BORBA PROTIV VISOKOTEHNOLOŠKOG KRIMINALA U SRBIJI

Dostignuća i izazovi

Marija Pavlović
Beogradski centar za bezbednosnu politiku

Beograd, maj 2022.

prEUgovor predlog praktične politike

B | T | D The Balkan Trust for Democracy
A PROJECT OF THE GERMAN MARSHALL FUND

Norway

BORBA PROTIV VISOKOTEHNOLOŠKOG KRIMINALA U SRBIJI

Dostignuća i izazovi

Marija Pavlović
Beogradski centar za bezbednosnu politiku

Beograd, maj 2022.

BORBA PROTIV VISOKOTEHNOLOŠKOG KRIMINALA U SRBIJI
DOSTIGNUĆA I IZAZOVI

Izdavači

Za koaliciju prEUgovor:

Transparentnost Srbija
Palmotićeva 31/III Beograd
www.transparentnost.org.rs

Beogradski centar za bezbednosnu politiku
Đure Jakšića 6/5, Beograd
www.bezbednost.org

Autorka
Marija Pavlović (Beogradski centar za bezbednosnu politiku)

Lektura
Tatjana Hadžić Jovović

Dizajn i prelom
Jelena Pejić Nikić

ISBN-978-86-84711-53-5

Publikacija je deo projekta *„PrEUgovor za vladavinu prava i EU integracije”* čije sprovođenje su omogućili Balkanski fond za demokratiju, projekat Nemačkog Maršalovog fonda SAD, i Ambasada Kraljevine Norveške u Beogradu. Stavovi izraženi u publikaciji ne odražavaju nužno stavove navedenih donatora ili njihovih partnera.

Uvod

Zvanična statistika ukazuje na porast broja slučajeva visokotehnološkog kriminala (VTK) u Srbiji. Prema Izveštaju Nacionalnog centra za prevenciju bezbednosnih rizika u informaciono-komunikacionom (IKT) sistemima (Nacionalni CERT), u Srbiji je tokom 2020. godine zabeleženo oko 26 miliona sajber napada na IKT sisteme koji imaju poseban značaj. Najzastupljenija grupa incidenata bila je pokušaj upada u IKT sistem i neovlašćeno prikupljanje podataka.[1] Od početka 2022. godine zabeleženo je nekoliko pokušaja prevara putem interneta, te krađe identiteta i podataka korisnika Rajfajzen banke i Pošte Srbije, a učestale su i pretnje upućene novinarima preko društvenih mreža. Poslednji u nizu je slučaj masovnih dojava putem imejla o postavljenim bombama u različitim javnim i privatnim ustanovama, kao što su bolnice, škole, aerodromi, železničke stanice, tržni centri, zoološki vrt itd. Iako su nadležni organi ustanovili da su bile lažne, dojave su uspele da zabrinu društvo i privremeno onemoguće normalan rad pogođenih institucija.

Visokotehnološki kriminal i sajber napadi postali su deo naše svakodnevice i može se očekivati da će pretnje upućene putem interneta i društvenih mreža u budućnosti biti intenzivirane i usložnjene, zbog čega je važno da državni organi budu spremi da brzo i učinkovito odgovore na sve izazove, rizike i pretnje, poštujući pritom ljudska prava i vladavinu prava. Od suštinskog značaja biće i saradnja državnih organa Srbije sa drugim državama i međunarodnim organizacijama, poput INTERPOL-a i EUROPOL-a, zbog anonimnosti napadača i prekograničnog karaktera ove vrste kriminala.

Beogradski centar za bezbednosnu politiku se temom visokotehnološkog kriminala bavi iz ugla pristupnih pregovora Srbije sa Evropskom unijom i praćenja napretka u klasteru 1 (Osnove), odnosno u Poglavlju 24 (Pravda, sloboda, bezbednost). U tom kontekstu predstavićemo dostignuća u pravnom i institucionalnom razvoju nadležnih organa u borbi protiv visokotehnološkog kriminala, analizu aktuelnih trendova i izazova u borbi protiv ove vrste kriminala u Srbiji.

[1] Napadi na IKT sisteme zabeleženi su u N-CERT-u radi statistike i eventualnog prikupljanja dokaza, a za krivično gonjenje tih napadača zadužено je Posebno tužilaštvo i Odeljenje za suzbijanje VTK-a MUP-a i na njih se odnose iste odredbe iz glave 27 Krivičnog zakonika.

Pravni i institucionalni okvir

Pravni okvir

Pravni okvir za borbu protiv VTK-a u Srbiji postoji još od 2005. godine, kada su, nakon potpisivanja Konvencije o visokotehnološkom kriminalu Saveta Evrope (Budimpeštanska konvencija), posebnim zakonom definisani pojam i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala.[2] Da bi ona bila usklađena sa strateškim i operativnim pristupom koji Evropska unija ima u ovoj oblasti, Vlada Srbije je prilagodila propise vršeći delimične ciljane promene pojedinih zakona, i to Krivičnog zakonika i Zakonika o krivičnom postupku. Krivični zakonik, koji je stupio na snagu 2005. godine, sadržao je 27. glavu pod nazivom „Krivična dela protiv bezbednosti računarskih podataka", koja obuhvata krivična dela VTK-a. Nakon ratifikacije Budimpeštanske konvencije 2009. godine, donesene su izmene i dopune Zakona o organizaciji i nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala, kao i izmene i dopune Krivičnog zakonika.

Krivična dela visokotehnološkog kriminala koja su propisana u Krivičnom zakoniku uslovno se mogu podeliti na dve grupe krivičnih dela – ona koja se odnose samo na VTK i ona koja imaju elemente VTK-a, ali nisu isključivo u nadležnosti organa specijalizovanih za suzbijanje visokotehnološkog kriminala (videti ispod). U prvu grupu spada osam krivičnih dela protiv bezbednosti računarskih podataka.[3] Druga grupa krivičnih dela je raznovrsnija i obuhvata krivična dela protiv intelektualne svojine (član 198, 199, 202), ali i pojedinačna krivična dela, kao što su ugrožavanje sigurnosti, najčešće putem društvenih mreža (član 138); neovlašćeno objavljivanje i prikazivanje tuđeg spisa, portreta i snimka (član 145); neovlašćeno prikupljanje ličnih podataka (član 146); prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju (član 185); iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnog dela protiv polne slobode prema maloletnom licu (član 185b); falsifikovanje i zloupotreba platnih kartica (član 243), kao i sva druga krivična dela ukoliko se kao sredstvo ili način izvršenja koriste računari ili računarske mreže.

Zakonik o krivičnom postupku propisuje dokazne radnje, koje se mogu primeniti u krivičnim postupcima za ova krivična dela. Zbog specifičnosti ovih krivičnih dela, ovaj zakon izmenjen je 2011. godine. Izmenama su definisani izrazi koji se koriste kada je reč o visokotehnološkom kriminalu, poput *elektronski zapis*, *elektronska adresa*, *elektronski dokument* i *elektronski potpis* (član 2, stav 29, 30, 31, 32). Pored toga nabrajaju se krivična dela u odnosu na koja se primenjuju posebne dokazne radnje (član 161 i 162), te za koja je posebnim zakonom određeno da postupa javno tužilaštvo posebne nadležnosti, u ovom slučaju Posebno tužilaštvo za borbu protiv VTK-a.[4]

[2] Konvencija o visokotehnološkom kriminalu Saveta Evrope doneta je 2001. godine, a stupila je na snagu 2004. godine. Srbija je Konvenciju potpisala 2005. godine i odmah je počela da radi na stvaranju pravnog okvira, ali je Konvenciju ratifikovala tek 2009. godine.

[3] Ova dela u Krivičnom zakoniku Republike Srbije obuhvataju sva krivična dela iz Glave 27, i to: 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 elektronskoj obradi podataka (član 302); sprečavanje i ograničavanje pristupa javnoj računarskoj mreži (član 303); neovlašćeno korišćenje računara ili računarske mreže (član 304), kao i pravljenje, nabavljanje i davanje drugom sredstva za izvršenje krivičnog dela protiv bezbednosti računarskih podataka (304a).

[4] Kada je reč o VTK-u, posebne dokazne radnje mogu se primenjivati za sledeća krivična dela iz ove oblasti: prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju (član 185, stav 2 i 3, KZ); neovlašćeno iskorišćavanje autorskog dela ili predmeta srodnog prava (član 199, KZ); oštećenje računarskih

Drugi zakoni značajni za ovu oblast su: Zakon o potvrđivanju Protokola uz Konvenciju o visokotehnološkom kriminalu, koji se odnosi na inkriminaciju dela rasističke i ksenofobične prirode izvršenih preko računarskih sistema; Zakon o potvrđivanju Konvencije Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja; Zakon o elektronskim komunikacijama; Zakon o informacionoj bezbednosti; Zakon o organizaciji i nadležnosti državnih organa u borbi protiv visokotehnološkog kriminala; Zakon o međunarodnoj pravnoj pomoći u krivičnim stvarima itd.

U kontekstu pristupanja Srbije Evropskoj uniji i usklađivanja sa njenim politikama i pravnim tekovinama, Vlada Srbije usvojila je 2018. godine i Strategiju za borbu protiv visokotehnološkog kriminala za period 2019–2023. i prateći Akcioni plan za sprovođenje Strategije za period 2019–2020. Akcioni plan je istekao 2020. godine, a Ministarstvo unutrašnjih poslova (MUP) u međuvremenu nije izradilo novi. Stručna javnost nije upoznata sa tim na koji način se Strategija sprovodi nakon što je istekao Akcioni plan, niti postoji mogućnost da se adekvatno oceni šta je u međuvremenu urađeno, budući da nema javno dostupnog izveštaja MUP-a. Sledeće godine ističe Strategija i malo je verovatno da će do tada biti usvojen novi Akcioni plan. Pored toga, Srbija je u maju 2022. bila među prvim potpisnicama Drugog dodatnog protokola uz Konvenciju o visokotehnološkom kriminalu o pojačanoj saradnji i otkrivanju elektronskih dokaza, koji je Savet Evrope odobrio krajem 2021. godine. Ratifikacija ovog Protokola podrazumeva dalje usklađivanje različitih propisa sa njegovim odredbama. Protokol je značajan, jer se njime jača saradnja država sa privatnim sektorom kako bi se zaštitila prava svih korisnika interneta i efikasnije prikupljali elektronski dokazi u skladu sa tehnološkim razvojem i novim pojavnim oblicima VTK-a. Zbog sve veće složenosti pribavljanja elektronskih dokaza, koji se mogu čuvati u različitim državama sa drugačijim pravnim sistemima, bilo je neophodno izraditi ovakav dokument.

Institucije nadležne za borbu protiv visokotehnološkog kriminala

U skladu sa Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visoko-tehnološkog kriminala, u okviru Višeg javnog tužilaštva u Beogradu 2007. godine osnovano je Posebno tužilaštvo za borbu protiv visokotehnološkog kriminala, koje ima nadležnost na celoj teritoriji Srbije. Do 2009. godine za suđenje u sporovima u oblasti VTK-a bilo je nadležno specijalizovano odeljenje u Višem sudu u Beogradu, dok je Apelacioni sud u Beogradu bio nadležan za odlučivanje u drugom stepenu. Kako je specijalizovano odeljenje Višeg suda u Beogradu prestalo da postoji 2009. godine, o predmetima visokotehnološkog kriminala sude sve sudije ovog suda i dobijaju ih i sva veća Apelacionog suda u Beogradu kao drugostepeni organ. Ukidanje specijalizovanog sudskog odeljenja dovelo je do brojnih problema u praksi. Najveći problem predstavlja to što u predmetima koji se odnose na VTK sude sudije koje nedovoljno razumeju tehnologiju i specifičnosti elektronskih dokaza. Nedovoljna obučenost sudija za suđenje u ovakvim predmetima, koji zahtevaju poznavanje terminologije vezane za VTK, dovodi do poteškoća tokom celog postupka. U praksi dolazi čak i do toga da se ceo postupak odbaci zbog nedovoljne digitalne pismenosti sudija i nepoznavanja specifičnosti materije.

podataka i programa (član 298, stav 3, KZ); računarska sabotaža (član 299, KZ); računarska prevara (član 301, stav 3, KZ); neovlašćeni pristup zaštićenom računaru, računarskoj mreži i elektronskoj obradi podataka (član 302, KZ).

Za borbu protiv VTK-a nadležno je i Ministarstvo unutrašnjih poslova, koje u okviru Sektora za borbu protiv organizovanog kriminala (SBPOK) ima posebno Odeljenje za suzbijanje visokotehnološkog kriminala. Odeljenje je osnovano 2008. godine i bilo je podeljeno na dva Odseka – Odsek za suzbijanje kriminaliteta u oblasti intelektualne svojine i Odsek za suzbijanje elektronskog kriminaliteta. Zbog pojave sve kompleksnijih i raznovrsnijih krivičnih dela visokotehnološkog kriminala, ovo odeljenje je 2019. godine reorganizovano i podeljeno na četiri odseka: Odsek za suzbijanje kriminaliteta u oblasti intelektualne svojine, Odsek za suzbijanje elektronskog kriminaliteta, Odsek za suzbijanje nedozvoljenih i štetnih sadržaja na internetu i Odsek za suzbijanje zloupotreba u oblasti elektronske trgovine, elektronskog bankarstva i platnih kartica na internetu. Odeljenje postupa prema zahtevima Posebnog tužilaštva, koje rukovodi predistražnim postupkom, ali i po zahtevima drugih tužilaštava ukoliko postoji potreba za prikupljanje i tumačenje dokaza koji su u elektronskom obliku. Podela unutar Odeljenja je važna, jer kompleksnost ovih krivičnih dela zahteva posebno obučen kadar policijskih službenika, koji će raditi na rasvetljavanju isključivo onih krivičnih dela za koje su specijalizovani.

Pored Posebnog tužilaštva i Odeljenja za suzbijanje visokotehnološkog kriminala u okviru MUP-a, postoje i drugi organi čije su nadležnosti značajne za ovu oblast. Ministarstvo pravde zaduženo je za usklađivanje domaćeg krivičnog zakonodavstva sa propisima Evropske unije. Ministarstvo finansija je u svojoj Upravi carina trebalo da stvori uslove za formiranje jedinice pod nazivom „Sajber carina" radi borbe protiv visokotehnološkog kriminala. Ona je trebalo da identifikuje krivična dela, koja su u suprotnosti sa carinskim propisima na internetu.[5] Međutim, ni Ministarstvo finansija ni Uprava carina do danas to nisu uradili. Takođe, Ministarstvo finansija ima i Upravu za sprečavanje pranje novca, koja je zadužena za prikupljanje, obradu i analizu podataka vezanih za pranje novca i finansiranje terorizma. Ukoliko pronađe dokaze o krivičnim delima, Uprava u skladu sa zakonom prosleđuje nadležnim organima informacije, podatke i dokumenta. Budući da je transakcije novca i malverzacije novcem moguće uraditi putem računara i računarskih sistema, ova Uprava ima značajnu ulogu u otkrivanju krivičnih dela visokotehnološkog kriminala.

Strategijom je još predviđeno i formiranje posebnih organizacionih jedinica za borbu protiv visokotehnološkog kriminala u sklopu Bezbednosno-informativne agencije (BIA) i Vojno-bezbednosne agencije (VBA). U skladu sa Zakonom o Bezbednosno-informativnoj agenciji, BIA je nadležna za suprotstavljanje svim oblicima visokotehnološkog kriminala ukoliko su njegove posledice takve da mogu destabilizovati nacionalnu bezbednost. Vojnobezbednosna agencija (VBA), u skladu sa Zakonom o Vojnobezbednosnoj agenciji i Vojnoobaveštajnoj agenciji, obavlja poslove bezbednosne i kontraobaveštajne zaštite Ministarstva odbrane i Vojske Srbije. U okviru toga obavlja i poslove otkrivanja, sprečavanja i dokazivanja krivičnih dela protiv bezbednosti računarskih podataka. Vojnobezbednosna agencija ovlašćena je i da sprovodi zaštitu IKT sistema Ministarstva odbrane i Vojske Srbije.

Značajnu ulogu u ovoj oblasti imaju i Narodna banka Srbije i Ministarstvo trgovine, turizma i telekomunikacija (MTTT), kao i Regulatorna agencija za elektronske komunikacije i poštanske usluge (RATEL). Narodna banka Srbije nadležna je za nadzor svih IKT sistema finansijskih institucija, koji su pod njenom kontrolom. Ministarstvo trgovine, turizma i telekomunikacija nadležno je za

[5] Obaveza propisana u Strategiji za borbu protiv visokotehnološkog kriminala za period od 2019–2013. godine, str. 26.

informacionu bezbednost u Srbiji, odnosno za bezbednost IKT sistema koji imaju poseban značaj. Pored ove nadležnosti, MTTT je osnovalo Nacionalni kontakt za bezbednost dece na internetu 19833, čiji je cilj podizanje svesti o opasnostima koje vrebaju decu na internetu. Ukoliko se krivično delo prijavi ovde, biće prosleđeno nadležnim organima za borbu protiv visokotehnološkog kriminala. U sklopu RATEL-a nalazi se Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (Nacionalni CERT). Nacionalnog CERT zadužen je za koordinaciju prevencije i zaštite od bezbednosnih rizika u IKT sistemima na nacionalnom nivou, kao i za prikupljanje i razmenu podataka o mogućim rizicima, te za obaveštavanje javnosti i lica koja upravljaju IKT sistemima o incidentima.

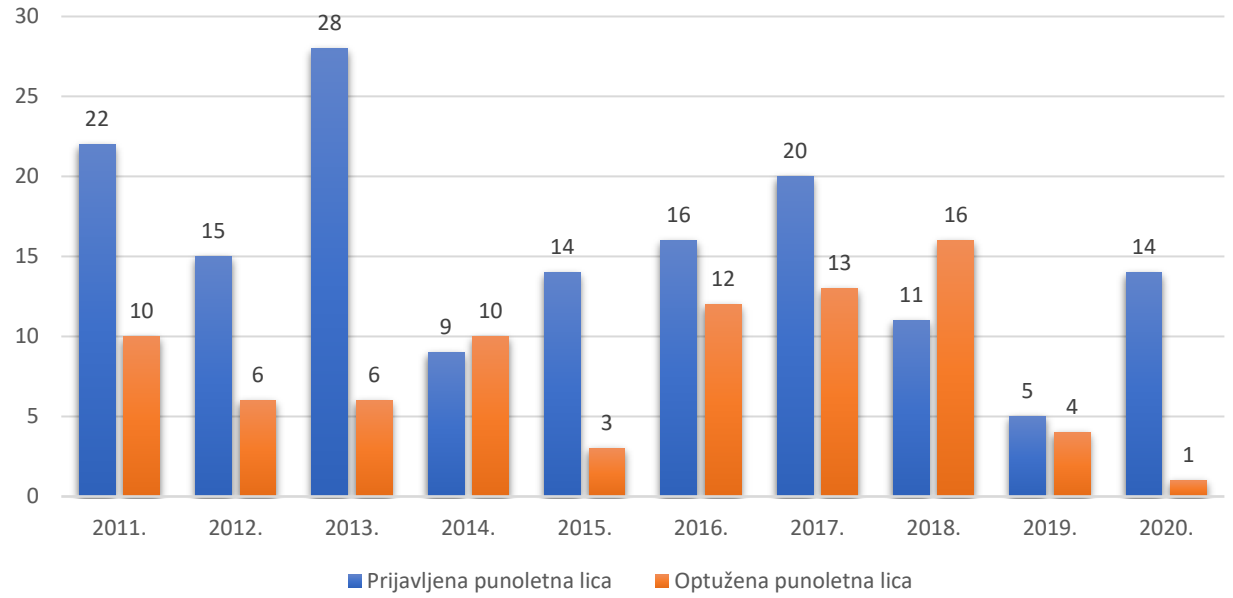
Saradnja nadležnih organa sa organizacijama civilnog društva (OCD) postoji, ali je ograničena na nekoliko međunarodnih i domaćih organizacija, kao što su organizacije *Save the children*, Fond B92 radi realizovanja projekta „Klikni bezbedno", te Fondacija Petlja i Centar za nestalu i zlostavljanu decu (nekadašnja Fondacija Tijana Jurić). Međutim, ostale zainteresovane organizacije civilnog društva nisu uključene u tu saradnju, kao što su, na primer, ženske organizacije, LGBTIQ organizacije, romske i druge organizacije koje se zalažu za prava marginalizovanih grupa u Srbiji. Organizacije civilnog društva ukazuju na različite oblike ugrožavanja prava i sloboda višestruko marginalizovanih grupa u Srbiji, uz korišćenje savremenih tehnologija, a strateški i pravni okvir u ovoj oblasti ne uočava uticaj savremene tehnologije na različite društvene grupe, osim na decu i mlade. Organizacije civilnog društva koje se bave ljudskim pravima smatraju da je to posledica nedovoljno inkluzivnog procesa izrade političkih dokumenata i zakonske regulative, jer te organizacije nisu ni konsultovane niti uključene u njihovu izradu u bilo kom obliku.[6]

Aktuelni trendovi u oblasti visokotehnološkog kriminala u Srbiji

Prema istraživanju Registra nacionalnog internet domena Srbije (RNIDS) za 2022. godinu, oko 74% građana Srbije koristi internet, što je povećanje od 25% u poslednjoj deceniji. Sa sve većim brojem korisnika interneta, računara i mobilnih uređaja i sa rastućom povezanošću putem interneta uvećavaju se i rizici po bezbednost. Prema izveštaju RNIDS, 41% korisnika interneta koji su doživeli napad ni ne zna ko su napadači, dok četvrtina korisnika ne zna ni da su bili meta sajber napada. Pored toga, treba navesti da većina građana Srbije nije upoznata sa time koje sve vrste dela spadaju u krivična dela VTK-a.

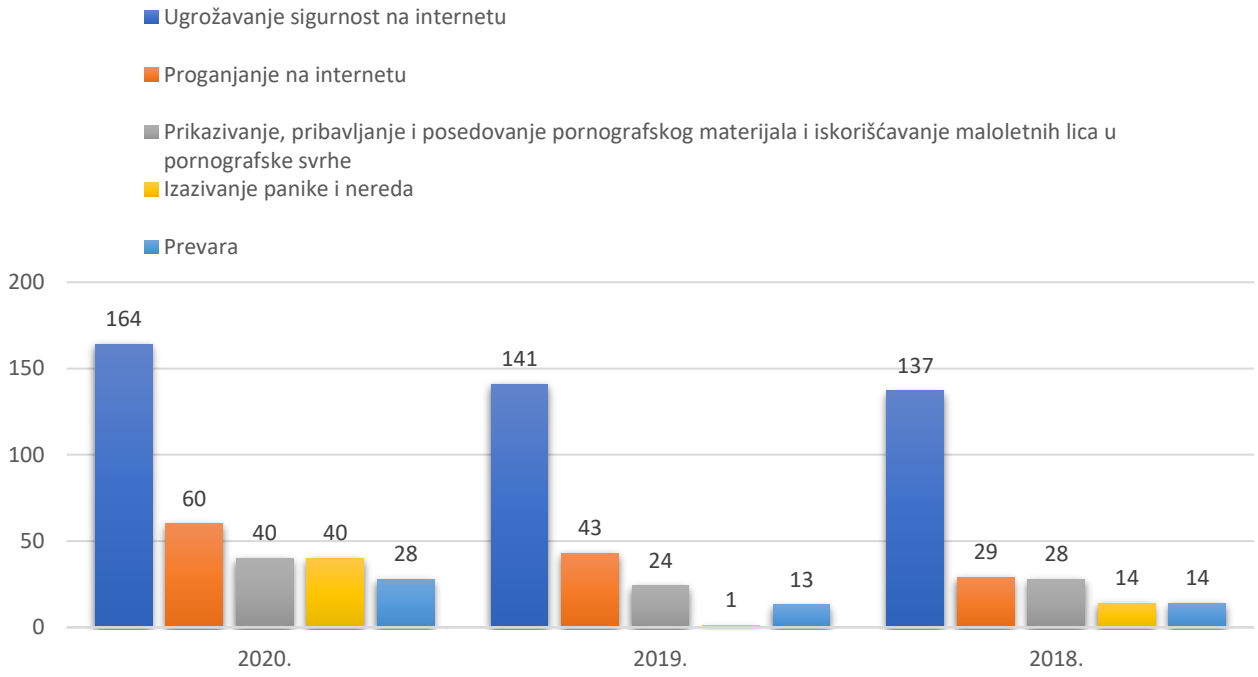
Na osnovu statistike MUP-a, primetan je i porast krivičnih dela povezanih sa VTK-om u Srbiji. U Izveštaju o stanju javne bezbednosti u radu MUP-a Republike Srbije navodi se da su 2018. godine otkrivena 622 krivična dela iz ove oblasti, 2019. godine policija je zabeležila 946 krivičnih dela, dok ih je 2020. godine otkriveno 760. Kada posmatramo samo krivična dela protiv računarskih podataka, uočavamo da postoji razlika između broja podnetih krivičnih prijava protiv punoletnih lica i broja optuženih lica (Grafikon 1).

[6] Intervju sa predstavnicama Autonomnog ženskog centra, mart 2022.



Grafikon 1. Punoletni učinioci krivičnih dela protiv računarskih podataka u RS, 2020.
Izvor: Republički zavod za statistiku

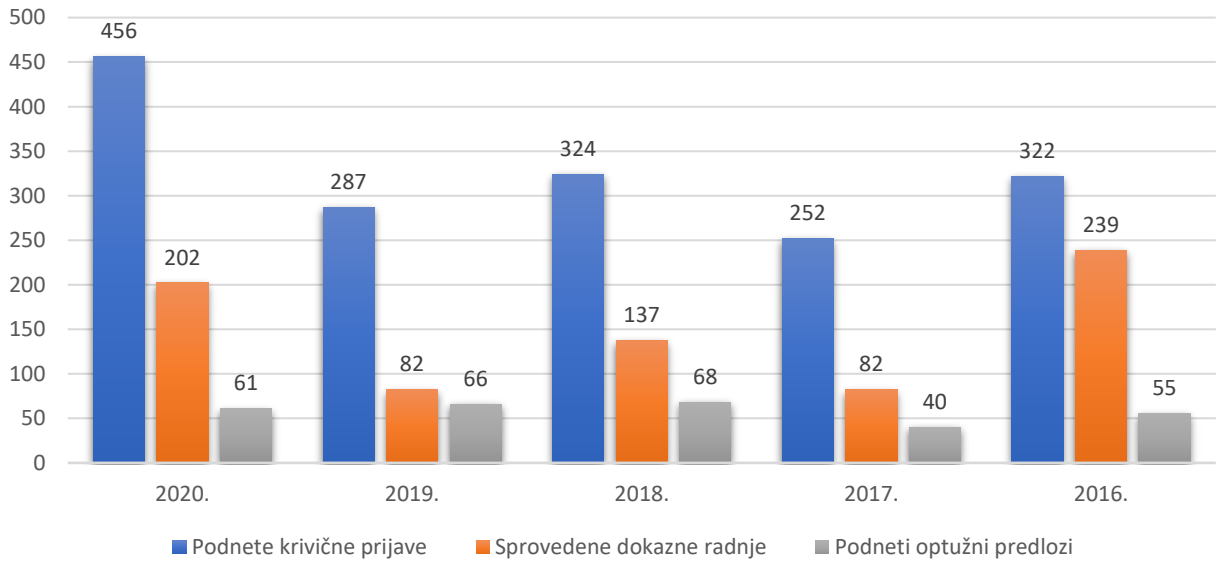
Razlika između broja podnetih krivičnih prijava i broja optuženih lica može se objasniti i time da u Posebnom tužilaštvu radi 14 zaposlenih, dok u Odeljenju za suzbijanje VTK-a rade 22 službenika policije, što je nedovoljno za prikupljanje dokaza, obradu i zavođenje tolikog broja predmeta. Pored nedostatka kadrovskih kapaciteta, treba napomenuti da nedostaju tehnički i prostorni kapaciteti Posebnog tužilaštva, što svakako utiče na njegov rad.



Grafikon 2. Pet najčešćih vrsta visokotehnološkog kriminala u Srbiji
Izvor: Republičko javno tužilaštvo

Krivično delo ugrožavanja sigurnosti je u poslednje tri godine u porastu u Srbiji. Ono ima elemente visokotehnološkog kriminala onda kada su pretnje upućene posredstvom društvenih mreža. U Srbiji je posebno ugrožena sigurnost branitelja ljudskih prava, (ekoloških) aktivista i novinara. Na primer, SHARE Fondacija na svom sajtu vodi evidenciju o ugrožavanjima digitalnih prava i sloboda, kao i o onlajn napadima na građane, javne ličnosti, novinare, aktiviste i branitelje ljudskih prava. U njihovom izveštaju stoji da su u poslednje tri godine (od januara 2019. do juna 2022. godine) podnete ukupno 92 krivične prijave protiv ugrožavanja sigurnosti ovih grupa ljudi. Napadi na pomenute društvene grupe postali su svakodnevica i gotovo su normalizovani, a glavni problem predstavlja nekažnjavanje ove vrste krivičnih dela, što samo dovodi do njegovog povećanja.

Pored ovog krivičnog dela, drugo najčešće krivično delo sa elementima VTK-a u Srbiji jeste zloupotreba dece u pornografske svrhe putem interneta (član 185). Prema „Proceni pretnje od organizovanog kriminala na internetu za 2021", koju je izradio EUROPOL, u Evropi se povećava količina materijala vezanog za eksploataciju dece u pornografske svrhe na mreži, što ozbiljno preopterećuje kapacitete policije i tužilaštava svih zemalja sveta, pa i Srbije.



Grafikon 3. Statistika o radu Posebnog tužilaštva za visokotehnološki kriminal
Izvori: Informator o radu Republičkog javnog tužilaštva za 2020, 2019, 2018, 2017 i 2016. godinu

Izazovi u borbi protiv visokotehnološkog kriminala u Srbiji

Razvojem nove tehnologije pojavljuju se novi oblici izazova, rizika i pretnji, koji nisu obuhvaćeni postojećim kaznenim zakonodavstvom. U praksi se pokazalo da postoji potreba za uvođenje izmena i dopuna Krivičnog zakonika kako bi se dodala pojedina krivična dela VTK-a. Na primer, osvetnička pornografija u srpskom zakonodavstvu nije označena kao krivično delo, iako bi, prema posledicama koje žrtva i društvo trpe, morala da bude. Postoje inicijative da se to delo definiše i unese u Krivični zakonik Republike Srbije. S obzirom na to da su do kraja 2022. godine planirane izmene i dopune Krivičnog zakonika, koalicija prEUgovor sačinila je predlog amandmana, kojima se, između ostalog, predlaže dodavanje novog krivičnog dela u Glavi 14 – Krivična dela protiv slobode i prava čoveka i građanina. Iza člana 145 bio bi dodat član 145a pod nazivom „zloupotreba

snimka polne sadržine". Predloženom izmenom sankcionisalo bi se veoma rasprostranjeno delo, koje ima velike i nadoknadive posledice po žrtve.[7]

Dobro zakonsko rešenje bilo bi da se neovlašćeno prikupljanje podataka o ličnosti, koje u nekim slučajevima poprima i masovne razmere, goni po službenoj dužnosti, umesto da se tereti po privatnoj tužbi.[8] Po važećem zakonodavstvu, žrtvama ovog krivičnog dela prepušteno je da samostalno traže dokaze o izvršenom krivičnom delu od privatnih firmi. Privatne firme nisu u obavezi to da učine i mogu da uskrate fizičkim licima tražene informacije i dokaze. To otežava prikupljanje dokaza i dovodi do toga da oštećene strane najčešće odustanu od krivičnog gonjenja.

Kada je reč o kapacitetima nadležnih organa za borbu protiv VTK-a, u prethodnom periodu ojačani su kapaciteti Posebnog tužilaštva. Tužilaštvo sada ima specijalnog tužioca za VTK, pet zamenika specijalnog tužioca, pet pomoćnika specijalnog tužioca i tri službenika koji se bave administrativnim poslovima. Dakle, ima ukupno 14 zaposlenih, kojima je, zbog povećanja broja predmeta, neophodno obezbediti veći kancelarijski prostor kako bi mogli normalno da rade. Posebno tužilaštvo u izveštajima o radu iz 2018, 2019. i 2020. godine navodi da *trenutna tehnička opremljenost Posebnog tužilaštva ne odgovara zahtevima koji se nameću u bavljenju tužilačke funkcije u okviru predistražnog postupka, a koji se ogledaju u potrebi za vršenjem uvida u dokazni materijal koji je obezbeđen u toku krivičnog postupka*. To znači da Posebno tužilaštvo, pored toga što nema dovoljan broj ljudi i smeštajnih kapaciteta, nema ni tehničke mogućnosti za adekvatno obavljanje poslova.

Iako dobar pravni okvir postoji više od deset godina, ograničeni resursi za borbu protiv VTK-a troše se mahom na krivična dela ugrožavanja sigurnosti putem društvenih mreža, gde policija prati delovanje lica koja na društvenim mrežama postavljaju negativne komentare o političarima.[9] Ova vrsta politizacije policije utiče na aktivnosti i praktičan rad Odeljenja, ali i na rad Posebnog tužilaštva, usled čega razna krivična dela ostaju neotkrivena. Osim smanjenja uticaja politike na operativni rad policije, veliki izazov predstavlja i borba protiv niskog nivoa znanja i nedovoljne upoznatosti sa procedurama policijskih službenika izvan Odeljenja za suzbijanje VTK-a, pogotovo na lokalu gde, usled nedovoljnog znanja policijskih službenika o krivičnim delima iz oblasti VTK-a, dolazi do odvraćanja građana da prijave takvo krivično delo.

Konačno, veliki izazov u borbi protiv visokotehnološkog kriminala predstavlja i nizak nivo bezbednosne kulture građana Srbije, odnosno nepostojanje svesti građana o problemu i mogućnostima za zaštitu od ovog vida kriminala. Nadležni organi ulažu napore da podignu stepen informisanosti stručne i šire javnosti o opasnostima VTK-a i njegovom uticaju na društvo, ali to nije dovoljno, jer su rizici od te vrste kriminala u stalnom porastu.

[7] Početkom 2021. godine u Srbiji je u javnost izašla informacija da postoje na desetine Telegram grupa, koje broje i po nekoliko desetina hiljada članova koji međusobno razmenjuju snimke i slike pornografskog sadržaja svojih bivših devojaka, ali i lične podatke devojaka sa snimaka i slika. Najveća takva grupa brojala je 36.000 članova i zvala se EX YU Balkanska soba. Takođe, postojale su i pojedinačne grupe podeljene po gradovima, kao što su Niš i Beograd.
[8] Član 153 u vezi sa članom 146 Krivičnog zakonika.
[9] Jelena Pejić Nikić (ur.) prEUgovor Alarm izveštaj o napretku Srbije u poglavljima 23 i 24, koalicija prEUgovor, Beograd, maj 2021, str. 91-92.

Zaključak sa preporukama

Uprkos postojanju dobrog zakonskog okvira, borba protiv VTK-a u Srbiji suočava se sa hroničnim manjkom kvalifikovanih kadrova, kao i sa politizovanim prioritetima nadležnih institucija. Tromost krivičnopravnog sistema ne ide u korak sa napretkom tehnologije i zbog toga novi oblici krivičnih dela, gde se kao sredstvo ili način izvršenja koriste računari ili računarske mreže, ostaju van krivičnopravnog okvira. Nedovoljna obučenost i poznavanje problematike svih aktera koji učestvuju u borbi protiv VTK-a, pre svega, sudija, advokata i policijskih službenika van Odeljenja za VTK, dovodi do velikog broja neprocesuiranih krivičnih dela, koja spadaju pod visokotehnološki kriminal. Da bi borba protiv VTK-a bila na najvišem nivou, neophodno je edukovati i širu javnost o vrstama krivičnih dela VTK-a i načinima zaštite i prevencije od ove vrste krivičnih dela.

Izdvajamo sledeće preporuke:

- Potrebno je izraditi novi Akcioni plan za sprovođenje Strategije za borbu protiv visokotehnološkog kriminala za period 2022–2023.
- Potrebno je povećati broj obučenih policijskih službenika u četiri odseka Odeljenja za suzbijanje visokotehnološkog kriminala radi efikasnije borbe protiv ove vrste kriminala.
- Potrebno je sprovoditi obuke za policijske službenike van Odeljenja za suzbijanje VTK-a kako bi se upoznali sa procedurama prikupljanja dokaza i prijavljivanja krivičnih dela.
- Posebnom tužilaštvu za visokotehnološki kriminal neophodno je obezbediti veće smeštajne kapacitete, povećati broj zaposlenih, ali i omogućiti adekvatnu tehničku opremljenost kako bi bili u mogućnosti da neometano obavljaju poslove za koje su zaduženi.
- Neophodno je uvesti kontinuiranu obuku za sudije i advokate koji se bave predmetima visokotehnološkog kriminala kako bi se izbegli problemi u postupcima, do kojih bi moglo da dođe usled nedovoljnog poznavanja materije.
- Potrebna je bolja saradnja na nacionalnom nivou između privatnog, javnog i civilnog sektora kako bi borba protiv visokotehnološkog kriminala bila uspešnija. Ta saradnja mora da bude kontinuirana, jer se u ovoj oblasti tehnologija i prateći bezbednosni izazovi, rizici i pretnje bez prestanka razvijaju.
- Potrebno je izmeniti i dopuniti odgovarajuće članove Krivičnog zakonika kako bi bilo predviđeno krivično delo „zloupotrebe snimka polne sadržine”. Kada je u pitanju krivično delo neovlašćenog prikupljanja podataka o ličnosti, posebno kada ono ima masovne razmere, potrebno je dodati da se takva dela gone po službenoj dužnosti.

O prEUgovoru

Koalicija prEUgovor je mreža organizacija civilnog društva osnovana radi praćenja politika koje se odnose na pregovore o pristupanju Srbije Evropskoj uniji, sa posebnim naglaskom na poglavlja 23 i 24. Cilj prEUgovora je da pomogne da se proces pristupanja EU iskoristi za ostvarenje suštinskog napretka u daljoj demokratizaciji srpskog društva.

Koaliciju prEUgovor čine:

ASTRA – Akcija protiv trgovine ljudima
www.astra.rs

Autonomni ženski centar (AŽC)
www.womenngo.org.rs

Beogradski centar za bezbednosnu politiku (BCBP)
www.bezbednost.org

Centar za istraživačko novinarstvo Srbije (CINS)
www.cins.rs

Centar za primenjene evropske studije (CPES)
www.cpes.org.rs

Grupa 484
www.grupa484.org

Transparentnost Srbija (TS)
www.transparentnost.org.rs

Glavni proizvod prEUgovora je polugodišnji izveštaj o napretku Srbije u klasteru 1.

Aktivnosti prEUgovora možete pratiti na sajtu, fejsbuku i tviteru.

ISBN-978-86-84711-53-5

B | T | D The Balkan Trust for Democracy
A PROJECT OF THE GERMAN MARSHALL FUND

Norway