važno je istaknuti da objavljivanje na internetu pokazuje da podaci nisu bili za njega osobno, nego su postali dostupni i pristupačni neograničenom broju osoba (*Buivids*, Mišljenje, t. 40.). Snimka policijskih službenika u slučaju *Buivids* objavljena je na stranici na kojoj korisnici mogu postavljati, gledati i dijeliti videosnimke, čime je snimatelj omogućio dostupnost podataka neodređenom broju osoba. Takvim načinom objave pokazuje se da se ne radi o kontekstu isključivo kućne uporabe niti radi nekih drugih osobnih potreba (*Lindqvist*, t. 47.; *Satakunnan*, t. 44.; *Ryneš*, t. 31., 33.; *Jehovan*, t. 42.). Primjer snimke policijskih službenika za kućnu uporabu mogla bi biti situacija neke interne svečanosti, godišnjeg radnog sastanka određene jedinice ili sličnih događaja koji ne izlaze u javnost. Poteškoće u tumačenju iznimaka mogu biti u nepoznavanju točnih razloga snimanja, odnosno snima li neka osoba radi objavljivanja na internetu ili radi svojih kućnih potreba.

9. NOVINARSKA IZNIMKA ZA PRIKUPLJANJE OSOBNIH PODATAKA

9.1. Novinarske svrhe objavljivanja osobnih podataka

Obrada osobnih podataka dopuštena je ako je namijenjena novinarskim aktivnostima (čl. 85. Uredbe). Ovakva se iznimka ne primjenjuje automatski, nego se uspoređuje pretežu li novinarska prava na slobodu izražavanja misli ili interesi zaštite privatnosti osobe čiji se podaci iskorištavaju (čl. 85. st. 2. Uredbe). Prema navedenoj odredbi, izuzeća i odstupanja u ovome području procjenjuju države članice, tako da ES njima prepušta utvrđivanje konkretnih okolnosti slučaja i primjenu načelnih kriterija s europske razine. Da bi se iznimka primjenjivala, mora se raditi o isključivim novinarskim ciljevima, što znači da u situaciji u kojoj postoje i neki drugi sporedni ciljevi, ovakva iznimka ne može biti primijenjena (*Coppel*, 2020: 422). Dio sadržaja kojeg obuhvaća ova iznimka prikazan je u poglavlju o razlici političara i javnih službenika. Uz ovu iznimku u istoj je odredbi spomenuta i iznimka umjetničkog ili znanstvenog rada, što znači da i umjetničke fotografije mogu biti izuzete od zaštite.

Novinarska iznimka ne pruža zaštitu od povrede pravila koja mogu biti propisana u drugim područjima prava (policijsko, prekršajno, kazneno zakonodavstvo itd.). Na primjer, ako su novinari uključeni u aktivnosti poput ometanja policijskih službenika, narušavanja javnog reda i mira, povrede osiguranja mjesta događaja ili u slične aktivnosti zbog kojih je prema njima potrebno postupanje - tada policijski službenici ne povređuju pravo na slobodu izražavanja time što bi novinare onemogućili u snimanju.

Europski sud za ljudska prava zaključio je da novinari koji su povrijedili pravne propise nemaju poseban status tijekom uhićenja. Policija nije povrijedila pravo novinara na slobodu izražavanja (čl. 10. EKLJP-a) koji je uhićen jer je bio dio skupine građana koji su nasilno narušavali javni red i mir te su se više puta oglušili na naredbe policijskih službenika, i time su ujedno počinili kazneno djelo (*Pentikäinen pr. Finske*, para. 54).[36] Slično tome, novinari se ne mogu pozivati na pravo slobode izražavanja ako sudjeluju u kažnjivim radnjama koje nisu vezane uz slobodu izražavanja; primjerice kada su rabili uređaje za prisluškivanje policije da bi mogli čim prije saznati gdje je mjesto događaja i snimiti ga za svoja izdanja (*Brambilla i dr. pr. Italije*, para. 62).[37] Sloboda izražavanja dopušta objavljivanje nekih povjerljivih dokumenata u okviru istraživačkog novinarstva ako postoji pretežiti javni interes (usp. *Stoll pr.* Švicarske, para. 102).[38]

9.2. Mogućnost uključivanja građana u novinarski rad

Iznimka se po prirodi stvari odnosi na aktivnosti profesionalnih novinara, ali je za ovu temu važno da pod određenim uvjetima može obuhvaćati i aktivnosti drugih subjekata, odnosno građana. Tumačenje je ovog područja važno jer ako bi građani mogli sudjelovati u

[36] „The District Court found it established that the applicant had committed a crime by disobeying the lawful orders of the police", *Pentikäinen pr. Finske*, para. 54.

[37] „applicants' actions were therefore to be classified as criminal conduct", *Brambilla i dr. pr. Italije*, para. 62.

[38] „journalists cannot, in principle, be released from their duty to obey the ordinary criminal law", *Stoll pr. Švicarske*, para. 102.

novinarskoj djelatnosti bez formalnog zapošljavanja, tada bi i njihove snimke ponekad bile izuzete od zaštite osobnih podataka. U mišljenju nezavisnog odvjetnika Suda prezentirana je dvojba pojedinih država koje su smatrale da novinarstvo traži određenu razinu formaliziranosti, profesionalnih postupaka i kontrole (*Buivids*, Mišljenje). Sud nije smatrao potrebnim uvoditi strogu granicu između podataka koje su prikupili profesionalni novinari i podataka koje su prikupili drugi subjekti, već je zauzeo načelno stajalište da se novinarske aktivnosti pod određenim uvjetima ne odnose samo na zaposlenike novinarskih kuća.

Nezavisni odvjetnik Suda smatrao je da pojedinac koji se bavi građanskim novinarstvom (engl. *citizen journalism*), odnosno prikuplja i širi vijesti, mišljenja i ideje, može biti obuhvaćen iznimkom obrađivanja podataka u novinarske svrhe (*Buivids*, Mišljenje, t. 53.). Potrebno je uzeti u obzir da se neke osobe ciljano bave istraživanjem pojedinih tema iako nemaju formalni radni odnos u medijima. Europski je sud izrazio gledište da se ne može prihvatiti teza da bi svaki podatak koji je objavljen na internetu ili u medijima morao automatski ulaziti u iznimku novinarske aktivnosti.

Problem je u tome što nove medijske mogućnosti i internetski portali predstavljaju veliki rizik za povrede privatnog života i to u većoj mjeri predstavlja opasnost negoli što je to nekad bilo moguće postići tiskom. Europski sud za ljudska prava naglasio je da se internetom može izazvati veća razina narušavanja privatnog života (*Delfi pr. Estonije*, para. 133). Iz vrste portala na kojem su snimke objavljene ne mogu se nužno izvlačiti zaključci koja je bila namjena snimaka (*Buivids*, t. 55.-57.). Okolnost da se novinarska iznimka u načelu može obuhvatiti na razne subjekte, ne znači da je svim subjektima u okviru svojih profesionalnih aktivnosti dopušteno javno iznositi podatke koji ulaze u područje privatnosti. Primjerice, podaci o liječenju, psihološkim tretmanima ili sličnim aktivnostima dodatno su zaštićeni posebnim propisima. Primjer takvih težih povreda jest iznošenje detalja o ozljedama ili bolestima (npr. ozljede ranjenog policijskog službenika). Naime, u više je slučajeva iznošenja zdravstvenih podataka pojedinih osoba, ESLJP zaključio da se radi o povredi privatnosti.[39]

9.3. Kriteriji za procjenu novinarskih radnji građana

Novinarske aktivnosti definirane su kao radnje kojima je cilj otkriti informacije, mišljenja i ideje (*Satakunnan*, t. 58. - 61.). To znači da bi snimatelj prije svega morao pokazati koju to ideju, mišljenje ili informaciju pokazuje snimkom (*O'Boyle*, 2020: 67). Osnova razmatranja odnosi se na važnost pitanja za javnost i prirodu objavljenih informacija. Europski sud upućuje na praksu ESLJP-a, prema kojoj je potrebno utvrditi radi li se o pitanjima koja na javnost utječu u tolikoj mjeri da se za njih građani mogu opravdano zanimati, koja privlače njihovu pozornost; odnosno teme koje ih se značajno tiču, osobito ako utječu na dobrobit građana ili zajednice. U slučaju *Buivids,* domaći je sud dostavio podatke prema kojima zaključuje da je *Buivids* bio u policiji u vezi s postupkom koji se samo njega ticao, a ne prikazuju se neke aktualne vijesti. Nijedan od snimljenih policajaca nije poznat kao javna osoba, niti su navedene neke informacije o prijašnjem nezakonitom ponašanju pojedinog od obuhvaćenih službenika. Iz takvih okolnosti nezavisni odvjetnik Suda zaključuje da mu se čini da nisu ispunjeni uvjeti postojanja (isključivih) novinarskih ciljeva, ali ističe da domaći sudovi moraju detaljnije

[39] Npr. *Mitkus pr. Latvije* o slučaju objavljivanja slike osobe zaražene HIV-om.

utvrditi sve činjenice i donijeti odluku. Ne može se svako snimanje radi pojedinih vlastitih ciljeva, znatiželje ili voajerizma - smatrati isključivo novinarskim potrebama.

Europski je sud ovo pitanje u skladu s Uredbom ostavio domaćim sudovima koji moraju procijeniti sve okolnosti slučaja (*Buivids*, t. 59.). Sud navodi da ni snimljena nezakonitost ne znači da se radi o novinarskoj iznimci. Europski je sud u slučaju *Buivids* istaknuo da bi trebalo razmotriti da se navodno na snimci radi o nezakonitoj praksi, ali ako je snimljena nezakonitost javnih službenika, to ne znači da bi snimka automatski potpadala pod primjenu novinarske iznimke. Takvo je tumačenje vjerojatno pod utjecajem stajališta da bi snimku trebalo dostaviti mjerodavnom tijelu radi procjene zakonitosti postupanja službenika i pokretanja odgovarajućeg postupka.

10. UPORABA SNIMAKA U KAZNENOM POSTUPKU

10.1. Snimanje kažnjive radnje ili počinitelja na javnome mjestu

Pravni sustav nema legitimnih interesa za generalno dopuštanje snimanja svih osoba na javnome mjestu, ali u odnosu na počinitelja stanje je drugačije - jer takav događaj predstavlja teško narušavanje prava u društvu. Okolnost počinjenja kaznenog djela bitno razlikuje počinitelja od obične pojavnosti na javnome mjestu koja ne povređuje ničija prava. Postupke prema počiniteljima uređuje posebno pravno uređenje u kaznenom i policijskom zakonodavstvu (*lex specialis*) koje se temelji na potrebi ograničavanja pojedinih prava. U čl. 2. st. 2. t. d. Uredbe navedena je mogućnost prikupljanja osobnih podataka za potrebe istrage, odnosno otkrivanja ili progona počinitelja kaznenih djela kao zadaća državnih tijela. Nije navedeno da bi se ova osnova mogla primjenjivati u odnosu na snimanje koje provode fizičke osobe, ali takva osnova postoji u drugim odredbama. U čl. 23. st. 1. Uredbe navedeno je više osnova zbog kojih se domaćim zakonodavstvom može propisivati ograničenja osobnih podataka radi javne sigurnosti (t. c), sprječavanja, otkrivanja ili progona kaznenih djela (t. d). U uvodnim izjavama Uredbe (t. 19.) predviđena je mogućnost zakonske regulacije ograničenja radi nužne i proporcionalne mjere održavanja interesa javne sigurnosti te otkrivanja i progona kaznenih djela.[40]

Počinitelju je moguće na mjestu događaja ograničiti slobodu kretanja, primjerice, nazočni građani mogu spriječiti bijeg osumnjičenika kako bi osigurali njegovu dostupnost za kazneni postupak (čl. 106. ZKP-a). Ako je situacija takva da nazočne osobe ne mogu koristiti tjelesnu silu prema počinitelju jer bi time ugrozili svoju ili tuđu sigurnost, snimanje počinitelja može biti znatno blaži oblik neizravnog osiguranja dostupnosti počinitelja. Svjedoci koji su zapazili kazneno djelo, imaju obvezu iskazivati prema odredbama kaznenog postupka, čak i uz prijetnju kaznom. Kod prijave kaznenog djela policiji, prijavitelj navodi podatke o počinitelju koji su mu poznati, što znači da su takvi podaci potrebni kao pomoć u provođenju policijskih poslova i u potvrđivanju vjerodostojnosti navoda (čl. 62. st. 4. t. 4. ZPPO-a).

[40] „Kada osobne podatke obrađuju privatna tijela [...] ova Uredba trebala bi predvidjeti mogućnost da države članice pod posebnim uvjetima zakonom ograniče određene obveze i prava kada takvo ograničenje predstavlja nužnu i proporcionalnu mjeru u demokratskom društvu za očuvanje posebnih važnih interesa, uključujući javnu sigurnost te sprečavanje, istragu, otkrivanje ili progon kaznenih djela ...“, t. 19. uvodnih izjava Uredbe.

Neprijavljivanje kaznenog djela također je ponekad kažnjivo. Pravne osobe moraju poduzeti mjere za očuvanje dokaza, a i inače je svatko dužan prijaviti kazneno djelo (čl. 204. ZKP-a). Ovakve zadaće opravdavaju prikupljanje podataka s ciljem provođenja dužnosti građana i potpomaganja ciljeva tijela vlasti. Snimke građana tijekom većih oblika narušavanja sigurnosti (talačke situacije, neredi, terorizam itd.) pružaju korisne materijale za učinkovito postupanje i za pripremu policije kako bi bilo manje žrtava tijekom postupanja.

Kazneno djelo utječe na nazočne osobe jer neki od njih mogu postati žrtve, a neki će možda morati fizički braniti sebe ili druge. Oštećenik napadnut kaznenim djelom ili drugi nazočni građani mogu se braniti razmjernom silom u okviru nužne obrane regulirane kaznenim pravom. Snimanje može u nekim situacijama biti oblik djelovanja kojim bi se osoba mogla obraniti od počinitelja ili eventualno navesti počinitelja na prekid kaznenog djela.

Promatrajući sigurnosne aspekte bilo bi vrlo neobično kada bi svjedok trebao prethodno zatražiti pristanak počinitelja na snimanje, najaviti mu razlog snimanja i još mu reći svoj identitet; osobito ako se radi o počinitelju nasilnog kaznenog djela. Žrtva koja nakon napada uspije snimiti bijeg počinitelja, ili slučajni prolaznik koji naiđe na počinitelja teškog kaznenog djela pa ga snimi, ne bi mogli tražiti njegovo dopuštenje bez ugrožavanja vlastite sigurnosti. Pojedine su poteškoće izražene u slučajevima složenih kaznenih djela u kojima nije moguće ponavljanje dokaza (npr. traženje mita), ili kada su uključeni sudionici čija bi moćnija društvena uloga (npr. političar, službenik itd.) mogla dovoditi u pitanje vjerodostojnost ili dobronamjernost prijaviteljevih navoda koji je inferioran. Osim takvih konkretnih posljedica na mjestu događaja, na generalnoj razini postoje posebna tijela kojima je isključivi cilj istraživanje kaznenih djela što ne mogu raditi bez pomoći građana. U europskim je državama pokrenut trend otvaranja profila na društvenim mrežama na kojima policija zaprima anonimne snimke građana, radi nadomještanja pada sudjelovanja građana u svojstvu svjedoka.

Procjena dopustivosti snimaka pripada u područje kaznenog postupovnog prava. U kaznenom postupku smiju se rabiti tehničke snimke nastale javnom slikovnom ili zvučnom registracijom činjenica, bez obzira na to je li osoba znala da ju se snima (*Krapac*, 2014: 517). Snimka osumnjičenika na javnome mjestu s ciljem prikupljanja dokaza znatno je lakši zahvat od dugotrajnog snimanja u privatnim prostorijama ili od tajnog snimanja za koje bi bio potreban sudski nalog prema odredbama o posebnim dokaznim radnjama (*Karas*, 2015). Prema brojnim odlukama Vrhovnog suda u slučajevima u kojima je bilo provođeno kontinuirano snimanje javnih prostora ili prodavaonica, snimka na javnom mjestu bila je dopustiva za dokazivanje u kaznenom postupku, neovisno o tome što nije bilo istaknutog upozorenja ili sličnih formalnosti jer to nisu bitni uvjeti propisani u kaznenom postupovnom pravu (*Karas*, 2014). Takvo tumačenje odnosi se i na prigodne kratkotrajne snimke, neovisno o vrsti zanimanja kojom se bavi snimljena osoba; što znači da ni policijski službenici nisu iznimka ako je na snimci obuhvaćeno neko njihovo kazneno djelo. Takvih je primjera već i bilo u sudskoj praksi.

Ponekad se može naići na gledišta da radi toga što je u iznimnim situacijama moguće snimati osumnjičenike na javnome mjestu, ujedno je moguće snimati i sve druge osobe, a naročito službenike - uz opravdanje da su skloni nezakonitostima. Takva stajališta ne uvažavaju da nedužna osoba koja se kreće na javnom mjestu i ne povređuje tuđa prava, jednako kao i javni ili državni službenik koji provodi propisane zakonske ovlasti, trebaju imati odgovarajuću zaštitu osobnih podataka. Osim toga, takva se stajališta baziraju na pretpostavci krivnje službenika na javnome mjestu, što je u suprotnosti s osnovnim načelima pravnog

uređenja. Pretpostavka krivnje (franc. *le présumé coupable*) koja se navodi u pojedinim interpretacijama srednjovjekovnih inkvizitornih postupaka čak nije bila izričito propisana ni u takvom obliku povijesnog postupka (*Spencer*, *Delmas-Marty*, 2002: 23); a potpuna je nepoznanica u suvremenom kontinentalnom pravu (*Damaška*, 1973: 531).

U slučaju privatnog detektiva koji je prikupljao osobne podatke pojedinih osoba u okviru istraživanja disciplinske povrede regulirane profesije (*IPI*, t. 51.), ES je zaključio da takvo istraživanje kojim se prikupljaju osobni podaci može biti dopušteno domaćim zakonodavstvom (*Brkan*, 2017: 17). To znači da prikupljanje podataka s ciljem istraživanja može biti utemeljeno u posebnom zakonodavstvu pa tako ne postoje ograničenja ni za snimanje policijskih službenika u sličnim situacijama. Za uporabu snimke u kaznenom postupku postoje posebna proceduralna pravila o uvidu u snimke, načinu korištenja, mogućnosti provjere u dokaznom postupku i brojna druga pravila koja imaju prednost pred odredbama o pravu pristupa ili uvida - a kakve su propisane u Uredbi (*Coppel*, 2020: 328).[41] Problem bi mogao nastati ako bi snimke umjesto za navodne potrebe kaznenog postupka bile objavljene u medijima na način koji bi predstavljao povredu osobnih podataka.

S druge pak strane, zaštita osobnih podataka ne obvezuje samo građane koji snimaju policijske službenike nego obveza vrijedi i obratno. Povreda bi postojala kada bi u medijima umjesto u kaznenom postupku bile korištene službene snimke iz pojedinih dokaznih radnji koje prikazuju osobne podatke građana (npr. snimka ispitivanja, snimka iz posebnih dokaznih radnji itd.). U takvim je slučajevima moguće pokretanje postupka prema odgovornim subjektima ili tijelima vlasti koja su medijima dostavila snimku, a osim toga je pred ESLJP-om moguće provjeriti odgovornost države u smislu nepostojanja prikladne zaštite privatnosti osoba i pitanja učinkovitosti istraživanja načina odavanja podataka (*Draskas pr. Litve*, para. 60).[42]

10.2. Prepuštanje kazne društvenim mrežama

Poteškoće sa snimkama mogu nastati ako nije provjereno radi li se doista o kaznenom djelu, niti je snimka dostavljen tijelu koje je nadležno za kazneni progon, nego je objavljen na internetskim portalima uz neprovjerene navode ili namjerne netočnosti. U takvim okolnostima može dolaziti do površnog i neodgovornog komentiranja nekog postupanja s ciljem podupiranja lažnih optužbi i neosnovanog etiketiranja osoba, a to može imati brojne negativne posljedice kako u odnosu na snimljene građane tako i u odnosu na policijske službenike. Pojave lažnog optuživanja radi poticanja nasilja ili osvete u teoriji su nazvane internetski vigilantizam ili online suđenje (*Hurt*, 2018).

Jedan od novijih primjera neosnovanog internetskog suđenja u odnosu na policijske službenike jest pokušaj identifikacije napadača na tri afroamerička prosvjednika protiv policijske brutalnosti u Baltimoreu u srpnju 2020. godine. Pojedini korisnici na internetu bez ikakvog su utemeljenja optužili pogrešnu osobu za napad, bivšeg policijskog službenika

[41] U kaznenom postupku osim toga postoje i posebna pravila vezana uz mogućnost uskrate pojedinih osobnih podataka, primjerice korištenje pseudonima za svjedoka u čl. 295. st. 5. ZKP-a.

[42] Slučaj *Draskas pr. Litve* odnosi se na objavljivanje snimaka iz posebnih dokaznih radnji što je ESLJP označio kao povredu čl. 8. EKLJP-a jer nije bila osigurana zaštita privatnosti iako su se tijela vlasti trebala brinuti za tajnost podataka, a naknadno istraživanje o načinu odavanja snimke medijima nije bilo provedeno učinkovito.

Damskeya (bijelac). Drugi korisnici koji su poznavali navedenog službenika potom su bez ikakve provjere objavljivali njegove razne osobne podatke, adresu i fotografije, olako se nadovezujući na prethodno neprovjerene komentare. To je u situaciji velikih rasnih napetosti i nemogućnosti kontrole agresivne mase predstavljalo iznimnu opasnost. Naknadno je otkriven pravi počinitelj napada i protiv njega je pokrenut kazneni postupak. Kao posljedica sličnih grupa na društvenim mrežama koje su bile usmjerene na ugrožavanje policijskih službenika tijekom tzv. prosvjeda žutih prsluka u Francuskoj, u parlamentarnu je proceduru upućen poseban zakon.[43] Za objave koje imaju cilj ugrožavanje drugih osoba, bilo bi potrebno razmatrati prilagođavanje pojedinih kaznenih odredaba i u našem kaznenom zakonodavstvu.

Primjer namjernih manipulacija prema policijskim službenicima jest objavljivanje snimaka koji fragmentarno pokazuju neki događaj. Na snimkama se ponekad izostavlja kažnjivo ponašanje osumnjičenika ili njegov napad na policijske službenike, te se započinje snimati tek kada policija započne postupati. Takvim se fragmentarnim pristupom, događaj na snimci nastoji prikazati kao neosnovana uporaba prisile, a prilikom objave u naslove stavljaju netočne navode da bi inicirali negativne internetske komentare. Ovakve su situacije također jedan od argumenata koji podupiru potrebu zaštite identiteta od javnosti i prepuštanja postupka nadležnim službama.

Ne radi se samo o policijskim službenicima. Primjer nerazmjernih posljedica za građane jest snimka osobe koja nije počistila iza svojeg ljubimca na javnome mjestu. Snimka je neočekivano postao vrlo gledan u toj državi i nakon što je netko prepoznao vlasnicu, a drugi otkrili njezino radno mjesto, korisnici su se počeli nadmetati u agresivnim komentarima. Pod pritiskom društvenih mreža, poslodavac joj je dao otkaz samo zato da bi izbjegao negativan publicitet za tvrtku iako se radi o prekršaju prema komunalnim odredbama i nije propisana sankcija u radnom odnosu (*Zittrain*, 2008: 211). Trebala je biti kažnjena na zakonit način u pravnoj proceduri, ali su društvene mreže potaknule prekomjerno sankcioniranje koje se odrazilo na njezino pravo na rad i eventualno na buduću karijeru. Internet ostvaruje utjecaj koji se naziva hiperskrutiniziranom realnošću i privlači pojedince željne pokazivanja moći nad drugima. *Zittrain* navodi brojne primjere u kojima su osobe pretrpjele razne posljedice, poput premlaćivanja pogrešne osobe a nakon svojevrsne internetske potjernice. Neodgovornost i depersonalizacija na društvenim mrežama uz dojam izostanka regulacije, može dovoditi do stanja sličnijeg javnom linču ili prijekoj kazni - negoli objektivnoj provjeri zakonitosti i prepuštanja postupka nadležnim tijelima.

Javno iznošenje osobnih podataka građana ili policijskih službenika nije nužno za raspravu o zakonitosti, osobito kada se radi o neprovjerenim okolnostima. Potrebno je razlikovati koji dio podataka predstavlja osobna prava, koji je dio snimke zaštićen drugim propisima (npr. klasificirani podatak), a koji je preostali dio moguće objaviti radi javnog predočavanja nekog problema. Proglašavanje nekog građanina ili službenika unaprijed krivim za navodno kršenje pojedinih pravila, ne pokazuje zabrinutost za zakonitost, nego predstavlja ključno negiranje funkcija pravosuđa.

[43] Prema prijedlogu zakona iz srpnja 2020. godine, kazna za objavu slike ili podatka policijskog službenika iznosi godinu dana zatvorske kazne ili 15.000 eura.

11. ZAKLJUČAK

Brojni aspekti zaštite osobnih podataka detaljno su protumačeni tijekom dugačkog razdoblja razvoja spomenutog prava na europskoj razini. Europski je sud utvrdio da izgled osobe i slična tjelesna obilježja na temelju kojih je moguće odrediti identitet osobe - ulaze u definiciju osobnih podataka, te da snimanje ili fotografiranje predstavlja oblik obrade podataka. Pravo na zaštitu osobnih podataka jedno je od temeljnih prava iz Povelje, što pokazuje da je prepoznato kao pravo koje je jednake važnosti kao i brojna druga prava koja su imala prednost u tranzicijskim državama. Detaljnija regulacija ostvarena je Uredbom u kojoj su osobni podaci definirani vrlo široko te obuhvaćaju brojna obilježja povezana s pojedinom osobom. Ako osoba, koju se (video)snima, nije prethodno dala pristanak, snimanjem se povređuju njezina prava. Prema judikaturi ESLJP-a, pravo pristanka ili odbijanja proširuje se na objavljivanje snimke, te na primjerke koji su pohranjeni kod snimatelja; a država bi trebala omogućiti odgovarajuću zaštitu ovoga prava u domaćem pravnom sustavu. Pojedine od ovih definicija važne su za primjenu našega zakonodavstva s obzirom na to da su pojmovi osobnih podataka i njihove obrade dio opisa kaznenog djela nedozvoljene uporabe osobnih podataka.

Okolnost da su neki osobni podaci kao što je izgled osobe dostupni na javnome mjestu, ne znači da ih je moguće obuhvaćati aktivnostima koje su invazivnije od promatranja, odnosno koje potpadaju u definiciju obrade podataka. Osobe na javnome mjestu po prirodi stvari pristaju da ih drugi zapaze, ali svaka intenzivnija aktivnost nadilazi uobičajeni društveni kontakt i može potpadati u definiciju prikupljanja osobnih podataka te predstavljati povredu Uredbe, osobito ako se registrira u digitalnom obliku kojim se podaci mogu proširivati. Brzi razvoj tehnologije i učestalo korištenje kamera postalo je primarnim razlogom detaljnije regulacije zaštite, uz uvažavanje gledišta da ne postoji opravdani cilj radi kojeg bi takva snimanja trebalo omogućavati. Znatiželja o tuđoj privatnosti nije legitiman pravni interes, tako da ni u Povelji, a ni u EKLJP-u, niti u bilo kojem drugom bivšem ili važećem europskom izvoru o temeljnim pravima - ne postoji pravo na snimanje drugih na javnome mjestu; kao ni pravo prikupljanja podataka o drugim građanima, neovisno o njihovoj profesiji ili radnome mjestu. Kada bi netko zastupao takvo pravo, time bi negirao zaštitu osobnih podataka kao temeljnog prava iz Povelje, a uz to bi naišao na poteškoće u predočavanju europskih ili domaćih pravnih izvora iz kojih bi proizlazilo takvo fiktivno pravo.

Ovakav europski model primjenjuje ista pravila i na građane koji su zaposleni kod raznih poslodavaca, neovisno o tome rade li u privatnom ili javnom sektoru. Ovakva osobna prava ne nestaju zapošljavanjem. To znači da videosnimanje policijskih službenika (ili drugih javnih ili državnih službenika) bez njihove suglasnosti također predstavlja povredu njihovih osobnih podataka. Prema počinitelju povrede moguća je primjena odgovarajućih policijskih ovlasti i pokretanje odgovarajućih postupaka. Ako je na javnome mjestu snimljeno počinjenje kaznenog djela u kojem sudjeluje službenik ili neka druga osoba, dopustivost takve snimke za dokazivanje jest predmet procjene kaznenog postupovnog prava kao posebnog zakonodavstva i na taj dio ne utječe zaštita osobnih podataka. Snimke se odavno prihvaćaju za dokazivanje u praksi naših najviših sudova.

U slučaju *Buivids* iz 2019. godine u kojem se osoba opravdavala da je snimala policijske službenike kao javne službenike na prostoru koji je bio dostupan javnosti, Europski sud nije prihvatio navode snimatelja nego je utvrdio da videosnimanje i objavljivanje njihova izgleda predstavlja obradu osobnih podataka (kao i bilo koje druge osobe u istoj situaciji). Europski

je sud zaključio da status službenika nije na razini političara niti javnih osoba čija privatnost može biti u većem stupnju izložena radi interesa javnosti. To je moguće opravdati time što građani, koji su zaposleni kao policijski službenici, nemaju društveni utjecaj kao političari, postupaju na temelju propisa i prema smjernicama nadređenih tijela; te ne nastupaju u službi kao privatne osobe. Novinarska iznimka može obuhvaćati pojedine aktivnosti građanskog novinarstva, ali Europski sud upućuje na kriterije ESLJP-a koji uvažavaju samo one novinarske aktivnosti koje su usmjerene na konkretnu temu i poneke ideje, a ne na voajerstvo. Novinarske aktivnosti ne izuzimaju novinare od pravila u drugim područjima zakonodavstva, primjerice zakonskih ograničenja radi osiguranja mjesta događaja ili radi održavanja javnog reda i mira.

Prikazano uređenje prava na zaštitu osobnih podataka u Povelji i povezana tumačenja ne predstavljaju novost za znanstvenu ili stručnu javnost u većini članica EU-a s obzirom na to da su sukladna s tradicionalnim poimanjem privatnosti kao afirmaciji osobnih prava građana. Štoviše, neke europske države imaju strože uređenje zaštite od snimanja u posebnom zakonodavstvu i propisane visoke odštete, te ovaj model predstavlja minimalnu zajedničku razinu. Ovakav model uvažava dostojanstvo svakog pojedinca i promiče temeljna prava nasuprot beskorisnom prenošenju tuđih podataka. Ovakvo pravo predstavlja novost uglavnom u nekim novijim člancima koje nisu imale razvijeno predmetno područje. Neobična je posljedica da ova pravila u takvim državama ujedno ostvaruju i funkciju zaštite građana koji su zaposleni kao policijski službenici, iako je u brojnim europskim državama taj dio također zasebno zakonski uređen u policijskom zakonodavstvu i drugim izvorima.

Europski model zaštite prikladniji je od američkog sustava u kojem postoji pravo snimanja drugih na javnome mjestu kao posljedica ustavnog tumačenja striktnih razlika između privatnog posjeda i javnog mjesta, ali je to pravo ograničeno na zakonskoj razini u gotovo svim saveznim državama. Američke policijske jedinice prema teorijskim mjerilima pripadaju u nekoordinirane i decentralizirane sustave; odnosno osnivaju se lokalno bez disciplinske hijerarhije na razini države. To predstavlja naročitu poteškoću u održavanju zakonitosti vidljivu u brutalnostima kakve su nepoznanica u europskim okvirima. Zbog toga društvena uloga snimanja policijskih službenika u tom sustavu ima posve drugačiji kontekst.

LITERATURA

Članci i knjige

1. Alderman, J. (2010). *Police Privacy in the iPhone Era: The Need for Safeguards in State Wiretapping Statutes to Preserve the Civilian's Right to Record Public Police Activity*. First Amendment Law Review, 9, 487-524.
2. Balzer, T., Nugel, M. (2014). *Minikameras im Straßenverkehr – Datenschutzrechtliche Grenzen und zivilprozessuale Verwertbarkeit der Videoaufnahmen.* Neue Juristische Wochenschrift, 67(23), 1622-1628.
3. Bessant, C. (2015). *The application of Directive 95/46/EC and the Data Protection Act 1998 when an individual posts photographs of other individuals online*. European Journal of Law and Technology, 6(2), 1-27.
4. Brkan, M. i dr. (2017). *Courts, Privacy and Data Protection in the Digital Environment*. Cheltenham: Edward Elgar Publishing.

5. Buchmann, A. (2019). *Kommunikation und Datenschutz bei Großveranstaltungen*. u: Groneberg, C., Veranstaltungskommunikation. Wiesbaden: Springer, 211-239.
6. Bygrave, L. (2002). *Data protection law: approaching its rationale, logic and limits*. Information Law Series. Hague: Kluwer Law International.
7. Coppel, P. (2020). *Information Rights: A Practitioner's Guide to Data Protection, Freedom of Information and other Information Rights*. London: Bloomsbury Publishing.
8. Čizmić, J., Boban, M. (2018). *Učinak nove EU Uredbe 2016/679 (GDPR) na zaštitu osobnih podataka u Republici Hrvatskoj*. Zbornik Pravnog fakulteta Sveučilišta u Rijeci, 39(1), 377-406.
9. Delmas-Marty, M., Spencer, J. (2002). *European Criminal Procedures*. Cambridge: Cambridge University Press.
10. Demetzou, K. (2020). *Risk to the Rights and Freedoms*. u: Hallinan, D., Data Protection and Privacy: Data Protection and Democracy. London: Bloomsbury Publishing, 127-145.
11. Doyle, A., Lippert, R., Lyon, D. (2013). *Eyes Everywhere: The Global Growth of Camera Surveillance*. Abingdon: Routledge.
12. Feinberg, M., Willer, R., Stellar, J., Keltner, D. (2012). *The virtues of gossip: Reputational information sharing as prosocial behavior*. Journal of personality and social psychology, 102(5), 1015-1030.
13. Gawronski, M. (2019). *Guide to the GDPR*. Alphen aan den Rijn: Kluwer Law International.
14. Gumzej, N., Dragičević, D. (2019). *Video Surveillance in the Workplace Under the Croatian Act on Implementation of the General Data Protection Regulation*. Zbornik Pravnog fakulteta u Zagrebu, 69(3), 327-346.
15. Hurt, A. (ur.). (2018). *Trial by Internet*. New York: Greenhaven Publishing.
16. Karas, Ž. (2014). *Sudska praksa o policijskom postupanju: snimanje na javnom mjestu, pregled motocikla, sastav vrste za prepoznavanje*. Policija i sigurnost, 23(4), 283-290.
17. Karas, Ž. (2015). *Sudska praksa o zakonitosti dokaza: tajno snimanje sugovornika; vaganje nezakonitih dokaza; snimka nadzora*. Policija i sigurnost, 24(4), 348-360.
18. Kraljić, S., Ünver, Y. (2019). *Street Photography in Light of Information Privacy*. Compendium of Contemporary Legal Issues. Maribor: University of Maribor Press.
19. Krapac, D. i sur. (2014). *Kazneno procesno pravo: Institucije*. Zagreb: Narodne novine.
20. Krause, H. (1965). *The Right to Privacy in Germany: Pointers for American Legislation?*. Duke Law Journal, 1965(3), 481-530.
21. Kühn, Z. (2018). *The Ryneš Case and Liability for Invasion of Privacy in the 21st Century*. Croatian Yearbook of European Law and Policy, 14(1), 241-253.
22. Lippert, R., Wood, D. (2012). *New Urban Surveillance: Technology, Mobility, and Diversity in 21st Century Cities*. Surveillance and Society, 9(3), 257-262.
23. Loveluck, B. (2019). *The many shades of digital vigilantism. A typology of online self-justice*. Global Crime, 1-29.
24. Lynskey, O. (2015). *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press.
25. Mahieu, R., Van Hoboken, J., Asghari, H. (2019). *Responsibility for Data Protection in a Networked World: On the Question of the Controller, Effective and Complete Protection and Its Application to Data Access Rights in Europe*. Journal of Intellectual Property, Information Technology and Electronic Commerce Law, 10, 85-105.

26. Martinović, I., Tripalo, D. (2017). *Zvučno i slikovno snimanje u kaznenom materijalnom i procesnom pravu - teorijski i praktični izazovi novih tehnologija i zakonskih rješenja*. Hrvatski ljetopis za kaznene znanosti i praksu, 24(2), 499-523.
27. McAndrew, F., Bell, E., Garcia, C. (2007). *Who do we tell and whom do we tell on? Gossip as a strategy for status enhancement*. Journal of Applied Social Psychology, 37(7), 1562-1577.
28. Mishra, D. (2007). *Undermining excessive privacy for police: Citizen tape recording to check police officers' power*. Yale Law Journal, 117, 1549-1558.
29. Morgan, R., Boardman, R. (2012). *Data Protection Strategy: Implementing Data Protection Compliance*. London: Sweet and Maxwel.
30. Nekovee, M., Moreno, Y., Bianconi, G., Marsili, M. (2007). *Theory of rumour spreading in complex social networks*. Statistical Mechanics and its Applications, 374(1), 457-470.
31. O'Boyle, M. (2020). *Human rights challenges in the digital age: Judicial perspectives*. Strasbourg: Council of Europe.
32. O'Malley, K. (2015). *Too many eyes in the sky: The impact of private sector drone use on the right to privacy and data protection*. Helsinki Law Review, 9(1), 7-24.
33. Richards, N., Solove, D. (2010). *Prosser's privacy law: A mixed legacy*. California Law Review, 98, 1887-1924.
34. Schwartz, P., Peifer, K. (2010). *Prosser's Privacy and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?*. California Law Review, 1925-1987.
35. Tzanou, M. (2020). *Personal Data Protection and Legal Developments in the European Union*. Hershey: IGI Global.
36. Voigt, P., Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Berlin: Springer.
37. Warso, Z. (2013). *There's more to it than data protection - Fundamental rights, privacy and the personal/household exemption in the digital age.* Computer Law and Security Review, (29), 491-500.
38. Westin, A. (1967). *Privacy and Freedom*. New York: Athenum.
39. Whitman, J. (2004). *The Two Western Cultures of Privacy: Dignity versus Liberty*. Yale Law Yournal, 113, 1153-1219.
40. Zittrain, J. (2008). *The future of the Internet - and how to stop it*. New Haven: Yale University Press.

Službeni dokumenti

1. DPWP - Data Protection Working Party (2004). Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance. 11th February 2004, 11750/02/EN.
2. DPWP - Data Protection Working Party (2001). Opinion 8/2001 on the Processing of Personal Data in the Employment Context. 13 September 2001, 5062/01/EN/Final.
3. DPWP - Data Protection Working Party (2002). Working Document on the Surveillance of Electronic Communications in the Workplace. 29 May 2002, 5401/01/EN/Final.
4. EDPB - European Data Protection Board (2019). Guidelines 3/2019 on processing of personal data through video devices. Plenary meeting, 09-10 July 2019.
5. EDPB - European Data Protection Bord (2020). Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020.

6. EDPS - European Data Protection Supervisor (2010). Video-surveillance Guidelines. 17 March 201.
7. CJPD - Project Group on Data Protection (2003). Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance. European Committee on Legal Co-operation (CDCJ) 78th meeting. 20-23 May 2003.
8. WP - Article 29 Data Protection Working Party (2018). Guidelines on consent under Regulation 2016/679. 10 April 2018, WP 259.
9. WP - Article 29 Data Protection Working Party (2011). Opinion 15/2011 on the definition of consent. 13 July 2011, WP 187.
10. AZOP - Agencija za zaštitu osobnih podataka (2016). Fotografiranje/snimanje policijskog službenika, mišljenje, klasa 004-02/16-01/530 urbr. 567-02/03-16-02 od 17. studenoga 2016.
11. AZOP - Agencija za zaštitu osobnih podataka (2017). Fotografiranje/snimanje policijskog službenika, odgovor, klasa 004-02/16-01/530 urbr. 567-02/03-17-04 od 2. veljače 2017.
12. AZOP - Agencija za zaštitu osobnih podataka (2017b). Fotografiranje policijskih službenika, preporuka za unaprjeđenje zaštite osobnih podataka, klasa 041-02/17-05/27, urbr. 567-02/03-17-02 od 9. listopada 2017.

Presude Europskog suda i mišljenja nezavisnih odvjetnika

1. Buivids Sergejs pr. Datu valsts inspekcija, mišljenje nezavisne odvjetnice od 27. rujna 2018., C-345/17.
2. Buivids Sergejs pr. Datu valsts inspekcija, presuda suda od 14. veljače 2019., C-345/17.
3. ClientEarth, Pesticide Action Network Europe (PAN Europe) pr. Europska agencija za sigurnost hrane, presuda suda od 16. srpnja 2015., C-615/13.
4. Digital Rights Ireland, Seitlinger Michael i dr. pr. Commissioner of the Garda Síochána i dr., presuda suda od 8. travnja 2014., C-594/12.
5. Europska komisija pr. Bavarian Lager Co., presuda suda od 29. lipnja 2010., C-28/08.
6. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos i Mario Costeja González, presuda suda od 13. svibnja 2014., C-131/12.
7. IPI Institut professionnel des agents immobiliers pr. Geoffrey Englebert, presuda suda od 7. studenoga 2013., C-473/12.
8. Jehovan todistajat, presuda suda od 10. srpnja 2018., C-25/17.
9. Lindqvist Bodil, mišljenje nezavisnog odvjetnika od 19. rujna 2002., C-101/01.
10. Lindqvist Bodil, presuda suda od 6. studenog 2003., C-101/01.
11. Rechnungshof pr. Österreichischer Rundfunk i dr., i Christa Neukomm i Joseph Lauermann pr. Österreichischer Rundfunk, presuda suda od 20. svibnja 2003., spojeni predmeti C-465/00, C-138/01 i C-139/01.
12. Ryneš František pr. Úřad pro ochranu osobnich údajů, mišljenje nezavisnog odvjetnika od 10. srpnja 2014., C-212/13.
13. Ryneš František pr. Úřad pro ochranu osobnich údajů, presuda suda od 11. prosinca 2014., C 212/13.
14. Schecke Volker i Markus GbR, i Hartmut Eifert, presuda suda od 9. studenoga 2010., C-92/09, C-93/09.

15. Smaranda Bara i dr. pr. Agenţia Naţională de Administrare Fiscală, mišljenje nezavisnog odvjetnika od 9. srpnja 2015., C-201/14.
16. Tietosuojavaltuutettu pr. Satakunnan Markkinapörssi Oy and Satamedia Oy, presuda suda od 16. prosinca 2008., C-73/07.
17. Worten Equipamentos pr. Autoridade para as Condições de Trabalho, presuda suda od 30. svibnja 2013., C-342/12.

Odluke ESLJP-a

1. Amann pr. Švicarske, br. 27798/95, 16 veljače 2000.
2. Bogomolova pr. Rusije, br. 13812/09, 20. lipnja 2017.
3. Brambilla i dr. pr. Italije, br. 22567/09, 23. rujna 2016.
4. Bremner pr. Turske, br. 37428/06, 13. listopada 2015.
5. Delfi AS pr. Estonije [GC], br. 64569/09, 16. lipnja 2015.
6. Draksas pr. Litva, br. 36662/04, 31. srpnja 2012.
7. Hachette Filipacchi Associés pr. Francuske, br. 71111/01, 14. lipnja 2007.
8. Herbecq i dr. pr. Belgije, br. 32200/96 i 32201/96, 14. siječnja 1998.
9. Janowski pr. Poljske, br. 25716/94, 3. prosinca 1997.
10. Krone Verlag GmbH pr. Austrije, br. 34315/96, 26. veljače 2002.
11. Leander pr. Švedske, br. 9248/81, 26. ožujka 1987.
12. Lillo-Stenberg i Sæther pr. Norveške, br. 13258/09, 16. travnja 2014.
13. Mitkus pr. Latvije, br. 7259/03, 2. listopada 2012.
14. Niemitz pr. Njemačke, br. 13710/88, 16. prosinca 1992.
15. Oberschlick pr. Austrije (no. 2), br. 20834/92, 1. srpnja 1997.
16. Peck pr. Ujedinjenog Kraljevstva, br. 44647/98, 28. siječnja 2003.
17. Pedersen i Baadsgaard pr. Danske [GC], br. 49017/99, 17. prosinca 2004.
18. Pentikäinen pr. Finske, br. 11882/10, 20. listopada 2015.
19. Reklos i Davourlis pr. Grčke, br. 1234/05, 15. siječnja 2009.
20. Rotaru pr Rumunjske, br. 28341/95, 4. svibnja 2000.
21. Satakunnan Markkinapörssi Oy i Satamedia Oy pr. Finske [GC], br. 931/13, 21. srpnja 2015.
22. Stoll pr. Švicarske [GC], br. 69698/01, 10. prosinca 2007.
23. Von Hannover pr. Njemačke, br. 59320/00, 24. rujna 2004.

Summary

Željko Karas

Video Recording Police Officers as a Violation of the European Data Protection Law

The author analyzes European regulations and court decisions on the protection of personal data in cases of video recording of persons in a public place without their consent. The analysis includes European regulations (GDPR, etc.), judgments of the European Court of Justice, the European Court of Human Rights and guidelines of the relevant authorities. Based on legal sources, the author analyzed the interpretation of the definition of personal data, data processing by video recording or publication, the role of the person being recorded, the characteristics of the public place, the status of officials, exceptions that may exclude violation (journalist exception and home use exception) and the use of recordings in criminal proceedings.

The analysis results show that European standards protect all types of personal data and that there are no exceptions for civil or public servants. Video recording or publishing of appearances or other physical features on the basis of which it is possible to determine the identity of police officers represents the processing of their personal data as well as of those of other citizens in a public place. Recording of police officers is allowed only with their prior consent or on legal grounds (according to the judgment of the European Court in the Buivids' case). Violation can be a criminal offense, depending on how it is regulated in the national legal system, and it is possible to initiate appropriate proceedings against the perpetrators. This model has its roots in the right to self-determination, according to which an individual can decide on certain aspects of their own privacy, and this right is retained in the workplace.

Keywords: video recording, police officers, personal data protection, European Court of Justice, European Court of Human Rights, GDPR.