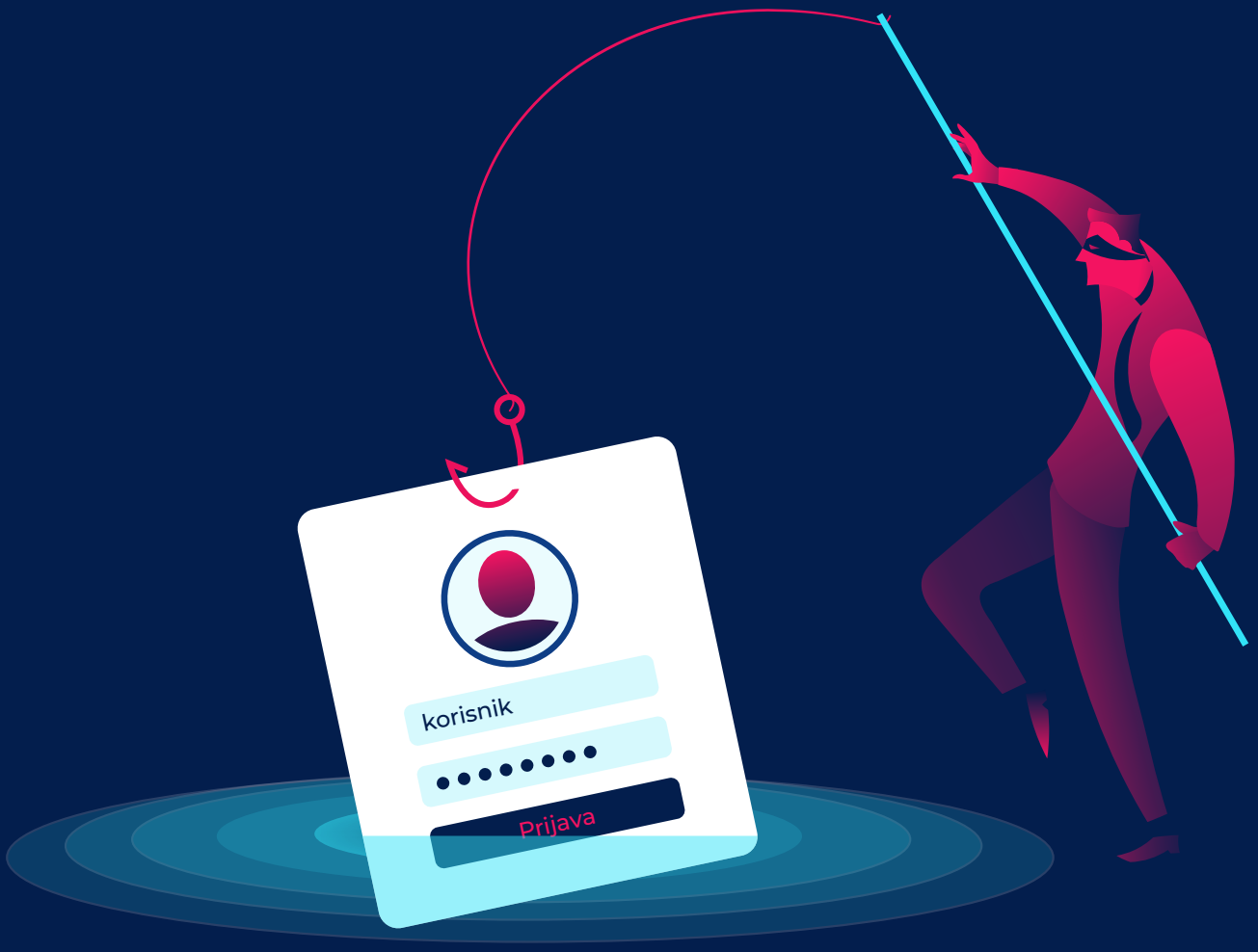
PARTNERI SRBIJA

Analiza stanja u oblasti borbe protiv visokotehnološkog kriminala i inspekcijskog nadzora u oblasti informacione bezbednosti

(uz pregled sudske i tužilačke prakse za period od 01.07.2022. do 30.06.2023. godine)



Norway

SMART Balkans
Civil Society for Shared Society in the Western Balkans

Autori:
dr Milana Pisarić
Mihailo Pavlović
Milan Stefanović
Milica Tošić

Recenzentkinja:
Ana Toskić Cvetinović

Izdavač:
Partneri Srbija

Prelom i dizajn:
Kliker dizajn

Beograd, decembar 2023. godine

Ova publikacija je izrađena uz podršku regionalnog projekta SMART Balkan – Civilno društvo za povezan Zapadni Balkan koji implementira Centar za promociju civilnog društva (CPCD), Center for Research and Policy Making (CRPM) i Institute for Democracy and Mediation (IDM), a finansijski podržava Ministarstvo spoljnih poslova Kraljevine Norveške. Sadržaj publikacije je isključiva odgovornost izdavača i ne odražava nužno stavove Centra za promociju civilnog društva, Center for Research and Policy Making (CRPM), Institute for Democracy and Mediation i Ministarsvta spoljnih poslova Kraljevine Norveške.

Sadržaj

Uvod **5**

Pravni okvir **7**

Dela visokotehnološkog kriminala **9**

Visokotehnološki kriminal u smislu Konvencije i Dodatnog protokola 9

Visokotehnološki kriminal u smislu ZVTK 10

Krivična dela protiv bezbednosti računarskih podataka 11

Krivična dela protiv polne slobode 13

Krivična dela protiv intelektualne svojine 14

Nadležni državni organi **16**

Ovlašćenja nadležnih organa **20**

Operativne mere i radnje 20

Dokazne radnje 22

Inspekcijski nadzor koji vrši Inspekcija za informacionu bezbednost **27**

Analiza prakse domaćih sudova i praksa Evropskog suda za ljudska prava **35**

Metodologija i dobijeni podaci 35

Krivično delo računarska prevara iz člana 301 Krivičnog zakonika 38

Krivično delo neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka iz člana 302 Krivičnog zakonika 38

Krivično delo neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199 Krivičnog zakonika iz člana 199 krivičnog zakonika 39

Krivično delo prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju iz člana 185 Krivičnog zakonika 39

Sporazumi o priznanju krivice.....39

Presude nakon glavne rasprave.....41

Zaključak analize domaće sudske prakse.....44

Praksa Evropskog suda za ljudska prava 47

Zaključak i preporuke..... 50

Uvod

S razvojem informacione tehnologije razvijaju se i načini njene zloupotrebe i pojavni oblici sajber kriminala, od kojih države nastoje da zaštite pojedince, privredu i društvo. *Ultima ratio* u zaštiti navedenih dobara je krivično pravo: odredbama materijalnog krivičnog prava određena ponašanja se inkriminišu, odnosno predviđaju kao krivična dela protiv poverljivosti, celovitosti i dostupnosti računarskih podataka, a odredbama krivičnog procesnog prava propisuju se ovlašćenja nadležnih organa radi otkrivanja izvora nedozvoljene radnje i prikupljanja podataka o krivičnom delu i učiniocu, a koji mogu biti upotrebljeni kao dokaz u krivičnom postupku.

S obzirom na transnacionalnu prirodu sajber kriminala, jednu od prepreka efikasnom odgovoru država predstavlja neadekvatnost materijalnih i procesnih pravila u nacionalnom krivičnom zakonodavstvu. Pored toga, neuniformnost nacionalnih propisa, između ostalog, otežava međunarodnu saradnju u krivičnim stvarima, koja je imperativ u suzbijanju ovog oblika kriminala. Solidnu osnovu za prevazilaženje ovih prepreka, odnosno za prilagođavanje krivičnog materijalnog i procesnog zakonodavstva specifičnostima sajber kriminala i sajber prostora, harmonizaciju nacionalnih propisa država i ostvarivanje delotvorne i pravovremene prekogranične saradnje predstavlja Konvencija o sajber kriminalu[1] (u daljem tekstu: Konvencija). Uz Konvenciju su usvojena dva protokola: Dodatni protokol koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih upotrebom računarskih sistema iz 2003.[2] (u daljem tekstu: Dodatni protokol) i Drugi dodatni protokol o pojačanoj saradnji i otkrivanju elektronskih dokaza 2022.[3] (u daljem tekstu: Drugi dodatni protokol). Iako usvojena u okviru Savetu Evrope, Konvencija je otvorena i za države ne-članice, i za sada je jedini međunarodni ugovor globalnog dometa, u čemu se ogleda njen naročiti značaj.

Put naše zemlje ka usklađenim propisima i efikasnim mehanizmima za prevenciju i borbu protiv visokotehnološkog kriminala je samo započet ratifikacijom ovih međunarodnih akata.

[1] *Council of Europe Convention on cybercrime (No. 185)*, http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. Usvojena je 2001, a stupila na snagu 2004. godine.

[2] *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)*, https://rm.coe.int/168008160f. Usvojen 2003, a stupio na snagu 2006. godine.

[3] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), https://rm.coe.int/1680a49dab. Usvojen 2022, još uvek nije stupio na snagu.

Cilj ove analize je da pruži sveobuhvatan pregled normativnog okvira Republike Srbije kada su u pitanju organizacija i nadležnost državnih organa za borbu protiv visokotehnološkog kriminala, krivična dela, ovlašćenja nadležnih institucija, kao i dokazne radnje, kako bi se istakle oblasti u kojima je moguće unaprediti popise. Analiza daje i pregled prakse i kapaciteta Posebnog tužilaštva za visokotenološki kriminal i Višeg suda u Beogradu, pri postupanju u predmetima za dela visokotehnološkog kriminala. Najzad, analiza daje i uvid u trenutno stanje kada je u pitanju informaciona bezbednost u Srbiji, a naročito nadzor koji vrši inspekcija za informacionu bezbednost.

Istraživanje koje je prethodilo izradi ove publikacije obuhvatilo je desk analizu – istraživanje zakonskih propisa, rada državnih organa i institucija značajnih za ovu oblast, istraživanje rešenja iz uporedne prakse, kao i drugih dostupnih informacija. Takođe, autori su podatke o praksi javnog tužulaštva i suda, kao i njihovim kapacitetima, prikupljali slanjem zahteva za slobodan pristup informacijama od javnog značaja ovim institucijama.

Pravni okvir

Pravni okvir za suzbijanje sajber kriminala u Srbiji čine potvrđeni međunarodni ugovori i zakoni.

Srbija je Konvenciju i Dodatni protokol potpisala 2005. i ratifikovala 2009. godine. Donošenjem Zakona o potvrđivanju Konvencije o visokotehnološkom kriminalu,[4] Srbija se obavezala da usvoji određene zakonodavne i druge mere – odnosno, da u krivičnom materijalnom zakonodavstvu predvidi kao krivična dela određena štetna ponašanja koje Konvencija prepoznaje kao sajber kriminal, da propiše ovlašćenja i procedure za krivično gonjenje i krivični postupak za dela obuhvaćena sajber kriminalom,[5] kao i da propiše ovlašćenja za prikupljanje elektronskih dokaza bez obzira na to o kom se krivičnom delu radi,[6] a sve uz poštovanje određenih uslova i ograničenja ljudskih prava. Ratifikacijom Dodatnog protokola,[7] Srbija se obavezala da u krivičnom materijalnom zakonodavstvu predvidi kao krivično delo određena

[4] Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu ("Sl. glasnik RS – Međunarodni ugovori", br. 19/2009).

[5] Konvencija od države potpisnice zahteva da *inkriminiše određena ponašanja*, koja su obuhvaćena pojmom sajber kriminala (poglavlje II, odeljak I). Radi se o sledećim grupama štetnih radnji koje treba propisati kao krivična dela:

1) dela protiv poverljivosti, celovitosti i dostupnosti računarskih podataka i sistema (Naslov 1), i to: neovlašćeni pristup računarskom sistemu (čl. 2), neovlašćeno presretanje računarskih podataka (čl. 3), neovlašćeno ometanje računarskih podataka (čl. 4), neovlašćeno ometanje računarskog sistema (čl. 5), zloupotreba uređaja (čl. 6);
2) dela u vezi sa računarima (Naslov 2), i to: računarsko falsifikovanje (čl. 7) i računarska prevara (čl.8);
3) dela u vezi sa sadržajem (Naslov 3) – radi se o delima u vezi sa dečjom pornografijom (čl. 9); i
4) dela u vezi sa kršenjem autorskih i srodnih prava (Naslov 4) (čl. 10).

[6] Konvencija sadrži zahtev državama potpisnicama da u nacionalnom propisu urede *mere i radnje za prikupljanje elektronskih dokaza*, kako o krivičnim delima koja se smatraju sajber kriminalom, tako i o svim drugim krivičnim delima: 1) hitno čuvanje pohranjenih računarskih podataka (čl. 16); 2) hitno čuvanje i delimično otkrivanje podataka o saobraćaju ostvarenih komunikacija (čl. 17); 3) izdavanje naloga za predaju računarskih podataka (čl.18); 4) pretresanje računara i računarske mreže i oduzimanje računarskih podataka (čl. 19); 5) prikupljanje podataka o saobraćaju u realnom vremenu (čl. 20), i 6) presretanje komunikacija (čl. 21) (poglavlje II, odeljak II).

[7] Zakon o potvrđivanju Dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema ("Sl. glasnik RS – Međunarodni ugovori", br. 19/2009).

štetna ponašanja.[8] Tokom 2022. Srbija je potpisala i ratifikovala i Drugi dodatni protokol,[9] čime se obavezala da u krivičnom procesnom zakonodavstvu propiše postupke radi unapređenja saradnje sa nadležnim organima država potpisnica i pružaocima usluga.

Relevantni zakoni uključuju Krivični zakonik (KZ),[10] koji predviđa krivična dela, Zakonik o krivičnom postupku (ZKP), [11] koji propisuje ovlašćenja nadležnih državnih organa za otkrivanje i dokazivanje krivičnih dela, i Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala (ZVTK)[12], koji uređuje pojedina organizaciona pitanja nadležnih državnih organa.

Srbija je delimično izvršila preuzete obaveze iz Konvencije – ono na šta se obavezala u pogledu krivičnog materijalnog prava gotovo u potpunosti je ispunjeno, jer su određena krivična dela propisana na manje-više zadovoljavajući način u KZ. U pogledu krivičnog procesnog prava, ZKP nije u potpunosti usaglašen sa zahtevima Konvencije. Što se tiče obaveza preuzetih ratifikovanjem protokola, može se reći da ih je Srbija ispunila na odgovarajući način u pogledu Dodatnog protokola, ali ne i pogledu Drugog dodatnog protokola. Iako Drugi dodatni Protokol još uvek nije stupio na snagu, trebalo bi pravovremeno razmotriti način ispunjavanja preuzetih obaveza, te raditi na izmeni i dopuni propisa koji uređuje krivičnu proceduru, tim pre što nije usaglašen ni sa tekstom Konvencije.

[8] Dodatni protokol od države potpisnice zahteva da *inkriminiše određena ponašanja*, i to : širenje rasističkog i ksenofobičnog materijala preko računarskih sistema (čl. 3) ; pretnja motivisana rasizmom i ksenofobijom (čl. 4) ; uvreda motivisana rasizmom i ksenofobijom (čl. 5) i poricanje, značajno umanjivanje, odobravanje ili opravdavanje genocida ili zločina protiv čovečnosti (čl. 6).

[9] Zakon o potvrđivanju Drugog dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu o pojačanoj saradnji i otkrivanju elektronskih dokaza (“Sl. glasnik RS – Međunarodni ugovori”, br. 7/2022).

[10] “Sl. glasnik RS“, br. 85/2005, 88/2005 - ispravka, 107/2005 - ispravka, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019.

[11] “Sl. glasnik RS”, br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - odluka US i 62/2021 - odluka US.

[12] “Sl. glasnik RS”, br. 61/2005, 104/2009, 10/2023 i 10/2023 – dr. zakon.

Dela visokotehnološkog kriminala

Potvrđujući Konvenciju, zakonodavac se umesto za transkribovanu reč „sajber", opredelio za izraz „visokotehnološki kriminal". Ni KZ ne sadrži izraz „sajber kriminal", iz razloga što su obe reči iz ove kovanice strane terminologiji krivičnog prava. Štaviše, KZ ne koristi ni izraz „visokotehnološki kriminal" , što važi i za ZKP. Osim u zakonu kojim se potvrđuje Konvencija, izraz „visokotehnološki kriminal" upotrebljen je u ZVTK, koji određuje pojam visokotehnološkog kriminala (VTK) i ustanovljava posebne organizacione jedinice nadležnih državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela obuhvaćena tim pojmom.

Visokotehnološki kriminal u smislu Konvencije i Dodatnog protokola

Gotovo sva štetna ponašanja, koja Konvencija određuje kao sajber kriminal i čije inkriminisanje zahteva (s izuzetkom neovlašćenog presretanja računarskih podataka iz čl. 3 Konvencije), predviđena su kao krivična dela u KZ, u nekoliko glava. [13] Sva štetna ponašanja, čije inkriminisanje zahteva Dodatni Protokol uz Konvenciju,

[13] Dela iz *prve dve grupe* iz Konvencije propisana su među krivičnim delima protiv bezbednosti računarskih podataka (glava dvadeset sedam KZ), na sledeći način: 1) neovlašćeni pristup računarskom sistemu iz čl. 2 Konvencije inkriminisan je u čl. 302 KZ (neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka); 2) neovlašćeno presretanje računarskih podataka iz čl. 3 Konvencije nije na adekvatan način inkriminisano u KZ (štetno ponašanje čije se inkriminisanje traži ne bi se moglo podvesti pod radnju krivičnog dela neovlašćenog prisluškivanja i snimanja iz čl. 143 KZ niti pod neko od krivičnih dela iz glave dvadeset sedam); 3) neovlašćeno ometanje računarskih podataka iz čl. 4 Konvencije predstavlja krivično delo u smislu čl. 298 KZ (oštećenje računarskih podataka i programa); 4) neovlašćeno ometanje računarskog sistema iz čl. 5 Konvencije pokriveno je delimično inkriminacijom iz čl. 298 (oštećenje računarskih podataka i programa) a delom inkriminacijom iz čl. 299 KZ (računarska sabotaža); 4) zloupotreba uređaja iz čl. 6 Konvencije predviđena je kao krivično delo u čl. 304a KZ (pravljenje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka); 6) računarsko falsifikovanje iz čl. 7 i računarska prevara iz čl. 8 Konvencije delimično odgovaraju inkriminaciji iz čl. 301 KZ (računarska prevara).

predviđena su kao krivična dela izmenama krivičnog zakonodavstva, tj. donošenjem ZID KZ 2009. godine.[14]

Drugim rečima, u smislu Konvencije i Dodatnog protokola, pod sajber kriminalom u Srbiji smatraju se, pored krivičnih dela protiv bezbednosti računarskih podataka (glava dvadeset sedam KZ), i krivično delo prikazivanja, pribavljanja i posedovanja pornografskog materijala i iskorišćavanja maloletnog lica za pornografiju (čl. 185 KZ), krivična dela protiv intelektualne svojine (glava dvadeseta KZ), krivično delo rasne i druge diskriminacije (čl. 387 st. 4, 5 i 6 KZ) i krivično delo povrede ugleda zbog rasne verske, nacionalne ili druge pripadnosti (čl. 174 KZ).

U odnosu na pomenuto, domaći zakonodavac je u ZVTK pojam visokotehnološkog kriminala odredio drugačije.

Visokotehnološki kriminal u smislu ZVTK

ZVTK određuje visokotehnološki kriminal kao vršenje krivičnih dela kod kojih se kao *objekat* ili *sredstvo* izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže, računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku (čl. 2 st. 1).

U narednom članu, potom, zakonodavac takstativno navodi grupe krivičnih dela radi čijeg otkrivanja, krivičnog gonjenja i suđenja se primenjuje ovaj zakon, odnosno bliže određuje krivična dela koja se imaju smatrati visokotehnološkim kriminalom (čl. 3): 1) krivična dela protiv bezbednosti računarskih podataka određena Krivičnim zakonikom; 2) krivična dela protiv intelektualne svojine, imovine, privrede i pravnog saobraćaja, *pod uslovom* da se a) računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku javljaju kao *objekat ili sredstvo izvršenja* krivičnih dela, i da b) broj primeraka

Dela u vezi s dečjom pornografijom u smislu Konvencije propisana su u okviru krivičnih dela protiv polne slobode (glava osamnaesta KZ) – radi se o krivičnom delu Prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju (čl. 185).

Dela u vezi s *kršenjem autorskih i srodnih prava* u smislu Konvencije propisana su u okviru krivičnih dela protiv intelektualne svojine (glava dvadeseta).

[14] Dela iz čl. 3, 4 i 5 Protokola inkriminisana su u okviru krivičnih dela protiv čovečnosti i drugih dobara zaštićenih međunarodnim pravom (glava trideset četvrta), i to kao radnje krivičnog dela rasna i druga diskriminacija u čl. 387 KZ: širenje rasističkog i ksenofobičnog materijala preko računarskih sistema - kao radnja krivičnog dela iz čl. 387 st. 4 KZ; pretnja motivisana rasizmom i ksenofobijom - kao radnja krivičnog dela iz čl. 387 st. 6; poricanje, značajno umanjivanje, odobravanje ili opravdavanje genocida ili zločina protiv čovečnosti - kao radnja krivičnog dela iz čl. 387 st. 5 KZ. Uvreda motivisana rasizmom i ksenofobijom iz čl. 5 Protokola predviđena je u čl. 174 KZ, među krivičnim delima protiv časti i ugleda (glava sedamnaesta), kao krivično delo povreda ugleda zbog rasne verske, nacionalne ili druge pripadnosti.

autorskih dela prelazi 2000, odnosno nastala materijalna šteta prelazi iznos od 1.000.000 dinara; 3) krivična dela protiv sloboda i prava čoveka i građanina, polne slobode, javnog reda i mira i ustavnog uređenja i bezbednosti Republike Srbije, pod uslovom da se zbog *načina izvršenja ili upotrebljenih sredstava* mogu smatrati krivičnim delima visokotehnološkog kriminala, u skladu sa čl. 2 st. 1. ovog zakona.

Postupajući na taj način, zakonodavac je pojam VTK daleko šire odredio u odnosu na Konvenciju, što nije loše rešenje. S druge strane, uočava se da krivična dela protiv intelektualne svojine samo uslovno smatraju VTK, a da to čak ni uslovno ne važi u pogledu krivičnih dela koja su uneta u KZ nakon ratifikovanja Dodatnog protokola. Time su ova krivična dela ostala van nadležnosti posebnih organizacionih jedinica nadležnih organa.[15]

U nastavku ćemo se fokusirati na krivična dela predviđena Krivičnim zakonikom koja i Konvencija prepoznaje kao dela visokotehnološkog kriminala.

Krivična dela protiv bezbednosti računarskih podataka

Potrebu za krivičnopravnom zaštitom računarskih sistema i mreža zakonodavac je prepoznao i pre potpisivanja (2005) i ratifikovanja (2009) Konvencije. Naime, izmenama i dopunama iz 2003. u tada važeći Krivični zakon Srbije uneto je sedam krivičnih dela protiv bezbednosti računarskih podataka, prihvatanjem rešenja iz Nacrta KZ SR Jugoslavije iz 2000. godine. Krivični zakonik iz 2005. propisao je sedam krivičnih dela u glavi dvadeset sedam, s neznatno izmenjenenim inkriminacijama u odnosu na 2003. godinu. Nakon ratifikovanja Konvencije (2009) precizirana je radnja krivičnog dela iz čl. 302, uneto je još jedno krivično delo (čl. 304a) u pogledu kog je izvršena sitnija intervencija 2016, tako da trenutno važeći KZ sadrži osam krivičnih dela protiv bezbednosti računarskih podataka.

U ovu glavu krivičnih dela spadaju oštećenje računarskih podataka i programa (član 298), računarska sabotaža (član 299), pravljenje i unošenje računarskih virusa (član 300), računarska prevara (član 301), neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektonskoj obradi podataka (član 302), sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 303), neovlašćeno korišćenje računara i računarske mreže (član 304) i pribavljanje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka (član 304a). Specifičnost ove grupe dela leži u tome što izvršenje svakog od njih

[15] Krivično delo povrede ugleda zbog rasne, verske, nacionalne ili druge pripadnosti iz čl. 174 KZ i pojavni oblici krivičnog dela rasne i druge diskriminacije iz čl. 387 KZ (st. 4, 5 i 6) ne smatraju se VTK iz razloga što krivična dela protiv časti i ugleda (glava sedamnaesta), odnosno protiv čovečnosti i drugih dobara zaštićenih međunarodnim pravom (glava trideset četvrta), u okviru kojih su sadržana navedena krivična dela, nisu nabrojana u čl. 3 ovog zakona.

podrazumeva korišćenje računara i računarskih sistema kao sredstva ili cilja izvršenja krivičnog dela. Zakon propisuje da će se oduzeti uređaji i sredstva koji su korišćeni ili proizvedeni u okviru izvršenja krivičnog dela. Sva dela iz ove glave gone se po službenoj dužnosti, osim dela iz člana 304, koje se goni po privatnoj tužbi. Za izvršenje ovih krivičnih dela propisana je kazna zatvora ili novčana kazna, sa rasponom u zavisnosti od (oblika) dela koje je izvršeno.

Oštećenje računarskih podataka i programa ima osnovni i dva teža oblika. Osnovni oblik čini onaj ko neovlašćeno izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program. Izvršenje ovih prestacija postavljeno je alternativno, a označenje da se delo može izvršiti „i na drugi način“ upućuje na to da se delo može izvršti na bilo koji način koji je podoban da se računarski podatak ili program učnine neupotrebljivim. Smatra se da je računarski podatak, odnosno program, neupotrebljiv onda kada se više ne može koristiti shodno svojoj nameni. Teži oblici postoje ako je izvršenjem dela iz člana 1 prouzrokovana šteta koja prelazi iznos od 450.000,00 dinara (stav 2), odnosno iznos od 1.500.000,00 dinara (stav 3).

Računarska sabotaža ima dva osnovna oblika. Prvi oblik čini onaj ko unese, uništi, izbriše, izmeni, ošteti, prikrije ili na drugi način učini neupotrebljivim računarski podatak ili program, a drugi oblik čini onaj ko uništi ili ošteti računar ili drugi uređaj za elektronsku obradu i prenos podataka sa namerom da onemogući ili znatno omete postupak elektronske obrade i prenosa podataka koji su od značaja za državne organe, javne službe, ustanove, preduzeća ili druge subjekte.

Pravljenje i unošenje računarskih virusa ima osnovni i teži oblik. Osnovni oblik iz stava 1 čini onaj ko napravi računarski virus u nameri njegovog unošenja u tuđi računar i računarsku mrežu. Teži oblik iz stava 2 čini onaj ko unese računarski virus u tuđ računar ili računarski mrežu i time prouzrokuje štetu. Zakon propisuje da je računarski virus računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka.[16] Ovo krivično delo je zanimljivo posmatrati u kontekstu pribavljanja Sky i EnchroChat komunikacije od strane nadežnih državnih institucija, imajući u vidu da su dosadašnja globalna istraživanja pokazala da se pribavljanje ovih komunikacija vrši ubacivanjem virusa u sisteme. [17]

Računarska prevara predstavlja poseban oblik krivičnog dela prevare, propisanog članom 301 KZ. Računarska prevara ima jedan osnovni, dva teža i jedan lakši oblik. Ovo delo čini onaj ko unese netačan podatak, propusti unošenje tačnog podatka ili

[16] Član 112, stav 20 KZ

[17] Više o ovome videti u radu dr Vanje Bajović „EncroChat i Sky ECC komunikacija kao dokaz u krivičnom postupku“

na drugi način prikrije ili lažno prikaže podatak i time utiče na rezultat elektronske obrade i prenosa podataka u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist i time drugom prouzrokuje imovinsku štetu. Teži oblici postoje onda kada je izvršenjem dela iz stava 1 pribavljena imovinska korist koja prelazi iznos od 450.000,00 dinara (stav 2) odnosno iznos od 1.500.000,00 dinara (stav 3). Lakši oblik iz stava 4 čini onaj ko delo učini samo u nameri da drugog odšeteti, a ne i da time pribavi protivpravnu imovinsku korist.

Neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektonskoj obradi podataka ima osnovni i dva teža oblika. Osnovni oblik čini onaj ko se, kršeći mere zaštite, neovlašćeno uključi u računar ili računarsku mrežu, ili neovlašćeno pristupi elektronskoj obradi podataka. Teži oblik čini onaj ko snimi ili upotrebi podatak dobijen činjenjem ovog dela (stav 2), kao i ako je usled činjenja ovog dela došlo do zastoja ili ozbiljnog poremećaja funkcionisanja elektronske obrade i prenosa podataka ili mreže, ili su nastupile druge teške posledice (stav 3).

Sprečavanje i ograničavanje pristupa javnoj računarskoj mreži čini onaj ko neovlašćeno sprečava ili ometa pristup javnoj računarskoj mreži. Teži oblik ovog dela postoji kada službeno lice u vršenju službe sprečava ili ometa pristup javnoj računarskoj mreži, a da za to nema ovlašćenje.

Neovlašćeno korišćenje računara ili računarske mreže čini onaj ko neovlašćeno koristi računarske usluge ili računarsku mrežu u nameri da sebi ili drugom pribavi protivpravnu imovinsku korist. Ovo je jedino delo iz ove glave koje se goni po privatnoj tužbi, a ne po službenoj dužnosti Posebnog tužilaštva za visokotehnološki kriminal.

Pribavljanje, nabavljanje i davanje drugom sredstava za izvršenje krivičnih dela protiv bezbednosti računarskih podataka ima osnovni i lakši oblik. Osnovni oblik iz stava 1 čini onaj ko proizvodi, prodaje, nabavlja radi upotrebe, uvozi, distribuira ili na drugi način stavlja na raspolaganje sredstva za izvršenje nekog od krivičnih dela protiv bezbednosti računarskih podataka koje se goni po sužbenoj dužnosti. Lakši oblik iz stava dva čini onaj ko poseduje neko od ovih sredstava u nameri da ih iskoristi za izvrešnje nekog od krivičnih dela protiv bezbednosti računarskih podataka.

Krivična dela protiv polne slobode

Nakon ratifikovanja Konvencije, naš Krivični zakonik je 2009. godine pretrpeo određene promene, kojima je između ostalog izmenjen naziv i opis dela prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju (član 185) i dodato delo iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnih dela protiv polne slobode prema maloletnom licu (član 185b) u grupu dela protiv polne slobode.

Delo iz člana 185 ima dva osnovna oblika – kada se maloletniku čini dostupnim pornografski sadržaj (stav 1) i kada se maloletnik iskorišćava za proizvodnju predmeta ili predstavu pornografske sadržine (stav 2). Stav 3 propisuje kvalifikovani oblik, koji postoji onda kada su prethodna dva oblika izvršena prema detetu.[18] Ovo delo ima i dva posebna oblika – pribavljanje, posedovanje, prodaja, prikazivanje, javno izlaganje ili činjenje dostupnim pornografske sadržine nastale iskorišćavanjem maloletnog lica (stav 4) i svesno pristupanje pornografskom sadržaju putem sredstava informacionih tehnologija, nastalom iskorišćavanjem maloletnog lica (stav 5). Za izvršenje ovog krivičnog dela propisana je kazna zatvora i/ili novčana kazna, sa rasponom u zavisnosti od oblika dela. Ovo delo se smatra krivičnim delom visokotehnološkog kriminala samo kada se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci.[19]

Delo iz člana 185b čini lice koje u nameri izvršenja taksativno nabrojanih krivičnih dela protiv polne slobode[20], koristeći računarsku mrežu ili komunikaciju drugim tehničkim sredstvima dogovori sa maloletnikom sastanak i pojavi se na dogovorenom mestu radi sastanka (stav 1). Izvršenje ovog dela je uslovljeno kumulativnim postojanjem ove dve radnje (dogovaranje i pojavljivanje na dogovorenom mestu). Stav 2. predviđa kvalifikovani oblik, kada se delo iz stava 1 izvrši prema detetu.

Svi oblici ova dva krivična dela mogu se izvršiti samo sa umišljajem. Umišljaj mora da obuhvata i okolnost da se radi o maloletniku, odnosno detetu. Oba dela se gone po službenoj dužnosti.

Krivična dela protiv intelektualne svojine

Krivični zakonik predviđa niz krivičnih dela protiv intelektualne svojine, kojima se zaštita daje autorskom pravu, srodnim pravima (pravo interperatora, pravo proizvođača fonograma, pravo proizvođača videograma, pravo proizvođača emisija, pravo proizvođača baze podataka i pravo proizvođača slobodnog dela) i pravima industrijske svojine (patentno pravo, pravo žiga, pravo na dizajn, pravo geografskih oznaka porekla i pravo zaštite topografija integrisanih kola).

U ovu grupu krivičnih dela spadaju povreda moralnih prava autora i interpretatora (član 198), neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava (član 199), neovlašćeno uklanjanje ili menjanje elektronske informacije o autorskom

[18] Član 112 KZ propisuje da se detetom smatra lice koje nije navršilo četrnaest godina, maloletnikom lice koje je navršilo četrnaest godina, a nije navršilo osamnaest godina, a maloletnim licem ono lice koje nije navršilo osamnaest godina.

[19] Član 3, stav 1, tačka 3 Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala

[20] čl. 178. stav 4, 179. stav 3, 180. st. 1. i 2, 181. st. 2. i 3, 182. stav 1, 183. stav 2, 184. stav 3, 185. stav 2. i 185a

i srodnim pravima (član 200), povreda pronalazačkog prava (član 201) i neovlašćeno korišćenje tuđeg dizajna (član 202).

Za ovu glavu krivičnih dela vrlo je značajno donošenje Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, koji se, pod određenim uslovima primenjuje i prilikom otkrivanja, krivičnog gonjenja i suđenja za krivična dela protiv intelektualne svojine u slučajevima kada se kao objekt radnje ili kao sredstvo izvršenja javljaju računari, računarske mreže, računarski podaci i njihovi proizvodi u materijalnom ili elektronskom obliku[21]. Tek kada se ovi uslovi ispune, naborojana dela se smatraju krivičnim delima visokotehnološkog kriminala i za postupanje su nadležni Posebno javno tužilaštvo i Odeljenje Višeg suda za borbu protiv visokotehnološkog kriminala.

[21] Član 3, stav 1, tačka 2

Nadležni državni organi

U Srbiji je prisutna svojevrsna specijalizacija državnih organa nadležnih za postupanje u predmetima za krivična dela obuhvaćenim pojmom sajber kriminala (pri tome treba istaći da Konvencija ne sadrži obavezu formiranja specijalizovanih nadležnih organa).

Kao što je već pomenuto, 2005. usvojen je Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, kojim se uređuje obrazovanje, organizacija, nadležnost i ovlašćenja posebnih organizacionih jedinica državnih organa radi otkrivanja, krivičnog gonjenja i suđenja za krivična dela koja su određena kao visokotehnološki kriminal. Zakon je izmenjen i dopunjen u dva navrata: 2009.[22] i 2023.[23] godine.

Pored toga što određuje pojam visokotehnološkog kriminala (čl. 2 st. 1) i krivična dela na koje se ovaj zakon primenjuje (čl. 3), ZVTK propisuje postupanje posebnih organizacionih jedinica državnih organa za celu teritoriju Republike Srbije. Na taj način zakonodavac je odstupio od opštih pravila za određivanje stvarne i mesne nadležnosti suda i javnog tužilaštva, pa je bez obzira na to što bi spram zaprećene kazne za pojedina krivična dela moglo biti nadležno osnovno javno tužilaštvo i osnovni sud, i bez obzira na mesto izvršenja krivičnog dela, uspostavljena isključiva nadležnost posebnih organizacionih jedinica.

Za postupanje u predmetima krivičnih dela iz čl. 3 ZVTK nadležno je *Više javno tužilaštvo u Beogradu* (čl. 4 st.1), u kom je obrazovano Posebno odeljenje za borbu protiv VTK, a koje Zakon potom naziva Posebnim javnim tužilaštvom (čl. 4 st. 2). Propisano je da se na njega primenjuju odredbe zakona kojim se uređuje javno

[22] Zakon o izmenama i dopunama Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala ("Sl. glasnik RS", br. 104/ 2009) sadrži neznatne izmene i dopune u pogledu značenja pojedinih izraza u čl. 2 i izmene radi usklađivanja sa Zakonom o uređenju sudova i Zakonom o javnom tužilaštvu iz 2008. godine.

[23] Zakon o izmenama Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala ("Sl. glasnik RS", br. 10/2023) usvojen je radi usklađivanja sa Zakonom o javnom tužilaštvu ("Sl. glasnik RS", br. 10/2023). Na osnovu čl. 8 , ovaj zakon stupa na snagu danom objavljivanja u „Službenom glasniku Republike Srbije", a primenjuje se od dana konstituisanja Visokog saveta sudstva, odnosno Visokog saveta tužilaštva (konstituisani maja 2023).

tužilaštvo, ako ovim zakonom nije drukčije određeno. U smislu Zakona o javnom tužilaštvu (ZJT),[24] javna tužilaštva posebne nadležnosti su Javno tužilaštvo za organizovani kriminal i Javno tužilaštvo za ratne zločine, a drugim zakonom se može osnovati i drugo javno tužilaštvo posebne nadležnosti (čl. 13 st. 2 ZJT). Međutim, iako se tako naziva, Posebno javno tužilaštvo za VTK nije javno tužilaštvo posebne nadležnosti u smislu ZJT, nego je obrazovano na osnovu čl. 13. st. 9 ZJT, u kom stoji da javno tužilaštvo (u ovom slučaju Više javno tužilaštvo u Beogradu) može imati posebno odeljenje koja se obrazuju za gonjenje određenog krivičnog dela, u skladu sa zakonom.[25] Ovo je važno istaći u vezi sa ovlašćenjima za sprovođenje posebnih dokaznih radnji, kako će biti prikazano.

Radom Posebnog javnog tužilaštva rukovodi posebni javni tužilac za VTK, koga zakon naziva *Posebnim javnim tužilocem, a postavlja* Vrhovni javni tužilac,[26] na period od šest godina, bez mogućnosti ponovnog postavljanja,[27] iz reda javnih tužilaca višeg javnog tužilaštva, apelacionog javnog tužilaštva, javnog tužilaštva posebne nadležnosti ili Vrhovnog javnog tužilaštva. Propisano je da prednost prilikom postavljenja imaju javni tužioci koji poseduju posebna znanja iz oblasti informatičkih tehnologija (čl. 5 ZVTK) – dakle, posedovanje posebnih znanja nije propisano kao obavezan kriterijum.

Pored toga, ZVTK više ne uređuje mogućnost upućivanja javnih tužilaca u ovo odeljenje: izmenama iz 2023. prestao je da važi član 8 ZVTK, po kom je tako nešto bilo moguće,[28] ali je propisano da rešenje o upućivanju zamenika javnog tužioca u Posebno odeljenje doneto pre dana konstituisanja Visokog saveta tužilaštva (maj 2023) važi do isteka vremena upućivanja. Zakon nije posebno uredio šta se dešava

[24] Zakon o javnom tužilaštvu („Sl. glasnik RS“, br. 10/23).

[25] Kao što su formirana posebna odeljenja pojednih viših javnih tužilaštava za suzbijanje korupcije.

[26] Uporedi: Radom Javnog tužilaštva za ratne zločine rukovodi Glavni javni tužilac Javnog tužilaštva za ratne zločine (Glavni javni tužilac), koji se ne postavlja, nego ga bira Visoki savet tužilaštva, na šest godina (čl. 4 st. 2 Zakona o organizaciji i nadležnosti državnih organa u postupku za ratne zločine: 67/2003-4, 135/2004-71, 61/2005-7, 101/2007-10, 104/2009-4, 101/2011-272 (dr. zakon), 6/2015-7, 10/2023-4). Isto tako, radom Javnog tužilaštva za organizovani kriminal rukovodi Glavni javni tužilac za organizovani kriminal (Glavni javni tužilac), koji se ne postavlja, nego ga bira Visoki savet tužilaštva, na šest godina (čl. 5 st. 2 Zakona o organizaciji i nadležnosti državnih organa u suzbijanju organizovanog kriminala, terorizma i korupcije: 94/2016-14, 87/2018-24 (dr. zakon), 10/2023-51).

[27] Do izmena iz 2023. posebnog tužioca postavljao je Republički javni tužilac na period od četiri godine, uz mogućnost ponovnog postavljanja. Rešenje o postavljenju posebnog tužioca za visokotehnološki kriminal doneto pre dana konstituisanja Visokog saveta tužilaštva (maja 2023) važi do isteka vremena postavljenja. Vid. čl. 7 st. 1 Zakona o izmenama Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Sl. glasnik RS”, broj 10/2023-3).

[28] Vid. čl. 7 st. 2 Zakona o izmenama Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Sl. glasnik RS”, broj 10/2023-3).

po isteku tog vremena, pa se primenjuje opšti režim iz ZJT, odnosno odredbe o trajnom premeštaju (čl. 68), odnosno o privremenom upućivanju (čl. 69).

Posebni javni tužilac ima prava i dužnosti kao glavni javni tužilac (čl. 6 st. 1 ZVTK)-dakle, onako kako to propisuje ZJT i ZKP. Ipak, ne samo da ga Vrhovni javni tužilac postavlja, nego je predviđeno i da, ako dođe do saznanja da se u krivičnom predmetu radi o slučajevima VTK, Posebni javni tužilac treba da mu se u pismenoj formi obrati, zahtevajući od njega da mu poveri ili prenese nadležnost (čl. 6 st. 1 ZVTK).[29]

Radi obavljanja poslova organa unutrašnjih poslova u vezi sa delima iz čl. 3 ZVTK obrazovana je u okviru Ministarstva unutrašnih poslova Služba za borbu protiv visokotehnološkog kriminala (Služba). Izričito je propisano da Služba postupa po zahtevima Posebnog javnog tužioca, u skladu sa zakonom – odnosno kako to, pre svega, uređuje ZKP i Zakon o policiji. Starešinu Službe, po pribavljenom mišljenju Posebnog javnog tužioca, postavlja i razrešava Ministar nadležan za unutrašnje poslove. Ministar, takođe, bliže uređuje rad Službe.

Što se tiče suda, ZVTK određuje da je za postupanje u predmetima krivičnih dela iz čl. 3, bez obzira na zaprećenu kaznu i mesto izvršenja, za teritoriju Republike Srbije, nadležan *Viši sud u Beograd*u (čl. 10 st. 1), u kom je obrazovano Odeljenje za borbu protiv VTK (Odeljenje) (čl. 11).

Za razliku od zakonskog rešenja pre izmena iz 2023, po kom je predsednik Višeg suda u Beogradu mogao rasporediti u to odeljenje i sudije drugih sudova upućenih na rad u taj sud, prema važećem Zakonu u ovo Odeljenje mogu biti raspoređene samo sudije Višeg suda u Beogradu (čl. 11 st. 2).[30] Više nije propisano koliko dugo može da traje takvo raspoređivanje.[31] Prilikom raspoređivanja, propisano je da prednost

[29] Slična odredba ne postoji u pogledu Glavnog javog tužiloca za ratne zločine niti Glavnog javnog tužioca za organizovani kriminal. Štaviše, ni u pogledu rukovodilaca posebnih odeljenja viših javnih tužilaštava za suzbijanje korupcije.

[30] Rešenje o raspoređivanju sudije u Odeljenje za borbu protiv visokotehnološkog kriminala Višeg suda u Beogradu doneto pre konstituisanja Visokog saveta sudstva (maj 2023) važi do isteka vremena raspoređivanja, odnosno upućivanja na rad u taj sud. Vid. čl. 7 st. 3 Zakona o izmenama Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Sl. glasnik RS", broj 10/2023-3). Prema zakonskom rešenju pre izmena iz 2023, raspoređivanje je moglo trajati najduže dve godine, a moglo je biti produženo odlukom Predsednika Višeg suda, uz pisanu saglasnot sudije (čl. 11 st. 3 ranije važećeg ZVTK).

[31] Rešenje o raspoređivanju sudije u Odeljenje za borbu protiv visokotehnološkog kriminala Višeg suda u Beogradu doneto pre konstituisanja Visokog saveta sudstva (maj 2023) važi do isteka vremena raspoređivanja, odnosno upućivanja na rad u taj sud. Vid. čl. 7 st. 3 Zakona o izmenama Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala („Sl. glasnik RS", broj 10/2023-3). Prema zakonskom rešenju pre izmena iz 2023, raspoređivanje je moglo trajati najduže dve godine, a moglo je biti produženo odlukom Predsednika Višeg suda, uz pisanu saglasnot sudije (čl. 11 st. 3 ranije važećeg ZVTK).

imaju sudije koje poseduju posebna znanja iz oblasti informatičkih tehnologija – dakle, posebna znanja predviđena su kao neobavezan kriterijum čije ispunjenje daje prioritet u odabiru. Pored ovakvog raspoređivanja, Visoki savet sudstva može, u skladu sa Zakonom o sudijama, da privremeno uputi sudiju iz drugog suda na rad u Odeljenje[32] (pri čemu sudija koji se privremeno upućuje mora ispunjavati uslove za izbor sudije višeg suda – nije predviđeno da se prilikom upućivanja kao prednost uzima posedovanje posebnih znanja iz oblasti informatičkih tehnologija).

Za postupanje po žalbi nadležan je Apelacioni sud u Beogradu (čl. 10 st. 2 ZVTK) – nije propisano da se u okviru njega obrazuje nekakvo posebno odeljenje.

[32] U čl. 20 st. 2 Zakona o sudijama propisano je da se sudija može privremeno uputiti najduže na godinu dana, bez mogućnosti ponovnog privremenog upućivanja u isti sud.

Ovlašćenja nadležnih organa

Ovlašćenja nadležnih organa za otkrivanje i dokazivanje VTK uređena su u ZKP. Ovaj propis ne poznaje izraze elektronski i digitalni dokaz, ali prepoznaje računarski podatak kao dokaz. Naime, u članu 2. kojim se određuje značenje pojedinih izraza, svaki predmet ili *računarski podatak* koji je podoban ili određen da služi kao dokaz činjenice koja se utvrđuje u postupku smatra se *ispravom* (tačka 26). Drugim rečima, ZKP tretira elektronske dokaze kao isprave. Drugo je pitanje kako se isprave prikupljaju i kako se njima vrši dokazivanje.

Pored operativnih mera i radnji, koje se preduzimaju radi otkrivanja i obezbeđivanja tragova i predmeta za potrebe krivičnog postupka za dela koja se gone po službenoj dužnosti – pa *i* za dela VTK - ZKP razlikuje dve vrste dokaznih radnji koje su relevantne za elektronske dokaze: *opšte dokazne radnje*: primenjive bez obzira na vrstu krivičnog dela; i *posebne dokazne radnje*: namenjene za otkrivanje i dokazivanje određenih, posebnih krivičnih dela, koja se u konkretnom slučaju teško ili otežano otkrivaju i dokazuju preduzimanjem opštih dokaznih radnji - *među njima su samo pojedina dela VTK*.

Operativne mere i radnje

U čl. 286 st. 1, čiji rubrum glasi „Ovlašćenja policije“, ZKP propisuje dužnost policije da, ukoliko postoje *osnovi sumnje* da je izvršeno *krivično delo* za koje se goni *po službenoj dužnosti*, preduzme potrebne mere da se pronađe učinilac krivičnog dela, da se učinilac ili saučesnik ne sakrije ili ne pobegne, da se otkriju i obezbede tragovi krivičnog dela i predmeti koji mogu poslužiti kao dokaz, kao i da se prikupe sva obaveštenja koja bi mogla biti od koristi za uspešno vođenje krivičnog postupka. Koje su to mere i radnje ZKP bliže određuje u sledećem stavu istog člana, primerično ih navodeći, a potom koristi i izraz „druge potrebne mere i radnje“. O činjenicama i okolnostima koje su utvrđene prilikom preduzimanja pojedinih radnji iz čl. 286 ZKP, a mogu biti od interesa za krivični postupak, kao i o *predmetima* koji su pronađeni ili oduzeti, sastavlja se se zapisnik ili službena beleška. Dakle, ukoliko prilikom primene ovih ovlašćenja policija pronađe određene *predmete* – npr. uređaje koji su potencijalni nosioci elektronskih dokaza - može ih oduzeti (u skladu sa čl. 147 ZKP). Međutim, njihova sadržina ne bi mogla da se sazna preduzimanjem operativnih mera i radnji, nego bi se to moglo činiti samo kroz sprovođenje dokaznih radnji.

Dalje, u st. 3 istog člana propisano je da je policija ovlašćena da, po *nalogu* sudije za prethodni postupak, a na predlog javnog tužioca, pribavi evidenciju (već) ostvarene telefonske komunikacije i korišćenih baznih, kao i da izvrši lociranje mesta "sa kojeg se obavlja komunikacija" (u realnom vremenu). Ovde se zapravo radi o podacima koje je, u smislu Zakona o elektronskim komunikacijama (ZEK),[33] operator dužan da zadrži[34] i čuva 12 meseci od dana obavljene komunikacije.[35]

U smislu ovog zakona, ostvarivanje pristupa zadržanim podacima bez pristanka korisnika je nedopušteno, osim „na određeno vreme i na osnovu odluke suda" ukoliko je to neophodno „radi vođenja krivičnog postupka ili zaštite bezbednosti Republike Srbije, na način predviđen zakonom" (čl. 128 st. 2 ZEK). Pristup zadržanim podacima nadležni državni organ ostvaruju *sa ili bez ostvarivanja pristupa* prostorijama, elektronskoj komunikacionoj mreži, pripadajućim sredstvima ili elektronskoj komunikacionoj opremi operatora, ili tako što im operatori *dostavljaju tražene podatke*. Za potrebe krivičnog postupka pristup zadržanim podacima bio bi, dakle, dozvoljen samo „na određeno vreme i na osnovu odluke suda", dok bi način trebalo da propiše ZKP, što ovaj propis ne čini na dovoljno precizan i ispravan način.

Formulacija „na određeno vreme" odgovara formulaciji iz čl. 41 st. 2 Ustava u kom se načelno propisuje odstupanje od tajnosti pisama i drugih sredstava opštenja, što znači da bi odluka kojom se dozvoljava pristup zadržanim podacima trebalo da sadrži i određeno vremensko ograničenje. Dalje, pravni osnov za pristupanje

[33] Iako je 2023. usvojen novi Zakon o elektronskim komunikacijama („Sl. glasnik RS", br. 35/23), stupanjem koga na snagu je prestao da važi Zakon o elektronskim komunikacijama ("Sl. glasnik RS", br. 44/10, 60/13 - US, 62/14 i 95/18 - dr. zakon), u čl. 180 st. 1 je propisano da i dalje važe pojedine odredbe prethodnog zakona – među njima su i odredbe o zadržavanju podataka. Odredbe koje se citiraju u ovom tekstu su iz XVII poglavlja (Tajnost elektronskih komunikacija, zakonito presretanje i zadržavanje podataka) Zakona o elektronskim komunikacijama ("Sl. glasnik RS", br. 44/10, 60/13 - US, 62/14, 95/18 - dr. zakon i 35/23 - dr. zakon) koje se još uvek primenjuju.

[34] Sto se tiče *oblika i kvaliteta* zadržanih podataka propisano je da je operator je dužan da zadrži podatke u izvornom obliku ili kao podatke obrađene tokom obavljanja delatnosti elektronskih komunikacija koji moraju biti istog kvaliteta i nivoa zaštite, kao i podaci u izvornom obliku (čl. 128 st. 4 ZEK). U pogledu načina zadržavanja podataka, operator je obavezan da ih zadržava tako da im se *bez odlaganja može pristupiti*, odnosno da se *bez odlaganja mogu dostaviti* na osnovu odluke suda (čl. 128 st. 7 ZEK). Dodatno, u čl. 130 propisani su zahtevi koje je operator dužan da ispuni u pogledu kvaliteta zadržanih podataka.

[35] Radi se o podacima koji su potrebni za: 1) praćenje i utvrđivanje izvora komunikacije; 2) utvrđivanje odredišta komunikacije; 3) utvrđivanje početka, trajanja i završetka komunikacije; 4) utvrđivanje vrste komunikacije; 5) identifikaciju terminalne opreme korisnika; 6) utvrđivanje lokacije mobilne terminalne opreme korisnika (čl. 129 st. 1 ZEK). Takvi podaci zadržavaju se i o uspostavljenim pozivima koji nisu odgovoreni (ne i o pozivima čije uspostavljanje nije uspelo) (čl. 129 st. 2 ZEK), a izričito je propisana zabrana zadržavanja podataka koji otkrivaju sadržaj komunikacije (čl. 129 st. 3 i 6 ZEK).

zadržanim podacima u smislu ZEK je odluka suda. Međutim, "nalog" iz čl. 286. st 3 ZKP nije sudska odluka, jer ZKP poznaje tri vrste odluka u krivičnom postupku: naredbu, rešenje i presudu (čl. 269 ZKP). Prema tome, takav nalog ne predstavlja odgovarajući pravni osnov za pristup zadržanim podacima u smislu ZEK, a ovakvo rešenje je protivno Ustavu. Pored toga, kako se ovlašćenje iz čl. 286 st. 3 odnosi samo na pribavljanje pojedinih podataka o saobraćaju, i to samo za telefonsku komunikaciju, ne i za ostale vidove elektronske komunikacije, i to samo za već ostvarenu komunikaciju, ne bi se moglo reći da takvo rešenje predstavlja adekvatno ispunjenje obaveza iz čl. 16, 17 i 20. Konvencije.

Dokazne radnje

ZKP predviđa da se uviđaj preduzima kada je za utvrđivanje ili razjašnjenje neke činjenice u postupku potrebno neposredno opažanje organa postupka, a da predmet uviđaja može biti lice, stvar ili mesto. Za vršenje uviđaja nije potrebna nikakva formalna odluka suda niti javnog tužioca. Uviđaj preduzima organ postupka (u zavisnosti od faze postupka, to je policija, javni tužilac ili sud), a propisano je da se, po pravilu, traži pomoć stručnog lica forenzičke, saobraćajne, medicinske ili druge struke, koji, po potrebi, pronalazi, obezbeđuje ili opisuje tragove, vrši potrebna merenja i snimanja, sačinjava skice, uzima potrebne uzorke radi analize ili prikuplja druge podatke (čl. 133 st. 3). Takođe, na uviđaj se može pozvati i veštak, ukoliko organ postupka proceni da bi njegovo prisustvo bilo korisno za davanje nalaza i mišljenja. Pri tome, veštak ima pravo da prilikom uviđaja predloži da se razjasne pojedine okolnosti (čl. 120 st. 4 ZKP).

Dalje, svako – pa i osumnjičeni - dužan je prilikom preduzimanja uviđaja da organu postupka *omogući pristup stvarima i pruži potrebna obaveštenja* (čl. 135 st. 2). Kako u pogledu ove dužnosti nisu predviđeni izuzeci, u pogledu okriveljnog je na ovaj način poništena privilegija od samooptuživanja, pa bi ZKP trebalo u tom delu izmeniti (kao što je u čl. 157 st. 3 ZKP propisano za pretresanje uređaja i opreme iz čl. 152 st. 3).

Iz navedenog proizlazi da bi organ postupka prilikom preduzimanja uviđaja nad uređajima koji su potencijalni nosioci elektronskih dokaza, po pravilu, trebalo da pozove stručno lice forenzičke struke (stručnjaka za digitalnu forenziku), koji bi mogao na licu mesta da vrši *live* forenziku – da pronađe, obezbedi ili opiše (samo) nepostojane računarske podatke kao tragove. Međutim, ne bi mogao i da oduzima računarske podatke jer je propisano da se *pokretne stvari*, koje su predmet uviđaja mogu privremeno oduzeti, i to pod uslovima iz čl. 147 ZKP (čl. 135 st. 2). To, dakle, znači da se prilikom uviđaja mogu oduzeti uređaji i oprema, kao predmeti, ali ne i računarski podaci koji su isprave (za razliku od oduzimanja prilikom pretresanja, jer u čl. 153 st. 1 izričito stoji da se mogu oduzimati predmeti *i isprave*).

Privremeno se oduzimaju predmeti koji se po Krivičnom zakoniku mogu oduzeti ili poslužiti kao dokaz u krivičnom postupku (čl. 147 st. 1), a u koje spadaju i uređaji za automatsku obradu podataka i uređaji i oprema na kojima se čuvaju ili se mogu čuvati elektronski zapisi (čl. 147 st. 3). Držalac predmeta je dužan da organu postupka: 1) omogući pristup predmetima, 2) pruži obaveštenja potrebna za njihovu upotrebu, i 3) na zahtev organa postupka da ih preda, a za nepostupanje po ovim dužnostima predviđena je mogućnost novčanog kažnjavanja (čl. 148 st. 2 i 3). Izričito je predviđeno da su okrivljeni i lica iz čl. 93 tačka 1 i 2, oslobođeni od dužnosti predaje stvari, ali ne i od dužnosti da organu postupka omoguće prostup predmetima i pruže obaveštenja potrebna za njihovu upotrebu. Ovakva odredba u pogledu okrivljenih nije u skladu s privilegijom od samooptuživanja, pa bi ZKP trebalo u tom delu izmeniti (kao što je u čl. 157 st. 3 ZKO propisano za pretresanje uređaja i opreme iz čl. 152 st.3).

Pretresanje se preduzima *radi pronalaženja* okrivljenog, tragova krivičnog dela ili predmeta važnih za postupak. Izričito je propisano da predmet pretresanja mogu biti i uređaji za automatsku obradu podataka i oprema na kojoj se čuvaju ili se mogu čuvati elektronski zapisi (čl. 152 st. 3), a oni se pretresaju da bi se pronašli računarski podaci. Za razliku od pretresanja stana i drugih prostorija ili lica, koji se izuzetno mogu sprovesti i ukoliko ne postoji sudska odluka, za pretresanje uređaja i opreme iz čl. 152 st. 3 predviđeno je da se preduzima *po naredbi suda*[36] – dakle, bez izuzetka.

Zakonik određuje pretpostavke za pretresanje (čl. 156), ali pretresanju se može pristupiti i ukoliko nisu ispunjene ove pretpostavke (u slučajevima predviđenim u čl. 156 st. 3), u pogledu čega ZKP ne predviđa izuzetke u pogledu uređaja i opreme iz čl. 152 st. 3. Pretresanje sprovodi *organ postupka* određen naredbom - najčešće policija. U ZKP je propisano da se pretresanja nad uređajima iz čl. 152 st. 3 preduzima po potrebi uz pomoć stručnog lica, ali bi trebalo propisati kao pravilo da pretresanje vrši stručno lice u skladu s pravilima digitalne forenzike (kao što je propisano da organ postupka prilikom uviđaja traži, po pravilu, pomoć stručnog lica).

[36] Naredba se izdaje na obrazložen zahtev javnog tužioca, u kom bi trebalo da označi predmet pretresanja i navede razlog pretresanja, što podrazumeva iznošenje činjenica koje ukazuju na postojanje verovatnoće da se će nešto pronaći, što je materijalni uslov za izdavanje naredbe. U čl. 155 takstativno je navedeno šta naredba o pretresanju treba da sadrži. Između ostalog, u njoj treba jasno da se označi predmet pretresanja, odnosno da precizno odredi uređaj i oprema iz čl. 152 st. 3 koje treba pretresti. Kao obavezni element naredbe predviđen je razlog pretresanja, odnosno potrebno je da se obrazloži zašto se određuje pretresanje, tj. da se bliže odredi koji računarski podaci se očekuju da će biti pronađeni prilikom pretresanja.

Postupak pretresanja uređen je u čl. 157. ZKP.[37] Specifičnost pretresanja uređaje i opreme iz čl. 152. st. 3 ogleda se u tome što je u st. 3 propisana obaveza držaoca predmeta ili prisutnog lica da omogući pristup i da pruži obaveštenja potrebna za njihovu upotrebu, pri čemu su od ove dužnosti izuzeti okrivljeni, kao i lice koje je isključeno (čl. 93) ili oslobođeno od dužnosti svedočenja (čl. 94. st. 1) ili od davanja odgovora na pojedina pitanja (čl. 95. st. 2).

U čl. 153. st. 1 propisano je da se predmeti i isprave (računarski podaci) koji su pronađeni prilikom pretresanja, a u vezi sa svrhom pretresanja, privremeno oduzimaju. U narednom stavu stoji da se privremeno mogu oduzeti i predmeti koji nisu u vezi sa krivičnim delom zbog koga je pretresanje preduzeto, ali koji ukazuju na drugo krivično delo za koje se goni po službenoj dužnosti – kako se za razliku od stava 1 u ovom stavu ne pominju isprave, to znači da se računarski podaci kao „slučajni nalaz" ne bi mogli privremeno oduzeti ukoliko nisu u vezi sa krivičnim delom povodom koge se pretresanje preduzelo.

O svakom pretresanju se sačinjava zapisnik u kome se tačno opisuju predmeti i isprave (računarski podaci) koji se oduzimaju i mesto na kome su pronađeni, a uz koji se prilažu određeni snimci i fotografije (čl. 157 st.4). [38]

Uopšte, što se tiče odredaba o uviđaju, privremenom oduzimanju predmeta i pretresanju postoji dosta prostora za poboljšanje radi uskladjivanja sa čl. 18 i 19 Konvencije, a naročito sa zahtevima iz čl. 14 i 15 Konvencije.

Kako ZKP računarski podatak tretira kao ispravu, relevantna je i dokazna radnja *dokazivanje ispravom*, što podrazumeva prikupljanje i saznavanje sadržaja isprave i ocenu dokazne snage isprave. Što se tiče prikupljanja isprava, prema članu 139, ispravu po službenoj dužnosti ili na predlog stranaka pribavlja organ postupka ili je podnose stranke. Ukoliko lice ili državni organ odbije da na zahtev organa postupka dobrovoljno preda ispravu, postupa se u skladu s odredbama čl. 147. ZKP koje uređuju oduzimanje predmeta.

---

[37] Predviđeno je da se zaključane prostorije, nameštaj ili druge stvari otvaraju silom samo ako njihov držalac nije prisutan ili neće dobrovoljno da ih otvori ili to odbije da učini prisutno lice, kao i da se prilikom otvaranja izbegava nepotrebno oštećenje (čl.157 st. 2). Ove odredbe bi trebalo da se primenjuju i na uređaje i opremu iz člana 152 stav 3, ukoliko su „zaključani", odnosno ukoliko je pristup onemogućen enkripcijom ili primenom drugih tehničkih sredstava.

[38] Naime, predviđeno je da se tok pretresanja može tonski i optički snimiti, i da se predmeti pronađeni tokom pretresanja mogu posebno fotografisati. Ukoliko je pretresanje izvršeno bez prisustva svedoka, snimanje i fotografisanje je obavezno. Obaveznost snimanja i fotografisanja celishodno je propisati i za pretresanje uređaja i opreme iz čl.152 st. 3, imajući u vidu potrebu da se obezbede autentičnost i neizmenjenost elektronskih dokaza prikupljenih u skladu s pravilima digitalne forenzike.

Zakonik dalje predviđa da se sadržaj isprave saznaje čitanjem, gledanjem, slušanjem ili uvidom u sadržaj isprave na drugi način (čl. 138) - saznavanje sadržaja računarskog podatka kao isprave, s obzirom na njegovu prirodu, podrazumeva *uvid u sadržaj* na drugi način, a to je moguće *samo kroz veštačenje*, jer samo lice s potrebnim stručnim znanjem i veštinama može računarskom podatku dati značaj (elektronskog) dokaza u krivičnom postupku, primenom pravila digitalne forenzike. Osim toga, kako je propisano da se verodostojnost isprava (sem ukoliko je reč o javnoj ispravi) utvrđuje izvođenjem drugih dokaza (čl. 138. st. 4), *autentičnost* računarskog podatka kao isprave utvrđuje se uvek i to, po pravilu, *veštačenjem*, a u skladu s pravilima digitalne forenzike, koja služe za autentifikaciju.

Kada je za *utvrđivanje ili ocenu neke činjenice* u postupku potrebno stručno znanje, organ postupka donosi pisanu naredbu o veštačenju. Izuzetno, veštačenje se može odrediti i bez pisane naredbe, ukoliko postoji opasnost od odlaganja, ali tada postoji obaveza sastavljanja službene beleške (čl. 117. st. 1). Taksativno je navedeno šta naredba sadrži (čl. 118), a naročito je važno označenje predmeta veštačenja i pitanja na koja veštak treba da odgovori.

Nakon određivanja veštačenja, sledi izvođenje veštačenja, koje obuhvata pripremu i samo veštačenje (koje se vrši u skladu sa standardima određene struke), a rezultat veštačenja je nalaz i/ili mišljenje.

Posebne dokazne radnje predviđene u ZKP su: tajni nadzor komunikacije (čl. 166-170), tajno praćenje i snimanje (čl. 171-173 ZKP), simulovani poslovi (čl. 174-177), računarsko pretraživanje podataka (čl. 178-180), kontrolisna isporuka (čl. 181-182) i prikriveni islednik (čl. 183-187). Ove radnje mogu se odrediti prema licu za koje postoje osnovi sumnje da je učinilo neko od krivičnih dela iz čl. 162, a na drugi način se ne mogu prikupiti dokazi za krivično gonjenje ili bi njihovo prikupljanje bilo znatno otežano. Izuzetno, mogu se odrediti i prema licu za koje postoje osnovi sumnje da priprema neko od krivičnih dela iz čl. 162, ukoliko okolnosti slučaja ukazuju da se na drugi način krivično delo ne bi moglo otkriti, sprečiti ili dokazati, ili bi to izazvalo nesrazmerne teškoće ili veliku opasnost (čl. 161 ZKP).

Sve ove radnje bilo bi smisleno i korisno odrediti i sprovesti i radi prikupljanja dokaza za dela VTK. Međutim, analizom odredbi čl. 162. ZKP, koji određuje za koja krivična dela se posebne dokazne radnje mogu odrediti, dolazi se do zaključka da je to moguće samo u *pogledu malog broja krivičnih dela koja se smatrtaju VTK*, u smislu čl. 2 i 3 ZVTK.[39] Na ovaj način, ne bi se moglo reći da je ZKP u saglasnosti za čl. 21 Konvencije.

[39] Naime, u čl. 162 st. 1 tačka 1) stoji da se posebne dokazne radnje mogu odrediti u odnosu na krivično dela za koja je posebnim zakonom određeno da postupa javno tužilaštvo posebne nadležnosti. Posebno javno tužilaštvo za VTK nije javno tužilaštvo posebne nadležnosti u smislu ZJT, tako da automatski krivična dela u njegovoj nadležnosti nisu pokrivena tačkom 1. U tački 2) takstativno su navedena pojedina krivična dela, a među njima je svega nekoliko krivičnih dela koja se smatraju VTK u smislu čl. 3 a u vezi sa čl. 2 ZVTK. U tački 3) navedeno je i krivično delo sprečavanje i ometanja dokazivanja (čl. 336 st. 1 KZ) ako je učinjeno u vezi s krivičnim delom iz tačke 1) i 2).

U čl. 162 st. 2 stoji da se prikriveni islednik može odrediti samo za krivična dela iz tačke 1) – drugim rečima ni za jedno delo koje je je određeno kao VTK.

U čl. 162 st. 3 dodatno je propisano da se tajni nadzor komunikacije može odrediti, osim za krivična dela iz tačke 1-3, i za neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava (čl. 199 KZ) i četiri krivična dela protiv bezbednosti računarskih podataka.

Iz navedenog proizlazi, da se za dela protiv bezbednosti računarskih podataka od posebnih dokaznih radnji, jedino može odrediti tajni nadzor komunikacije, i to samo za sledeća krivična dela: oštećenje računarskih podataka i programa (čl. 298. st 3. KZ), računarska sabotaža (čl. 299 KZ), računarska prevara (čl. 301 st. 3 KZ) i neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (čl. 302 KZ) – dakle, ne i radi prikupljanja dokaza za ostala krivična dela iz glave dvadesetsedam KZ. Ni za jedno od ovih krivičnih dela ne bi se mogao odrediti tajno praćenje i snimanje ili računarsko pretraživanje podataka, a što bi bilo izuzetno korisno, kao ni druge posebne dokazne radnje.

U odnosu na druga krivična dela koja se smatraju VTK u smislu Konvencije, posebne dokazne radnje (s izuzetkom prikrivenog islednika) mogle bi se odrediti u odnosu na prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju (čl. 185 st. 2 i 3 KZ). U pogledu krivičnih dela protiv intelektualne svojine samo u pogledu krivičnog dela neovlašćenog iskorišćavanja autorskog dela ili predmeta srodnog prava (čl. 199 KZ) mogao bi se odrediti tajni nadzor komunikacije, ali ne i druge posebne dokazne radnje. Posebne dokazne radnje ne mogu se odrediti u odnosu na krivična dela koja su propisana, nakon ratifikovanja Dodatnog protokola (krivično delo rasne i druge diskriminacije (čl. 387 st. 4, 5 i 6 KZ) i krivično delo povrede ugleda zbog rasne verske, nacionalne ili druge pripadnosti (čl. 174 KZ)

U pogledu ostalih krivičnih dela koja se smatraju VTK u smislu čl. 2 i 3. ZVTK, posebne dokazne radnje (s izuzetkom prikrivenog islednika) mogu se odrediti u odnosu na iznudu (čl. 214 st. 4 KZ) – ne i u pogledu ostalih dela protiv imovine a koja bi se mogla smatrati VTK, falsifikovanje novca (čl. 241 st. 1 do 3 KZ); pranje novca (čl. 245 st. 1 do 4 KZ) - ne i u pogledu ostalih dela protiv privrede a koja bi se mogla smatrati VTK; i pojedina dela protiv ustavnog uređenja i bezbednosti Republike Srbije. Drugim rečima, posebne dokazne radnje ne bi se mogle odrediti u odnosu na pojedina dela koja bi se mogla smatrati VTK u smislu ZVTK, a za koje bi moglo biti korisno da se ona ovaj način prikupe dokazi – za dela protiv imovine, npr. ucena (čl. 215); za dela protiv privrede, npr. odavanje poslovne tajne (čl. 240 KZ); za dela protiv pravnog saobraćaja, npr. falisikovanje isprave (čl. 355 KZ); za dela protiv sloboda i prava čoveka i građanina, npr. ugrožavanje sigurnosti (čl. 138), proganjanje (čl. 138a), neovlašćeno prikupljanje ličnih podataka (čl. 146).

Inspekcijski nadzor koji vrši Inspekcija za informacionu bezbednost

Inspekcija za informacionu bezbednost i elektronsko poslovanje vrši inspekcijski nadzor nad primenom Zakona o informacionoj bezbednosti i radom operatora IKT sistema od posebnog značaja, osim samostalnih operatora IKT sistema i IKT sistema za rad sa tajnim podacima. Inspekcijski nadzor se vrši u skladu sa Zakonom o informacionoj bezbednosti (čl. 28. i 29) u materijalnopravnom smislu, te Zakonom o inspekcijskom nadzoru („Službeni glasnik RS“, br. 36/15, 44/18 - dr. zakon i 95/18 – u daljem tekstu: ZoIN) i Zakonom o opštem upravnom postupku („Službeni glasnik RS“, br. 18/16, 95/18 - autentično tumačenje i 2/23 - odluka US – u daljem tekstu: ZUP), kao zakonima koji se primenjuju na postupak inspekcijskog nadzora.

Poslove inspekcije za informacionu bezbednost obavlja Ministarstvo informisanja i telekomunikacija, kao ministarstvo nadležno za poslove informacione bezbednosti, preko inspektora za informacionu bezbednost. Organizaciono gledano, u pitanju je Odsek za informacionu bezbednost i elektronsko poslovanje u Sektoru za informaciono društvo, u kome je u vreme pripreme ovog teksta zaposleno dva inspektora.

U okviru inspekcijskog nadzora rada operatora IKT sistema, inspektor za informacionu bezbednost utvrđuje da li su ispunjeni uslovi propisani Zakonom o informacionoj bezbednosti („Službeni glasnik RS“, br. 6/16, 94/17 i 77/19 – u daljem tekstu: ZIB) i propisima donetim na osnovu ovog zakona.

Saglasno članu 21. ZoIN, inspektor, radi utvrđivanja činjenica u postupku inspekcijskog nadzora, ima ovlašćenje da:

- izvrši uvid u javne isprave i podatke iz registara i evidencija koje vode nadležni državni organi, organi autonomne pokrajine i organi jedinice lokalne samouprave i drugi nosioci javnih ovlašćenja, ako

su neophodni za inspekcijski nadzor, a nije mogao da ih pribavi po službenoj dužnosti, i da ih kopira, u skladu sa zakonom;

- izvrši uvid u ličnu kartu ili drugu javnu ispravu sa fotografijom koja je podobna da se identifikuju ovlašćena lica u nadziranom subjektu, druga zaposlena ili radno angažovana lica, fizička lica koja su nadzirani subjekti, svedoci, službena lica i zainteresovana lica, kao i fizička lica zatečena na mestu nadzora;

- uzima pisane i usmene izjave nadziranih subjekata - fizičkih lica i zastupnika, odnosno ovlašćenih lica u nadziranom subjektu - pravnom licu i drugih zaposlenih ili radno angažovanih lica, svedoka, službenih lica i zainteresovanih lica, i da ih poziva da daju izjave o pitanjima od značaja za inspekcijski nadzor;

- naloži da mu se u određenom roku stave na uvid poslovne knjige, opšti i pojedinačni akti, evidencije, ugovori i druga dokumentacija nadziranog subjekta od značaja za inspekcijski nadzor, a u obliku u kojem ih nadzirani subjekat poseduje i čuva;

- vrši uviđaj, odnosno pregleda i proverava lokaciju, zemljište, objekte, poslovni i drugi nestambeni prostor, postrojenja, uređaje, opremu, pribor, vozila i druga namenska prevozna sredstva, druga sredstva rada, proizvode, predmete koji se stavljaju u promet, robu u prometu i druge predmete kojima obavlja delatnost ili vrši aktivnost, kao i druge predmete od značaja za inspekcijski nadzor;

- uzme potrebne uzorke radi njihovog ispitivanja i utvrđivanja činjeničnog stanja, u skladu sa posebnim zakonom i propisima donetim na osnovu zakona;

- fotografiše i snimi prostor u kome se vrši inspekcijski nadzor i druge stvari koje su predmet nadzora;

- obezbedi dokaze.

Inspekcija za informacionu bezbednost i elektronsko poslovanje donosi godišnji plan inspekcijskog nadzora, na osnovu prikupljenih podataka i praćenja i analiziranja stanja u oblasti nadzora iz svog delokruga i procenjenog rizika. Godišnji plan se sprovodi kroz operativne (šestomesečne, tromesečne i mesečne) planove inspekcijskog nadzora i naloge za inspekcijski nadzor.

Inspekcijski nadzor, prema vrsti, može biti redovan, vanredan, mešoviti, kontrolni i

dopunski. Redovan inspekcijski nadzor vrši se prema planu inspekcijskog nadzora. Vanredan inspekcijski nadzor je vrsta nadzora koja nije planirana, a koju inspekcija za informacionu bezbednost i elektronsko poslovanje vrši po prijavama i zahtevima fizičkih i pravnih lica i na osnovu neposrednih saznanja o postojanju nezakonitosti, odnosno sumnji na povredu propisa. Kontrolni inspekcijski nadzori služe da se utvrdi izvršenja mera naloženih u okviru redovnog ili vanrednog inspekcijskog nadzora.

Saglasno godišnjem planu nadzora za 2023. godinu, ova inspekcija vrši redovne inspekcijske nadzore kod operatora IKT sistema od posebnog značaja i pružalaca kvalifikovanih usluga od poverenja (nadzirani subjekti).

Redovni inspekcijski nadzori se vrše kod onih IKT sistema od posebnog značaja koji su, na osnovu delatnosti koje obavljaju, procenjeni kao naročito važni – a samim tim i nose visok rizik - i u kojima je zbog toga potrebno uspostaviti i održavati adekvatan nivo informacione bezbednosti.

Vanredni inspekcijski nadzori se vrše kao prioritetni, kada inspekcija oceni da se hitno moraju preduzimati određene mere i ukoliko se dođe do saznanja o postojanju nezakonitosti.

Prema obliku, inspekcijski nadzor može biti terenski i kancelarijski. Terenski inspekcijski nadzor se vrši izvan službenih prostorija inspekcije, neposrednim uvidom u objekte, prostorije, uređaje i druge predmete, akte i dokumentaciju nadziranog subjekta, kao i uzimanjem pisanih i usmenih izjava od odgovornih lica i svedoka o pitanjima koja su od značaja za utvrđivanje činjeničnog stanja. Kancelarijski inspekcijski nadzor se vrši u službenim prostorijama inspekcije, uvidom u poslovne knjige i drugu dokumentaciju nadziranog subjekta koja se odnosi na obavljanje poslova koji su predmet inspekcijskog nadzora, kao i uvidom u podatke o nadziranom subjektu pribavljene po službenoj dužnosti.

Inspekcijski nadzori se vrše kako u sedištu operatora IKT sistema od posebnog značaja, tako i u njihovim poslovnim jedinicama.

Posle svakog postupka redovnog ili vanrednog inspekcijskog nadzora, koji je okončan nalaganjem ili predlaganjem određenih mera, vrši se kontrolni inspekcijski nadzor, kojim se utvrđuje izvršenje mera naloženih ili predloženih u postupku redovnog ili vanrednog inspekcijskog nadzora.

Predmet inspekcijskog nadzora nad primenom ZIB čine sledeća pitanja:

- da li je donet Akt o bezbednosti;
- da li je Akt o bezbednosti donet u skladu sa postojećim propisima

(član 8. ZIB i Uredba o bližem sadržaju Akta o bezbednosti IKT sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti IKT sistema od posebnog značaja);

- da li su primenjene mere zaštite;
- da li je izvršena godišnja provera usklađenosti primenjenih mera zaštite;
- da li je u skladu sa propisima sačinjen izveštaj o godišnjoj proveri IKT sistema od posebnog značaja;
- da li je izvršen upis u Evidenciju operatora IKT sistema od posebnog značaja;
- da li su Nacionalnom CERT-u dostavljeni tačni statistički podaci o incidentima u IKT sistemu u skladu sa članom 11b Zakona o informacionoj bezbednosti.

Predmet inspekcijskog nadzora nad primenom Zakona o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju („Službeni glasnik RS“, br. 94/17 i 52/21) čine sledeća pitanja:

- da li pružalac kvalifikovane usluge od poverenja (u daljem tekstu: pružalac usluge) ima zaposlene koji poseduju neophodnu stručnost, iskustvo i kvalifikacije za primenu administrativnih i upravljačkih procedura koje odgovaraju domaćim i međunarodnim standardima;
- da li je pružalac usluge osiguran od rizika odgovornosti za štetu nastalu vršenjem usluge kvalifikovane usluge od poverenja, u skladu sa propisima (ZEP i Pravilnik o iznosu osiguranja od rizika odgovornosti za štetu nastalu vršenjem kvalifikovane usluge od poverenja);
- da li pružalac usluge ima sigurne uređaje i proizvode koji su zaštićeni od neovlašćene promene i garantuju tehničku bezbednost i pouzdanost procesa koje podržavaju;
- da li pružalac usluge koristi sigurne sisteme za čuvanje podataka koji su mu povereni;
- da li pružalac usluge sprovodi mere protiv falsifikovanja i krađe podataka;
- da li pružalac usluge čuva u odgovarajućem vremenskom periodu sve relevantne informacije koje se odnose na podatke koji su kreirani ili primljeni od strane pružaoca;

- da li pružalac usluge vodi ažurnu, tačnu i bezbednim merama zaštićenu bazu podataka izdatih elektronskih sertifikata, odnosno drugih podataka za čiju tačnost i integritet garantuje u okviru pružanja usluge;

- da li pružalac usluge ima ažuran plan završetka rada koji osigurava kontinuitet kvalifikovanih usluga od poverenja;

- da li pružalac usluge ima Opšte uslove za pružanje usluga, u skladu sa propisima, koji su javno objavljeni;

- da li je, u skladu sa propisima, pružalac usluge doneo Politiku pružanja usluge, Praktična pravila za pružanje usluga i Politiku informacione bezbednosti;

- kod pružaoca usluge izdavanja kvalifikovanih elektronskih sertifikata za elektronski potpis, odnosno pečat, pored ostalih opštih uslova za obavljanje kvalifikovanih usluga od poverenja, proverava se da li kvalifikovani elektronski sertifikati ispunjavaju uslove utvrđene propisima (ZEP i Pravilnik o uslovima koje moraju da ispunjavaju kvalifikovani elektronski sertifikati), kao i da li pružalac usluge čuva kompletnu dokumentaciju o izdatim i opozvanim kvalifikovanim elektronskim sertifikatima, u skladu sa propisima;

- kod pružalaca usluge kvalifikovanog elektronskog vremenskog žiga proverava se, pored ostalih opštih uslova za obavljanje kvalifikovanih usluga od poverenja, da li jedinica za formiranje vremenskih žigova koristi izvor tačnog vremena sinhronizovan sa koordiniranim univerzalnim vremenom (UTC) tako da se sprečava svaka mogućnost promene podataka koja se ne može otkriti i da se obezbedi da se svaka promena rada časovnika izvan predviđenih parametara odmah ustanovi;

- kod pružalaca usluge kvalifikovanog elektronskog čuvanja, pored ostalih opštih uslova za obavljanje kvalifikovanih usluga od poverenja, proverava se da li priprema dokumenata za pouzdano elektronsko čuvanje ispunjava propisane uslove (iz ZEP i Uredbe o uslovima za pripremu dokumenta za pouzdano elektronsko čuvanje i formatima dokumenta koji su pogodni za dugotrajno čuvanje), kao i da li pouzdano elektronsko čuvanje ispunjava propisane uslove (iz ZEP i Pravilnika o uslovima za postupke i tehnološka rešenja koji se koriste tokom pouzdanog elektronskog čuvanja dokumenta);

- da li pružalac usluge kvalifikovane elektronske dostave vodi ažurnu, tačnu i bezbednim merama zaštićenu bazu podataka o slanju, prosleđivanju i prijemu elektronskih poruka, kao i o ostalim relevantnim informacijama koje je dužan da čuva na osnovu Pravilnika

o uslovima za pružanje usluge kvalifikovane elektronske dostave i sadržaju potvrde o prijemu i dostavi elektronske poruke;

- da li pružalac usluge kvalifikovane elektronske dostave obavlja usluge kvalifikovane elektronske dostave u svemu u skladu sa uslovima iz člana 6. Pravilnika o uslovima za pružanje usluge kvalifikovane elektronske dostave i sadržaju potvrde o prijemu i dostavi elektronske poruke;

- da li kvalifikovani elektronski sertifikati za autentikaciju veb sajtova ispunjavaju posebne uslove utvrđene propisima (čl. 58. i 59. ZEP-a i u čl.26-29. Pravilnika o uslovima koje moraju da ispunjavaju kvalifikovani elektronski sertifikati).

- da li pružalac usluge elektronske identifikacije proverava identitet korisnika radi izdavanja sredstava elektronske identifikacije u skladu sa nivoom šeme koju pruža (Uredba o bližem uređenju uslova koje moraju da ispune šeme elektronske identifikacije za određene nivoe pouzdanosti);

- da li pružalac usluge elektronske identifikacije isporučuje sredstvo elektronske identifikacije na način koji osigurava isporuku samo licu kojem je namenjeno;

- da li pružalac usluge elektronske identifikacije sprovodi autentikacioni mehanizam za šemu elektronske identifikacije u skladu sa nivoom šeme koju pruža (Uredba o bližem uređenju uslova koje moraju da ispune šeme elektronske identifikacije za određene nivoe pouzdanosti);

- da li pružalac usluge elektronske identifikacije ispunjava tehničke, organizacione i bezbednosne uslove za izdavanje šema elektronske identifikacije (Uredba o bližem uređenju uslova koje moraju da ispune šeme elektronske identifikacije za određene nivoe pouzdanosti);

- da li sredstva za elektronsku identifikaciju ispunjavaju propisane uslove (Uredba o bližem uređenju uslova koje moraju da ispune šeme elektronske identifikacije za određene nivoe pouzdanosti).

U sklopu ovlašćenja inspektora za informacionu bezbednost, ZIB – uz konstataciju da je inspektor za informacionu bezbednost ovlašćen za nalaganje mera za koje je ovlašćen inspektor u postupku vršenja inspekcijskog nadzora utvrđenih zakonom - u članu 29. izdvaja ovlašćenja na nalaganje otklanjanja utvrđenih nepravilnosti u određenom roku i zabranu korišćenja postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost u određenom roku, koje predstavljaju upravne mere. Saglasno članu 25. stav 1. ZoIN, inspektor može nadziranom subjektu

izreći upravnu meru, i to preventivnu meru, meru za otklanjanje nezakonitosti, posebnu meru naredbe, zabrane ili zaplene ili meru za zaštitu prava trećih lica, koje su dalje uređene u čl. 26 – 29. ovog zakona. Inspektor izriče one mere koje su srazmerne procenjenom riziku i otkrivenim, odnosno verovatnim nezakonitostima i štetnim posledicama, tako da se rizikom delotvorno upravlja, i kojima se najpovoljnije po nadziranog subjekta postižu cilj i svrha zakona i drugog propisa. Istovremeno, inspektor se obavezno stara o tome da ove mere budu srazmerne ekonomskoj snazi nadziranog subjekta, da se njihove štetne posledice svedu na najmanju meru i nastavi održivo poslovanje i razvoj nadziranog subjekta.

Inspektor informacione bezbednosti, zavisno od utvrđenog stanja u postupku inspekcijskog nadzora, a saglasno ovlašćenjima utvrđenim zakonom, preduzeće sledeće mere:

- naložiti otklanjanje utvrđenih nepravilnosti, nedostataka ili propusta i odrediti rok za njihovo otklanjanje;
- privremeno zabraniti korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost;
- zabraniti upotrebu neadekvatnih postupaka i infrastrukture, i dati rok pružaocu usluga u kojem je dužan da obezbedi adekvatne postupke i infrastrukturu;
- privremeno zabraniti vršenje usluge pružaoca kvalifikovanih usluga od poverenja do otklanjanja neadekvatnosti postupaka i infrastrukture;
- narediti privremeni opoziv nekog ili svih sertifikata izdatih od strane pružaoca kvalifikovanih usluga od poverenja, ako postoji osnovana sumnja da se radi o neadekvatnom postupku ili falsifikatu;
- podneti prijavu nadležnom organu za učinjeno krivično delo ili privredni prestup, odnosno podneti zahtev za pokretanje prekršajnog postupka;
- druge mere i aktivnosti.

Zakonodavstvo u nastanku - Nacrt zakona o informacionoj bezbednosti u članu 38. predviđa uređenje ovlašćenja inspektora za informacionu bezbednost na potpuniji način u odnosu na važeći ZIB (član 29). Ovaj nacrt zakona predviđa da je inspektor za informacionu bezbednost ovlašćen da u postupku sprovođenja nadzora, pored nalaganja mera za koje je ovlašćen - inspektor u postupku vršenja inspekcijskog nadzora utvrđenih zakonom:

- naloži otklanjanje utvrđenih nepravilnosti i za to utvrdi razuman rok;
- zabrani korišćenje postupaka i tehničkih sredstava kojima se ugrožava ili narušava informaciona bezbednost i za to ostavi rok;
- zahteva od operatora IKT sistema od posebnog značaja da izvrši skeniranje mreže u cilju utvrđivanja eventualnih bezbednosnih ranjivosti, a u skladu sa procenom rizika;
- naloži da nadzirani subjekt učini dostupnim javnosti informacije koje se tiču nepoštovanja odredbi ovog zakona, a za koje postoji opravdan interes javnosti na utvrđeni način;
- naloži da nadzirani subjekt odredi lice sa tačno utvrđenim ovlašćenjima koje će u utvrđenom vremenskom periodu nadzirati i pratiti usaglašenost sa odredbama ovog zakona i naloženim merama.

Za operatora IKT sistema od posebnog značaja koji ne postupi po nalogu inspektora za informacionu bezbednost u ostavljenom roku iz člana 29. stav 1. tačka 1. ovog zakona, kao i za odgovorno lice u tom operatoru IKT sistema od posebnog značaja, članom 30. stav 1. tačka 6) i stav 2. ZIB propisan je prekršaj sa zaprećenom novčanom kaznom u iznosu od 50.000 do 2.000.000 dinara, odnosno od 5.000 do 50.000 dinara.

Inspekcija za informacionu bezbednost sprovodi i preventivno delovanje, pored „klasičnih“ inspekcijskih nadzora, i to objavljivanjem kontrolnih lista i planova inspekcijskog nadzora, kao i organizovanjem službenih savetodavnih poseta i drugih aktivnosti usmerenih ka podsticanju i podržavanju zakonitosti i bezbednosti postupanja u oblasti informacione bezbednosti i elektronskog poslovanja. Naročito značajan oblik preventivnog delovanja su službene savetodavne posete, koji se sastoji u pružanju stručne i savetodavne podrške nadziranom subjektu od strane inspekcije na licu mesta, a koju inspekcija organizuje van postupaka inspekcijskog nadzora. U službenoj savetodavnoj poseti ne primenjuju se pravila iz postupka inspekcijskog nadzora, upravnog postupka i iniciranja pokretanja prekršajnog postupka, odnosno izdavanja prekršajnog naloga, nego je suština u podršci poslovanju koje je usklađeno sa zakonom kroz davanje saveta, kao i preporuka u slučaju ustanovljenih propusta.

U cilju delotvornijeg suzbijanja delatnosti ili aktivnosti neregistrovanih subjekata, inspekcija nadležna za informacionu bezbednost sarađuje sa drugim inspekcijama i organima, radi međusobnog obaveštavanja, razmene podataka, pružanja pomoći i preduzimanja zajedničkih mera i radnji od značaja za inspekcijski nadzor.

Analiza prakse domaćih sudova i praksa Evropskog suda za ljudska prava

Cilj ovog dela analize jeste da sagleda sudske postupke koji su vođeni pred Višim sudom u Beogradu od strane Posebnog javnog tužilaštva za borbu protiv visokotehnološkog kriminala, a koji su vezani za korpus dela iz ove oblasti. Analiza je sprovedena kako bi se uočilo na koji način tužilaštvo i sud pristupaju ovim predmetima, kakve sankcije sud izriče za izvršena krivična dela, koje okolnosti smatra olakšavajućim, odnosno otežavajućim prilikom izricanja sankcije, koje vrste mera, pored sankcija za izvršeno delo, eventualno izriče okrivljenima i kako se odnosi prema žrtvama krivičnih dela iz ovog korpusa.

Metodologija i dobijeni podaci

U svrhu izrade analize, upućeni su zahtevi za pristup informacijama od javnog značaja Višem sudu u Beogradu i Posebnom javnom tužilaštvu za borbu protiv visokotehnološkog kriminala.

Od tužilaštva je traženo da dostave podatke o tome koliko postupaka se trenutno aktivno vodi za krivična dela: - protiv bezbednosti računarskih podataka iz člana 298, člana 299, člana 300, člana 301, člana 302, člana 303, člana 304 i člana 304a Krivičnog zakonika; - protiv intelektualne svojine iz člana 198, člana 199, člana 200, člana 201 i člana 202 Krivičnog zakonika, kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku, ako broj primeraka autorskih dela prelazi 2000, ili nastala materijalna šteta prelazi iznos od 1.000.000 dinara; - protiv polne slobode iz člana 185 i 185b Krivičnog zakonika, kod kojih se kao objekat ili sredstvo izvršenja krivičnih dela javljaju računari, računarski sistemi, računarske mreže i računarski podaci, kao i njihovi proizvodi u materijalnom ili elektronskom obliku. Pored ovih podataka, traženi su i podaci o tome koliko nosilaca javnotužilačke funkcije je raspoređeno u Posebno tužilaštvo za borbu

protiv visokotehnološkog kriminala Višeg javnog tužilaštva u Beogradu i koliko tih nosilaca javnotužilačke funkcije poseduje posebna znanja iz oblasti informatičkih nauka, kao i podatak o tome da li postoji pravilnik, odluka ili neki drugi akt kojim su definisani parametri koji određuju šta se podrazumeva pod „znanjima iz oblasti informatičkih nauka“, propisanih članom 5 stav 2 Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, dostavljanje takvog akta, ili, ukoliko ga nema, razjašnjenje kriterijuma po kojima se određuje da li javni tužilac poseduje „znanja iz oblasti informatičkih nauka“.

Od suda su tražene kopije prvostepenih i drugostepenih presuda u svim postupcima koji su stekli svojstvo pravnosnažnosti u periodu od 1. jula 2022. godine, do 30. juna 2023. godine za krivična dela koja su navedena i u zahtevu upućenom tužilaštvu, kao i podaci o tome koliko sudija je raspoređeno u Odeljenju za borbu protiv visokotehnološkog kriminala Višeg suda u Beogradu, potom koliko tih sudija poseduje posebna znanja iz oblasti informatičkih nauka i da li postoji pravilnik, odluka ili neki drugi akt kojim su definisani parametri koji određuju šta se podrazumeva pod „znanjima iz oblasti informatičkih nauka“, propisanih članom 11 stav 2 Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. Od suda je traženo dostavljanje takvog dokumenta ili, ukoliko ne postoji, razjašnjenje kriterijuma po kojima se određuje da li sudija poseduje „znanja iz oblasti informatičkih nauka“.

Tužilaštvo je u svom odgovoru dostavilo podatke o broju predmeta koji su predstavljeni u sledećoj tabeli:

Član Krivičnog zakonika	Predistražni postupak	Istraga	Glavni pretres
298	10	X	1
299	13	X	X
301	20	9	4
302	37	15	2
303	2	X	1
304a	X	1	X
198	2	X	X
199	36	X	1
185	112	X	19

U Posebno javno tužilaštvo za borbu protiv visokotehnološkog kriminala je, prema dostavljenim podacima, raspoređeno pet nosilaca javnotužilačke funkcije i svi

poseduju posebna znanja iz oblasti informatičkih tehnologija. U ovom odeljenju ne postoji poseban akt kojim je određeno šta se podrazumeva pod „znanjima iz oblasti informatičkih tehnologija“, ali su ona, po navodima iz odgovora, stečena kroz višegodišnje obuke organizovane od strane domaćih institucija (Pravosudna akademija) i međunarodnih organizacija (Savet Evrope, Ujedinjene nacije i dr.), kao i kroz postupanje tužilaca u više hiljada predmeta za krivična dela iz člana 3 Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala. U planu je donošenje i posebnog pravilnika koji bi regulisao institute od značaja za rad Posebnog javnog tužilaštva za visokotehnološki kriminal, nakon donošenja novog Zakona o visokotehnološkom kriminalu.

Viši sud u Beogradu je u svom odgovoru dostavilo podatke koji su predstavljeni u sledećoj tabeli:

Član Krivičnog zakonika	Broj pravnosnažnih presuda za traženi period
298	X
299	X
300	X
301	2
302	1
303	X
304	X
304a	X
198	X
199	1
200	X
201	X
202	X
185	31

Viši sud je odgovorio da, u okviru tog suda, ne postoji posebno odeljenje za borbu protiv visokotehnološkog kriminala i da je godišnjim rasporedom poslova određeno da sve sudije prvostepenog krivičnog odeljenja postupaju u predmetima visokotehnološkog kriminala. Sud je naveo da ne raspolaže podatkom da postoji poseban akt koji određuje šta se podrazumeva pod „znanjima iz oblasti informatičkih tehnologija“ propisanih članom 11 (2) Zakona o organizaciji i nadležnosti državnih

organa za borbu protiv visokotehnološkog kriminala, ukazujući istovremeno da tom odredbom nije propisana dužnost posedovanja posebnih znanja iz ove oblasti za postupanje sudija u predmetima visokotehnološkog kriminala, već je predviđeno jedino da će sudije koje eventualno poseduju posebne sertifikate o takvim znanjima imati prednost prilikom raspoređivanja u eventualno formirano Odeljenje za borbu protiv visokotehnološkog kriminala.

Viši sud u Beogradu je dostavio ukupno 42 presude (35 prvostepenih i 7 drugostepenih odluka) po podnetom zahtevu za pristup informacijama od javnog značaja, za sva krivična dela u kojima je raspolagao podacima za traženi period. Od 35 prvostepenih odluka, 16 postupaka je okončano sporazumom o priznanju krivice (15 postupaka po članu 185 KZ i jedan postupak po članu 301 KZ), dok su preostali postupci okončani nakon vođenja glavnog pretresa.

Krivično delo računarska prevara iz člana 301 Krivičnog zakonika

U periodu od 1. jula 2022. godine do 30. juna 2023. godine donete su ukupno dve odluke za ovo krivično delo.

Presudom Kpo3-43/2021 od 28. septembra 2022. godine odbijena je optužba okrivljenima zbog nastupanja apsolutne zastarelosti koji su, prema navodima optužnice, uspostavili mehanizam mobilnog telefoniranja sa inostranstvom po cenama nacionalnog poziva sa domaće SIM kartice, čime su zaobilazili legalne međunarodne rute za odvijanje međunarodnog telefonskog saobraćaja.

Sa druge strane, sporazumom o priznanju krivice, SPK Po3-53/2022 od 27. decembra 2022. godine, okrivljena je priznala krivicu za delo iz člana 301 stav 3 u vezi sa stavom 1 KZ i osuđena je na godinu dana kućnog zatvora bez elektronskog nadzora. Okrivljena je priznala da je unosila netačne podatke i evidentirala nepostojeće uplate depozita na naloge igrača igara na sreću, čime je uticala na elektronsku obradu i prenos podataka u sistemu preduzeća u kom je radila. Bez nekog dodatnog obrazloženja, sud je prihvatio sporazum o priznanju krivičnog dela tužilaštva i okrivljene.

Krivično delo neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka iz člana 302 Krivičnog zakonika

Presudom Kpo3-43/2022 od 22. decembra 2022. godine okrivljeni je osuđen za izvršenje tri krivična dela. Pored dela iz člana 302 KZ, osuđen je i za izvršenje krivičnog dela polno uznemiravanje iz člana 182a st. 1 KZ i za izvršenje krivičnog dela ucena iz člana 215 st. 1 KZ. Okrivljenom je izrečena jedinstvena kazna zatvora za sva tri dela u trajanju od jedne godine i pet meseci, a presuda je odmah postala

pravnosnažna jer su se stranke odrekle prava na žalbu. Samim tim, presuda i nije imala obrazloženje, tako da se jedino moglo zaključiti iz izreke da je okrivljeni osuđen zbog toga što je pristupio korisničkom Facebook nalogu oštećene koristeći kôd koji je dobio zloupotrebom naloga njene prijateljice, da bi je potom ucenjivao da će njene nage i poluodevene fotografije do kojih je došao, poslati njenim prijateljima i poznanicima, ukoliko mu ne bude platila određenu sumu novca.

Krivično delo neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava iz člana 199 Krivičnog zakonika iz člana 199 krivičnog zakonika

Presudom Kpo3-89/2021 od 22. septembra 2022. godine šest okrivljenih je oslobođeno optužbe da su izvršili krivično delo iz člana 199 stav 3 u vezi sa stavom 2 KZ delom zbog nastupanja apsolutne zastarelosti krivičnog gonjenja, a delom zbog nedostataka dokaza.

Njima je stavljeno na teret da su neovlašćeno pribavili, držali i stavili u promet bazu podataka – elektronske podatke Agencije za privredne registre Srbije (registre finansijskih izveštaja i podatke o bonitetu pravnih lica i preduzetnika) koji su potom objavljeni na posebnoj internet stranici i nudili i prodavali izrade bonitetskih izveštaja klijentima. Pored toga što je u jednom delu nastupila apsolutna zastarelost krivičnog gonjenja, sud je utvrdio i da je okrivljenima stavljeno na teret izvršenje ovog dela i u vremenskom periodu za koji tužilaštvo nije dostavilo nijedan dokaz da su okrivljeni, upravo u tom periodu, izvršili bilo koju radnju koja bi se mogla podvesti pod krivično delo.

Krivično delo prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju iz člana 185 Krivičnog zakonika

Najveći broj odluka za traženi period je donet u vezi sa krivičnim delom iz člana 185 KZ. Prema podacima koje je dostavio Viši sud u Beogradu, u navedenom periodu su donete 32 odluke, od kojih je u 16 predmeta potpisan sporazum o priznanju krivice, dok je preostalih 16 okončano u redovnom postupku. Od 16 odluka koje su okončane u redovnom postupku, sedam je dobilo epilog pred drugostepenim sudom. Viši sud je dostavio i drugostepene odluke u tim postupcima.

Sporazumi o priznanju krivice

U periodu od 1. jula 2022. godine do 30. juna 2023. godine potpisano je ukupno 16 sporazuma o priznanju krivice. Od 16 presuda, u 15 je potpisan sporazum za krivično delo iz stava 4 člana 185 KZ-a, dok je u jednom predmetu sporazum potpisan za delo iz stava 1 i 2 ovog člana.

U 13 predmeta u kojima je potpisan sporazum iz člana 185 st. 4 KZ je izrečena kazna od godinu dana kućnog zatvora bez elektronskog nadzora, u jednom predmetu je izrečena kazna kućnog zatvora (bez pominjanja elektronskog nadzora)[40], dok je u poslednjem predmetu za ovo delo izrečena uslovna osuda od godinu dana zatvora koja se neće izvršiti ako okrivljeni u roku od tri godine od pravnosnažnosti ne izvrši novo krivično delo[41].

Za krivično delo iz člana 185 st. 1 i 2 KZ-a izrečena je kazna od godinu dana kućnog zatvora uz primenu elektronskog nadzora.[42]

Ni u jednoj od navedenih presuda sudovi nisu obrazlagali razloge zbog kojih su prihvatili sporazum o priznanju krivice, niti razloge zbog kojih sankciju smatraju adekvatnom, navodeći samo da su ispunjeni svi uslovi iz člana 317 Zakonika o krivičnom postupku (ZKP) i da nema smetnji za zaključenje sporazuma propisanih članom 338 st. 1 ZKP-a.

U svim presudama je izrečena mera bezbednosti oduzimanja predmeta (mobilni telefoni, računari sa dodatnom opremom i hard diskovi) i izrečene su posebne mere iz člana 7 Zakona o posebnim merama za sprečavanje vršenja krivičnih dela protiv polne slobode prema maloletnim licima[43]:

- obavezno javljanje nadležnom organu policije i Uprave za izvršenje krivičnih sankcija;
- zabrana posećivanja mesta na kojima se okupljaju maloletna lica (vrtići, škole i sl.);
- obavezno posećivanje profesionalnih savetovališta i ustanova;
- obavezno obaveštavanje o promeni prebivališta, boravišta ili radnog mesta;
- obavezno obaveštavanje o putovanju u inostranstvo.

Ove mere su izrečene kumulativno uz njihovo sprovođenje najduže 20 godina posle izvršene kazne zatvora, s tim što će sud koji je doneo prvostepenu presudu, po službenoj dužnosti, nakon isteka svake četiri godine od početka primene posebnih odlučiti o potrebi njihovog daljeg sprovođenja.

[40] SPK Po3 - 10/2023

[41] SPK Po3 - 39/2022

[42] SPK Po3 – 55/2022

[43] “Službeni glasnik RS”, broj 32 od 8. aprila 2013.

Izvršioci ovog krivičnog dela su pribavaljali i posedovali fotografije ili audio-vizuelne zapise maloletnih lica, uglavnom preko različitih društvenih mreža ili chat aplikacija i čuvali ih u svojim telefonima, računarima, hard diskovima ili memorijskim karticama, što je i otkriveno prilikom pretresa njihovih stanova i drugih prostorija. Okrivljeni su priznali izvršenje krivičnog dela i potpisivali sporazume o priznanju krivice sa tužilaštvom, koje je sud potvrđivao pomenutim presudama.

Presude nakon glavne rasprave

Viši sud u Beogradu je u navedenom periodu doneo ukupno 15 odluka za krivično delo iz člana 185 KZ-a. U istom periodu je Apelacioni sud u Beogradu doneo sedam presuda po žalbama na prvostepene odluke. U nastavku sledi tabelarni prikaz presuda donetih u prvom stepenu.

REDNI BROJ	BROJ PREDMETA	DATUM ODLUKE	ČLAN/OVI KZ KOJI SU OKRIVLJENIMA STAVLJENI NA TERET	DA LI SU OKRIVLJENI OSUĐENI
1	Kpo3-6/2022	12.12.2022.	185/1; 185/3	Da
2	Kpo3-10/2022	16.06.2022.	185/4	Da
3	Kpo3-20/2023	29.05.2023.	135/1; 185/2 i 185/4	Da
4	Kpo3-21/2021	08.11.2022.	185/4	Ne
5	Kpo3-22/2022	01.06.2023.	185/1	Da
6	Kpo3-27/2022	15.11.2022.	135/1; 135/2 i 185/2	Da
7	Kpo3-31/2022	29.6.2022	185/4	Ne
8	Kpo3-38/2021	28.06.2022.	185/4	Da
9	Kpo3-45/2022	27.10.2022.	185/4	Da
10	Kpo3-48/2022	08.11.2022.	185/4	X
11	Kpo3-64/2021	15.07.2022.	185/4	Da
12	Kpo3-81/2021	13.02.2023.	185/2	Ne
13	Kpo3-82/2021	20.12.2022.	185/4	Da
14	Kpo3-85/2021	14.07.2022.	185/4	Da
15	Kpo3-36/2021	09.03.2023.	185/4	Da

Od tri predmeta u kojima okrivljeni nisu osuđeni, u dva je nastupila apsolutna zastarelost krivičnog gonjenja, dok u predmetu Kpo3-81/2021 nisu ostvarena bitna obeležja krivičnog dela jer okrivljeni nije mogao da zna koliko godina ima oštećena, zbog čega je izostao umišljaj kao bitan element krivičnog dela.

Izrečene sankcije u prvostepenom postupku su predstavljene u sledećoj tabeli:

REDNI BROJ	BROJ PREDMETA	IZREČENA KAZNA	IZREČENA MERA BEZBEDNOSTI	IZREČENA MERA ZABRANE	ČLAN 7 - POSEBNE MERE
1	Kpo3-6/22	Jedinstvena uslovna osuda od godinu dana (tri godine provere)	Oduzimanje telefona	Ne	Ne
2	Kpo3-10/2022	Novčana kazna od 100.000 RSD,na 4 rate	Oduzimanje laptopa i dva hard diska	Ne	Ne
3	Kpo3-20/2023	godinu dana kućnog zatvora uz elektronski nadzor	Oduzimanje telefona	Zabrana približavanja i komunikacije sa oštećenim na 100 metara	Da
4	Kpo3-21/2021	Nije osuđen zbog nastupanja apsolutne zastarelosti	Oduzimanje hard diska	X	X
5	Kpo3-22/2022	zatvor, 4 meseca	Ne	Ne	Da
6	Kpo3-27/2022	Jedinstvena kazna, dve godine zatvora	Oduzimanje telefona	Proterivanje stranaca iz zemlje na period od pet godina	Da
7	Kpo3-31/2022	Nije osuđen zbog nastupanja apsolutne zastarelosti	X	X	X
8	Kpo3-38/2021	Deset meseci kućnog zatvora uz elektronski nadzor	Oduzimanje 10 komada DVD i jedan HD	X	Da
9	Kpo3-45/2022	Uslovna osuda od godinu dana (tri godine provere)	Oduzimanje telefona i 2 Hard diska	Ne	Da

REDNI BROJ	BROJ PREDMETA	IZREČENA KAZNA	IZREČENA MERA BEZBEDNOSTI	IZREČENA MERA ZABRANE	ČLAN 7 - POSEBNE MERE
10	Kpo3-48/2022	Nije osuđen	Obavezno psihijatrijsko lečenje na slobodi (ne duže od tri godine) i oduzimanje predmeta (laptop, telefon, Hard disk, kartice)	Ne	Ne
11	Kpo3-64/2021	Uslovna osuda od godinu dana (tri godine provere)	Oduzimanje telefona	Ne	Ne
12	Kpo3-81/2021	Nije osuđen	X	X	X
13	Kpo3-82/2021	Zatvor u trajanju od jedne godine	Oduzimanje dva telefona	Ne	Da
14	Kpo3-85/2021	Zatvor u trajanju od jedne godine i osam meseci	Oduzimanje laptopa i telefona	Ne	Ne
15	Kpo3-36/2021	Uslovna osuda na deset meseci (dve godine provere)	Oduzimanje laptopa i hard diska	Ne	Da

Prilikom uzimanja u obzir otežavajućih okolnosti, sudovi su samo u dva predmeta našli njihovo postojanje; u predmetu Kpo3-27/2022 sud je cenio bezobzirnost u izvršenju dela, izazivanje uznemirenosti i straha i korišćenje naivnosti i lakomislenosti oštećenih, dok je u predmetu Kpo3-85/2021 sud posebno cenio upornost u vršenju inkriminisane radnje i prikupljanje fotografija beba.

Sa druge strane, u oceni olakšavajućih okolnosti, u devet presuda je sud kao olakšavajuće okolnosti uzimao korektno držanje pred sudom, zaposlenost, obavezu samoizdržavanja, mladost izvršilaca, neosuđivanost, okolnost da se oštećeni nisu pridružili krivičnom gonjenju ili isticali imovinskopravni zahtev, priznanje izvršenog dela, iskreno kajanje i svest o greškama; zdravstvene probleme, visinu primanja, okolnost da okrivljeni ima maloletno dete i manju količinu posedovanog materijala koja je pronađena kod okrivljenog.

Sedam drugostepenih odluka je predstavljeno u sledećoj tabeli:

REDNI BROJ	BROJ PRVOSTEPENOG PREDMETA	BROJ DRUGOSTEPENOG PREDMETA	DRUGOSTEPENA ODLUKA
1	Kpo3-10/2022	Kž1 Po3 - 20/2022	Tri meseca kućnog zatvora uz elektronski nadzor i izricanje mere iz člana 7 Zakona; po mišljenju žalbenog veća, pogrešno su primenjene odredbe o ublažavanju kazne i prevelik značaj je dat olakšavajućim okolnostima.
2	Kpo3-21/2021	Kž1 Po3-7/2023	Preinačeno jer je žalbeno veća zaključilo da je zastarelost krivičnog gonjenja ranije nastupila.
3	Kpo3-27/2022	Kž1 Po3 - 3/2023	Jedinstvena kazna zatvora od tri godine; po stavu žalbenog veća, nedovoljan značaj dat otežavajućim okolnostima.
4	Kpo3-82/2021	Kž2 Po3-1/2023	Odlukom je ukinuto prvostepeno rešenje koje se odnosi na pritvor, uvažena je žalba branioca i predmet vraćen na ponovno odlučivanje.
5	Kpo3-85/2021	Kž1 Po3-21/2022	Kazna smanjena na godinu dana kućnog zatvora, izrečene mere iz člana 7 Zakona, a zdravstveno stanje je uzeto kao dodatna olakšavajuća okolnost.
6	Kpo3-36/2021	Kž1 Po3-17/2023	Otklonjene sankcije iz člana 7 Zakona.
7	Kpo3-23/2022	Kž1 Po3-10/2023	Izrečena uslovna osuda od tri meseca (godinu dana provere). Prvostepenom presudom je izrečena kazna od godinu dana kućnog zatvora, oduzimanje predmeta i mere iz člana 7 Zakona.

Drugostepene odluke pokazuju da su u dva predmeta kazne preinačene na štetu okrivljenih, dok je u preostalim predmetima, odluka žalbenog veća bila u njihovu korist.

Zaključak analize domaće sudske prakse

Iz sadržine dostavljenih presuda, može se zaključiti da sudovi ne pridaju poseban značaj, niti prave bilo kakvu razliku između krivičnih dela iz korpusa visokotehnološkog kriminala i krivičnih dela koja ne spadaju u ovaj korpus. Ne može se uočiti da sudovi posebnu pažnju obraćaju na specifičnosti obeležja ovih krivičnih

dela, niti da adekvatno cene sve okolnosti i štetne posledice koje ona mogu izazvati. To se posebno vidi kod ocene olakšavajućih okolnosti prilikom odmeravanja sankcije učiniocima krivičnog dela, gde se npr. kao olakšavajuća, uzima okolnost da okrivljeni ima maloletno dete ili da je kod njega pronađena manja količina posedovanog (pornografskog) materijala.

Razloge za ovakve propuste bi, između ostalog, trebalo tražiti u izostanku posebnih znanja iz oblasti informatičkih tehnologija. Za razliku od tužilaštva (oformljenog kao posebno tužilaštvo za ovu oblast) koje je navelo da su ova znanja sticana kako kroz praksu tužilaca, tako i kroz višegodišnje obuke organizovane od strane domaćih i međunarodnih organizacija, Viši sud ne da nema specijalizovana odeljenja za ovu oblast, već ne zahteva ni posedovanje posebnih znanja iz ove oblasti. Ovakva praksa Višeg suda očigledno nije u skladu sa odredbama Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala koji u članu 11 izričito propisuje obrazovanje Odeljenja za borbu protiv visokotehnološkog kriminala. Istim članom zakona je propisano da sudije u ovo odeljenje raspoređuje predsednik Višeg suda i da prednost imaju sudije koje poseduju posebna znanja iz oblasti informatičkih tehnologija, zbog čega se ne može zaključiti da Viši sud u Beogradu postupa saglasno imperativnoj normi.

Posledica izostanka akta koji bi definisao posebna znanja iz ove oblasti i neusklađenosti sa Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala vidljiva je kroz sudske odluke, s obzirom na to da sudije ovim postupcima ne pristupaju značajnije od bilo kog drugog postupka, uprkos činjenici da su ova krivična dela u očiglednoj ekspanziji. Formiranje posebnog tužilaštva za borbu protiv visokotehnološkog kriminala bi trebalo da bude praćeno i formiranjem posebnog odeljenja suda za ovu oblast, uz insistiranje na posedovanju posebnih znanja o informatičkim tehnologijama, saglasno zahtevu koji postavlja pomenuti član 11 Zakona.

U svim predmetima u kojima su bili ispunjeni uslovi, sud je izrekao mere bezbednosti oduzimanja predmeta, dok su mere zabrane (u okviru mera bezbednosti) izrečene u svega dva predmeta, s tim što se samo jedan od njih odnosio na zabranu približavanja i komunikacije sa oštećenim. S obzirom na prirodu krivičnog dela, posebno dela iz člana 185 KZ-a, utisak je da se mera zabrane približavanja i komunikacije sa oštećenim nedovoljno često izriče. Sa druge strane, u gotovo svim predmetima su sudovi izrekli i posebne mere iz člana 7 Zakona o posebnim merama za sprečavanje vršenja krivičnih dela protiv polne slobode prema maloletnim licima, što zaslužuje pozitivnu ocenu u radu suda.

U konačnom, presude ne pokazuju da postoji bilo kakav afirmativan odnos suda prema žrtvama, posebno onima koji su bili žrtve deljenja pornografskog sadržaja. Naprotiv, u nekoliko presuda je sud, kao olakšavajuću okolnost prilikom odmeravanja

sankcije, uzimao u obzir to što se oštećeni nisu pridružili krivičnom gonjenju, niti su isticali imovinskopravni zahtev, što se teško može racionalno opravdati. Okolnost da žrtve pornografije ne žele da istaknu imovinskopravni zahtev ne bi trebalo nužno smatrati olakšavajućom okolnošću za okrivljenog, već pre posledicom toga da oštećeni ne žele da se pojavljuju u javnosti na bilo koji način koji bi ih dodatno stigmatizovao, posebno ako uzmemo u obzir činjenicu da je reč o maloletnim licima. Stoga bi ovaj pristup suda trebalo razmotriti i iz ugla oštećenih i ličnih razloga zbog kojih se ne pridružuju gonjenju, niti ističu odštetne zahteve.

Praksa Evropskog suda za ljudska prava

Pitanjem visokotehnološkog kriminala, Evropski sud za ljudska prava (u daljem tekstu: ESLJP) se, u najvećoj meri, bavio kroz povredu prava na poštovanje privatnog i porodičnog života zagarantovanog članom 8 Evropske konvencije o ljudskim pravima (u daljem tekstu: EKLJP). Iako praksa suda nije prebogata, ona ipak datira iz perioda od pre par decenija, zbog čega se može zaključiti da je ESLJP izgradio određene standarde u zaštiti privatnog života pojedinaca.

Jedna od najstarijih presuda je doneta 2008. godine (po predstavci iz 2002. godine) u predmetu *K.U protiv Finske*[44] gde je nepoznato lice 1999. godine postavilo oglas seksualne prirode na internet stranici za upoznavanje u ime podnosioca predstavke, koji je u to vreme imao 12 godina, bez njegovog znanja. U oglasu su bile navedene pojedinosti o uzrastu, godini rođenja i fizičkim osobinama podnosioca predstavke i da on želi da stupi u intimni odnos sa osobom muškog pola. Oglas je sadržao link ka njegovoj internet stranici, na kojoj se nalazila njegova fotografija i broj telefona. Podnosilac predstavke je saznao za oglas kada je primio elektronsku poruku od jednog muškarca koji mu je predlagao da se sastanu. Podneta je prijava policiji, ali je pružalac internet usluga odbio da otkrije identitet osobe koja je postavila oglas jer je smatrao da mora da se pridržava pravila o tajnosti. Sud je predstavku razmatrao iz ugla člana 8 EKLJP, s obzirom na moguću opasnost po njegovu fizičku i psihičku dobrobit i osetljiv uzrast. Postavljanje internet oglasa o podnosiocu predstavke je, po stavu ESLJP-a, predstavljalo krivično delo koje je dovelo do toga da je ovaj maloletnik postao meta pedofila. Takvo ponašanje je iziskivalo krivičnopravnu reakciju i delotvorno odvraćanje mogućih učinilaca od vršenja krivičnog dela putem odgovarajuće istrage i gonjenja. Deca i ostali osetljivi pojedinci imaju pravo na zaštitu države od tako ozbiljnog mešanja u njihov privatni život, dok mogućnost dobijanja odštete od treće strane, u ovom slučaju pružaoca usluga, nije predstavljalo dovoljan pravni lek. Morao je da postoji pravni lek koji bi omogućio utvrđivanje identiteta i privođenje pravdi stvarnog učinioca dela (lica koje je postavilo oglas) i žrtvi omogući da od njega dobije materijalnu odštetu. Država po zaključku suda, nije mogla da tvrdi da nije imala mogućnost da uvede sistem zaštite dece od pedofila na internetu s obzirom na to da je u vreme kada se ovaj incident dogodio već bila opšte poznata rasprostranjenost problema seksualnog zlostavljanja dece i

[44] Dostupna na: https://hudoc.echr.coe.int/?i=001-89964

opasnosti od upotrebe interneta u kriminalne svrhe. Država stoga nije zaštitila pravo podnosioca predstavke na poštovanje njegovog privatnog života, pošto je dala prvenstvo zahtevima o poverljivosti nad njegovom fizičkom i moralnom dobrobiti.

U presudi *Söderman protiv Švedske*[45] od 12. novembra 2013. godine, podnositeljka predstavke se pritužila sudu zbog propusta države da ispuni svoju obavezu prema članu 8 EKLJP da joj obezbedi pravne lekove kojima bi zaštitila lični integritet protiv svog očuha koji je pokušao da je tajno snimi golu u kupatilu kada je imala 14 godina, uz istovremeno pozivanje na povredu člana 13 Konvencije. Sud je zaključio da relevantni zakonski propisi koji su bili na snazi u to vreme u Švedskoj, nisu obezbedili adekvatnu zaštitu prava podnositeljke predstavke na poštovanje njenog privatnog i porodičnog života, kada je očuh podnositeljke pokušao da je snimi golu u svom kupatilu u seksualne svrhe. Predmetni čin je, po stavu suda, narušio integritet podnositeljke predstavke, što je dodatno otežano činjenicom da je ona bila maloletna, da se incident dogodio u njenoj kući gde je trebalo da se oseća bezbedno, da je izvršilac bio njen očuh – osoba od koje je očekivala poverenje. Kako zakonodavni okvir nije pružio podnositeljki ni krivični, ni građanski pravni lek kojim bi mogla da ostvari efikasnu zaštitu u konkretnim okolnostima slučaja, ESLJP je utvrdio povredu prava iz člana 8 EKLJP.

Predstavka u predmetu *Buturugă protiv Rumunije*[46] razmatrana je u presudi od 11. februara 2020. godine kojom se podnositeljka pritužila na povredu člana 3 i člana 8 EKLJP. Predstavka je podneta zbog povrede pozitivne obaveze države da obezbedi poštovanje njene prepiske, odnosno zbog propusta organa vlasti da sprovedu delotvornu istragu o sajbernasilju kao obliku nasilja u porodici, pošto je suprug podnositeljke presreo njenu privatnu prepisku i sačuvao je. Sud je zaključio da tvrdnje podnositeljke predstavke da je njen bivši suprug nezakonito presreo, koristio i sačuvao njenu elektronsku prepisku, nisu meritorno ispitane od strane organa vlasti, jer nisu preduzete mere u cilju prikupljanja dokaza koji bi omogućili da se utvrdi istinitost činjenica ili njihova pravna kvalifikacija. ESLJP je smatrao da su nacionalne vlasti formalistički pristupile slučaju kada su odbacile bilo kakve veze sa incidentima nasilja u porodici na koje je podnositeljka skrenula pažnju, pa su samim tim i propustili da uzmu u obzir mnoge oblike koje nasilje u porodici može imati, uključujući i sajbernasilje.

Citirane presude pokazuju da je polje koje bi trebalo štititi krivičnopravnim odredbama daleko šire od onog na šta se fokusiraju domaći sudovi. Visokotehnološki kriminal, po mišljenju ESLJP-a, zadire mnogo dublje u sve sfere života i to ne samo u pribavljanje ili posedovanje pornografskog materijala, već ima i brojne druge pojavne oblike koji se očigledno ignorišu u srpskom pravosuđu. I u ovom slučaju bi razloge

[45] Dostupno na: https://hudoc.echr.coe.int/?i=001-128043

[46] Dostupna na: https://hudoc.echr.coe.int/?i=001-201342

trebalo tražiti u izostanku adekvatnog znanja o informatičkim tehnologijama, ali i restriktivnoj i formalističkoj primeni prava. Takav pristup za posledicu ima potpuno skrajnutu žrtvu u krivičnom postupku koja, uz odsustvo dosuđivanja odštetnog zahteva tokom samog krivičnog postupka i upućivanje u parnicu da tamo ostvari svoj imovinskopravni zahtev, vodi sekundarnoj, pa i tercijarnoj viktimizaciji upravo onih zbog kojih je postupanje okrivljenih i ustanovljeno kao krivično delo.

Zaključak i preporuke

Iako je Republika Srbija potpisivanjem i ratifikacijom Konvencije Saveta Evrope i njenih Dopunskih protokola postigla značajan napredak u usaglašavanju svog zakonodavstva sa Evropskim, naredni koraci su jednako značajni – usaglašavanje domaćih propisa, kao i primena istih. Dok je materijalno krivično pravo u znatnoj meri prilagođeno zahtevima navedenih akata, procesne odredbe i dalje predstavljaju problematičnu oblast. Zakon o krivičnom postupku ne samo da ne sledi smernice Konvencije i Dopunskih protokola, već se njegove odredbe često suprotstavljaju odredbama drugih zakona, što otežava njihovu primenu u praksi i ostavlja prostor za nesavesno postupanje pravosudnih organa.

Rezultati ovog istraživanja pokazali su da u Višem sudu u Beogradu trenutno ne postoji posebno Odeljenje za borbu protiv visokotehnološkog kriminala, što direktno protivreči ZVTK, koji je još pre 18 godina propisao osnivanje ovog odeljenja. Takođe, ostaje nejasno zašto zakonodavac nije propisao osnivanje posebnog odeljenja Apelacionog suda kao drugostepenog organa u ovim postupcima. Bez obzira na motivaciju, potrebno je razmotriti osnivanje ovakvog odeljenja u Apelacionom sudu, čime bi se postigao viši nivo stručnosti u sudskim postupcima vezanim za visokotehnološki kriminal.

Analiza sudske prakse pokazuje da sudije ne pridaju poseban značaj postupcima iz oblasti visokotehnološkog kriminala, u odnosu na ostale krivične postupke. Sama činjenica da je zakonodavac odredio da ovim postupcima treba da se bave tužioci i sudije koji poseduju istaknuta znanja iz oblasti informacionih tehnologija pokazuju da su ovi postupci specifični i da im treba pristupiti sa posebnom pažnjom i stručnim znanjem. Stoga ističemo uregentnu potrebu za donošenjem pravilnika, akta ili neke druge odluke koja će propisati šta se podrazumeva pod „posebnim znanjima u oblasti informacionih tehnologija“, kako se ova znanja stiču, kao i kako se vrši ocena znanja javnih tužioca i sudija. Imajući u vidu da se oblast informacionih tehnlogija ubrzano razvija, kao i da su učinioci dela iz ovog korpusa često korak ispred kada su u pitanju tehnička znanja i mogućnosti, neophodno je da se predstavnici pravosudnih organa koji postupaju u ovim predmetima konstantno usavršavaju i prate nove međunarodne trendove u ovoj oblasti.

Uporedo sa borbom protiv visokotehnološkog kriminala, nepohodno je jačati i standarde informacione bezbednosti. U trenutku objavljivanja ove analize, Odsek za informacionu bezbednost i elektronsko poslovanje u Sektoru za informaciono društvo kojim rukovodi Ministarstvo informisanja i telekomunikacija ima samo dva inspektora nadležna za celu teritoriju Republike Srbije (za razliku od prethodne godine, kada je imao jednog inspektora). Iako su kapaciteti i dometi ovog odseka upitni, dodatni problem predstavlja vrlo siromašna praksa prijavljivanja bezbednosnih incidenata, te je pitanje u kojoj meri je javnost uopšte upoznata sa stvarnim stanjem u ovoj oblasti. U susret usvajajnju novog Zakona o informacionoj bezbednosti[47], bitno je insistirati na transparentnom postupanju svih organa koji se bave ovom oblašću, naročito u smislu obaveštavanja javnosti o incidentima koji su se dogodili, poštovanju postojećih zakonodavnih rešenja, adekvatnom vršenju nadzora nad primenom ovog zakona, kao i reagovanju na povrede, utvrđivanju odgovornosti i sprovođenju propisane kaznene politike.

[47] U trenutku objavljivanja ove analize, još uvek je u formi nacrta.

Prilog

КОНТРОЛНА ЛИСТА

Контрола ИКТ система од посебног значаја

Закон о информационој безбедности и прописи донети на основу њега

КЛ-001-03/07

Датум усвајања на седници Координационе комисије:

Врсте инспекцијског надзора	Редовни	☐
	Ванредни	☐
	Допунски	☐
	Контролни	☐
Почетак инспекцијског надзора	Датум:	
	Време:	
Пословно име надзираног субјекта		
Адреса седишта надзираног субјекта	Место	
	Улица	
	Поштански број	
Подаци о надзираном субјекту	Телефон	
	Емаил	
	Матични број	
	ПИБ	
	Одговорно лице	
Назив/ознака огранка надзираног субјекта		
Адреса огранка надзираног субјекта	Место	
	Улица	
	Поштански број	

Подаци о огранку надзираног субјекта	Телефон	
	Емаил	
Представници надзираног субјекта присутни инспекцијском надзору		

Р.Б.	ПИТАЊА	ОДГОВОРИ		БОДОВИ
1.	Да ли је донет Акт о безбедности?	Да	☐	
		Не	☐	
2.	Да ли је Акт о безбедности донет у складу са постојећим прописима? [48]	Да	☐	
		У већој мери	☐	
		У мањој мери	☐	
		Не	☐	
3.	Да ли су примењене мере заштите?	Да	☐	
		У већој мери	☐	
		У мањој мери	☐	
		Не	☐	
4.	Да ли је извршена годишња провера усклађености примењених мера заштите?	Да	☐	
		Не	☐	
5.	Да ли је извештај о годишњој провери ИКТ система од посебног значаја сачињен у складу са прописима?	Да	☐	
		Не	☐	
6.	Да ли је извршен упис у Евиденцију оператора ИКТ система од посебног значаја?	Да	☐	
		Не	☐	
7.	Да ли су Националном ЦЕРТ-у достављени тачни статистички подаци о инцидентима у ИКТ систему у складу са чланом 11б Закона о информационој безбедности?	Да	☐	
		Не	☐	
УКУПНО БОДОВА				
УТВРЂЕНИ СТЕПЕН РИЗИКА				

[48] Акт о безбедности, његова структура и садржина уређују се чланом 8. Закона о информационој безбедности („Службени гласник РС“, бр. 6/16, 94/17 и 77/19) и Уредбом о ближем садржају Акта о безбедности ИКТ система од посебног значаја, начину провере и садржају извештаја о провери безбедности ИКТ система од посебног значаја („Службени гласник РС“, број 94/16)

БОДОВНА ЛИСТА И СТЕПЕН РИЗИКА		
Питање број 1	Да	15 бодова
	Не	0 бодова
Питање број 2	Да	20 бодова
	У већој мери	15 бодова
	У мањој мери	5 бодова
	Не	0 бодова
Питање број 3	Да	25 бодова
	У већој мери	20 бодова
	У мањој мери	5 бодова
	Не	0 бодова
Питање број 4	Да	10 бодова
	Не	0 бодова
Питање број 5	Да	10 бодова
	Не	0 бодова
Питање број 6	Да	5 бодова
	Не	0 бодова
Питање број 7	Да	5 бодова
	Не	0 бодова
Степен ризика	72-90	Незнатан
	56-71	Низак
	36-55	Средњи
	21-35	Висок
	0-20	Критичан

Надзирани субјект **Инспектор**