UDK 351.74

PREGLEDNI ČLANAK

ŽELJKO KARAS*

DUŽNOST ČUVANJA PODATAKA PRIKUPLJENIH POSEBNIM DOKAZNIM RADNJAMA PREMA ODLUKAMA ESLJP I MJERE ZA NJENU PROVEDBU

Sažetak

Autor u radu analizira dužnost čuvanja podatka koju Europski sud za ljudska prava (ESLJP) traži radi sprječavanja odavanja transkripta i drugih podataka prikupljenih posebnim dokaznim radnjama, te mjere koje su potrebne za provedbu te dužnosti. Prema judikaturi ESLJP, države imaju dužnost sigurnog čuvanja podataka i dužnost učinkovitog istraživanja u slučaju odavanja podataka. ESLJP je u svojim odlukama samo naveo preporuke odgovarajućeg organiziranja tijela vlasti i edukacije službenika, bez podrobnijeg određivanja načina provedbe navedenih standarda te je odabir mjera prepustio državama.

Autor u radu analizira aktivnosti koje se općenito preporučuju za zaštitu od nezakonitih aktivnosti zaposlenika, te razmatra njihovu primjenjivost za zaštitu dokumentacije o posebnim dokaznim radnjama. Najveći dio fizičkih mjera zaštite može biti usmjeren na prostorije, uređaje i zaposlenike. Korisne su mjere zaštite kojima se uz preventivni učinak ujedno registriraju podaci koji mogu omogućiti učinkovitije istraživanje nakon odavanja podataka.

Ključne riječi: *odavanje podataka, transkripti, fizička zaštita, posebne dokazne radnje, ESLJP*

1. UVOD

Za uspješnu provedbu posebnih dokaznih radnji, kriminalistička taktika preporučuje održavanje tajnosti u svim fazama provođenja, odnosno u fazi prije, tijekom i nakon provedbe radnji. Osnove sumnje o kaznenom djelu radi kojeg je potrebno korištenje posebnih dokaznih radnji najčešće proizlaze iz činjenica koje se moraju prikupljati drugim radnjama, a neke od njih također su prikrivenog karaktera. Tijekom

* izv. prof. dr. sc. Željko Karas, Veleučilište kriminalistike i javne sigurnosti, Zagreb

pripremanja materijala za traženje sudskog naloga, potrebno je održavati tajnost jer bi inače neovlaštene osobe mogle saznati za planirano istraživanje, čime bi mogla biti onemogućena uspješna provedba.

Tijekom provedbe posebnih dokaznih radnji prikuplja se velika količina podataka te bi odavanje moglo osumnjičenicima davati mogućnosti prikrivanja, a osim toga, ako bi saznali da su pod primjenom prikrivenih mjera, mogli bi navoditi službenike na netočne podatke, pokušavati otkrivati način na koji se provode prikrivene radnje, otkrivati prikrivene izvore s kojima policija surađuje i druge slične podatke. Uz to, provedbom posebnih dokaznih radnji prikupljaju se podaci iz privatnog života raznih obuhvaćenih osoba koje nisu povezane s počinjenjem kaznenih djela, te bi odavanje moglo štetno utjecati na njihovu privatnost. U fazi nakon dovršetka posebnih dokaznih radnji, odavanje prikupljenih podataka također može imati slične štetne učinke. Odavanjem podataka nastaju i druge poteškoće jer će prikriveni izvori ubuduće biti manje skloni surađivati zbog razvoja nepovjerenja prema istražnim tijelima. Odavanje podataka iz tijela vlasti o radnjama koje su tijekom provedbe bile tajne i koje predstavljaju intruzivne zahvate u privatnost, ostavlja dojam nepouzdane organizacije.

Cilj rada je analizirati stajališta Europskog suda za ljudska prava (ESLJP) o dužnosti čuvanja podataka prikupljenih posebnim dokaznim radnjama, te razmotriti primjenjivost zaštitnih mjera koje se općenito preporučuju za zaštitu podataka. U radu je uvodno prikazano nekoliko slučajeva o kojima je odlučivao ESLJP te su prikazana tumačenja o dužnosti čuvanja prikupljenih podataka kao minimalnog standarda potrebnog za zaštitu privatnosti. ESLJP ne određuje koje vrste mjera su potrebne za učinkovito čuvanje podataka, ali ističe potrebu prikladnog organiziranja i edukacija što pretpostavlja odgovarajuće preventivne mjere unutar tijela vlasti. U ostalim dijelovima rada su analizirane mjere koje se preporučuju u teoriji i praksi zaštite podataka. Prema Pravilniku o tajnosti službenih podataka Ministarstva unutarnjih poslova, podaci vezani uz posebne dokazne radnje (planovi, metode, tehnička sredstva itd.) spadaju u kategoriju ograničeno (čl. 11.) a podaci o osobama koje su sudjelovale u tim radnjama i mogle bi biti ugrožene, spadaju u kategoriju povjerljivo (čl. 10.).

2. DUŽNOST ČUVANJA PODATAKA

Odavanje podataka prikupljenih posebnim dokaznim radnjama predstavlja povredu prava privatnosti zaštićenog u čl. 8. Europske konvencije o zaštiti ljudskih prava (EKLJP). Iz presuda ESLJP proizlazi potreba zaštite sadržaja prikupljenih prikrivenim radnjama jer se ne radi o javnim podacima. ESLJP je u više presuda odlučivao o navedenom pitanju i dosljedno je naglašavao dužnost čuvanja podataka. U slučaju Apostu pr. Rumunjske bivšem gradonačelniku je nakon uhićenja određen istražni zatvor zbog sumnje na korupciju. Prije postupka su u nekoliko medija objavljeni dijelovi razgovora prikupljeni tajnim nadzorom telefona. Sud je utvrdio da dostupnost takvih podataka

koje su prikupila tijela vlasti predstavlja povredu prava na poštivanje privatnog života. Država je propustila dužnost sigurnog čuvanja (eng. *safe custody*) podataka koje je prikupila. ESLJP je radi navedenog utvrdio postojanje povrede čl. 8. EKLJP, te naglasio postojanje odgovornosti države u organiziranju službi i obrazovanju službenika na takav način koji može osigurati da niti jedan podatak ne bude javno dostupan (§ 119).

U presudi Căşuneanu pr. Rumunjske transkripti snimke telefonskih razgovora koji su snimljeni mjerama tajnog nadzora objavljeni su u medijima prije nego je započelo suđenje u kaznenom postupku. Transkripti se odnose na razgovor u kojem jedan senator i sudac komentiraju jedan sudski slučaj i nagađaju je li bilo utjecaja drugih osoba na ishod postupka. ESLJP u presudi ponavlja da je odgovornost nacionalnih vlasti organizirati službe i obrazovati službenike kako bi se osigurala zaštita prikupljenih podataka (§ 81). ESLJP u konkretnom slučaju nije utvrdio predanost tijela vlasti u pokušaju utvrđivanja počinitelja navedene povrede (§ 95), te iz navedenog zaključuje kako je država propustila obvezu sigurnog držanja podataka koje posjeduje.

Prema stajalištu ESLJP, odavanje snimke prikupljene zakonitim radnjama tajnog nadzora telefona predstavlja povredu privatnosti (Drakšas pr. Litve). Tijelo vlasti koje je prikupljalo snimke trebalo ih je čuvati na odgovarajući način. Ovaj slučaj se odnosi na snimku razgovora iz nadzora telefona kojeg je provodila agencija državne sigurnosti. Pola godine kasnije snimka je objavljena u programu televizijskih kuća. ESLJP je utvrdio da agencija koja provodi nadzor ima dužnost čuvati tajne snimke i učinkovito istraživati odavanje podataka. Radi propusta u navedenom, utvrđen je nedostatak zaštite privatnosti, te je Sud utvrdio povredu privatnosti iz čl. 8. Konvencije.

U predmetu Craxi pr. Italije (br. 2) ESLJP je utvrdio povredu u slučaju u kojem su transkripti tajno snimanog telefonskog razgovora bivšeg premijera objavljeni u medijima. Sud je utvrdio da odavanje transkripata medijima predstavlja zahvat u privatni život te da bi trebalo provesti neophodne korake kako bi zaštitili prava osobe, kroz odgovarajuću zaštitu podataka i efikasno istraživanje. Vlasti nisu provele navedeno i zato je utvrđena povreda čl. 8. Konvencije.

3. ZAŠTITA PODATAKA OPĆENITO

3.1. Organiziranje sustava zaštite

Kao osnovne preporuke, ESLJP u prikazanim presudama ponavlja potrebu prikladnog organiziranja tijela vlasti i provođenja edukacija službenika, ali detaljnije ne određuje koje su mjere neophodne za provedbu navedenih preporuka. Organiziranje načina rada za provedbu dužnosti čuvanja podataka može se odnositi na fizičku zaštitu te nadzor objekata, prostorija, osoba i dokumenata. Sustavi zaštite mogu biti pasivni ako se odnose na uspostavljanje tehničkih uvjeta radi kojih bi nepravilno korištenje dokumenata bilo otežano, ili aktivni sustavi zaštite kojima se reagira na nepravilnosti i pokušava se detektirati počinitelj. Mjere zaštite mogu se odnositi na prostor, dokumente i zaposlenike,

te na njihove procedure i upoznavanje s mogućnostima nastanka nepravilnosti. Fizička sigurnost se odnosi na sigurnost infrastrukture i osoba koje ju koriste, na sigurnost određenog šireg prostora, računalne ili fizičke dokumente i drugo (Vacca, 2017:965). Uvođenjem procedura zaštite, povećava se vjerojatnost uočavanja činjenica na temelju kojih je moguće reduciranje odavanja podataka i uspješnije otkrivanje počinitelja (Bunn, Sagan, 2017:155). Odgovarajuća provedba preventivnih mjera izravno je povezana s učinkovitim istraživanjem, jer nakon otkrivanja događaja, registrirani podaci omogućuju određivanje užeg kruga osoba kojima su bili dostupni određeni dokumenti. Čini se da je radi toga ESLJP isticao potrebu prikladnog organiziranja zaštite.

Cilj zaštite je sprječavanje i otkrivanje neovlaštenog pristupa te neovlaštenog korištenja podataka. Politika obrazovanja o zaštiti podataka sastavni je dio svakog modela zaštite, te zaposlenici nakon edukacije trebaju potpisati dokumente o upoznavanju s načinom rada (Shabtai, 2012:6). Obrazovanje je preporučljivo provoditi kroz analize stvarnih slučajeva kako bi zaposlenici jednostavnije razumijevali razloge za nastanak pojedinih mjera, a u protivnom bi dio savjeta mogli podcjenjivati. Edukacije se periodično ponavljaju radi podsjećanja, obično jednom na godinu. Obrazovanje doprinosi kulturi sigurnosti i može biti važniji čimbenik sustava sigurnosti nego ugrađena oprema (Bunn, Sagan, 2017:159). Osim obrazovanja, potrebno je promicati lojalnost i motiviranost zaposlenika te svijest o zajedničkom doprinosu ciljevima ustanove. Ako se javljaju problemi u sigurnosti, to može negativno utjecati na rad svih pojedinaca u ustanovi, te bi svi trebali doprinositi poboljšavanju zaštite odnosno otkrivanju nepravilnosti. U okviru obrazovanja, naglašava se potreba prijavljivanja uočenih nepravilnosti s ciljem pomaganja zaposlenicima koji imaju poteškoća u radu.

ESLJP ne propisuje pravila potrebna za prikladno organiziranje zaštite u tijelima vlasti kako bi se prevenirale nezakonite radnje zaposlenika, niti je slična pravila donijelo neko drugo europsko tijelo, već uređenje ovisi o nacionalnom zakonodavstvu. Od općenitih odredbi o zaštiti, u našem zakonodavstvu čl. 5. Zakona o informacijskoj sigurnosti propisuje standarde i mjere poput nadzora pristupa podacima te postupanja prilikom neovlaštenog otkrivanja, a čl. 8. propisuje sigurnosnu provjeru, fizičku sigurnost i druge mjere. Navedene mjere detaljnije se uređuju podzakonskim propisima.[1] Uredba o mjerama informacijske sigurnosti obuhvaća mjere kao što su fizička sigurnost i provjera zaposlenika (čl. 10.). Prema čl. 18. Zakona o tajnosti podataka, pristup klasificiranim podacima mogu imati osobe nakon pozitivno provedene sigurnosne provjere.

Primjer pravila specifično usmjerenih na zaštitu od kažnjivih radnji zaposlenika je američka Nacionalna politika za suzbijanje opasnosti od zaposlenika (engl. *National Insider Threat Policy*)[2] u kojoj je propisana obveza implementacije fizičkih mjera

[1] Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava iz 2008. se ne objavljuje u Narodnim novinama, kao niti Pravilnik o standardima fizičke sigurnosti iz 2011.

[2] Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, 2012.

zaštite, nadzora korištenja tajnih dokumenata i računalnih sustava (nadzor pristupa, registriranje korisnika itd.), provjera zaposlenika (nepravilnosti u radu, imovina, poligraf, neuobičajene aktivnosti itd.), obrazovanje o potrebi zaštite (edukacija, prepoznavanje prijetnji, prijavljivanje itd.), provedbi nadzora i usklađivanju mjera (analiza svih podataka iz zaštitnih mjera i njihovo unaprjeđivanje itd.). Navedene aktivnosti uobičajeno se navode u teoriji zaštite podataka i primjenjivane su u praksi raznih tijela vlasti (obavještajne agencije, redarstvene vlasti itd.) ili drugih subjekata (tiskare novčanica, nuklearna postrojenja, skladišta dijamanata itd.). Odavanje podataka ili krađe sitnih predmeta na radnom mjestu u navedenim poslovanjima mogu nanositi vrlo visoku štetu kao što su pokazali neki primjeri (Contos, 2006:47).

Organiziranje procesa unutar određenog tijela vlasti podrazumijeva donošenje politike postupanja s podacima. Za uspostavu sustava zaštite potrebna je procjena rizika i izrada plana zaštite, odnosno razrađivanje procedura potrebnih za čuvanje, odgovarajuće upravljanje zaštitom te usavršavanje i obrazovanje (Vacca, 2017:8). U okviru organiziranja, periodično se provode procjene mogućnosti počinjenja, tijekom kojih se nastoje kreirati novi scenariji i pripremati za razne varijante radi smanjivanja ranjivosti sustava (Bunn, Sagan, 2017:138).

Šteta od odavanja podataka može se promatrati kao izravna i neizravna šteta u odnosu na držatelja podataka. Izravna šteta odnosi se na konkretni slučaj odavanja, štetu koju će biti potrebno isplatiti u slučaju tužbi, troškove istraživanja, troškove kazni, narušavanja redovnog poslovanja i slično. Neizravna šteta ima širi utjecaj u smislu razvoja nepovjerenja, narušavanja ugleda određenog dijela vlasti, prilagodbi počinitelja nakon uvida u način rada redarstvenih vlasti i slično (Vacca, 2017:530). Prosječna šteta od unutarnjeg odavanja je veća nego od vanjskih napada jer su unutarnjim počiniteljima poznate procedure zaštite, kao pouzdane osobe imaju pristup podacima, i poznato im je gdje se nalaze (Gaonjur, 2006). Zaštitne mjere bi trebale biti ujednačene u svim tijelima vlasti koja se bave istom vrstom dokumentacije. Ako jedno tijelo vlasti primjenjuje zadovoljavajuće mjere a neko drugo tijelo ne provodi slične mjere iako prima istu vrstu podataka, tada zaštita podataka nije koordinirana i umanjene su mogućnosti prevencije.

3.2. Mjere zaštite prostora i dokumentacije

Za visoku razinu fizičke zaštite prostora i dokumentacije, potrebno je uspostaviti prikladne mjere ovisno o okolnostima rada pojedinih tijela vlasti. Zaštita podataka znači osiguravanje njihove dostupnosti samo osobama koje su ovlaštene za uvid, uz svako registriranje uvida ili korištenja podataka te korištenja identifikacijskih sustava kako bi zaposlenici razvijali svijest o svojoj odgovornosti za čuvanje jer su aktivnosti registrirane pod njihovim identitetom. Ključni dio je nadzor dokumentacije i interakcija zaposlenika s dokumentacijom. Uobičajena zaštita uključuje fizičke mjere poput zaključanih prostora u kojima se drži dokumentacija, odlaganje tajnih podataka u sefovima, ugradnja sustava

za nadzor ulaska, sustava za provjere identiteta, alarmnih sustava i potrebnih senzora, nadzora izlaza i provjere predmeta koje zaposlenici iznose i slične mjere (Wettering, 2000:367). Osiguranje pristupa podacima je određivanje koji dio podataka će biti dostupan određenom službeniku nakon što će korisniku biti provjeren identitet. Potrebno je čim uže odrediti krug osoba kojima bi određeni dokumenti trebali biti dostupni, prema načelu uvida samo ako je to nužno za obavljanje poslova.

Za potrebe fizičke zaštite prostorija, potrebno je promatrati razne okolnosti poput vidljivosti pojedinih sadržaja iz vanjskog prostora, odnosno iz hodnika ako zidovi nisu do stropa, vrste brava na vratima, veličine prozora, opremljenost ladica bravama, periodične promjene bitnih brava i slično. U odnosu na spise u radu, preporučuje se pravilo čistog stola (engl. *clear desk policy*) bez ostavljanja vidljivih spisa, a uz to je moguće podizanje pregrada oko stolova i sličnih oblika zaštite. Spise bi bilo preporučljivo odlagati u zaključanom prostoru čim prestane potreba korištenja. Preporučuje se izbjegavanje situacije u kojoj bi dokumenti ili predmeti bili duže vremena izvan zaključanog prostora ako se ne koriste (npr. na radnom stolu, u otvorenoj torbi, po podovima itd.), već bi svaki put trebali biti odloženi na sigurno mjesto, a to ujedno doprinosi detaljnijem registriranju frekvencije uvida u dokumente i povećava svijest o vlastitoj ulozi zaposlenika svaki put kad preuzima materijal. Za presnimavanje sadržaja s pojedinih nositelja podataka (CD, DVD, memorijske jedinice) počinitelju ne treba puno vremena ako je duže promatrao rutinu ili navike pojedinih zaposlenika.

Ako se spisi ne koriste samo u službenim prostorijama nego se iznose do drugih tijela vlasti, to je također potrebno registrirati i provoditi potrebne mjere zaštite tijekom iznošenja, prenošenja te odlaganja kod odredišnog tijela. Spremnici ili torbe za prenošenje mogu biti opremljene uređajima za praćenje ili uređajima koji registriraju otvaranje spremnika tijekom prijenosa. Potrebna je odgovarajuća sigurnosna politika u odnosu na podatke koji se službeno iznose. Nakon završetka rada na spisima, potrebno je regulirati način na koji se uništavaju. Povremeno se obavljaju provjere otpada službenika s ciljem provjere sadržavaju li podatke koji su trebali biti propisno uništeni.

U nekim objektima vrlo visoke razine sigurnosti uočavani su propusti isključivanjem pojedinih uređaja za nadzor ako su prečesto signalizirali pojave koje se nisu pokazale kažnjivima, ostavljanjem nezaključanih vrata, ladica i sličnih propusta. Njihovo učestalo ili periodično ponavljanje može omogućiti planiranje počiniteljevih aktivnosti. O navedenom je potrebno odgovarajuće obrazovanje službenika (Vacca, 2017:9). Navedene aktivnosti preporučuju se na generalnoj razini kao oblik fizičke zaštite u raznim područjima rada tijela vlasti, ali su u većem dijelu primjenjive u odnosu na materijale prikupljene posebnim dokaznim radnjama.

3.3. Zaštita računalnih sustava

Velik dio poslova vezanih za posebne dokazne radnje provodi se kroz digitalne sustave na kojima je također potrebno provoditi odgovarajuće mjere zaštite. Snimke koje se prikupljaju posebnim dokaznim radnjama preslušavaju se preko računalnih sustava, na računalnim sustavima se sastavlja dokumentacija, podaci se prenose i dostavljaju također u digitalnom formatu na optičkim ili drugim medijima (CD, DVD) što pokazuje veliku važnost odgovarajuće zaštite. Moguće je primjenjivati generalne preventivne mjere kao i inače u računalnim sustavima kako podaci ne bi bili korišteni izvan svrhe kojoj su namijenjeni. Za komunikaciju između pojedinih istražnih tijela potrebno je koristiti zaštićene oblike prijenosa.

Mjere mogu biti usmjerene na općeniti način rada sustava, ograničavanje pristupa neovlaštenim osobama, ograničavanje pojedinih radnji s dokumentima i podacima. Pojedina programska rješenja onemogućuju razne aktivnosti koje bi zaposlenici mogli koristiti za nezakonite radnje. Na primjer, moguće je blokiranje raznih aktivnosti:izrade kopija datoteka s računala, izrade preslike ekrana, prenošenja datoteka na vanjske jedinice računala, slanje materijala s ključnim riječima iz dokumenata i sličnih aktivnosti. Programskim rješenjima može se nadzirati i registrirati način korištenja izlaznih i ulaznih jedinica na računalima kako bi se onemogućilo kopiranje ili prebacivanje datoteka na prijenosne diskove. Programi mogu spriječiti prijenos na vanjske memorije, ispisivanje, faksiranje, slanje osjetljivih dokumenata kao priloga, dodavanja u neku drugu vrstu komunikacije, dodavanje na zajedničke mape u lokalnu mrežu, otvaranje podataka u drugim programima radi izbjegavanja zaštite, kriptiranje prije slanja, promjene dijela datoteke i slično. Sustavi koji nadziru mrežni promet prema internetu mogu pregledavati promet po ključnim riječima koje preuzimaju iz pojedinih dijelova tajnih dokumenata. Na računalnim sustavima je dopušteno koristiti samo provjerene vanjske jedinice memorije, ne bi bilo preporučljivo koristiti privatne uređaje.

Moguće je provoditi nadzor nad lokalnom mrežom, te prijelaz na vanjski internet, kroz pretraživanje uobičajenih protokola slanja podataka (e-mail, instant poruke itd.) te nasumičnom provjerom drugih sadržaja radi provjere korištenja novih oblika slanja. Sustav može pretraživati elektroničku poštu, dostavu dokumenata, nadzirati službena računala i laptope, te sustave masovnog pohranjivanja. Ako sustav zaštite pronađe zaštićeni materijal u komunikaciji, izdvaja ga i sprema na drugu lokaciju, neke su opcije da ga može kriptirati, obavijestiti administratora, staviti u karantenu i zatim omogućiti detaljniju naknadnu provjeru. Ovakva programska rješenja mogu djelomično raditi i na pojedinačnim računalima dok nisu spojena na mrežu. Vrlo su korisna ako je računalo ukradeno ili izgubljeno te ga počinitelj pokuša spojiti na internet. Ovakvi oblici nadzora ne znače permanentno nadziranje svih sadržaja zaposlenika nego su mjere ciljane na pojedine ključne dijelove podataka kroz automatsko djelovanje sustava. Navedena

programska rješenja registriraju i pohranjuju pojedine podatke te se uvid u njih može ostvariti nakon uočavanja pojedinog događaja i postojanja odgovarajuće pravne osnove.

Podaci u računalnim sustavima trebali bi biti kriptirani kako bi se povećala zaštita, a računala bi se trebala automatski zaključavati lozinkom nakon kratkog razdoblja neaktivnosti zaposlenika (Vacca, 2017:406). Kriptiranje je važna aktivnost za razne vrste podataka. Ponekad zaposlenici nemaju loše namjere, primjerice kopiraju podatke na drugi uređaj kako bi radili kod kuće, ali nakon gubitka navedenog mogu nastati problemi ako sadržaji nisu bili kriptirani.

Zaštita digitalnih podataka je otežana razvojem tehnologija. Nekad je dovoljno bilo tražiti registriranje kod korištenja fotokopirnog uređaja, pristupa dokumentima ili ulaza i izlaza iz zgrade. Nastao je niz tehnologija kojima se jednostavno može prekopirati i poslati vrlo velike količine podataka u kratkom vremenu. Kao posljedica razvoja tehnologije, mjere se proširuju na privatne uređaje zaposlenika koji moraju biti registrirani tijekom ulaska ili im je ograničeno unošenje. U tijelima koje rade s klasificiranim podacima, ograničeno je unošenje uređaja kojima se može preuzimati, nadzirati ili presnimavati podatke. Moguće je provođenje povremenih provjera zaposlenika ili prostorija, uz disciplinsku odgovornost kod pronalaska navedenih ili započinjanja prikrivenog istraživanja ako postoji sumnja u neke teže nepravilnosti.

U analizi stranih slučajeva odavanja podataka, kao najučestalija metoda počinjenja korišteno je prebacivanje klasificiranih podataka na prijenosne medije, pri čemu je najviše korišten optički medij (CD ili DVD) a u nešto manjem udjelu memorijski štapići i prijenosni tvrdi diskovi (HDD, SSD). Kod prijenosa na daljinu, najviše je korištena elektronička pošta u oko četvrtini otkrivenih slučajeva pri čemu je polovica od tih počinitelja koristila dvije metode. Po učestalosti slijedi prebacivanje na drugo računalo, a u malenom udjelu počinitelji su koristili složenije metode za dijeljenje podataka (FTP sustavi i slično). Neki počinitelji su podatke prije slanja komprimirali, kriptirali i poslali ih u manjim paketima na vanjski server s kojeg su ih kasnije preuzimali. Neke metode su poznate prosječnim korisnicima poput slanja elektroničkom poštom, ispisa, pohranjivanja na mrežne mape, a neke metode prijenosa posebnim programima za dijeljenje podataka spadaju u složenije oblike (Cappelli, 2012:90). Navedene općenite mjere zaštite su uglavnom primjenjive u području rada tijela vlasti u skladu s zahtjevima ESLJP, te se mogu prilagođavati slično kao i u radu raznih institucija kojima je potrebna zaštita dokumentacije.

3. MJERE ZAŠTITE OD ZAPOSLENIKA

3.1. Uloga zaposlenika

Odavanje podataka može biti posljedica slučajne ili namjerne aktivnosti zaposlenika tijela vlasti. Podatke mogu odavati unutarnji subjekti (engl. *insider*, zaposlenik), vanjski počinitelji (napad drugih počinitelja na sustav), treće strane (održavanje sustava) ili

korisnici. Zaštita od unutarnjih počinitelja složenija je nego od vanjskih napada jer su zaposlenicima poznate mjere sigurnosti i dublje su uključeni u aktivnosti s dostupnim materijalima, a zbog dugogodišnje povezanost i razvoja odnosa s drugim kolegama, teže je pretpostavljati da bi bili uključeni u nezakonito odavanje podataka (Bunn, Sagan, 2017:3). Zaposlenici mogu biti pasivni ako čekaju odgovarajuće prilike (nezaključani ured ili ladicu sa spisima) ili aktivni ako sami stvaraju prilike (pokušaj otvaranja zaključane ladice, krađe identifikacijske kartice i slično).

Neovlašteno prikupljanje podataka mogu počiniti službenici zaduženi za te podatke ali i razne vrste pomoćnog osoblja (dostavljanje, čišćenje, održavanje prostorija i slično), rukovoditelji i drugi. Na izlazu iz objekta pregledava se sadržaj kojeg osobe iznose, a zbog razvoja tehnologija i smanjivanja uređaja na koje se može prekopirati vrlo velika količina podataka, takav način nadzora je otežano provoditi te se djelovanje više usmjerava na skenere tijela i slične uređaje (Wettering, 2000).

Interno odavanje podataka može biti motivirano raznim okolnostima poput financijskih problema, ucjena, povezanosti s organiziranim kriminalnim skupinama ili raznih privatnih motiva (Cappelli, 2012:116; Vacca, 2017:532). Veliku ulogu može imati nezadovoljstvo radnom okolinom ili uvjetima, sukobi s kolegama ili rukovoditeljima, degradacije na niže radno mjesto i slični kadrovski problemi (Bunn, Sagan, 2017:160). Analize su pokazale da je 97% počinitelja već bilo uočeno po nekim sumnjivim događajima pred svojim kolegama, ali ih oni nisu prijavljivali nadležnim unutarnjim jedinicama jer su ih smatrali nevažnima (Bunn, Sagan, 2017:154), što ukazuje na nedostatke organizacije procesa prijavljivanja. Otkrivanju doprinosi razvijena kultura prijavljivanja nepravilnosti koje su uočene u radu drugih kolega.

Navedene generalne mjere uglavnom su primjenjive u području zaštite dokumentacije u skladu s općenitim zahtjevima ESLJP, ali neke posebne mjere zaštite kakve se mogu koristiti u tijelima visoke razine sigurnosti s ciljem sprječavanja iznošenja dokumenata i papirnatih materijala teško bi bile primjenjive u uredskom obliku rada s velikom količinom dokumentacije (npr. radna odjeća bez džepova u tiskari novčanica, potpuno skidanje prije ulaska i izlaska iz postrojenja, blokiranje i preventivno pretraživanja svih zaposlenika nakon nasumičnog oglašavanja zvučnog signala, otvaranje uređaja za tiskanje isključivo uz dva ključa iz različitih jedinica itd.; Bender, 2006:38).

3.2. Sigurnosne provjere zaposlenika

Korisno je provođenje periodičnih sigurnosnih provjera zaposlenika te poligrafskih provjera. Prema iskustvima iz ranijih slučajeva odavanja podataka, provjeravaju se okolnosti koje bi mogle dovoditi do razvoja motiva za odavanje podataka kao što su zlouporabe droga, alkohola, financijski problemi, bračni problemi, prostitutke i slična sredstva koja su za ucjenjivanje iskorištavali vanjski subjekti koji su nastojali prikupljati podatke. Navedene provjere moraju biti usklađene s propisima o zaštiti osobnih podataka.

Sigurnosne provjere predstavljaju općenito utvrđivanje podataka te se istraživanje može nastavljati u odnosu na pojedinu osobu u slučaju poklapanja više indicija. Primjer je službenik na slabije plaćenom poslu koji posjeduje dva luksuzna vozila, jedan sportski auto i gliser, da bi nakon detaljnijih provjera bili pronađeni dokumenti koje je spremao u garažu i prodavao (Wettering, 2000:272).

Periodične provjere mogu biti korisno sredstvo ako se provode radi provjere pridržavanja sigurnosnih pravila. Primjeri su službenici koji su imali slučajeva nepridržavanja pravila, korištenja droge, većih dugova, ucjena i sličnih motiva za suradnju s vanjskim počiniteljima u odavanju podataka (Camp, 2019). Prema analizama otkrivenih slučajeva odavanja podataka u stranoj praksi, počinitelji su koristili svoje svakodnevne ovlasti, uz propuste u preventivnim mjerama prema pojedinim spisima, preširokih ovlasti uvida u pojedine materijale, vrata ponekad nisu bila zaključana itd. Uglavnom su otkriveni na temelju pretjeranog pokazivanja imovinske koristi, korištenja dokumenata izvan radnog vremena i sličnih indicija.

U nekim sustavima zaštite, ključne osjetljive aktivnosti s vrlo važnim predmetima ili materijalima ne smije nasamo provoditi jedna osoba, nego tada uvijek mora biti nazočan još jedan službenik iz neke druge jedinice (tzv. pravilo dvije osobe, engl. *two person rule,* odnosno pravilo četiri oka, engl. *four eyes principle*), a uz to se provodi video nadzor iz više kutova. Ovakvo pravilo se koristi u raznim vrstama aktivnosti (aktivnosti s nuklearnim materijalima, skladišta dijamanata, otvaranje trezora itd.) ali se uglavnom radi o centraliziranim radnjama koje se ne događaju često te bi bila upitna široka primjenjivost u odnosu na dokumente koji se često koriste u istražnim tijelima. Takav oblik zaštite je složen i zahtijevao bi velik broj zaposlenika, te se koristi samo kod posebno osjetljivih materijala odnosno kod faza otvaranja ili iznošenja pojedinih ključnih dijelova u poslovanju.

Za procjenjivanje unutarnjih prijetnji, potrebno je proučavanje bihevioralnih i organizacijskih karakteristika. Ako se osoba sprema za odlazak u drugu tvrtku, smanjena je razina lojalnosti te iskustva pokazuju potrebu premještaja na radna mjesta na kojima nema osjetljivih materijala, uz promjenu ključeva za prostorije i lozinki koje je koristio. Ako je predmet zaštite raširen tako da ga može koristiti velik broj osoba, pokušava se nadzirati čim više aktivnosti na radnom mjestu. Ne može se oslanjati samo na jednu mjeru, potrebno je zajedničko djelovanje većeg broja preventivnih mjera (Camp, 2019).

U nekim sustavima učestalo se provode provjere poštivanja sigurnosnih pravila, odnosno kontrolni pregledi jesu li svi uređaji i dokumenti čuvani kako bi trebalo, čime doprinose povećanju svijesti o kulturi sigurnosti. Moguće je povremeno pretraživanje uređaja s ciljem utvrđivanja koristi li se oprema u skladu s informacijskim pravilima određenog tijela vlasti. Provjere se provode radi traženja neovlaštenih uređaja, posjedovanje softvera za hakiranje i slično. Preporučuje se nagrađivanje zaposlenika koji se pridržavaju pravila ili koji su pokazali neku novu mogućnost ugrožavanja sigurnosti. Ponekad je otežano uvoditi razne vrste nadzora s jedne strane, a ujedno pokazivati

poštovanje zaposlenika i motivirati ih s druge strane, te je potrebno prikazivati da je to neophodno radi osjetljive vrste poslova koja i njima daje na važnosti, te da su svi u organizaciji jednako obuhvaćeni navedenim pravilima.

Najveća razina ugrožavanja računalnih sustava moguća je od administratora ili održavatelja računalnih sustava koji imaju najšire ovlasti izvan kontrole drugih subjekata, te mogu masivno kopirati veliki broj datoteka (npr. Manning za Wikileaks ili Snowden). U najviše slučajeva takvih zlouporaba, zlonamjerni kodovi su uneseni tijekom navodnog održavanja ili izmjena sustava jer su kontrole tada bile slabije nego kod prvog uvođenja (Cappelli, 2012:136). Za preveniranje takvih slučajeva potrebno je registriranje svih oblika ulaska u sustav neovisno o razini ovlasti administratora, dijeljenje funkcija subjekta koji izrađuje programska rješenja i subjekta koji ih odobrava, te provjere izvornog koda (eng. *code review*), izrada sigurnosnih kopija cijelog sustava, te daljnji nadzor i registriranje svih izmjena izvornog programskog koda (Cappelli, 2012:143). Analiza primjera iz strane kriminalističke prakse pokazuje brojne primjere programerskih ulaza u sustav (tzv. stražnja vrata, eng. *back door*) kroz kojeg su bez znanja istražnih tijela preuzimali podatke, mijenjali ih ili brisali, otvarali nove profile za ulazak, isključivali neke korisnike, prekidali rad cijelog sustava, ostavljali programe za brisanje cijelog sustava (tzv. logička bomba), preuzimali tuđe lozinke, kopirali cijeli sustav na vanjske servere i slično. Najviše uhvaćenih počinitelja bilo je motivirano imovinskom koristću, a preostali dio je bio motiviran osvetom ili nekim osobnim razlozima (poslove administracije preuzima vanjska tvrtka, svađa s kolegama, tražio premještaj suradnika itd.). Složeno je provoditi zaštitu u slučajevima ako je više zaposlenika međusobno povezano na raznim funkcijama te s raznih strana omogućuju iznošenje podataka i međusobnu zaštitu odnosno osujećivanje pojedinih zaštitnih sredstava. U takvim slučajevima je moguće počinjenje unatoč višestrukim mjerama zaštite, ali detaljno registriranje podataka osigurava naknadno otkrivanje počinitelja (npr. krađa dijamanata iz središnjeg skladišta u Antwerpenu 2003.).[3]

4. ISTRAŽIVANJE ODAVANJA PODATAKA

Kao što je u dosadašnjem izlaganju prikazano, naglasak u suzbijanju neovlaštenog odavanja podataka nije u oslanjanju na mogućnosti istraživanja nakon što se odavanje podatka već dogodilo (reaktivno istraživanje), nego na preventivnom pristupu s ciljem smanjivanja mogućnosti odavanja i registriranja interakcija kako bi se mogao utvrditi uži krug mogućih počinitelja (proaktivni pristup). Nakon otkrivanja počinjenja odavanja

[3] Krađa je počinjena iz trezora dvije razine ispod zemlje u središtu tzv. gradske četvrti dijamanata u Antwerpenu u Belgiji u kojoj je 80% svjetske trgovine dijamantima i koja je široko pokrivena sredstvima fizičke zaštite (pomične zapreke na svim izlazima iz četvrti, video nadzor ulica, policijska postaja itd.), a uz to je zgrada posebno opremljena sustavima zaštite (senzori svjetla, pokreta, topline, magnetizma, radarski nadzor, posebna skupina čuvara itd.). Šteta od krađe iznosila je preko 100 milijuna eura, dio počinitelja je osuđen, dijamanti nisu pronađeni.

podataka, provodi se istraživanje okolnosti počinjenja s ciljem utvrđivanja okolnosti povrede, načina počinjenja i korektivnih mjera za unaprjeđenje sustava zaštite (Shabtai, 2012:13). U kriminalističkom istraživanju potrebno je utvrditi motive i druge okolnosti (Vacca, 2017:415). Većina odavanja podataka o kojima je odlučivano u presudama ESLJP počinjena je u fazi prije početka postupka dok još nije bio uključen velik broj službenika raznih tijela vlasti ili drugih subjekata, radi čega je bilo moguće usmjeravanje daljnjeg istraživanja odgovornih subjekata na uži krug osoba. Planiranje istraživanja treba prilagoditi vrsti radnog mjesta osumnjičenika, dužini staža, motivaciji, načinu počinjenja i drugim okolnostima koje mogu biti važne za istraživanje.

Nije preporučljivo započeti s otvorenim istraživanjem osim ako postoje pouzdani podaci o dokazima, nego je taktički korisnije započeti prikrivene radnje kako osumnjičene osobe ne bi saznale da su pod nadzorom i kako bi se moglo učinkovitije prikupljati više dokaza. Prerano pokazivanje sumnje može biti štetno za ciljeve istraživanja. Mjerama tajnog nadzora moguće je prikupljati znatno više korisnih podataka poput obilježja o načinu počinjenja, otkrivanja drugih uključenih suradnika, načina obilaženja zaštitnih mjera, odavanja podataka kriminalnim krugovima i sličnih okolnosti koje ne bile razjašnjene na drugačiji način. Istraživanje je potrebno provoditi diskretno uz čim manje narušavanje rada jedinice ili cijele organizacije. Nije preporučljivo općenito istraživati sve zaposlenike nakon odavanja. Istraživanje svih zaposlenika u situacijama kada nema konkretnih podataka može imati štetan učinak na moral ostalih jer bi se stvarao dojam da se svi sumnjiče za neovlašteno odavanje, a učinkovitost takvih taktika istraživanja nije značajna. Radi toga bi bilo povoljnije za kulturu sigurnosti usmjeravati konkretne mjere samo na uži krug osoba (Bunn, Sagan, 2017:127).

U okviru prikrivenih mjera prema užem krugu osoba, preporučuje se koristiti klopke u obliku simuliranih spisa ili dokumenata, odnosno obilježavanja nekih postojećih spisa te tajnog nadzora i snimanja užeg kruga osoba. Klopka se može sastojati od iste vrste spisa ili snimke koju osumnjičena osobe inače može koristiti, a provodi se s ciljem nadziranja aktivnosti koje će provoditi s dokumentacijom. Klopku je moguće ostaviti na digitalnom sustavu u obliku simuliranih dokumenata ili snimki te se zatim promatra daljnji tijek i način rada osumnjičenika (Valli, 2005). Osnovne prednosti računalne klopke su u jednostavnijem praćenju i analiziranju podataka o načinu korištenja i daljnjem tijeku slanja (Spitzner, 2003). Prednost klopki je utvrđivanje daljnjeg tijeka počinjenja i otkrivanju više dokaza koji mogu omogućiti unapređenje zaštitnih sustava (Booth, 2014). Cilj je utvrditi na koji način počinitelj pristupa podacima. Simulirani dokumenti ili snimke izrađuju se na temelju stvarnih spisa kako bi oponašali sva obilježja a postoje i programska rješenja koja ih izrađuju, a također se može raditi o stvarnom spisu u kojem je izmijenjeno nekoliko ključnih podataka (engl. *decoy documents*; Bowen, 2009). Korištenje klopki u istraživanju odavanja podataka je stara metoda koja se tradicionalno pokazala vrlo uspješnom u otkrivanju počinitelja koji surađuju s vanjskim subjektima (Stoll, 1989).

Nakon što je prikupljeno dovoljno podataka da bi se istraživanje moglo nastaviti klasičnim dokaznim radnjama bez prikrivanja daljnjeg rada, provodi se pretraživanje ureda, dokumenata, opreme, računala, uređaja za komunikaciju i drugih dostupnih materijala. Kod istraživanja odavanja podataka, velik udio imaju materijalni dokazi poput podataka iz računalnih sustava (memorijska istraživanja) ili video nadzora, ali također vrlo korisni mogu biti personalni izvori poput osumnjičenikovih kolega ili suradnika koji bi mogli otkrivati i razne druge aktivnosti osumnjičenika. Potrebno je obavljati razgovore s kolegama s kojima je surađivao. Ne treba zanemarivati ulogu razgovora jer ponekad može biti korisniji od tehničkih metoda. Ponekad će tek osoba koja svakodnevno provodi istu vrstu poslova uočiti određenu anomaliju u radu koja je obuhvaćena video nadzorom. Pripremanje za počinjenje je najčešće moralo trajati duže vremena tijekom kojeg bi trebali nastati korisni dokazi koje su možda primijetili njegovi kolege. Kod izuzimanja računalnih podataka potrebno je primjenjivanje stručnih preporuka jer bi vještiji počinitelji mogli pripremiti skrivene sustave za brisanje podataka ili pokušati narušavati druge dijelove sustava organizacije, te je potrebno ograničiti osumnjičenikove lozinke, ključeve, identifikacijske kartice i drugo. Primopredaja podataka između počinitelja se najčešće ne provodi osobno niti uz nazočne svjedoke već će se dokazivati drugim oblicima ovisno o načinu predaje, i za to će često biti potrebno utvrđivanje internetskih adresa s kojih su podaci poslani ili primljeni, profile računa s kojih je provođena komunikacija i slično (mrežna istraživanja). Personalni izvori poput svjedoka s radnog mjesta mogu biti korisni za utvrđivanje postupaka počinitelja i načina funkcioniranja mjera zaštite. Ponekad će biti potrebno vještačenje prikupljenih digitalnih podataka.

Niti jedan rad o teoriji ili praksi zaštite podataka nije preporučio usmjeravanje na primatelje podataka kao učinkovite početne izvore u kriminalističkom istraživanju, osobito ako se radi o subjektima koji u skladu s zakonskim uređenjem ne moraju iskazivati o izvorima od kojih su dobili podatke (npr. novinari). Ako bi se istraživanje oslanjalo na takve subjekte kao osnovu prikupljanja podataka o internim pitanjima, to bi pokazivalo nedovoljnu razinu mjera koje su trebale biti preventivno implementirane u internom segmentu. Ako su unutarnje zaštitne mjere bile zadovoljavajuće provedene, trebalo bi biti prikupljeno dovoljno podataka za učinkovito istraživanje. Potrebno je pretraživati računalne uređaje i dokumente na radnom mjestu, te otkrivati druge lokacije na kojima je počinitelj mogao skrivati dokumentaciju, novac, uređaje i druge dokaze. Na uređajima koje je počinitelj koristio za počinjenje mogu biti pronađeni podaci i o drugim nepravilnostima. U uređajima za komunikacije traže se podaci o kontaktima, slanju ili primanju pojedinih dokumenata, kretanju na pojedinim lokacijama i slično. Iz uređaja kojima se provode mjere zaštite moguće je prikupljati podatke o učestalosti korištenja pojedine dokumentacije i sličnim okolnostima. Provode se i druge dokazne radnje ovisno o okolnostima događaja. Nakon utvrđivanja načina počinjenja, potrebno je provjeriti postoje li mogućnosti da su i neki drugi zaposlenici koristili sličan način.

5. ZAKLJUČAK

ESLJP u presudama traži minimalne standarde odgovarajućeg organiziranja i edukacije zaposlenika tijela vlasti s ciljem ispunjavanja dužnosti čuvanja podataka. ESLJP nije preporučio smjernice niti detaljnija pravila o tome na koji način bi bilo potrebno provoditi organiziranje zaštite i educiranje, ali u teoriji i praksi postoji niz preporuka o mjerama fizičke zaštite koje su primjenjive u predmetnom području. Najčešće se koriste mjere fizičke zaštite prostorija, dokumenata u digitalnom ili fizičkom obliku te zaštite od zaposlenika. Provedena analiza pokazuje da se navedene mjere mogu uspješno primjenjivati za ispunjavanje standarda ESLJP. Naši propisi sadržavaju uobičajena pravila o mjerama zaštite kakve se primjenjuju i u drugim sustavima. Podaci prikupljeni mjerama zaštite mogu biti dovoljni za sužavanje kruga počinitelja i za uspješno planiranje kriminalističkog istraživanja. Pojedine vrste preventivnih i istraživačkih mjera potrebno je povezivati i kombinirati te nije moguće ostvariti uspješnu zaštitu samo jednom vrstom.

Organiziranje procedura ima ulogu detaljnijeg registriranja svih ključnih interakcija zaposlenika s dokumentima ili prostorima. Nakon otkrivanja užeg kruga osoba, jednostavnije je provoditi prikrivene radnje s ciljem otkrivanja više detalja o načinu počinjenja, uključenim suradnicima i drugim okolnostima. Nije preporučljivo započeti otvoreno istraživanje ili neosnovano sumnjičiti sve zaposlenike jer to može dovoditi do smanjivanja motivacije. U teoriji i praksi zaštite podataka nisu izražavane preporuke da bi radnje istraživanja ili nadzora trebale započeti od vanjskih subjekata koji bi mogli primati podatke, nego je naglasak na internim segmentima funkcioniranja u kojima se može ostvariti dovoljno visoka razina učinkovitosti u pronalaženju bitnih dokaza.

Učestala odavanja podataka iz posebnih dokaznih radnji u našim medijima u posljednjih petnaestak godina ne pokazuju ujednačenost zaštite u svim uključenim tijelima vlasti koje primaju podatke prikupljene posebnim dokaznim radnjama. Takvo stanje je posljedica različitog uređenja pojedinih faza kaznenog postupka zbog čega mogu nastajati povrede konvencijskog prava. Policijske jedinice su tijekom provedbe posebnih dokaznih radnji dužne koristiti prikladne mjere zaštite na temelju propisa o tajnosti, ali je problem što nakon dovršetka posebnih dokaznih radnji i dostave podataka drugim tijelima te započinjanja drugih faza postupka, takve mjere više nisu propisane i po tome naš sustav nije usklađen s standardima koje ESLJP traži za cjelovitu zaštitu. Kao posljedica takvog pravnog uređenja, nastavak rada na podacima koje je prikupila policija nije obuhvaćen propisanim mjerama zaštite podataka, što može dovoditi do povreda konvencijskih standarda o dužnosti čuvanja podataka. Prema presudama ESLJP, dužnost čuvanja je na svim tijelima vlasti sve do faze u kojoj sud u skladu s zakonskim pravilima odlučuje o uvidu u spis ili snimke iz tajnog nadzora izvodi kao dokaze u kaznenom postupku.

U usporedbi s razinom zaštite kod drugih tijela vlasti (npr. obavještajne agencije) ili subjekata koji rade s osjetljivim materijalima i primjenjuju visoke standarde sigurnosti (npr. tiskare novčanica, nuklearna postrojenja, farmaceutska industrija itd.), kada bi se u njihovom poslovanju učestalo i u dugačkom vremenskom razdoblju događale ovakve pojave neovlaštenog iznošenja materijala, vjerojatno to ne bi bilo okarakterizirano kao profesionalno postupanje već bi trebalo dovoditi do brze promjene organiziranja rada, te bi i istražna vlasti zadužena za privatne podatke trebala unaprijediti mjere zaštite u svojem postupanju.

LITERATURA

1. Bender, K. (2006). *Moneymakers: The Secret World of Banknote Printing*. John Wiley.
2. Booth, R. (2014). *State Department Counterintelligence: Leaks, Spies, and Lies*. BrownBooks.
3. Bunn, M., Sagan, S. (2017). *Insider Threats*. Cornell University Press.
4. Camp, N., Williams, A. (2019). *Preliminary Results from a Comparative Analysis of Counterintelligence and Insider Threat Mitigation in Nuclear Facilities*. Sandia National Lab.
5. Cappelli, D. i dr. (2012). *The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes*. Boston: Addison-Wesley.
6. Contos, B. T. (2006). *Enemy at the Water Cooler: True stories of insider threats and enterprise security management countermeasures*. Elsevier.
7. Gaonjur, P., Bokhoree, C. (2006). Risk of insider threats in information technology outsourcing: can deceptive techniques be applied? *Journal of Security and Management*, 522–529.
8. Shabtai, A., Elovici, Y., Rokach, L. (2012). *A survey of data leakage detection and prevention solutions*. New York: Springer Science.
9. Spitzner, L. (2003). *Honeypots: catching the insider threat*. Proceedings, 19th Annual Computer Security Applications Conference, 170–179.
10. Stalling, W., Brown, L. (2007). *Computer Security: Principles and Practice*. Prentice Hall.
11. Stoll, C. (1989). *The Cuckoo's Egg*. Doubleday.
12. Vacca, J. R. (2017). *Computer and information security handbook*. Cambridge: Elsevier.
13. Valli, C. (2005). Honeypot technologies and their applicability as a strategic internal countermeasure. *International Journal of Information and Computer Security*, 1(4), 30–436.
14. Wettering, F. (2000) Counterintelligence: The Broken Triad, *International Journal of Intelligence and Counter Intelligence*, 13(3), 265-300

Propisi

1. Pravilnik o načinu provođenja posebnih dokaznih radnji, Nar. nov. 102/09
2. Pravilnik o tajnosti službenih podataka Ministarstva unutarnjih poslova, Nar. nov. 107/12
3. Uredba o mjerama informacijske sigurnosti, Nar. nov. 46/08
4. Zakon o informacijskoj sigurnosti, Nar. nov. 79/07
5. Zakon o tajnosti podataka, Nar. nov. 79/07, 86/12

Presude ESLJP

1. Craxi pr. Italije (br. 2), br. 25337/94, 17. srpnja 2003.
2. Apostu pr. Rumunjske, br. 22765/12, 3. veljače 2015.
3. Căşuneanu pr. Rumunjske, br. 22018/10, 16. travnja 2013.
4. Drakšas pr. Litve, br. 36662/04, 31. srpnja 2012.

ŽELJKO KARAS*

Measures for Implementing the Obligation to Safe Custody of Data Collected by Covert Evidentiary Actions According to ECtHR Decisions

Summary

In the paper, the author analyses the measures necessary to implement the obligation to safe custody of data, which the European Court of Human Rights (ECtHR) requires to prevent the release of transcripts and other data collected using covert evidentiary actions. According to ECtHR jurisprudence, states have a duty to securely store data and a duty to investigate officials in the event of data disclosure effectively. The aforementioned duties are positive obligations for the authorities, and appropriate physical protection measures are necessary for their implementation. In its decisions, the ECHR only listed recommendations for the appropriate organisation and the education of officials without specifying in detail how to implement the aforementioned standards.

In the paper, the author analyses the activities commonly recommended for protection against illegal activities of employees and considers their applicability for the protection of documentation on covert evidentiary actions. Most protection measures can be aimed at premises, devices and employees similarly as in other areas of protection with necessary adjustments. Protection measures are useful, which, in addition to the preventive effect, also register data that can enable more effective research after the data has been disclosed.

Keywords*: disclosure of information, transcripts, physical protection, ECtHR.*

* Željko Karas, University of Applied Sciences in Criminal Investigation and Public Security