Ministarstvo unutrašnjih poslova

UPRAVA POLICIJE CRNE GORE
POLICE OF MONTENEGRO

CRNOGORSKA REVIJA ZA BEZBJEDNOST

Naučno-stručni časopis za teoriju i praksu iz oblasti bezbjednosti

Godište 3 • Broj 3 • Podgorica, Crna Gora, 2025.

ISSN 3027-3390

Ministarstvo
unutrašnjih
poslova

CRNOGORSKA REVIJA ZA BEZBJEDNOST

Naučno-stručni časopis za teoriju i praksu
iz oblasti bezbjednosti

MONTENEGRO REVIEW FOR SECURITY

Scientific and professional magazine for
theory and practice in the field of security

Godište 3 · Broj 3 · Podgorica, Crna Gora, 2025.
ISSN 3027-3390

CRNOGORSKA REVIJA ZA BEZBJEDNOST
Naučno-stručni časopis iz oblasti bezbjednosti

Godina 3/broj 3, 2025.

Izdavač: Ministarstvo unutrašnjih poslova Crne Gore

Za izdavača: Danilo Šaranović

Kontakt adresa: Bulevar Sv. Petra Cetinjskog br: 22, Podgorica

Tiraž: 500 primjeraka

Štampa: 3M Makarije

SADRŽAJ

UDK 343.434:004

HIBRIDNE PRIJETNJE I INFORMACIJE
HYBRID THREATS AND INFORMATION

dr Mitar Radonjić
Crnogorski bezbjednosni forum
kontakt@radonjicmitar.me

Apstrakt

Kako živimo u vremenu ekspanzivnog razvoja tehnologije od suštinskog je značaja da razumijemo na koje sve načine ona utiče na različite segmente ljudskog života. U tijesnoj vezi sa progresijom digitalnog doba jesu i savremeni načini ratnih sukobljavanja, dok standardni pojam bojnog polja postaje sve više fluidan. Hibridne prijetnje predstavljaju posebne i vrlo specifične, neposredne ali i posredne oblike ugrožavanja društva i državnog integriteta. Izbjegavajući otvorene oružane sukobe koji najčešće podrazumijevaju velike troškove po državu koja objavljuje rat kao i niz drugih sankcija, mnoge države umjesto direktnog vojnog sukoba sa ciljem da poraze neprijatelja, primjenjuju niz strateških operacija i taktika sa svrhom kontinuiranog slabljenja neprijatelja i njegove potpune dezorganizacije. U vremenu u kojem internet dominira kao komunikaciono sredstvo i sredstvo širenja propagandnih informacija on postaje pogodno oružje u ratu dezinformacijama i obavještajnim informacijama. Kako je čovjek jedna od najslabijih karika obavještajnog sistema nije teško pretpostaviti da bi udar na državni integritet i kohezitet društva mogao doći upravo iz tog pravca. Globalna je tendencija velikih sila da posredstvom propagande utiču na kolektivnu svijest sa ciljem ostvarivanja manipulacije i kontrole konkretnog područja. Ovakvi uticaji bivaju još intenzivniji kada se koristi i sajber prostor. Međutim, kada su hibridne prijetnje u pitanju i vojno slabiji protivnici prikriveno i konstantno vrše napade pokušavajući da neprijatelja drže u stanju kontinuiranog straha i dezorganizacije. Držeći neprijatelja u takvom stanju strepnje uzrokuju mu i ekonomsku nestabilnost, jer druga strana pravi velike izdatke utrošene na vojnu opremu i naoružanje, svakog trenutka očekujući vojni sukob. U ovom radu nastojaćemo da ostvarimo dublji uvid u savremene hibridne prijetnje i njihove pojavne oblike uz osvrt na aktuelne međunarodne

sukobe. Takođe ćemo apostrofirati značaj tajnih operacija i obavještajnih informacija za tranziciju hibridnih prijetnji u hibridni rat, a potom i potpunu dezorganizaciju državnog i društvenog integriteta.
Ključne riječi: *hibridne prijetnje, hibridni rat, informacije, medijska pismenost, dezinformacije, obavještajni podaci.*

Abstract

As we live in a time of expansive technology development, it is essential to understand the ways in which it affects different segments of human life. In close connection with the progression of the digital age are the modern ways of war conflicts, while the standard concept of the battlefield is becoming more and more fluid. Hybrid threats represent special and very specific, direct and indirect forms of endangering society and state integrity. Avoiding open armed conflicts, which most often entail high costs for the country that declares war, as well as a number of other sanctions, many countries, instead of direct military conflict with the aim of defeating the enemy, apply a series of strategic operations and tactics with the aim of continuously weakening the enemy and its complete disorganization. At a time when the Internet dominates as a means of communication and a means of disseminating propaganda information, it becomes a suitable weapon in the war against disinformation and intelligence information. Since man is one of the weakest links in the intelligence system, it is not difficult to assume that an attack on state integrity and the cohesion of society could come from exactly that direction. It is a global tendency of great powers to influence the collective consciousness through propaganda with the aim of achieving manipulation and control of a specific area. Such influences become even more intense when cyberspace is also used. However, when it comes to hybrid threats, even militarily weaker adversaries covertly and constantly carry out attacks trying to keep the enemy in a state of continuous fear and disorganization. Keeping the enemy in such a state of anxiety also causes him economic instability, because the other side makes large expenditures on military equipment and weapons, expecting a military conflict at any moment. In this work, we will try to achieve a deeper insight into contemporary hybrid threats and their emerging forms with reference to current international conflicts. We will also apostrophize the importance of secret operations and intelligence information for the transition of hybrid threats into hybrid war and then the complete disorganization of state and social integrity.
Keywords: *hybrid threats, hybrid war, information, media literacy, disinformation, intelligence data.*

UVOD

Sukobi koji su se odvijali na globalnoj sceni prethodnih decenija imaju specifične karakteristike. Mnogi istraživači i analitičari složili su se da sukobi evoluiraju na nivou koji više ne postulira standardno bojno polje. Štaviše, bojno polje kao tačku sukoba dvije ili više suprostavljenih sila u standardnom smislu, mnogo je teže odrediti. Analogno tome i pojam sukoba nije moguće u potpunosti izjednačiti sa ratom. Rat postoji do kad seže ljudska istorija i vodio se u skladu sa mehanizmima koji su u datom istorijskom trenutku bili raspoloživi. Kako je napredovala civilizacija uporedo se razvijao i koncept ratovanja. Sukob u najširem obliku možemo odrediti kao ukrštanje najmanje dvije suprostavljene sile sa ciljem da jedna odnese prevagu i ostajući kao jača, dok se druga povlači kao slabija. Sukobljene sile u ovom smislu, imaju različite interese koji su antagonističke, zbog čega nije moguć konsenzus. Pobjeda jače strane može se ogledati kroz bilo koji cilj koji je ostvarila sukobom. Rat proizilazi iz sukoba, a kako sukob ne mora nužno biti oružani, takva odrednica može da determiniše i pojam rata. Ukoliko ljudi mogu da se sukobljavaju na verbalnom i virtuelnom nivou, takva analogija mogla bi se prenijeti i na koncept ratovanja. Dakle, rat možemo posmatrati kao jedan od oblika sukobljavanja. Nakon Drugog svjetskog rata nije bilo značajnih većih i otvorenih sukoba između velikih sila kako je to do tada bio slučaj, već se sukob dešavao na jednom novom nivou kao u slučaju Rusije i SAD-a i to ne samo kroz primjer Hladnog rata već i kroz primjer pomaganja suprostavljenim vojnim silama širom svijeta, posredno (Krivokapić, 2013).

Poznato nam je makar iz dva velika Svjetska rata koja su istorijski gledano vrlo blizu sadašnjem vremenu, da su ratna razaranja odnijela veliki broj života i da često vinovnici ratnog vihora nijesu imali potpunu kontrolu nad njim. Zajedno sa ciljevima koje su ratom željele ostariti bilo je i mnogo negativnih propratnih efekata, stradanja stanivništva, nekontrolisanih pobuna stanovništva, upotrebe oružja koje humanitarno pravo ne dozviljana i tome slično. Sledstveno tome, nekad se tokom ratova paralelno sa regularnom vojskom formiraju i paravojne jedinice nad kojima država nema (ili barem tvrdi tako) kontrolu, da se dešavaju ratni zločini i da se principi humanitarnog prava malo ili nikako ne poštuju, te da su civili neizbježna kolateralna šteta. Tome slijede velike ratne odštete, narušavanje kredibiliteta i reputacije države u svijetu i kod lokalnog stanovništva. Posjedovanje nuklearnog naoružanja je jedan od važnih faktora zbog čega se ratovi dešavaju mnogo rjeđe između velikih sila, koje umjesto na ratovanje značajna sredstva izdvajaju na ekonomski prosperitet. Vojni teoretičar Karl fon Klauzevic (1951) napisao je u svojoj knjizi „O ratu" da je rat nastavak politike drugim sredstvima. Međutim, pomenuta sredstva političkog ratovanja, iako se u poslednje vrijeme koristi termin "političko nadmetanje", podrazumijevaju legalna sredstva kao što su vojno-politički međunarodni savezi, ekonomsko osnaživanje i „bijela" propaganda, ali i ilegalne tajne operacije kao što su tajna podrška „prijateljskim" stranim elementima, psihološki rat, pa i podsticanje otpora u neprijateljskim državama.

Ova ilegalna sredstva suštinski predstavljaju međudržavno političko nasilje. Iza tih namjera koje podstiču neku vrstu sukoba uvijek postoji određeni interes. Sama činjenica da su oružani sukobi manje isplativi i mnogo više rizični, ne umanjuje pretenzije za određeni interes. Ovakvoj koncepciji išla je na ruku ekspanzija tehnologije, naročito sajber prostora, ali i masovni mediji. Način ostvarivanja interesa sve više dobijao je oblik posrednih napada na protivnika i to u ovom slučaju čak i kada je mnogo jači u tom vojnom smislu. Posredni napadi na drugu stranu omogućavaju dinamičnost kakvu oružanu sukobi rijetko ili nikako ne postižu prije potpunog prelaska na teritoriju neprijatelja, zbog čega su ih mnogi autori nazivali hibridnim (Vuković, 2018). Hibridni napadi nazivaju se još i nekonvencionalnim jer u sebi sadrže više različitih elemenata koji ih čine podmuklim, prikrivenim i samim tim i nelegalnim, ali istovremeno nimalo jednostavnim za otkrivanje. Takvi napadi su pažljivo i namjenski konstruisani i sinhronizovani i u ovom radu označićemo ih kao hibridne prijetnje. U oružanim sukobima žrtve su vidljive, napadi autentični, podložni opisu kvalitativnom i kvantitativnom, šteta mjerljiva kriterijuma koji su definisani. Međutim, kako izmjeriti štetu nastalu podmetanjem pogrešne obavještajne informacije ili dezinformacija koje mijenjaju svijest jednog naroda? Upravo u tome očitava se fluidnost i difuzija hibridnih prijetnji, a ono što je u najvećoj mjeri fluidno i prodorno, što nanosi štetu a teško se dolazi do uzročnika i još teže uklanja njegove posledice, jeste ni manje ni više nego informacija.

OBAVJEŠTAJNI PODACI

Riječ informacija je latinskog porijekla i znači stavljanje u određenu formu, odnosno davanje značenja nečem (Đurđević i Radović, 2017). Ipak definisanje pojma informacije nije jednostavan zadatak budući da obuhvata jedno široko i raznoliko područje. Informacija se definiše i kao preslikavanje stanja jednog subjekta pri čemu to preslikavanje ne mora biti jednako za sve subjekte (prema Pomerantsev, 2015). U ovoj definiciji nazire se značaj komuniciranja odnosno prenošenja nečeg s jedne tačke na drugu s ciljem. Kako je pojam informacije sveobuhvatan, potrebno je razjasniti njegovu ulogu u određenom kontekstu, odnosno u vezi sa drugim relevantnim pojmom za ovaj rad, a to je podatak. Iako se često pojmovi podatak i informacija poistovjećuju potrebno je naglasiti da nije riječ o sinonimima. Ukoliko uzmemo da je podatak neka sporadično zabilježena činjenica koja se može odnositi i na običan predmet kao na primjer sat, onda će informacija predstavljati skup više takvih podataka koji komuniciraju o određenom sadržaju u određenom kontekstu: *ručni sat je veoma skup i nosi ga moj prijatelj*. U bezbjednosnom sistemu nemaju sve informacije epitet obavještajne informacije. Samo evaluirana i „pročišćena" informacija pod određenim uslovima može postati obavještajna informacija i obavještajni podatak. Kao informacija ona je sakupljena, ali još nije upotrebljiva. Kao obavještajna informacija ima upotrebnu vrijednost i moguće ju je koristiti.

Obavještajne informacije su izvor obavještajnih podataka (Arena & Wolford, 2012). Dakle, obavještajni podaci predstavljaju posebno znanje dobijeno iz obavještajnih informacija, a koje je neophodno za rješavanje konkretnih bezbjednosnih problema (Dellerman et al., 2019). Ovi objavještajni podaci koji se izdvajaju i nastaju iz obavještajnih informacija predstavljaju materijal iz kojeg se proizvodi obavještajno znanje. Dakle, cilj obavještajnih djelatnosti je prikupljanje informacija koje će kroz analitički proces postati koristan obavještajni podatak. Ovi obavještajni podaci veoma su značajni s aspekta nacionalne bezbjednosti jedne države, jer sadrže informacije o protivniku koje se mogu prikupljati kako iz javno dostupnih izvora tako i primjenom posebnih metoda za tajnu opservaciju. Od ostalih podataka obavještajni podaci se razlikuju po tome što imaju svoj poseban značaj za državu i značajno utiču na formiranje političkih odluka, pravca vođenja unutrašnje i vanjske politike i slično.

U stranoj literaturi za obavještajne podatke koristi se termin engleskog jezika *intelligence*, ali se ovaj termin može odnositi i na službu koja je zadužena za prikupljanje ovih podataka (prema Dellerman et al., 2019). Formulacija ovog pojma osnov je za njegovu adekvatnu upotrebu u ovom radu, jer se ovaj termin prvenstveno koristi u različitim kontekstima. Prema Carteru (2009) termin *intelligence* predstavlja krajnji proizvod analitičkog procesa u okviru kojeg se relevantni podaci ekstrahuju, obrađuju i iz njih se izvode zaključci i donose odluke, u ovom slučaju od nacionalnog značaja.

Analitički proces dobijanja obavještajnih podataka najčešće teče kroz nekoliko faza obrade kao što su planiranje, priprema, prikupljanje, obrada i obavještajni proizvod. Prvi korak obavještajnog procesa (planiranje) sastoji se iz aktivnosti koje uključuju procjenu situacije, predstavljanje željenog ishoda (poznat još kao predstavljanje vizije), identifikovanje relevantnih informacija i obavještajnih zahtjeva, razvijanje strategija operacije, upravljanje operacijom i sinhronizaciju aktivnosti poput izviđanja i nadzora nad prikupljanjem podataka. Planiranje, koordiniranje i upravljanje ovim operacijama od suštinskog je značaja za dobijanje informacija koje će dati konkretan i upotrebljiv obavještajni proizvod ključan za donošenje kritičnih odluka. Faza pripreme podrazumijeva sve one aktivnosti koje se podrazumijevaju po prijemu strategije operacije. Faza prikupljanja podataka posebno je bitna i nekad je poznata i kao *operacija unutar operacije* (Scott & Jackson, 2004). Vrši se prikupljanje podataka iz različitih izvora (javnih i tajnih) o neprijatelju, njegovoj vojnoj i ekonomskoj moći, kritičnoj infrastrukturi, državnim resursima, naučnim otkrićima, kao i informacije o geografskim i ekološkim karakteristikama od značaja za ciljano područje. Tokom faze obrade veliki broj pristiglih informacija i podataka se „prečišćava" kroz pažljivu analizu kako bi mogla imati upotrebnu vrijednost kao obavještajni podatak. Obrada podrazumijeva i sortiranje velike količine prikupljenih podataka. Nakon pažljive obrade i analize obavještajni podaci dostavljaju se nadležnom Vladinom tijelu nakon čega se može vršiti i reevaluacija u zavisnosti od novodobijenih informacija. Potreb-

no je naglasiti da ovaj proces dobijanja obavještajnih podataka nije mehanički i rigidan, sa čvrsto postavljenim redosledom faza, već vrlo dinamičan i shodno potrebama prilagodljiv (ukoliko je nekad potrebno vratiti se jednu fazu unazad i sl).

Poznato je iz literature više izvora obavještajnih podataka kao što su to OSINT (open source intelligence), HUMINT (human intelligence), TECHINT (technical intelligence) (Crosston & Valli, 2017). Prikupljanje podataka od strane ljudi (HUMINT) najstariji je način obavještajne djelatnosti koji datira čak do antičkog doba, kada su vladari slali svoje vojnike da izviđaju tajno teritoriju neprijatelja, da informišu o vojnoj brojnosti, geografskim determinantama neprijateljske teritorije koje bi poslužile za okupaciju, načine obučavanja vojnika, itd. Obavještajni podaci su od naročite vrijednosti i tokom sukoba sa neprijateljem i oni se pribavljaju kontinuirano u najvećoj tajnosti. Istraživanja su pokazala da je najkorisniji metod pribavljanja podataka onaj u kojem se koristi više izvora informacija, dok su one operacije koje su na bojnom polju ili neprijateljskoj teritoriji izvođene samo koristeći informacije pribavljene iz izvora koje su predstavljajli tehnički uređaji (TECHINT, SIGINT), ili samo onih informacija pribavljenih od strane ljudskog izvora, vodile do toga da budu najčešće neuspješne (Scott, 2007). Svakako je važno da se obavještajni podaci i informacije sa terena prikupe i provjere iz više izvora pred početak vojne operacije. Pojedinačni izvori često mogu biti nepouzdani, ali i površni i ishitreni kada je u pitanju ljudski izvor.

Bezbjednosno okruženje je višedimenzionalno i složeno, zbog čega nekad i pored brižljivo sprovedene faze planiranja nije moguće izbjeći dodatne varijable i napraviti propust, ili uvažiti informacije koje mogu nanijeti štetu bezbjednosnoj strukturi države. S druge strane, neka sasvim bezazlena situacija koja je „maskirana" pod težinom plasiranih dezinformacija ili uticaja stranih struktura s diplomatskim imunitetom koji operišu unutar države tajno, može predstavljati hibridnu prijetnju. Informacije do kojih službe dolaze trebaju biti posebno razmatrane u pogledu njihove vjerodostojnosti od strane kontraobavještajnih struktura (Lewin, 1981). Obavještajna procjena zna biti veoma kompleksna jer su indikatori koji ukazuju na prijetnje u okviru prikupljenih informacija i sami vrlo kompleksni. U ovom smislu, korisno je pomenuti i krađu obavještajnih informacija u sajber prostoru posredstvom angažovanih hakera sa Dark net-a, a pomoću kojih se hibridno napada neka država. Sajber napadi kao oblik hibridnih prijetnji sve su češći i vrlo podmukli, jer tehnologija toliko brzo napreduje da pravni okviri koji definišu sajber prostor i njegove elemente u datom trenutku, već u sledećem mogu biti neupotrebljivi, što ostavlja dovoljno prostora da poveća izvjesnost hibridnih uticaja. Međutim, kako je ova oblast sajber ratovanja prilično opširna i zahtijeva jednu ozbiljniju i dublju elaboraciju, u ovom radu ćemo se ovdje zaustaviti.

HIBRIDNE PRIJETNJE

Mogućnosti koje je obezbijedila digitalizacija iz godine u godinu sve su veće, što umnogome utiče na prirodu ljudske interkacije. Ekspanzija korišćenja sajber prostora i činjenica da sve više ljudi raspolaže digitalnim uređajima koji omogućavaju prostup internetu (bez obzira da li žive u urbanim ili ruralnim predjelima) značajno mijenja koncepciju svijeta i razmišljanja od strane javnog mnijenja. Ovakav iskorak čovječanstva morao je dotaći i načine rješavanja međudržavnih pitanja i donošenja političkih odluka. Sve više, umjesto u ratnu opremu koja bi brzo zastarijevala i gubila upotrebnu vrijednost, novac je ulagan u načine dolaska do podataka koje bi obezbjeđivale državama izvjesnu prednost u geopolitičkom i vojnom smislu. Vrijedna obavještajna informacija dobijala je veću vrijednost u odnosu na posjedovanje nekog savremenog oružanog elementa (naročito kada je riječ o produkciji nuklearnog i biološkog oružja) (Linkov et al., 2019). Drugim riječima, velike sile su prve postigle prećutni konsenzus da je mnogo isplativije djelovati na psihologiju mase i taj ranjivo ljudski faktor u tuđem bezbjednosnom sistemu, nego inicirati stvarne akcije sa mogućim stvarnim posledicama (Fridman). Prema Kolobaru (2019) dva su ključna aspekta hibridnog ratovanja u periodu nakon Hladnog rata i to uništavanje protivnika postepenim uništavanjem njegove kulture i sistema vrijednosti, kao i aspekt ekonomske, informacione i političke sile nasuprot fizičkoj vojnoj. Neprijatelj podriva izvana i infiltriran iznutra na način koji stvara takvu konfuziju (kao u slučaju korišćenja kriminalnih grupa), tako da napadnuta država ne može tačno da procijeni odakle opasnost dolazi.

U ovom dijelu korisno je osvrnuti se na razliku hibridnog ratovanja i hibridnih prijetnji. Hibridni rat označen je svojim početkom i upotrebom raznovrsnih metoda koji ne moraju biti u ravni sa fizičkim sukobom, ali koji (već) dovode do uticaja na političke odluke države neprijatelja, ekonomiju i opštu dezorganizaciju društva. Dakle, ciljevi se već sprovode i država trpi štetu koja je evidentna. S druge strane, hibridne prijetnje označene su neizvjesnošću koja može preći u rizik ali ne nužno, već predstavlja lebdeće stanje nekonvencionalne opasnosti koja ima za cilj da uzbunjuje protivnika, izaziva strah i nesigurnost zbog mogućeg napada (Hoffman, 2010). Hibridne prijetnje predstavljaju ozbiljan izvor ugrožavanja državnog poretka zbog čega ih treba shvatiti ozbiljno i uvrstiti u strategijske planove suprostavljanja potencijalnim narušiteljima nacionalne bezbjednosti.

Važnu ulogu u formiranju teorije o hibridnim prijetnjama imao je Frank Hoffman, novinar Deutsche Wellea i ekspert za sigurnost i međunarodne odnose. Hofman navodi da hibridne prijetnje obuhvataju sistem različitih načina ratovanja uključujući i konvencionalne sposobnosti, neregularne taktike i formacije, terorističke aktivnosti i mobilisani kriminal (Hoffman, 2018). Ono što je najviše karakteristično za hibridne prijetnje jeste da one kombinuju sa nelegalnim i neregularnim aktivnostima one re-

gularne, koje ih „maskiraju“ čineći hibridne prijetnje posebno efikasnim. Francuska bijela knjiga odbrane i nacionalne bezbjednosti iz 2013. godine ukazuje na značaj hibridnih prijetnji na način da nedržavni akteri tokom sukoba mogu kombinovati asimetrična sredstva sa državnim sredstvima ili mogućnostima napredne tehnologije (prema Pannier & Schmitt, 2019). Korišćenje konvencionalnih i nekonvencionalnih sredstava istovremeno otežava napadnutoj državi da kvalitetno usmjerava svoje odbrambene snage. U tom smislu, vođenje hibridnog rata postaje fluidno i sve više difuzno, miješajući istovremeno moralno sa neregularnim, zbog čega je opravdano postaviti pitanje da li je bilo šta u ovim ratovima bez krvavih žrtvi, zabranjeno. Iako su hibridni sukobi negdje započeli sa velikim silama očekujemo da će u budućnosti to biti sve češće način slabijim zemljama koje nisu sposobne uz pomoć oružanog sukoba da ostvaruju ciljeve, da oslabe svog protivnika. Negdje su očekivanja i da će hibridne prijetnje biti sve prisutnije u narednim godinama posredstvom kojih će treće države pretendovati da utiču kako na unutrašnje procese unutar država tako i na međudržavne odnose.

Kao najznačajniji sadržaj hibridnog ratovanja mogu se uzeti sljedeći oblici djelovanja na protivnika u cilju primoravanja na ispunjenje zahtjeva: informaciono-psihološko-ideološko djelovanje, političko djelovanje, ekonomski pritisci, obavještajno-subverzivna djelatnost, informatičke metode, kriminalne aktivnosti, terorizam i oružane pobune, konvencionalno vojno djelovanje. Tapio Pyysalo voditelj međunarodnih odnosa u Evropskom centru za borbu protiv hibridnih prijetnji (European Centre of Excellence for Countering Hybrid Threats – Hybrid CoE) sa sjedištem u finskom glavnom gradu, Helsinkiju, ukazuje da se zapadni svijet sve više suočava s hibridnim prijetnjama, iza kojih najčešće stoje Rusija, posebno nakon invazije na Ukrajinu, i Kina, koja svoj ogromni ekonomski uticaj upotrebljava da bi stekla stratešku moć u drugim zemljama. Akteri hibridnih prijetnji nikada ne spavaju – cijelo vrijeme mapiraju ranjivosti demokratskih društava kako bi mogli napasti kritičnu infrastrukturu i zamagliti stvarnost (https://lidermedia.hr/biznis-i-politika/tapio-pyysalo-157257).

RAT INFORMACIJAMA

U vojnom, političkom i ekonomskom svijetu postizanje nadmoći vrlo je bitno zbog čega je bitno o tim aspektima prikupiti od neprijatelja što više informacija, ali i istovremeno od neprijatelja sakriti lične slabosti. U današnjem vremenu takva borba biva nemilosrdna i prava informacija dobijena u pravo vrijeme može biti od suštinskog značaja. Kada su u pitanju hibridni ratovi i hibridne prijetnje, nekonvencionalni neprijateljski uticaj informacijama jedan je od glavnih instrumenata sukobljavanja, ali i ostvarivanja jednosmjernog uticaja na neprijateljsku državu emitovanjem onih hibridnih prijetnji koji dovode do podrivanja državnog poretka i destrukcije društva.

Zbog toga je za jednu državu ključno da zna kako da na pravilan način upravlja informacijama, kako da ih čuva i skladišti tako da neprijatelj ne bude u mogućnosti da im dođe u posjed. Upravljanje informacijama za jednu državu može biti korisno na način što će tako moći da utiče na političke odluke, na remećenje već donesenih odluka, kako bi se planovi i političko usmjerenje jedne države osujetili ili preusmjerili onim tokom koji suprostavljenoj strani više odgovara.

Jako precizan primjer jedne ovakve vrste podrivanja dogodio se u Crnoj Gori tokom izbora 2016.godine, kada je od strane obavještajnih struktura Rusije došlo do pokušaja izvođenja Državnog udara, a sve u cilju sprečavanja Crne Gore da postane dio NATO Alijanse. Informacije koje je ruska služba dobijala od svojih instaliranih struktura u Crnoj Gori u tom periodu bile su od ključnog značaja za njihovu logistiku pokušaja napada.

Još jedan primjer rata informacija vezan je za sukob Ukrajine i Rusije i plasiranje lažnih starijih snimaka događanja u Ukrajini koji su imali za cilj da šire narodne mase dovedu u zabludu i da na njih izvrše uticaj koji je emiteru jedne takve operacije, odnosno ruskoj strani, bio potreban. Uticaj Rusije posredstvom informacionog rata na stanovništvo evidentan je još od Hladnog rata i ima za cilj prevashodno da Zapad i zapadnu kulturu predstavi kao štetnu, usađujući im ideološke ciljeve koji u datom trenutku odgovaraju političkom establišmentu.

Kako je jedno od glavnih svojstava hibridnog djelovanja i hibridnih prijetnji je da podrivaju društveni poredak i izazivaju haos koji bi im pomogao da svoje stvarno djelovanje usmjeravaju u željenom smjeru. Već smo pomenuli da hibridna djelovanja dolaze spolja i u tom slučaju lakše ih je identifikovati, ali dolaze i iznutra i onda za državne strukture predstavljaju svojevrsni zadatak da ih otkriju na vrijeme kako bi se zaustavile štetne posledice. Naime, tokom hibridnih ratova plasiraju se i informacije koje su netačne i imaju za cilj da naruše vezu države i njenih građana, kako bi se izazvalo i produbilo nepovjerenje u državne instutucije i nosioce vlasti, čime se unaprijed priprema teren za anarhiju i nemire (Reza & Sunvy, 2023).

Jedan bitan segment informacionih operacija su obmane koje se zasnivaju na psihologiji i nekad je potrebna pažljiva analiza uz pomoć pažljivo odabranih stručnjaka kako bi se one razotkrile. U periodima neizvjesnosti pogrešne informacije itekako mogu da utiču na iskrivljeno tumačenje događaja, koje dalje vodi pogrešnim percepcijama i strateškim greškama. Obmane su usmjerene na narušavanje sposobnosti komandovanja i onih sistema za prikupljanje podataka kako bi njihovi emiteri ostvarili informacionu superiornost i stvorili dobre pretpostavke za uspjeh sopstvene operacije. Prenošenje informacija vrši se različitim javnim i tajnim kanalima, nekada i uz pomoć diplomatskih predstavništava kroz zloupotrebu određenih prava koja ih zastupaju u stranoj državi, nekada ubacivanjem stranih agenata ili vrbovanjem

domaćeg stanovništva da radi u korist drugih država (Linkov et al., 2019). Obmane se mogu sprovoditi i na taj način da zamagle cjelokupnu sliku javnog mnijenja o hibridnim prijetnjama i ko su njihovi ključni akteri, a propaganda i lažne vijesti često tu mogu biti od velike važnosti i uticaja. Dovoljno je da se prisjetimo načina na koji je agresivan rat i invaziju na Ukrajinu i njen narod predsjednik Rusije Vladimir Putin nazivao specijalnom operacijom, namjerno izostavljajući terminologiju koja je bila u vezi sa realnim i teškim oružanim sukobom s mnogo nedužnih žrtava koji se uistinu odigravao, stvarajući kod sopstvenog stanovništva sliku Rusije kao spasiteljke naroda, a ne agresora.

MEDIJI I DEZINFORMACIJE

Novu eru obilježila je ekspanzija tehnologije, naročito s aspekta upotrebe interneta. Za razliku od perioda od prije više decenija, sada je ogroman broj ljudi u mogućnosti da prati dešavanja u svojoj zemlji i svijetu iz udobnosti sopstvenog doma. Gotovo svaka medijska kuća, bez obzira na njen rejting i veličinu, ima svoje internet portale koji su dostupni kroz samo nekoliko klikova. Međutim, ono što je teško kontrolisati jeste na koji način će različite kategorije stanovništva filtrirati mnoštvo informacija sa interneta, u koje će povjerovati, a u koje ne. To postaje vrlo važno državno pitanje kada uzmemo u obzir da je stanovništvo vrlo heterogeno po obrazovanju, zbog čega i medijsko opismenjavanje prihvataju različito. To koliki je paradoks da je s jedne strane putem interneta dostupan veliki broj informacija iz udobnosti doma i s druge strane nemogućnost razaznavanja koje su informacije istinite i bitne, govori o ozbiljnom problemu današnjice. Ovaj problem vrlo lako postaje teren hibridnih prijetnji.

Pojam medijske pismenosti podrazumjeva način na koji se pristupa medijima, kako se razumiju poruke iz medija i na koji način i koliko je razvijeno kod nekog kritičko mišljenju prema trenutno dostupnom sadržaju (Posseti & Matthews, 2018). Određeni autori govore u prilog tome da mediji sami po sebi nisu ni dobri ni loši već zavisi kako se i u kom pravcu koriste, njihov uticaj na društvo (prema Arena & Wolford, 2012). Sam razvoj medijske pismenosti potrebno je posmatrati u kontekstu okruženja u kojem se posmatra, socio-ekonomski i kulturnim uslovima, kao i uslovima razvijenosti digitalizacije. Ekspanzivan tehnološki razvoj i razvoj digitalizacije nisu uvijek u liniji sa sposobnostima ljudi da ih odmah usvoje i primjenjuju, što se naročito problematizuje s aspekta informacija. Kroz istoriju nam je poznato da je istinsko znanje uglavnom bilo privilegija povlašćenih, dok bi se kritičko razmišljanje doživljavalo kao subverzivna aktivnost. Međutim, bez obzira što je današnjica obilježena demokratijom i slobodom govora opasnost od pogrešnog filtriranja informacija i podložnost uticaju dezinformacija koje se plasiraju sa neprijateljskim namjerama, je nikad veća.

Rezultati istraživanja ukazali su da demokratija može biti ugrožena srezmjerno brzinom i mogućnostima kojima se mogu širiti dezinformacije (Schiffrin, 2017). Osim medijskih izvještavanja značajan uticaj ostvaruju i društvene mreže koje poslednjih godina sve manje služe za zabavu, a sve više za plasiranje manipulativnih sadržaja. Dezinformacije se mogu širiti i sa ciljem humora, dok se neki sadržaji namjerno podmeću kako bi bili prihvaćeni kao istina. To se često radi sa ciljem narušavanja ugleda institucija, institucionalnih predstavnika ili čak i država. Postoji i emotivanje na medijima masovne komunikacije onih sadržaja koji su se stvarno dogodili, ali njihov emiter manipuliše kontekstom i vremenom u kojem su se dogodili. Takav je slučaj bio sa masovnim širenjem video snimaka o ubijenim civilima u Gazi, tokom poslednjeg izraelsko-palestinskog sukoba 2023 godine, dok je pažljivom istragom ustanovljeno da su u pitanju video snimci stari sedam godina.[1]

Dezinformacije koje se koriste u cilju hibridnog djelovanja su netačne i namjerno plasirane kako bi se kod javnosti stvorio određeni utisak, emocija ili formiralo mišljenje (Pomerentsev, 2015). Pored dezinformacije često se upotrebljavaju lažne vijesti (fake news) a govori se i o pogrešnim informacijama (missinformation) i malinformacijama odnosno zlonamjernim informacijama (Reza & Sunvy, 2023). Za razliku od dezinformacija koje uvijek imaju štetnu namjeru, za ove ostale to ne mora uvijek biti slučaj. Kreatori hibridnog djelovanja imaju tendenciju da analiziraju psihologiju mase stanovništva neprijateljske države i u skladu sa tim kreiraju i plasiraju one dezinformacije koje će kod te strukture stanovništva izazvati najjači efekat koji je u liniji sa tendencijom hibridnih prijetnji.

ZAKLJUČAK

Živimo u svijetu koji je možda kao nikad ranije obilježen brzim promjenama na različitim nivoima. Demokratija je napredovala i razvijala se zajedno sa ljudskim pravima. Savremeno shvatanje demokratije ne može se svesti samo na odnos vlasti i naroda u pojedinim državama, već se mora baviti i sudbinom demokratije pred licem globalne međuzavisnosti. Danas se sve više o problemima demokratije raspravlja, a da se ne poklanja dovoljna pažnja međuodnosima naroda i država. Novi nekonvencionalni pokušaji ostvarivanja uticaja na tuđoj teritoriji postaju sve više karakteristični ne samo za velike sile već i za slabije države ili nedržavne subjekte, koji se na drugi način vojno moćnijoj državi ne bi mogli suprostaviti. Jedna od osnovnih jedinica uticaja na neprijatelja sve više postaje informacija, u njenim različitim oblicima. Informacija pruža mogućnost da se dobiju podaci o slabosti neprijatelja i da bude upotrijebljena kako bi se uticalo na političke odluke ili na tok ekonomskog prosperiteta, vojnog udruživanja i sl. Informacija takođe ima moć da utiče na promjenu svijesti stanovniš-

1 Dostupno na: https://www.hrw.org/news/2023/10/11/real-or-fake-verifying-video-evidence-israel-and-palestine

tva neke države, da se stvara haos i anarhija, ili da probudi dodatne pozitivne ili negativne emocije prema nekom državnom subjektu. Kada su hibridni napadi u pitanju informacija postaje naročito značajna zbog njene fluidnosti koja podvlači sposbnost infiltracije u svaki subjekt uz pomoć medija. Očekuje se da će ratovi informacija i u budućnosti biti sve više korišćeni u cilju obmanjivanja stanovništva ili njegovog okretanja na stranu koja emiteru hibridnih uticaja u datom trenutku odgovara, zbog čega je veoma korisno uložiti što više sredstava u edukaciju stanovništva kada je u pitanju medijska pismenost, osnaživanju građana u pogledu zdravih ideoloških uvjerenja i patriotskih nastojanja, poboljšanje standarda življenja, koji bi mogli predupredити subverzivne djelatnosti i špijunažu među lokalnim stanovništvom.

Hibridne prijetnje nisu novi problem svijetu. One predstavljaju sposobnost državnih ili nedržavnih aktera da koristeći konvencionalne i nekonvencionalne mjere unutar i izvan prostora borbenog djelovanja, utiču na protivnički proces donošenja odluka. Uključuje stapanje djelovanja konvencionalnim naoružanjem, oružjem za masovno uništenje, terorizma, cyber napada i kriminala, sa efikasnim sprovedenim informacijskim operacijama. Razlog zbog kojeg hibridne prijetnje danas izazivaju posebnu pažnju jeste njihov nagli rast, ubrzanje tempa djelovanja, složenost, različitost, šire povezivanje aktera poput terorista i kriminala, transnacionalnost njihovih veza i djelovanja. Opasnost od njih ubrzano narasta zbog lakoće međusobnog komuniciranja, dostupnosti međunarodnih resursa koji uključuju finansiranje i pristup naoružanju.

Države će u neposrednoj budućnosti biti izvrgnute političkom, ekonomskom, socijalnom i informacijskom djelovanju svojih protivnika čime će nastojati povećati učinkovitost drugih oblika nevojnog i vojnog djelovanja koje već provode. Novi protivnici nemaju lako prepoznatljivu vojnu strukturu ili gravitacijska središta koja se mogu vojno neutralizirati, te se zacijelo neće ograničavati odredbama međunarodnog prava i postavki međunarodne zajednice. Takođe se od njih neće moći očekivati sklonost pregovorima ni popuštanje pod prijetnjama. Globalni manjak resursa, ekstremne promjene klime, ekonomske migracije, energetska ranjivost, usporen rast populacije i ideološki ekstremizam, pogodovat će jačanju i razvijanju hibridnih prijetnji.

LITERATURA

1. Arena, P., Wolford, S. (2012). *Arms, intelligence and war*. International Studies Quarterly, 56(2), 351-365.
2. Vuković, N. (2018). *Prilog pojmovnom određenju sintagme „hibridni rat"*. Institut za strategijska istraživanja, Beograd, 11-27.
3. Carter, D.L., Carter, J.G. (2009). *The intelligence Fusion Process for State, Local and Tribal Law enforcment. Criminal justice and Behaviour*, 36(12), 1323-1339.

4. Crosston, M., Valli, F. (2017). *An intelligence civil war: HUMINT vas TECHINT*. Cyber Intelligence and Security, 1(1), 67-81.
5. Dellermann D, Calma A, Lipusch N, Weber T, Weigel S, Ebel P (2019) *The future of human-ai collaboration: a taxonomy of design knowledge for hybrid intelligence systems*. In: Hawaii international conference on system sciences (HICSS). Hawaii, USA.
6. Đurđević, Z., Radović, N. (2017). *Kriminalistička operativa*. Kriminalističko-policijski univerzitet, Beograd.
7. Hoffman, F.G. (2010). *Hybrid Threats: Neither Omnipotent Nor Unbeatable*. Orbis, 54(3), 441-455.
8. Klauzevic, K. (1951). *O ratu*. Vojno delo, Beograd.
9. Kolobara, R. (2019). *Hibridne prijetnje u 21. stoljeću - teorija i istraživanje u nazivlja u Bosni i Hercegovini*. National security and the future, 1-2, 113-140.
10. Krivokapčić, B. (2013). *Pojam rata i klasifikacije ratova.* Megatrend revija, (10-3), 1-3.
11. Linkov, I., Baiardi, F., Florin, M.V., Greer, S., Lambert, J.H., Pollock, M., Trum, B. (2019). *Applying Resilience to Hybrid Threats*. Security & Privacy, 17(5), 78-83.
12. Lewin, R. (1981). *A signal-intelligence war*. Journal of Contemporary History, 16(3), 501-512.
13. Pannier, A., Schmitt, O. (2019). *To fight another day: France between the fight against terrorism and future warfare*. International Affairs, 95(4), 897-916.
14. Pomerantsev, P. (2015). *The Kremlin`s information war*. Journal of demokracy, 26(4), 22-36.
15. Posetti, J., Mathews, A. (2018). *A guide to the history of „fake news" and sisinformation*. International Center for Journalists.
16. Reza, R., Sunvy, A.S. (2023). *The role of fact-cheking sites during the Israeli-Palestine Conflict*. The Indonesian Journal of Communication study, 12, 193-211.
17. Scott, L., Jackson, P. (2004). *The study of intelligence in Theory and Practice*. Intelligence and national security, 19(2), 139-169.
18. Scott, L. (2007). *Sources and Methods in the study of Intelligence: A British view*. Intelligence and national security, 22(2), 185-205.
19. Schiffrin, A. (2017). *Disinformation and democracy*. Jornal of international affairs, 71(1), 117-126.
20. Tapio Pyysalo (Hybrid CoE): *Državni akteri hibridnih prijetnji često se skrivaju iza korisnih idiota*. Biznis i politika. Na sajtu: https://lidermedia.hr/biznis-i-politika/tapio-pyysalo-hybrid-coe-drzavni-akteri-hibridnih-prijetnji-cesto-se-skrivaju-iza-korisnih-idiota-157257. Očitano: 12.12.2024.

UDK 343.433:004(497.16)

AMBER ALERT SISTEM
AMBER ALERT SYSTEM

Mr Danijela Đurković
NVO "Korina"
e-mail: goranovicdanijela1992@gmail.com

Mr Mirko Manojlović
Ministarstvo unutrašnjih poslova / Uprava policije
e-mail: m.manojlovic@t-com.me

Apstrakt

Slučajevi nestanka maloljetnih lica zahtijevaju hitnu reakciju institucija, građana, ali i svih drugih subjekata, kako bi se pronašlo nestalo lice. Za to je, između ostalog, neophodno pravovremeno reagovanje i brz protok informacija. Prikupljanje i distribucija informacija vrši se posredstvom modernih računarskih mreža, evidencionih kartona i slično, ali i pomoću nekonvencionalnih, odnosno alternativnih metoda. Amber Alert sistem je ključan za pronalazak nestalih maloljetnih lica. Aktivira se samo kad su ispunjeni konkretni uslovi. Nastao je 1996. godine u Teksasu i motivisao je mnoge države da uspostave sistem nalik njemu, pa kao rezultat imamo veliki broj zemalja koje su integrisale ovakve sisteme i veliki broj djece je pronađen, zahvaljujući brzom protoku informacija i njihovoj lakoj dostupnosti.
Ključne riječi: *Amber Alert, nestanak maloljetnih lica, Crna Gora.*

Abstract

Cases of missing minors require an urgent response from institutions, citizens, and all other stakeholders to locate the missing person. This necessitates, among other things, timely reactions and rapid information flow. Information collection

and distribution are carried out through modern computer networks, record cards, and similar methods, but also through unconventional or alternative methods. The Amber Alert system is crucial for finding missing minors. It is activated only when specific conditions are met. It originated in 1996 in Texas and has motivated many countries to establish similar systems. As a result, we have a large number of countries that have integrated such systems and a significant number of children who have been found thanks to the rapid flow of information and its easy accessibility.
Keywords: *Amber Alert, missing minors, Montenegro.*

UVOD

Najranjiviji i najosjetljiviji dio svakog društva su djeca, odnosno maloljetna lica. Nestanak djeteta je uvijek posebno traumatičan, stresan i delikatan problem koji utiče prvenstveno na dijete, zatim na roditelje, porodicu, ali i cjelokupnu javnost. Ovakvi događaji ostavljaju ne samo pravne, već i psihološke, pa i socijalne posljedice. Zbog toga u rješavanju ovakvih problema moraju sudjelovati policija, tužilaštvo, centri za socijalni rad, sudovi, ali neizostavno mora biti prisutna pomoć građana i drugih subjekata.

U Crnoj Gori za sada ne postoji zvaničan sistem za pronalazak nestale djece, nalik na Amber Alert sistem. U ovakvim slučajevima policija postupa u skladu sa Zakonikom o krivičnom postupku, Krivičnim zakonom i Zakonom o unutrašnjim poslovima, kada potraga za nestalim licem počinje prijavom nestanka, odnosno, saznanjem policije da je lice nestalo.

Zakonik o krivičnom postupku Crne Gore dopušta policiji objavljivanje fotografije nestalih lica, ako postoje osnovi sumnje da je do smrti, odnosno nestanka tih lica došlo usljed krivičnog djela. Takođe, Zakon o unutrašnjim poslovima dopušta policiji da može zahtjevom prikupljati podatke od organa, privrednih subjekata, pravnih i fizičkih lica, koji su dužni da omoguće uvid u podatke ili da dostave podatke o kojima vode evidencije u okviru svojih nadležnosti i ovlašćenja.

Ipak, nestanak maloljetnih lica zahtijeva hitnu reakciju koja podrazumijeva, ne samo angožavnje policije, već i alarmiranje javnosti, kako bi se informacije što brže širile, a samim tim i dijete spasilo u što kraćem roku, po mogućnosti bez štetnih posljedica. U nastavku će biti riječ o sistemu koji uključuje širenje informacija i obavještavanje građana o nestanku lica putem televizije, društvenih mreža, radio stanica, bilborda, graničnih prelaza, mobilnih obavještenja i slično.

NASTANAK I RAZVOJ

Amber Alert je sistem koji je nastao 1996. godine u Teksasu kao produkt nezadovoljstva građana koji su krivili institucije da nijesu preduzele sve potrebne radnje, kako bi pronašli djevojčicu po imenu Amber Hagerman. Sam naziv predstavlja skraćenicu od *America's Missing: Broadcast Emergency Response*, a takođe je i akronim nastao po imenu djevojčice Amber (Miller, Griffin, Clinkinbeard i Thomas, 2009, str. 111-112).

Naime, dana 3. 1. 1996. godine u popodnevnim časovima nestala je djevojčica Amber. Majka joj je dopustila da vozi bicikl u blizini njihove kuće, nakon čega je njena kćerka nestala. Detalji nestanka su ostali nepoznati. Prema tvrdnjama svjedoka muškarac koji je vozio crni kamion uveo je djevojčicu u svoje vozilo ostavivši bickl iza sebe. Nakon četiri dana tijelo djevojčice je pronađeno u potoku (bemidjistate.edu, 2018).

Upravo je ovaj slučaj probudio građane i izazvao širenje nezadovoljstva, kao i nepovjerenja u institucije koje su nadležne za rješavanje slučajeva nestanka djece, odnosno otmica. Zahtijevali su da država pronađe način hitnog reagovanja u ovakvim slučajevima. Postojao je prijedlog da se uvede program stvaranja vanrednih situacija, odnosno podizanja uzbune, što je rezultiralo stvaranjem Amber sistema.

Nakon toga su i druge države težile da naprave sopstvene sisteme upozorenja koji bi se na kraju usvojio na nivou nacije. Može se reći da se značajni pomaci nijesu dešavali u periodu 1996 - 2001. godine. Na samom kraju 2001. godine samo su četiri države imale planove za navedeni sistem, da bi se 2002. godine desio značajan pomak. Tada je održana prva konferencija u Bijeloj kući na temu nestale, eksploatisane i odbjegle djece. Naredne godine, predsjednik Sjedinjenih Američkih Država potpisao je Zakon o zaštiti koji se odnosi na istragu i krivično gonjenje zločinaca koji su izvršili krivična djela nad djecom, pri čemu je koordinatoru Amber sistema dodijelio nova zaduženja: da olakša razvoj Amber mreže, da podrži razvoj državnih Amber sistema, da pokuša da otkloni geografske prepreke u Amber sistemima, da uspostavi regionalnu saradnju i tako dalje. Nakon toga donesene su konkretne smjernice za funkcionisanje sistema, a 2005. godine već je 50 država imalo ovaj sistem i radilo se na tome da bežični korisnici mogu primati upozorenja. Naredna godina obilježena je pokretanjem nacionalnih i multimedijalnih kampanja javnog servisa. Društvena mreža *Facebook* 2011. godine kreira pojedinačnu stranicu za svaku državu koja bi izdavala upozorenja, kao i jednu nacionalnu stranicu. Naredne godine i *Google* integriše Amber system, a 2013. godine zvanično počinju bežična upozorenja, kao i aktivacija sistema na *Twiteru*. Na kraju, 2015. godina je okarakterisana kao godina obučavanja policajaca i usavršavanja postojećih metoda (amberalert.ojp.gov).

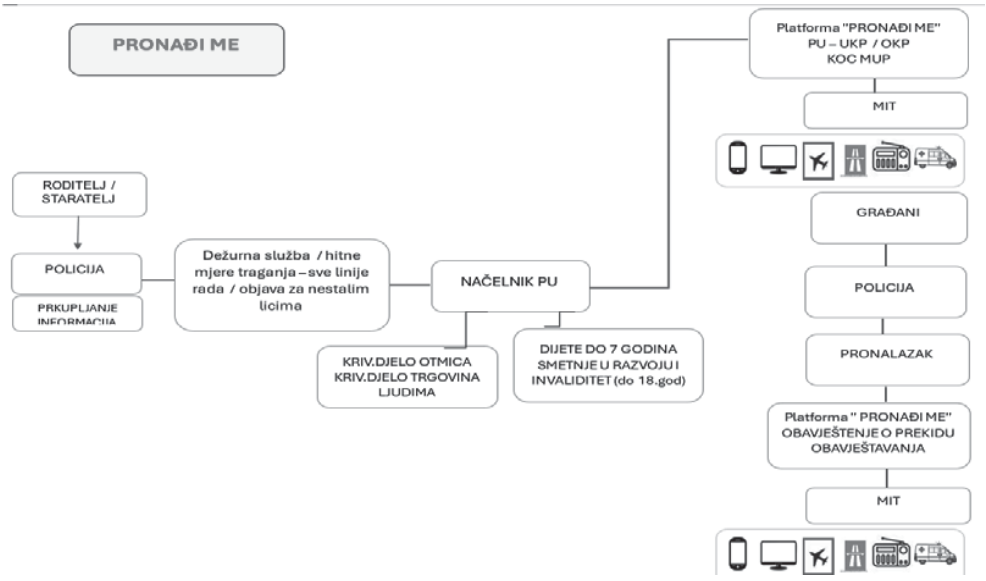
Očigledno je da su počeci uspostavljanja Amber sistema iziskivali dosta vremena, znanja i truda kako bi on bio funkionalan i efikasan kao što je danas. Slučaj djevojčice Amber doveo je do razvoja sistema upozorenja koji je zaslužan za spas velikog broja dječijih života.

SISTEMI ŠIROM SVIJETA PO UZORU NA AMBER ALERT SISTEM

Učinak Amber sistema za pronalazak nestale djece postaje uvažen i od drugih zemalja, van granica SAD-a gdje je i nastao. Vremenom, širom svijeta počeli su da se stvaraju novi sistemi po uzoru na Albert sistem. Međunarodni centar za nestalu i eksploatisanu djecu (*The International Centre for Missing and Exploited Children*) godinama pruža tehničku pomoć zemljama koje rade na stvaranju i razvijanju sistema uzbune za nestanak djece. Takođe, predstavljaju veznu tačku kontakata, što u mnogome olakšava razvoj sistema, razmjenu iskustava i mišljenja.

Osim Sjedinjenih Američkih Država, sljedeće države imaju sisteme stvorene po uzoru na Amber sistem: Albanija, Argentina, Australija, Belgija, Bugarska, Kanada, Kipar, Češka, Ekvador, Francuska, Grčka, Irska, Italija, Jamajka, Litvanija, Luksemburg, Malezija, Malta, Meksiko, Holandija, Novi Zeland, Poljska, Portugal, Rumijija, Slovačka, Južna Afrika, Južna Koreja, Španija, Švajcarska, Tajvan (pokrajina Kina), Ujedinjeni Arapski Emirati, Ujedinjeno Kraljevstvo (www.icmec.org, 2024.).

U Srbiji je 25. 10. 2023. godine pokrenut sistem „*Pronađi me*" za hitno obavještavanje javnosti u slučajevima nestanka maloljetnih lica. Svrha sistema je da se na najbrži način distribuiraju informacije (u slučajevima kada policija procijeni da treba aktivirati si-



Šematski prikaz funkcionisanja "Pronađi me" sistema u Srbiji

U Rusiji je 2019. godine Megafon razvio sopstveni sistem upozorenja. Obuhvata sve oblasti Rusije u kojima je MegaFon zastupljen i koristi se i za potragu za djecom i

odraslim. Maroko je 2023. godine razvio sistem pod nazivom „Tifli Moukhtafi“ (u prevodu „moje dijete je nestalo”). Ukrajina 2021. godine je najavila pokretanje Amber sistema. U 2008. godini u Holandiji je takođe stvoren sistem upozorenja.

Bitno za istaći je i to da je kreirana *Amber Alert Europe* fondacija 2013. godine, kako bi doprinijela boljoj prekograničnoj koordinaciji i saradnji u potrazi za nestalom djecom. Njena svrha je razmjena znanja, stručnosti i prakse po pitanju nestale djece. Ista povezuje stručnjake iz 44 vladine organizacije, posebno ministarstava unutrašnjih poslova i policije i nevladinih organizacija iz 27 zemalja širom Evrope. Takođe, fondacija vodi računa o zakonodavnim okvirima prilikom sprovođenja aktivnosti. Sve aktivnosti se sprovode u skladu sa Poveljom EU o osnovnim pravima i Strategijom EU o pravima djeteta i uz poštovanje privatnosti djece i zakona o zaštiti podataka (amberalert.eu, 2024).

STRATEGIJA AMBER SISTEMA

Strategija Amber Alert sistema podijeljena je u tri glavne cjeline. Strategija je nastala 2019. godine, a modifikovana 2023. godine. Njen cilj je da uspostavi prioritetne oblasti djelovanja i radi na njihovom prosperitetu i daljem napretku.

Prvi dio strategije vezan je za trenutnu procjenu aktivnosti Amber sistem upozorenja i određivanje lokalnih, državnih i regionalnih planova. Takođe, ovdje spadaju i poređenje operacija plana, kao i samih kriterijuma sistema. Na kraju, u ovom dijelu strategije spada i procjena dostupne tehnologije.

Drugi dio strategije je baziran na kreiranje koordinisanja mreže upozorenja i razvijanje smjernica o izdavanju upozorenja. Dalje, u ovom dijelu se govori o uspostavljanju partnerstava (lokalna, savezna, državna, plemenska, teritorijalna). Pored ostalog, tu je i promocija tehnološke kompatabilnosti među komunikacionim sistemima.

U poslednjem dijelu strategije govori se o naučenim lekcijama, o radu sa organima koji su zaduženi za sprovođenje zakona, kao i o podizanju svijesti javnosti o tome na koji način da zaštite djecu i spriječe otmice (amberalert.ojp.gov, 2023).

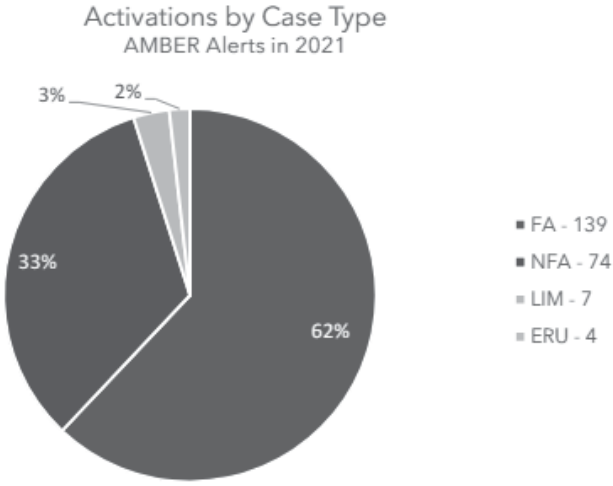
KATEGORIZACIJA SLUČAJEVA U AMBER SISTEMU

Postoje određene specifičnosti po kojima je moguće kategorizovati slučajeve, a u Amber sistemu postoje četiri ključne kategorije (amberalert.ojp.gov, 2006):

- porodična otmica / Family Abduction (FA)

- neporodična otmica / Nonfamily Abduction (NFA)
- izgubljeni, povrijeđeni ili nestali na drugi način / Lost, Injured or Otherwise Missing (LIM)
- ugroženi bjegunac / Endangered Runaway (ERU).

Porodičnom otmicom (FA) smatra se otmica gdje se u ulozi otmičara nađe član porodice otetog djeteta. Neporodična otmica (NFA) podrazumijeva za otmičara djeteta osobu koja nije povezana sa otetim djetetom i / ili sa porodicom djeteta. Izgubljeni, povrijeđeni ili nestali na drugi način (LIM) uključuje one slučajeve za koje su nepoznate okolnosti nestanka djeteta. Dakle, u ovoj kategoriji ne postoje informacije na koji način je došlo do nestanka. Ugroženi bjegunac (ERU) obuhvata slučajeve djece koja su pobjegla, a koja se nalaze u neposrednoj opasnosti.



U prethodnom dijagramu moguće je vidjeti slučajeve iz 2021. godine koji su objavljeni u godišnjem izvještaju Amber sistema. Naime, od ukupnog broja otmica za navedenu godinu najviše je bilo porodičnih otmica, gotovo dvije trećine. Porodične otmice smatraju se najbezbjednijim (Griffin i Miller, 2008, s. 160). Na drugom mjestu nalaze se neporodične otmice, a za njima oni slučajevi gdje je lice izgubljeno, povrijeđeno ili na neki drugi način nestalo. Najmanje slučajeva je bilo bježanja djece koja su se nakon toga nalazila u opasnosti (missingkids.org, 2022).

PROCEDURA ZA AKTIVACIJU

Jedan od najvećih problema sa kojim se susreću sve zemlje svijeta svakako je nestanak djece, odnosno maloljetnih lica. Kako bi odgovorili ovom izazovu, razvijene zemlje, ali i one koje su u tranziciji, usavršile su različite modalitete djelovanja i pre-

duzimanja mjera i radnji, služeći se savremenim naučno-tehničkim dostignućima. Kao što je već rečeno, jedan on najpoznatijih i najzastupljenijih sistema koji se koristi u cilju pronalaska nestalih maloljetnih lica je Amber sistem (*America's Missing: Broadcast Emergency Response*). Navedeni sistem u slučaju potrebe, podrazumijeva angažovanje organa za sprovođenje zakona, radio i televizijske industrije i mreže drugih medijsko-elektornskih uređaja i znakova. U Sjedinjenim Američkim Državama gdje je Amber sistem i nastao, a prema Kancelariji za maloljetničko pravosuđe i prevenciju delinkvencije, godišnje se prijavi nestanak gotovo 800 000 djece, odnosno oko 2000 djece na dnevnom nivou. Od ukupnog broja prijava, jedna trećina se odnosi na kidnapovanu djecu.

Osnovni princip na kom se zasniva Amber sistem jeste upoznavanje što većeg broja ljudi za što kraće vrijeme, kako bi se dijete pronašlo u prvih nekoliko sati nakon otmice. Prema studiji američkog Ministarstva pravde, 74% djece koja su oteta i kasnije pronađena u beživotnom stanju, ubijena su u prvih nekoliko sati nakon otmice.

Prema raspoloživim podacima iz država koje primenjuju ovaj sistem upozorenja ustanovljeni su približni kriterijumi za pokretanje Sistema (Nikač, Leštanin, 2021, str. 138-139):

- traga se za maloljetnim licem;
- po mišljenju policije aktiviranje Sistema neće ugroziti život lica za kojim se traga;
- postoji sumnja da otmičar ima namjeru da povrijedi oteto dijete;
- nestanak ima za posljedicu ugrožavanje života otetog lica;
- dostupne su informacije za aktiviranje Sistema (opis, grderoba i sl.);
- druge okolnosti.

DRUGA STRANA AMBER SISTEMA

Cilj ovog rada nije da predstavi Amber sistem kao savršeno sredstvo za pronalaženje otete djece, već da prikaže realnu sliku sistema sa njegovim, kako dobrim, tako i lošim stranama. Prije svega treba istaći da ovaj sistem i njemu slični, nijesu djelotvorni u svim slučajevima otmica djece.

Naime, sistem je izuzetno djelotvoran kada je u pitanju otmica koja je učinjena bez namjere da se dijete povrijedi ili liši života. To su uglavnom oni slučajevi gdje se kao otmičari pojavljuju roditelji, staratelji ili bliski srodnici djeteta. U slučajevima kada su otmičari druga lica, čije namjere nijesu povoljne po oteto dijete, postoji rizik da aktiviranje Amber sistema kod otmičara izazove paniku. Međutim, kako su ove otmice same po sebi rizične po dijete, prvi sati od otmice su najbitniji jer su tada najveće šanse da se dijete pronađe bez posljedica.

Dalje, za aktivaciju sistema kljiučno je brzo i pravovremeno reagovanje, postoji mogućnost distribucije netačnih informacija. U pitanju su prve informacije od kojih neke nerijetko budu pogrešne. Razlog je ne samo kratak vremenski period u kojem se prenose, već i sama zbunjenost, strah, panika kod roditelja ili drugih osoba koje daju prve informacije. Takođe, i svjedoci mogu biti ti koji će pružiti pogrešne informacije. Na primjer, neko lice je vidjelo automobil kojim je otmičar odvezao dijete. Pokušaće da zapamti marku automobila, boju kao i broj registaskih oznaka. Međutim, zbog brzine, iznenadnog događaja i straha, svjedok može permutovati brojeve registarskih oznaka i time potragu usporiti ili skrenuti u pogrešnom pravcu.

U američkim državama, građani su kao anomaliju ovog sistema naveli to što im obavještenja da je neko dijete nestalo izaziva strah i anksioznost. Neki su pak išli i dalje od toga, te su izjavljivali da su umorni od ovih upozorenja. Ovakav stav nije zanemarljiv jer nam govori da se zapravo građani vremenom mogu navići na činjenicu da je neko dijete nestalo što može dovesti do manjka empatije, odnosno do ravnodušnosti. Vjerujemo da se ovakav stav ne može čuti u državama koje imaju manji broj stanovnika, odnosno u državama u kojima nije velika stopa otmica djece, jer se sistem ne aktivira često, te ne može doći do „zasićenja".

Takođe, u Američkim državama primjetna je rasna nejednakost prilikom aktiviranja sistema. Naime, crni Amerikanci nestaju u značajnom broju u poređenju sa drugim rasama. Međutim, ovi slučajevi često budu odbačeni od strane policije zbog raznih predrasuda, odnosno dovođenja ovih lica u vezu sa kriminalom.

Kao jednu od mana ovog sistema navodi se i ugrožavanje bezbjednosti u saobraćaju. Ovdje se misli na skretanje pažnje vozačima prilikom vožnje. Neki smatraju da bilbordi, razna obavještenja, odnosno drugi načini prikazivanja informacija o nestalom djetetu, kao i obavještenja putem mobilnih telefona mogu vozaču narušiti koncentraciju, što može dovesti do izazivanja saobraćajne nezgode.

Većina navedenih mana u Crnoj Gori bi mogla da se eliminište. Ako bi uzeli u obzir broj stanovnika, stopu kriminala, učestalost nestanka lica i okolnosti pod kojima se sistem aktivira, možemo pretpostaviti da ne bi dolazilo do "zasićenja" i stvaranja ravnodušnosti kod građana, jer se Amber sistem se ne bi često upotrebljavao. Dakle, samo u specifičnim okolnostima, kada se zna da dosadašnje metode koje su korištene neće dati rezultat, kada je u pitanju maloljetno lice, bez obzira na rasu, pol, nacionalnost, vjeroispovjest i druga lična obilježja, Amber sistem bi se stavljao na raspolaganju nadležnim organima.

STATISTIČKI PODACI ZA 2022. GODINU - SAD

Tokom 2022. godine u SAD izdato je 181 Amber upozorenje. Ovim upozorenjima obuhvaćeno je 227 djece. Od ukupnog broja upozorenja 180 slučajeva je uspješno okončano. Do 10. marta 2023. (do izrade izvještaja za 2022. godinu) jedno dijete se još uvek vodi kao aktivno nestalo, dok je četvoro djece pronađeno mrtvo. Da nije svaki nestanak djeteta istinit, potvrđuje i to što je za šest slučajeva naknadno utvrđeno da su prevara, a za drugih šest da su neosnovani. Za slučajeve za koje je utvrđeno da nijesu lažni ili neosnovani, bilo je 98 porodičnih otmica, 59 neporodičnih otmica, sedmoro djece je pobjeglo od kuće ili iz ustanove i pet izgubljene, povrijeđene ili na drugi način nestale djece.

Kada je riječ o statistici otmičara za navedeni period identifikovano je 180 otmičara koji su učestvovali u 151 slučaju. Mahom su muškarci bili otmičari i to 61% (n=110), a 34% (n=62) otmičara je bilo je ženskog pola. Pol za četiri procenta (n=8) otmičara bio je nepoznat.

Bitno je istaći da kada su u pitanju otmice ne mora biti isključivo jedan otmičar, niti samo jedna veza između otmičara i otetog lica, pa se dešava da statistika prezentuje veći broj otmičara u odnosu na broj otmica. Kao primjer možemo uzeti dadilju koja je otela dijete. Za nju ne možemo reći da je potpuni stranac, već osoba koja je poznata porodici, vjerovatno i bliska. Međutim, ukoliko dadilja u otmicu uključi i svog prijatelja, onda i on postaje saučesnik otmičar koji se tretira kao nepoznata osoba.

Istom statistikom prezentovano je da je u 51 slučaju otmičar bio otac, u 35 slučajeva otmicu je izvršila majka, dok je nepoznato lice u 37 slučajeva bilo otmičar. U pogledu vremenskog protoka u 2022. godini 73% djece (n=16) se uspješno oporavilo u roku od tri sata od oglašavanja upozorenja (amberalert.rs, 2023).

ZAKONODAVNI OKVIR U CRNOJ GORI

Kao i ostale države i Crna Gora je problem otmice zakonodavno definisala. Tako je Krivičnim zakonikom Crne Gore, u dijelu Krivična djela protiv sloboda i prava čovjeka i građanina članom 164 navedeno krivično djelo otmice:

1. Ko silom, prijetnjom, obmanom ili na drugi način odvede ili zadrži neko lice u namjeri da od njega ili drugog lica iznudi novac ili kakvu drugu imovinsku korist ili da njega ili koga drugog prinudi da nešto učini, ne učini ili trpi, kazniće se zatvorom od jedne do osam godina.
2. Ko radi ostavarenja cilja otmice prijeti ubistvom ili teškom tjelesnom povredom otetom licu, kazniće se zatvorom od dvije do deset godina.

3. Ako je oteto lice zadržano duže od deset dana ili je prema njemu postupano na svirep način ili mu je teško narušeno zdravlje ili su nastupile druge teške posljedice ili ko djelo iz stava 1 ovog člana učini prema maloljetnom licu, učinilac će se kazniti zatvorom od dvije do dvanaest godina.
4. Ako je usljed djela iz st. 1, 2 i 3 ovog člana nastupila smrt otetog lica ili je djelo izvršeno od strane više lica na organizovan način, učinilac će se kazniti zatvorom od pet do petnaest godina.

Svakako povezana krivična djela kada je riječ o nestanku lica su i prinuda, protivpravno lišenje slobode, ugrožavanje sigurnosti, kao i zlostavljanje i mučenje.

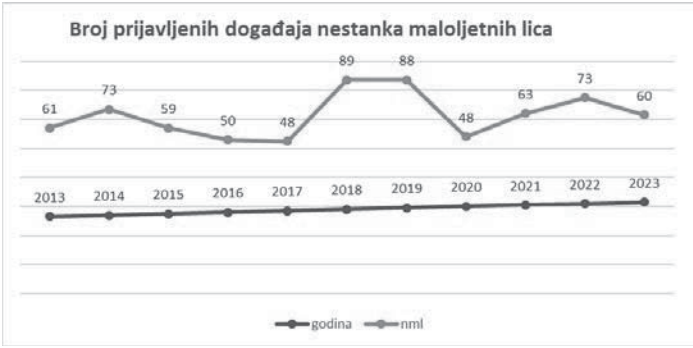
Slobode i prava čovjeka su osnovna prava koja su zaštićena kako na međunarodnom nivou tako i na nacionalnom. Ovdje je neizostavno spomenuti Univerzalnu deklaraciju o ljudskim pravima UN iz 1948. godine, kao i Evropsku konvenciju o ljudskim pravima i osnovnim slobodama iz 1950. godine.

Crna Gora prvenstveno Ustavom, kao najvišim pravnim aktom, štiti slobodu građana, a zatim i kroz zakonodavne odredbe.

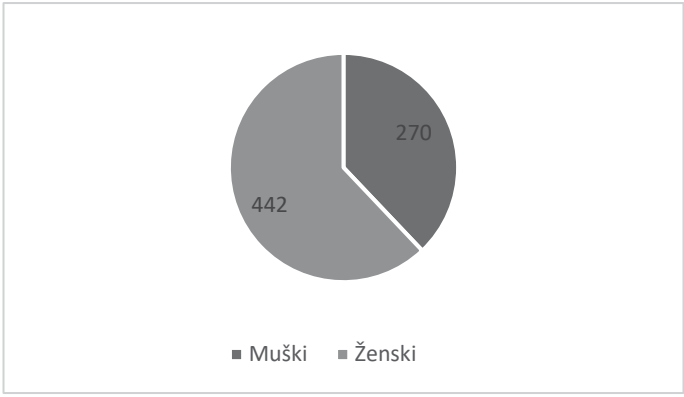
STATISTIČKI PODACI U CRNOJ GORI ZA PERIOD 2013-2023. GODINA

Na osnovu Zakona o slobodnom pristupu informacija Crne Gore, od strane Ministarstva unutrašnjih poslova Crne Gore, prikupljena je određena dokumentacija, nakon čega se primjenom metode dokumentacione analize došlo do podataka koji se odnose na broj nestalih i pronađenih maloljetnih lica i podataka koji se odnose na pol istih. Podaci koje se odnose na broj podnijetih odgovarajućih prijava nadležnim organima, podaci koji se odnose na pol i starost eventualnih izvršilaca krivičnih djela koja se mogu dovesti u vezu sa nestankom maloljetnih lica, vrijeme i mjesto nestanka maloljetnih lica i njihov uzrast, nijesu dostupne jer navedena institucija ne vodi evidenciju takvog tipa, pa samim tim ne raspolaže navedenim podacima.

Shodno navedenom, u Crnoj Gori za period od 10 godina (od 1. 1. 2013. godine do 1. 1. 2024. godine) prijavljen je nestanak 712 maloljetnih lica i isto toliko ih je pronađeno. Na teritoriji Crne Gore, za navedeni period nisu evidentirana maloljetna lica koja su žrtva otmice ili drugih nestanaka pod nerazjašnjenim okolnostima, već se nestanak u najvećem broju slučajeva odnosio na samovoljna udaljavanja, odnosno bjekstva maloljetnih lica od kuće ili ustanove nezavodskog tipa (JU Centar „Ljubović“). U narednim dijagramima dat je broj raspisanih potraga po godinama, za nestalim maloljetnim licima, kao i struktura pola nestalih maloljetnih lica.



Dijagram br. 1 - Broj raspisanih potraga po godinama, za nestalim maloljetnim licima



Dijagram br. 2 – Struktura pola nestalih maloljetnih lica

ANKETA

Za potrebe pisanja ovog rada, izvršeno je istraživanje na temu Amber Alert sistema u Crnoj Gori, pa je tokom maja 2024. godine sprovedena anketa u kojoj je učestvovao 501 ispitanik. Anketirana su punoljetna lica različite starosne dobi i oba pola, koji žive u Crnoj Gori i isti su odgovarali na više pitanja koja se tiču stanja bezbjednosti u Crnoj Gori i Amber Alert sistema. Nakon prikupljenih podataka isti su obrađeni gdje su dobijeni sledeći rezultati:

Od ukupno 501 ispitanika, njih 400 ili 79,84% je ženskog pola, dok je 101 ili 20,16% ispitanika muškog pola. Što se tiče starosne dobi, ista je podijeljena u tri kategorije i to: od 18 do 30 godina, od 30 do 60 godina i iznad 60 godina. U tom smislu, prva grupa ispitanika obuhvata 119 lica, odnosno 23,75%, druga grupa obuhvata 344 lica ili 68,66% i treća grupa obuhvata 38 lica odnosno 7,59%, pri čemu je najmlađi ispitanik

imao 18 godina, dok je najstariji imao 86 godina. Kako je anketa vršena na teritoriji Crne Gore, od ukupnog broja ispitanika, njih 15,97% (No. 80) je iz sjeverne regije, 61,8% (No. 307) iz centralne regije i 22,75% (No. 114) iz južne regije.

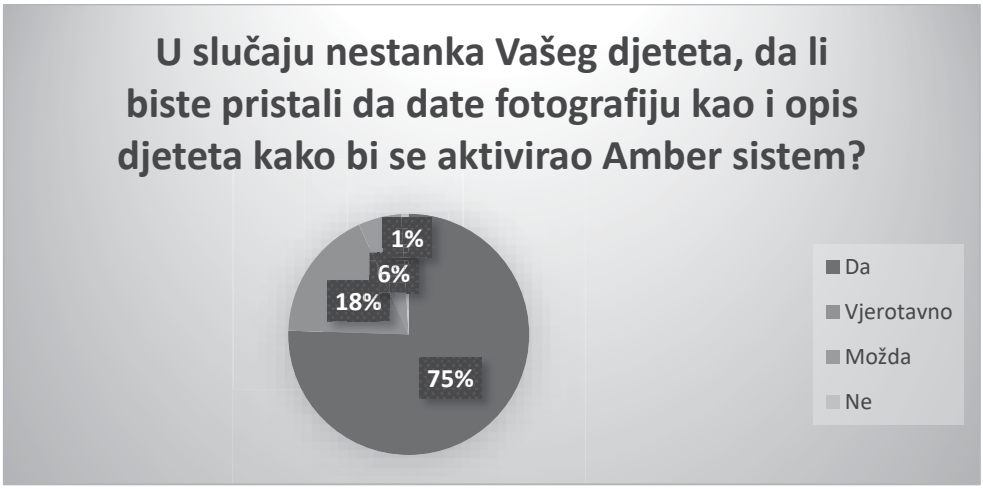
Na pitanje „Da li smatrate da je Crna Gora bezbjedna država za djecu?“, odgovori su podijeljeni u pet kategorija, a u narednom dijagramu je prikazan rezultat anketiranja:

Dijagram br. 3

Od ukupnog broja ispitanika, njih 180, odnosno 36% je odgovorilo da smatraju da je Crna Gora prilično bezbjedna, dok gotovo trećina smatra da je Crna Gora nedovoljno ili nije uopšte bezbjedna država za djecu.

Na pitanje “Da li ste čuli za sigurnosni sistem Amber Alert i da li ste upoznati sa njegovom svrhom?”, 78,8% ispitanika je odgovorilo potvrdno, dok je 21,2% ispitanika imalo negativan odgovor. Na pitanje “Da li smatrate da je Crnoj Gori potreban ovakav sistem brzog djelovanja u slučajevima nestanka djece?”, 94,6% ispitanika smatra da je Crnoj Gori potreban ovakav sistem.

Takođe, u sledećem dijagramu prikazan je rezultat analize odgovora na pitanje “U slučaju nestanka Vašeg djeteta da li biste pristali da date fotografiju kao i opis djeteta kako bi se aktivirao Amber sistem?”, gdje su ispitanici imali mogućnost odabira jednog od četiri odgovora:



Od ukupnog broja, čak ¾ ispitanika je odgovorilo da bi sa sigurnošću dostavilo potrebne informacije o svom djetetu kako bi se aktivirao Amber sistem, dok je 7% odgovorilo da bi možda ili ne bi uopšte dostavilo potrebne informacije.

Na pitanje "Ukoliko biste prepoznali dijete koje je predmet aktiviranja Amber Sistema, na koji način biste reagovali?" gotovo svaki ispitanik (96,8%) se izjasnio da bi pozvao policiju, dok su se ostali izjasnili da zavisi od konkretne situacije, da bi samoinicijativno djelovali ili se nisu izjasnili uopšte. Osim što bi pozvali policiju, najveći broj ispitanika se izjasnio da bi putem sredstava javnog informisanja ili putem društvenih mreža pokušali da daju svoj doprinos.

ZAKLJUČAK

Amber Alert predstavlja brzi i efikasni sistem širenja informacija u slučajevima nestanka djece, sa ciljem da se ista ponađu u što kraćem vremenskom periodu, sa što manje negativnih posljedica. U ovom sistemu postoje četiri ključne podjele nestanka djece. U pitanju su porodična otmica / family abduction (FA); neporodična otmica / nonfamily abduction (NFA); izgubljeni, povrijeđeni ili nestali na drugi način / lost, injured or otherwise missing (LIM); ugroženi bjegunac / endangered runaway (ERU). Takođe, postoji i jasna procedura za pokretanje ovog sistema, pa je potrebno da budu ispunjeni svi propisani uslovi, kako bi se isti aktivirao.

Mnoge zemlje osposobile su sisteme nalik Amber Alert sistemu. U Crnoj Gori za sada ne postoji ovakav sistem, već policija postupa u skladu sa Zakonikom o krivičnom postupku, Krivičnim zakonom i Zakonom o unutrašnjim poslovima, kada dođe u saznanje da je lice nestalo.

Iz navedenih rezultata istraživanja sprovedenog na teritoriji Crne Gore može se vidjeti da građani većinom smatraju Crnu Goru bezbjednom državom za djecu što korespondira podacima dobijenim iz MUP CG – da su sva nestala maloljetna lica i pronađena i da nije bilo otmica odnosno nestanaka pod nerazjašnjenim okolnostima.

S obzirom na dobijene rezultate istraživanja možemo zaključiti da u Crnoj Gori građani većinom žele ovakav sistem. Ukoliko bi se spasio makar jedan dječiji život pomoću sistema kao što je Amber Alert, on bi opravdao svoju svrhu postojanja i ne postoje materijalni izdaci koji mogu biti važniji od činjenice da jedno dijete može biti vraćeno svojoj porodici.

Posmatrajući kompletnu sliku ovakvih sistema, i uzimajući u obzir i njihove dobre i loše strane, smatramo da ovakvi sistemi mogu biti korisni u specifičnim slučajevima kada se pretpostavlja da se na drugačiji način ne mogu postići željeni rezultati. Takođe, smatramo da bi ovakvi sistemi trebali da obuhvataju lica do 18. godina starosti, a kada su u pitanju osobe sa smetnjama u razvoju starosna granica bi trebala biti veća.

LITERATURA

1. amberalert.eu, (2024). Amber Alert Europe foundation. Dostupno na: https://www.amberalert.eu/about-us, preuzeto: 24. 5. 2024. godine.
2. amberalert.ojp.gov (2006). Analysis of AMBER-Alert Cases in 2006. Dostupno na: https://amberalert.ojp.gov/sites/g/files/xyckuh201/files/media/document/06_amber_report.pdf, preuzetp 15. 5. 2024. godine.
3. amberalert.ojp.gov, (2023). National strategy. Dostupno na: https://amberalert.ojp.gov/about/national-strategy, preuzeto 27. 5. 2024. godine.
4. amberalert.ojp.gov, (2024). Amber Alert timeline. Dostupno na: https://amberalert.ojp.gov/sites/g/files/xyckuh201/files/media/document/amberalerttimeline-508c_0.pdf, preuzeto 24. 5. 2024. godine.
5. amberalert.rs, (2023). Statistika Amber Alerta za 2022. (SAD). Dostupno na: https://amberalert.rs/statistika-amber-alerta-za-2022-sad/, preuzeto 30. 5. 2024. godine.
6. bemidjistate.edu, (2018). An Analysis of the Unintended Effects of the AMBER Alert System. Dostupno na: https://www.bemidjistate.edu/academics/honors/wp-content/uploads/sites/73/2022/11/An-Analysis-of-the-Unitended-Effects-of-the-AMBER-Alert-System-Bloomquist-Josiah-4.23.18.pdf, preuzeto 17. 5. 2024. godine.
7. Griffin, T. i Miller, M. (2008). *Child Abduction, AMBER Alert, and Crime Control Theater*, Criminal Justice Review, Vol. 33, No. 2.

8. icmec.org, (2024). *Spurring community action to find missing children*. Dostupno na: https://www.icmec.org/global-missing-childrens-center/child-alerts/, preuzeto 24. 5. 2024. godine.
9. *Krivični zakonik Crne Gore*, Službeni list Crne Gore, br. 70/2003, 13/2004 - ispr. i 47/2006 i "Sl. list CG", br. 40/2008, 25/2010, 32/2011, 64/2011 - dr. zakon, 40/2013, 56/2013 - ispr., 14/2015, 42/2015, 58/2015 - dr. zakon, 44/2017, 49/2018 i 3/2020 (2020).
10. missingkids.org, (2022). Analysis of AMBER Alert Activations in 2021. Dostupno na: https://www.missingkids.org/content/dam/missingkids/pdfs/amber/2021_Annual_AMBER_Alerts_Report_Final.pdf, preuzeto 15. 5. 2024. godine.
11. Nikač, Ž. i Leštanin, B. (2021). *Zbornik radova Kopaoničke škole prirodnog prava. Uvođenje "Amber alert" Sistema u rad policije Srbije radi zaštite života dece i maloletnika*.
12. Savjet Evrope, (1950). *Evropska konvencija o o ljudskim pravima i osnovnim slobodama.*
13. Ujedinjene nacije, (1948). *Univerzalna deklaracija o ljudskim pravima*.
14. *Ustav Crne Gore*, Službeni list Crne Gore, br. 1/2007 i 38/2013 - Amandmani I-XVI (2013).
15. *Zakon o unutrašnjim poslovima*, Službeni list Crne Gore, br. 70/2021 i 123/2021 (2021).
16. *Zakonik o krivičnom postupku Crne Gore*, Službeni list Crne Gore, br. 57/2009, 49/2010, 47/2014 - odluka US, 2/2015 - odluka US, 35/2015, 58/2015 - dr. zakon, 28/2018 - odluka US i 116/2020 - odluka US (2020).

UDK 502/504:004(497.4)

E-WASTE: THE INVISIBLE DANGER TO INFORMATION SECURITY AND ENVIRONMENT

Dr Blaž Markelj
Associate Professor of Criminal Justice and Security,
Faculty of Criminal Justice and Security, University of Maribor, Slovenia
e-mail: blaz.markelj@um.si

Uroš Jelenc
Master's student, Faculty of Criminal Justice and Security,
University of Maribor, Slovenia
e-mail: uros.jelenc@student.um.si

Dr Katja Eman
Associate Professor of Criminology, Faculty of Criminal Justice and Security,
University of Maribor, Slovenia
Corresponding author at: Faculty of Criminal Justice and Security,
University of Maribor
e-mail: katja.eman@um.si

Abstract

E-waste refers to various types of waste electronic appliances and devices, from dishwashers and fridges to smartphones. They are not only hazardous to people and the environment because of their physical composition; many electronic devices can also jeopardise the security of personal data and be used for many forms of cyber crime. This paper focuses on the information security aspects of e-waste, such as PCs, laptops, smartphones, and other devices, that can contain data. These devices, which a user might have for days, months, or years, can contain large quantities of personal and business data. The problem posed by e-waste of this type is that it contains sensitive personal and business data that, unless adequately removed, remains on the device after it is disposed of, sold, or given away. This

paper explores how users handle e-waste and what factors influence their decision to erase data from a device. The results show that the way users currently handle e-waste does not ensure an adequate level of information security. Two factors that compel users to take measures to erase data from devices are: awareness of the limitations of the data-erasure process and past experience with cyber crime. Nevertheless, these cyber and environmental crime issues can pose new challenges for the police.
Key words: *information security, e-waste, cyber crime, environmental crime, erasure of data, electronic devices, Slovenia.*

E-WASTE AND THE THREAT TO INFORMATION SECURITY

Electrical and electronic equipment (EEO) has become an indispensable part of people's lives in various ways; for example, it enables them to carry out everyday tasks and improve their general quality of life. When an electronic device reaches the end of its life because it no longer works, works too slowly, or is replaced by a new model, it becomes e-waste (European Commission, 2013; Osibanjo & Nnorom, 2007; Schiller et al., 2016). A range of different items are classified as e-waste, from household and kitchen appliances to game consoles, mobile phones, and personal computers. Approximately 53.6 million tonnes of e-waste were generated in 2019, with some estimating that this quantity will double by 2050 (Forti et al., 2020).

The main problem is that we produce more e-waste than we can recycle. Forti et al. (2020) warn that only 17.4% of all waste electronic devices are officially collected and recycled. We do not know what happens to the remaining 82.6%, although it is likely disposed of, sold, or recycled in an environmentally damaging way. The lack of information about collecting and recycling e-waste shows that most of that waste is handled outside the official waste-collection system and sent to developing countries. This is a form of organised environmental crime that has been on the increase in the last decade. E-waste also contains dangerous substances, most commonly heavy metals such as lead, mercury, cadmium, and other toxic chemicals that have an adverse effect (bioaccumulation) on the environment and human health (Forti et al., 2020).

Rožnik (2020) has carried out research highlighting the e-waste problem in Slovenia. In her study of 28 cases of unlawful e-waste consignments, she found that Slovenia's geographical position makes it predominantly a transit country for e-waste (unlawful transport of e-waste to neighbouring countries). The findings showed that Slovenian companies exported unlawful e-waste abroad or received consignments of e-waste. E-waste was transported with deficient documentation, or no documentation at all, and with incorrect classification codes.

E-waste is generally divided into six categories depending on size and purpose (Forti et al., 2020): temperature exchange equipment (freezers, refrigerators, air conditioners, and heat pumps), screens and monitors, lamps, large equipment (washing machines, dishwashing machines, etc.), small equipment (toasters, scales, kettles, etc.), and small IT and telecommunications equipment. While not all e-waste contains sensitive data, this paper focuses on two categories of e-waste: 'small IT and telecommunications equipment', which includes mobile phones and personal computers, and 'screens and monitors', which includes laptops and tablets. These types of e-waste contain permanently stored data, hard disk drives (HDDs), solid state drives (SSDs), and read-only memory (ROM) (Hartwig, 2016; Hovav & Ferdani Putri, 2016).

The lack of regulation in the global e-waste industry presents numerous threats. In addition to threats to the environment and health, a new threat has emerged with the sale, recycling, and repair of e-waste: the retrieval of personal and business data on devices that have been disposed of (Chen et al., 2021; Debnath et al., 2020).

Personal computers, laptops, smartphones, and other devices enable us to have considerable amounts of data to hand. Technological advances mean that our devices have become more capable and can provide us with a wide variety of services and functions; however, this also means that our devices are accumulating more significant amounts of data (Zingerle & Kronman, 2019). Due to the speed of technological development and ever-greater data storage capacity, our devices contain more work-related, personal, and financial data than ever (Hartwig, 2016; Schafer, 2014). Data storage media are increasingly being designed to prevent data loss, which is useful for recovering data that a user might have accidentally erased (Ceci et al., 2021).

Unreliable methods are often employed to remove data, such as manual erasure, formatting, or factory resets (Ceci et al., 2021). In most cases, these methods do not completely remove data from a device; they only remove the link between the file name and the place on the device (copy of the metadata) where the file is physically located. Devices that no longer work, perhaps because the battery or power supply is broken, are also problematic, with users not opting to have the device repaired and, at the same time, not carrying out any erasure of data (AVAST, 2014; Blancco, 2017). The use of devices for personal and business purposes also presents a problem. A study by Markelj and Zgaga (2018), which had a sample size of 277, showed that the boundary between personal and business use had been erased; this brings new threats and raises questions regarding the steps that should be taken with a device that has reached the end of its life, as such devices contain business as well as personal data (Mihai, n.d.).

Devices that are disposed of or sold can contain various data, files, and information that disclose personal and business details (Wakolbinger et al., 2014). The possibility

of such information being obtained and used by unauthorised third parties presents a risk to the privacy and security of users and organisations (Debnath, 2020; Forti et al., 2020). Data on electronic devices can be used for extortion, identity theft, phishing, deepfake recording, social engineering, inducement to download or open malicious software, and so on. (ENISA, 2021b). Cyber crime can have direct or indirect financial consequences (Romanosky, 2016; Smith et al., 2019). Suppose it breaches the provisions of the General Data Protection Regulation (GDPR). In that case, an organisation can be fined EUR 20 million, or 4% of its annual worldwide turnover in the preceding fiscal year (General Data Protection Regulation, 2016). Cyber crime can also cause technical failure and reputational damage (Candiwan & Zafira, 2020; ENISA, 2021a; Roškot et al., 2020; Verizon, 2019).

From the point of view of information security, e-waste has not received the attention it deserves. In order to ensure information security for individuals, it is a topic that needs to be analyzed, studied, and clarified in more detail. This paper aimed to find out, based on research conducted in Slovenia, how users handled their e-waste, why they sold, disposed of, or gave away their existing devices, and what measures they took before the device left their possession. We also looked at whether individual factors, such as awareness of the threats associated with the sale of devices, past experience of cyber crime or awareness of the limitations of the data-erasure process affected their decision to remove data from their electronic devices. Nevertheless, these cyber and environmental crime issues can pose new challenges for the police. In the conclusion, the authors discuss the threats to individuals' information security in Slovenia and the possible measures and improvements that could be introduced to improve protection.

PREVIOUS STUDIES

Compared with a few decades ago, when some devices would last for more than ten years, technological changes and consumer demand have meant that few devices nowadays would be retained by their owner for more than a few years. Owners of devices decide to sell, give away, dispose of, and recycle their existing devices for a variety of reasons (European Commission, 2013; Osibanjo & Nnorom, 2007; Schiller et al., 2016). Continuous improvements to smart devices have led to the more rapid replacement of older and obsolete versions of devices with those that offer greater speed, more space, and a new design. Consequently, old devices that are no longer of any value to a user are given away, sold, or even thrown in the rubbish bin (Tan et al., 2018).

In a study conducted in Nigeria, Miner, Rampedi, Ifegbesan, and Machete (2020) examined how users handled e-waste (sample size of 228). They found that the rea-

sons why the respondents had stopped using a particular electronic device were as follows: the device no longer worked (35.1%), they wished to upgrade their existing device (32.9%), their device had been stolen (26.33 %) and a new design had arrived on the market (25.4%). The results of the study also showed that 27.6% of respondents kept the device at home, 25% disposed of it in their common household waste, 17% sold the device, 8% gave the device away, and 7% gave the device to a waste recycling intermediary. In a similar study in Saudi Arabia, Almulhim (2022) found, on a sample size of 523, that respondents changed their electronic devices for the following reasons: the device was broken (50.1%), they wished to upgrade their device (38.2%), they wished to purchase a new model (36.54%), and their device had been stolen (32.3%).

A Canadian study by Ceci et al. (2021) looked at how people dealt with their end-of-life e-waste. It found that around 73% of all respondents (sample size of 131, multiple answers possible) kept hold of their electronic devices (smartphones, laptops, tablets, disks), 44% gave them away, 41% sold them, 25% recycled them, 11% returned them to a retailer and 10% disposed of them in their common household waste. A study conducted in Ghana and Kagbetor (2022) found that 39% of users sold their e-waste, 31% kept hold of it, 24.5% gave it away, and 5.5% incinerated it (sample size of 200). In addition to what an individual does with their device when they no longer use it, it is important to consider what they do with it before disposing of it, selling it, or giving it away. The study by Ceci et al. (2021) found that 62% of the 131 respondents formatted the device, 25% erased data manually, and 5% erased data securely.

It was expected to find cases of sensitive data remaining on a used device (Hartwig, 2016). In their study, the Blancco Technology Group and Kroll Ontrack organisations (2015) set about trying to establish how much data could be obtained from second-hand devices purchased on eBay, Amazon, and Gazelle.com. For the purposes of the study, they purchased 122 items of used equipment, including mobile phones, hard disks, and SSDs. The findings showed that an attempt had been made to erase data or format the device on 57% of mobile phones and 75% of hard disks and SSDs. They found erased data or data traces on 48% of hard disks and SSDs and recovered thousands of email messages, calls, text messages, photographs, and video recordings on 35% of the mobile phones they purchased.

In a similar study, AVAST (2014) obtained 20 second-hand mobile phones on the US eBay site. They found that while data had been erased on all the devices, they were able to retrieve 40,000 personal photographs, including family photographs, photographs of children, and nude photographs, with the help of publicly available software. They also recovered 750 text emails and messages, contact names and email addresses, and 1,000 search inquiries and were also able to identify four of the previous owners of the devices.

For the purposes of their study, Zingerle and Kronman (2019) visited one of the world's largest e-waste dumps, Agbogbloshie, in the capital of Ghana. They purchased 22 hard disks from the various entities that obtained and recycled hard disks from desktop and laptop computers. Upon their return home, they sent the hard disks for analysis. They recovered 85 GB of data from six of the 20 hard disks still working. These disks contained personal photographs, recordings, documents, copies of passports, employment, and other contact details.

In a similar study carried out in 2011, journalism students from the University of British Columbia purchased a large number of hard disks at open-air markets at Agbogbloshie in Ghana. They found that data had not been erased from these disks. On one of the disks, they found sensitive financial information and contracts. The disk had belonged to an organisation that worked with the National Aeronautics and Space Administration (NASA), the Defence Intelligence Agency (DIA) and the Department of Homeland Security (DHS) (Bennion, n.d.).

Whenever we sell, give away, or dispose of a device, there is the possibility that some data will remain on it. Emptying the recycle bin, formatting the hard disk, and reinstalling the operating system does not ensure complete data erasure. Rather than erasing or wiping the data, the user marks it as available for writing if the hard disk requires space (Yusof et al., 2019). If the device falls into the wrong hands, it could place individuals or organisations at risk. This means that the possibilities for various forms of cyber crime are actually wide open, which means additional work for police investigators. Furthermore, end-used electronic devices often end up illegally disposed of, presenting environmental crime and opening a second task for the police.

REGULATIONS, STANDARDS, AND GUIDELINES FOR DATA CONTAINED IN E-WASTE

There are many recommendations and standards that address the handling of devices and the performance of data sanitisation when a device is no longer in use or has come to the end of its life. Devices such as computers and telephones can contain personal data. The General Data Protection Regulation (GDPR) sets out the rules regarding personal data protection and covers the organisation's entire lifecycle of data (General Data Protection Regulation, 2016). IT departments often erase data from electronic devices and contract with a company to remove and recycle devices. Companies in the EU and organisations outside the EU that provide goods or services to customers or companies in the EU are obliged to protect data in accordance with the provisions of the GDPR. Devices must be protected to the same extent after disposal as they are during use (General Data Protection Regulation, 2016). The international ISO 27001 standard defines the information security management system

and the entire lifecycle of the management of assets (or electronic devices) within an organisation: inventory of assets, ownership of media, information classification and so on (ISO/IEC, 2013a). ISO 27001 provides the framework that helps organisations of any size or industry protect its information methodically and cost-effectively. In general terms, ISO 27001 and 27002 set out how media are to be handled at the end of a device's use or lifecycle, but do not specifically define the methods and procedures for sanitising media to ensure information security.

NIST 800-88 ('Guidelines for Media Sanitization') is a unique US government document that provides methodical instructions for erasing data from electronic storage media. The Guidelines do not address all types of media, as these media are constantly changing and developing. The Guidelines are designed to apply universally to various media types, including those that may not have been invented (Ayers et al., 2014). NIST 800-88 sets out the three basic principles, 'Clear, Purge and Destroy', that can be applied to hard disks, SSDs, memory and other storage technologies (e.g. USB keys).

In order to sanitise media properly, one must first identify the type of media, of which there are many (hard disks, SSDs, USB keys, mobile devices, etc.). Another critical factor is whether a medium contains sensitive information, i.e. information that could, if disclosed, be used for the purposes of theft, extortion, access to critical information or the commission of any other type of cyber crime. The sanitisation method will also depend on whether the device will be reused, sold, given away or recycled, i.e. if the media is to leave the owner's possession. Sanitisation must also take into account time-related (media sanitisation can take several hours or days) and ecological factors (if the device can be reused, it does not need to be destroyed) (ISO/IEC, 2013b; ISO/IEC, 2013a; Kissel et al., 2014).

After the factors are identified, various sanitisation techniques can be employed. The type of sanitisation largely depends on the type of medium involved. NIST 800-88 mentions three principles of erasure. First, the data from the medium must be manually erased, overwritten, and formatted, or a factory reset must be performed on the device. This ensures that the data is not freely accessible on the device and is protected against non-invasive data retrieval techniques. The second principle includes methods such as data wiping with fixed bit sampling, block erase, crypto erase, and degaussing. These methods render data irretrievable, even with the use of laboratory techniques. The third principle (shredding, disintegration, pulverising or incineration) is applied to ensure that data is completely irretrievable, or if the first and second principles cannot be applied (Kissel et al., 2014).

Sanitisation is followed by verification to ensure that all data has been removed from all medium locations and that sanitisation has been successful (Ceci et al., 2021;

Kissel et al., 2014). After the verification has been performed, a media sanitisation document or certificate is produced. It should contain all the critical information, e.g., media source, media type, serial number, sanitisation type, post-sanitisation destination, and other details. This document constitutes an audit trail. Unless sanitisation has been verified and documented by a responsible person, there is no way of knowing whether all information from an electronic device or medium has been appropriately erased (Cullipher, 2019; Kissel et al., 2014).

STUDY

With the help of an online questionnaire, the study set out to examine how users of electronic devices in Slovenia handled their devices after they no longer used them and what factors influenced their awareness of measures to protect electronic devices. The survey's target population comprised social media users (Facebook, Twitter, LinkedIn) and users of messaging apps (Messenger, WhatsApp, Viber). The data was gathered with the help of an anonymous survey conducted between May and June 2022 using the 1ka online tool for publication on online social media and messaging apps, with non-probability sampling using the snowball method. The questionnaire comprised 27 questions divided into five sets. The questions were mainly of the closed type and arranged using a five-point Likert scale from 1 to 5, where 1 meant 'strongly disagree' and 5 meant 'completely agree'. The first set of questions establishes respondents' reasons for disposing of, selling, or giving away their electronic devices. With the help of eight variables, the second set checked respondents' awareness of the threats associated with the disposal, sale, or giving away of electronic devices. The third set, which contained five variables, looked at respondents' experiences of cyber crime. In comparison, the fourth (five variables) was designed to establish respondents' awareness of the protection measures that should be taken before a device is disposed of, sold, or given away. The fifth part of the questionnaire (four variables) contained questions designed to check the extent to which respondents were aware of the limitations of the file-erasure process, while the sixth and last part comprised demographic questions, including gender, age, and education. The questionnaire can be found in the appendix.

As the survey sample was not random, we cannot, without reservation, extrapolate the results to the entire population; instead, we should take the results merely as a preliminary indicator of how people act in relation to the threats to their information security that arise as a result of improper handling of some types of e-waste in Slovenia.

The sample comprised 132 (61.4%) female and 83 (38.4%) male respondents. The average age of the respondents was 33 (youngest 19, oldest 72). Respondents had mostly

completed post-secondary, university, or high levels of education (64.8%), followed by secondary education (27.1%) and vocational or technical education (8.1%).
In the first part of the questionnaire, we attempted to establish why people opted to sell, dispose of, or give away their electronic devices. Of the 216 respondents, 172 (80%) said they had done so because the device was broken, and 118 (55%) said they wished to upgrade their existing device because the new one was faster and had more space and a better camera. Seventeen respondents (8%) said that their device had been stolen, and eight (4%) said that they had replaced their existing device because the one they purchased subsequently had a new design.

We also attempted to establish what users did with devices they no longer used. Two-thirds (66%, or 143 respondents) said that they kept the device at home, 47% (101) had given the device away, 35% (75) had sold the device, 25% (54) had taken the device to a waste collection centre and 7% (15) had disposed of the device in their common household waste.

Table 1 shows the variables by which we examined the extent to which users were aware of the threats associated with e-waste, had been victims of cyber crime in the past and were aware of the limitations of the process of erasing data from electronic devices. Using factorisation, we formulated four factors: 'Awareness of the threats associated with the disposal, sale or giving away of electronic devices', 'Experience of cyber crime', 'Awareness of device-protection measures', and 'Awareness of the limitations of the data-erasure process'. These factors were used for the purposes of further analysis.

Table 1: Description of variables.

Variable	FW*	M	CK*	CS*	SD
Awareness of the threats associated with the disposal, sale, or giving away of electronic devices α = 0.95 | KMO = 0.91 | var = 69.67%					
It is possible to obtain personal data (name and surname, address) from electronic devices	0.77	4.09	-1.13	1.24	0.93
It is possible to obtain user data (username, password) from electronic devices	0.80	3.81	-0.95	0.34	1.07
It is possible to obtain payment card details from electronic devices	0.83	3.63	-0.69	-0.30	1.11
It is possible to obtain a browser history from electronic devices	0.77	4.00	-1.29	1.48	0.99
Data from electronic devices can be used to create malicious emails (phishing).	0.88	3.94	-1.15	1.05	1.03
Data from electronic devices can be used for extortion purposes.	0.91	4.03	-1,30	1.53	1.01
Data from electronic devices can be used for identity theft purposes.	0.84	3.96	-1.12	0.83	1.03

Data from electronic devices can be used to obtain a financial benefit	0.86	3.95	-1.20	1.20	1.03
Experience of cyber crime α = 0.72 | KMO = 0.73 | var = 35.45%					
I have been the victim of payment card abuse when making purchases online	0.51	2.00	-0.011	1.15	1.33
I have had my password or other user data stolen	0.71	2.47	-1.05	0.58	1.39
My computer has been infected with malicious software (virus)	0.49	3.23	-1.30	-0.35	1.43
I have experienced extortion via email or social and other media	0.66	2.31	-1.14	0.55	1.35
I have received an email from an unknown person requesting personal data, payment card details, or payment (phishing)	0.58	3.19	-1.43	-0.29	1.50
Awareness of device-protection measures α = 0.73 | KMO = 0.69 | var = 43.63%					
I erase data (photographs, recordings, documents) before disposing of/selling/giving a device away.	/	4.50	-1.89	4.46	0.76
I format/perform a factory reset before disposing of/selling/giving a device away	0.58	4.25	-1.46	1.45	1.05
I use secure data erasure tools (CCleaner, BCWipe, MobiWIPE, etc.) before disposing of/ selling/giving a device away	0.49	2.93	0.10	-1.31	1.42
I log out of all user accounts (Gmail, Facebook, Outlook) before disposing of/selling/giving a device away	0.65	4.15	-1.40	1.07	1.14
I erase browser history and cookies before disposing of/selling/giving a device away	0.86	3.76	-0.71	-0.90	1.36
Awareness of the limitations of the data-erasure process α = 0.80 | KMO = 0.77 | var = 51.15%					
After an electronic device is formatted or a factory reset is performed, it is still possible to recover the erased data	0.72	3.36	-0.08	-0.79	1.09
After files (photographs, recordings, documents) are manually erased from a device, it is still possible to recover the erased data	0.76	3.76	-0.49	-0.32	0.95
By manually erasing files in Windows/Android, I do not erase the whole file but only the data that shows the file location	0.80	3.70	-0.13	-0.59	0.90
Secure data erasure means that the data on the device is wiped, which prevents it from being reconstructed	0.56	3.76	-0.13	-0.48	0.85

FW* = Factor weight
CK* = Coefficient of kurtosis
CS* = Coefficient of skewness

Using multiple regression, we tried to establish whether factors such as awareness of cyber threats, experience of cyber crime and awareness of the limitations of the data-erasure process determined whether they took steps to erase data from their devices.

Before performing multiple regression, we checked the characteristics of the assessed regression model (ANOVA). As the p-value was less than 0.05 (Table 2), the regression model was statistically significant, which means that we could reject the null hypothesis that the regression coefficients were equal to zero (Šifrer & Erčulj, 2020). Table 2 shows an R-squared of 0.14 (14%), which means that we can use the predictor variables (awareness of the limitations of the data-erasure process, the experience of cyber crime, and awareness of the threats associated with the disposal, sale, or giving away of electronic devices) to explain the 14% variability of the dependent variable 'Awareness of the protection measures that should be taken before a device is disposed of, sold or given away'. The remainder can be attributed to other factors that do not form part of our analysis.

Table 2: Evaluation of regression coefficients

Model	N.C.*		S.C.*	t	p
	B	S.D.	Beta		
Constant*	2.77	0.35		7.97	0.00
Awareness of the threats associated with the disposal, sale, or giving away of electronic devices	0.10	0.12	0.10	0.78	0.44
Experience of cyber crime	0.19	0.07	0.18	2.63	0.01
Awareness of the limitations of the data-erasure process	0.35	0.10	0.27	3.44	0.00
R^2 = 14 % | ANOVA: F = 6.26 p-value = 0.00					

N.C.* = Non-standardised coefficient
S.C.* = Standardised coefficient
Constant* = Awareness of the protection measures that should be taken before a device is disposed of, sold, or given away

Table 2 shows that two of the three predictor variables ('Experience of cyber crime' and 'Awareness of the limitations of the data-erasure process') are statistically significant (p-value < 0.05). The composite variable 'Awareness of the threats associated with the disposal, sale or giving away of electronic devices' does not have a statistically significant effect on the dependent variable (p-value = 0.44).

The regression coefficient is positive in the statistically significant composite variables 'Experience of cyber crime' (b = 0.19) and 'Awareness of the limitations of the data-erasure process' (b = 0.35). If the value of the aforementioned composite variables increases in agreement with the statement by the respondents, the dependent variable, 'Awareness of the protection measures that should be taken before a device is disposed of, sold or given away,' also rises if the other independent variables do not change.

Using multiple regression, we found that the better a user's knowledge of the limitations of the data-erasure process, the greater the use of measures to erase data, leading to a reduction in the likelihood of cyber threats arising. The same applies to the factor of 'Experience of cyber crime'. Users with past cyber crime experience were more careful once the device left their possession.

DISCUSSION

As the quantity of e-waste is increasing from year to year (Forti et al., 2020), it is crucial to establish whether users of electronic devices are selling, giving away, or disposing of those devices and the reason for their decision. The study shows that the main reason why the respondents replaced their device was that it no longer worked (80%), followed by upgrading the device (55%), theft (8%), and new design (4%). Similar findings have been produced by Miner et al. (2020) and Almulhim (2022), with the main reasons for replacing a device being the fact that the device no longer worked and the wish to upgrade the existing device. It is essential to point out that a device that does not work (most often because of a non-functioning battery) can be the most vulnerable type of device because the user has not performed any data erasure (AVAST, 2014; Blancco, 2017). Advances in smart devices also induce users to replace working devices with new, faster, and better-looking devices, contributing to the global increase in e-waste (Tan et al., 2018).

With the increased quantity of e-waste worldwide comes an increase in the threats to information security (Forgor et al., 2019; Forti et al., 2020). Electronic devices contain large amounts of personal and business data that can be used to commission various forms of cyber crime (phishing emails, identity theft, social engineering, etc.). This can lead to financial damage, technical failure, and reputational damage. Unless data on an electronic device is wiped or the medium destroyed (the NIST 800-88 techniques of 'Clear, Purge and Destroy') and checks made to ensure that the data has been appropriately erased, it is impossible to say whether the data really has been removed.

The study also found that the Slovenian population did not differ significantly from other populations when it came to the handling of e-waste. On far too many occa-

sions, electronic devices are moved from a secure environment to a less secure one without the data on that device first being removed (Alghazo et al., 2018; Chen et al., 2021). Most respondents (66%) keep the device at home, 47% give it away, 35% sell it, 25% take it to a waste collection centre, and 7% dispose of it in their common household waste. Similar results have been produced in studies by Ceci et al. (2021) and Dzah et al. (2022), i.e., that most users sell their electronic devices. The failure to properly remove data from an electronic device that is sold, given away, or disposed of or that otherwise leaves the user's possession can lead to vulnerability (ISO/IEC, 2013a; Kissel et al., 2014).

Regarding information security, the steps users take before they dispose of, sell, or give away their e-waste are very important. The results of the survey show that users take steps such as factory reset, formatting, manual data erasure, and logging out of user accounts when they stop using a device. However, fewer steps are taken to securely erase or wipe data from a device. Ceci et al. (2021) produced similar findings in their study, with the fewest number of users opting for methods that removed data securely. Our findings, as well as those of Ceci et al. (2021), align with the findings of the Blancco Technology Group and Kroll Ontrack organisations (2015). They purchased second-hand electronic devices, examined them, and found that most of the devices had been formatted or had their data manually erased by their former users. This is a vulnerability from the point of view of information security.

This paper builds on existing studies conducted in Slovenia. In addition to examining how people handled their e-waste and what measures they took before selling, disposing of, or giving away a device, it found that factors such as the past personal experience of cyber crime and awareness of the limitations of the data-erasure process had a positive impact on the self-protective behaviour of users of electronic devices. In contrast, an awareness of threats had no impact at all. In their study, which had a sample size of 309, Markelj and Završnik (2016) found that awareness of threats did not, in and of itself, dictate the way a user handled their mobile device; instead, the handling of a device depended on the user's attitude/motivation. The NIS2 Directive highlighted the fact that the number of cyber attacks had increased in recent years and that they were becoming more sophisticated, targeted, and undetected (Negreiro, 2022). The survey findings show that the way users currently handle e-waste does not ensure adequate security, as data in a device's memory is vulnerable to retrieval by third parties. With the increasing threat to users' cyber security and privacy, it is crucial that users educate themselves and are aware of how to properly and securely handle their electronic devices and e-waste. This would reduce the likelihood of data being retrieved from e-waste and of that data being used in the commission of cyber crime. It is vitally important for information security to be strengthened across the board, from the time the device starts to be used to the time it stops being used, i.e., when it becomes e-waste that is sold, given away, or disposed of.

The quantity of e-waste increases yearly, as does the quantity of data on electronic devices. Regarding information security, how users handle e-waste presents a risk, as inadequate techniques are primarily used to erase data. Users must educate themselves and be aware of the shortcomings of manual data erasure and formatting and the possible consequences. In general, users of electronic devices need to be aware of how to use devices safely and remove data from devices. If they are not, their devices are vulnerable to third parties who wish to access financial data, information on family members and business data that could then be used in the commission of one of the many forms of cyber crime. As already mentioned, these (new) cyber and environmental crime issues present new challenges for the police.

REFERENCES

1. J. Alghazo, O. K. M. Ouda, A. E. Hassan, E-waste environmental and information security threat: GCC countries vulnerabilities, Euro-Mediterranean Journal for Environmental Integration 3 (1) (2018) 1–10. https://doi.org/10.1007/s41207-018-0050-4.
2. A. I. Almulhim, Household's awareness and participation in sustainable electronic waste management practices in Saudi Arabia. Ain Shams Engineering Journal, 13 (1) (2022) 1-16. https://doi.org/101729. 10.1016/j.asej.2022.101729.
3. AVAST, Avast demonstrates the risk of selling used smartphones – recovers 40,000 personal photos and emails from phones bought online. (2014) https://press.avast.com/avast-demonstrates-risk-of-selling-used-smartphones-recovers-40000-personal-photos-and-emails-from-phones-bought-online.
4. R. Ayers, W. Jansen, S. Brothers, Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1). NIST Special Publication, 1 (1) (2014) 85. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf.
5. J. Bennion, Drowning in Electronics: Where the Law Stands on E-Waste, (n.d.) https://www.pbs.org/frontlineworld/stories/ghana804/resources/ewaste.html. accessed: 2023-02-08
6. Blancco, What is cryptographic erasure. (2017) https://www.blancco.com/resources/article-what-is-cryptographic-erasure/. accessed: 2023-08-02
7. Blancco Technology Group, and Kroll Ontrack, Blancco Technology Group and Kroll Ontrack Study Finds Lingering Data After Used Electronics Are Resold Online Blancco. (2015) https://www.blancco.com/blancco-technology-group-and-kroll-ontrack-study-finds-lingering-data-after-used-electronics-are-resold-online/. accessed: 2023-04-05
8. B. Markelj, A. Završnik, Kibernetska korporativna varnost mobilnih naprav: zavedanje uporabnikov v Sloveniji. Revija za kriminalistiko in kriminologijo, 67 (1) (2016) 44-60.

9. B. Markelj, S. Zgaga, Kibernetska varnost in kibernetska kriminaliteta uporabnikov mobilnih naprav v Sloveniji. Revija za kriminalistiko in kriminologijo, 69 (1) (2018) 15-29.
10. Candiwan, N. H. Zafira An information security awareness investigation of E-commerce users: A case study of Traveloka. International Journal of Advanced Trends in Computer Science and Engineering, 9 (2) (2020) 1422–1429. https://doi.org/10.30534/ijatcse/2020/79922020.
11. J. Ceci, H. Khan, U. Hengartner, D. Vogel, Concerned but ineffective: user perceptions, methods, and challenges when sanitizing old devices for disposal. Proceedings of the 17th Symposium on Usable Privacy and Security, SOUPS 2021, 8 (10) (2021) 455–473. https://www.usenix.org/system/files/soups2021-ceci.pdf.
12. H. Chen, O. Turel, Y. Yuan, E-waste information security protection motivation: the role of optimism bias. Information Technology in People, 1 (1) (2021) 1–33. https://doi.org/10.1108/ITP-09-2019-0458.
13. V. Cullipher, What is NIST 800-88, and what Does "media sanitization" really mean. Blancco (2019) https://www.blancco.com/resources/blog-what-is-nist-800-88-media-sanitization/. accessed: 2023-11-12
14. B. Debnath, J. M. Alghazo, G. Latif, R. Roychoudhuri, S. K. Ghosh, Sustainable waste management: policies and case studies. Sustainable Waste Management: Policies and Case Studies, 1 (1) (2020) 403-419. https://doi.org/10.1007/978-981-13-7071-7.
15. C. Dzah, J. Agyapong, M. Apprey, K. Agbevanu, P. Kagbetor, Assessment of perceptions and practices of electronic waste management among commercial consumers in Ho, Ghana. Cogent Environmental Science, 8 (1) (2020) 1-16. https://doi.org/10.1080/27658511.2022.2048465.
16. ENISA, Cybersecurity challenges and recommendations (2021a) https://doi.org/10.2824/7703522 accessed: 2023-08-02
17. ENISA, Threat landscape 2021 (2021b) https://doi.org/10.2824/324797. accessed: 2023-08-02
18. European Commission, Equivalent conditions for waste electrical and electronic equipment (WEEE) recycling operations taking place outside the European Union (2013) https://ec.europa.eu/environment/pdf/waste/weee/Final report_EC S.pdf. accessed: 2023-08-03
19. V. Forti, C. P. Baldé, R. Kuehr, G. Bel, The global e-waste monitor 2020 (2020) http://ewastemonitor.info/wp-content/uploads/2020/12/GEM_2020_def_dec_2020-1.pdf. accessed: 2023-08-03
20. K. Hartwig, Digital waste in cyber crime: examining the relationship (2016) https://doi.org/10.13140/RG.2.2.32774.37445. accessed: 2023-08-04
21. A. Hovav, F. Ferdani Putri, This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy, Pervasive and Mobile Computing, 32 (2016) 35-49. https://doi.org/10.1016/j.pmcj.2016.06.007.
22. ISO/IEC, Information technology – security techniques – information security

management systems – requirements (2013a) https://eldritchdata.neocities.org/PDF/CS/SecManagmentSystemsReq.pdf. accessed: 2023-08-03
23. ISO/IEC, Information technology — security techniques — code of practice for information security control (2013b) from https://trofisecurity.com/assets/img/ISO-IEC_27002-.pdf. accessed: 2023-08-03
24. R. Kissel, A. Regenscheid, M. Scholl, K. Stine, NIST special publication 800-88 (revision 1) guidelines for media sanitization. NIST Special Publication 800-88, 1(1) (2014) 1–64. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf.
25. A. Mihai, Hacking E-waste is the "greatest little secret" of cyber-security, and it's worth paying attention. Heidelberg Laureate Forum Foundation (n.d.). https://www.newsroom.hlf-foundation.org/blog/article.html?tx_news_pi1%5Baction%5D=detail&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Bnews%5D=285&cHash=d96c53bc9cc7dab1e56315d944f49c9d. accessed: 2023-11-12
26. K. J. Miner, I. T. Rampedi, A. P. Ifegbesan, F. Machete, Survey on Household Awareness and Willingness to Participate in E-Waste Management in Jos, Plateau State, Nigeria. Sustainability, 12 (3) (2020) 1047. from https://doi.org/10.3390/su12031047.
27. M. Negreiro, The NIS2 Directive A high common level of cybersecurity in the EU (2022) https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf. accessed: 2023-12-12
28. O. Osibanjo, I. C. Nnorom, The challenge of electronic waste (e-waste) management in developing countries. Waste Management and Research, 25 (6) (2007) 489–501. https://doi.org/10.1177/0734242X07082028.
29. S. Romanosky, Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2 (2) (2016) 121–135. https://doi.org/10.1093/cybsec/tyw001.
30. M. Roškot, I. Wanasika, Z. Kreckova Kroupova, Cybercrime in Europe: surprising results of an expensive lapse. Journal of Business Strategy, 42 (2) (2020) 91–98. https://doi.org/10.1108/JBS-12-2019-0235.
31. A. Rožnik, Situacijska prevencija nezakonite trgovine z električnimi in elektronskimi odpadki [Doctoral dissertation]. Faculty of Criminal Justice and Security (2020) https://dk.um.si/IzpisGradiva.php?id=76573&lang=slv&prip=rul:8311585:d2. accessed: 2023-11-12
32. S. Schiller, J. Merhout, R. Sandlin, Enterprise IT asset disposition: an overview and tutorial. Journal of the Midwest Association for Information Systems, 2016 (2) 27–42. https://doi.org/10.17705/3jmwa.00019.
33. B. Schafer, D-waste: Data disposal as challenge for waste management in the Internet of Things. The International Review of Information Ethics, 22 (12) (2014) 101–107. https://doi.org/10.29173/irie131.
34. K. T. Smith, A. Jones, L. Johnson, L.M. Smith, Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communi-

cation and Ethics in Society, 17 (1) (2019) 42–60. https://doi.org/10.1108/JICES-02-2018-0010.

35. Q. Tan, H. Duan, L. Liu, J. Yang, J. Li, Rethinking residential consumers' behavior in discarding obsolete mobile phones in China. Journal of Cleaner Production, 195 (1) (2018) 1228–1236. https://doi.org/10.1016/j.jclepro.2018.05.244.
36. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, OJ L 119, 4.5.2016 (p. 1–88)
37. Verizon, 2019 data breach investigations report (2019) https://www.phishingbox.com/assets/files/images/Verizon-Data-Breach-Investigations-Report-DBIR-2019.pdf. accessed: 2023-11-12
38. T. Wakolbinger, F. Toyasaki, T. Nowak, A. Nagurney, When and for whom would e-waste be a treasure trove? Insights from a network equilibrium model of e-waste flows. International Journal of Production Economics, 154 (1) (2014) 263–273. https://doi.org/10.1016/j.ijpe.2014.04.025.
39. N. A. B. Yusof, S. N. H. B. S. Abdullah, M. F. E. bin M. Senan, N. Z. binti Z. Abidin, M. B. Sahri, Data sanitization framework for computer hard disk drive: A case study in Malaysia. International Journal of Advanced Computer Science and Applications, 10 (11) (2019) 398–406. https://doi.org/10.14569/IJACSA.2019.0101155.
40. A. Zingerle, L. Kronman, Information diving on an e-waste dump global data breach. In M. Verdicchio, M. Carvalhais, L. Ribas and A. Rangel (ed.), Conference on Computation, Communication, Aesthetics in X (2019) (pp. 164–176). https://2019.xcoax.org/xCoAx2019.pdf

UDK 502/504.004(497.4)

E-OTPAD: NEVIDLJIVA OPASNOST ZA INFORMACIONU BEZBJEDNOST I OKOLINU[1]

Dr Blaž Markelj
Associate Professor of Criminal Justice and Security,
Faculty of Criminal Justice and Security, University of Maribor, Slovenia
e-mail: blaz.markelj@um.si

Uroš Jelenc
Master's student, Faculty of Criminal Justice and Security,
University of Maribor, Slovenia
e-mail: uros.jelenc@student.um.si

Dr Katja Eman
Associate Professor of Criminology, Faculty of Criminal Justice and Security,
University of Maribor, Slovenia
Corresponding author at: Faculty of Criminal Justice and Security,
University of Maribor
e-mail: katja.eman@um.si

Abstrakt

E-otpad se odnosi na razne vrste odbačenih elektroničkih uređaja, od mašina za pranje posuđa i frižidera, do pametnih telefona. Oni nisu samo opasni za ljude i okolinu zbog svog fizičkog sastava, mnogi elektronski uređaji takođe mogu ugroziti bezbjednost ličnih podataka i koristiti se za mnoge oblike kibernetičkog kriminala. Ovaj se rad usredsređuje na aspekte informacione bezbjednosti e-otpada, kao što su personalni kompjuteri, prenosivi računari, pametni telefoni i drugi uređaji koji mogu sadržati podatke. Ovi uređaji, koje korisnik može imati danima, mjesecima ili godinama, mogu sadržati velike količine ličnih i poslovnih podataka. Problem koji predstavlja e-otpad ove vrste je taj što sadrži osjetljive lične i poslovne podatke koji,

1 Prevod Redakcije

ako se ne uklone na odgovarajući način, ostaju na uređaju nakon što se odloži, proda ili pokloni. Ovaj rad istražuje kako korisnici postupaju s e-otpadom i koji činioci utiču na njihovu odluku o brisanju podataka s uređaja. Rezultati pokazuju da način na koji korisnici trenutno postupaju s e-otpadom ne obezbjeđuje odgovarajući nivo informacione bezbjednosti. Dva činioca koji tjeraju korisnike da preduzmu mjere za brisanje podataka s uređaja su: svijest o ograničenjima procesa brisanja podataka i prošlo iskustvo s kibernetičkim kriminalom. Uprkos tome, ova pitanja kibernetičkog kriminala i kriminala protiv okoline mogu predstavljati nove izazove za policiju.
Ključne riječi: *informaciona bezbjednost, e-otpad, cyber kriminal, ekološki kriminal, brisanje podataka, elektronski uređaji, Slovenija.*

E-OTPAD I PRIJETNJA INFORMACIONOJ BEZBJEDNOSTI

Električna i elektronska oprema (EEO) postala je neizostavan dio života ljudi koja im na razne načine omogućava obavljanje svakodnevnih zadataka i poboljšanje opšteg kvaliteta života. Kada elektronski uređaj dođe do kraja svog vijeka trajanja jer više ne radi, radi presporo ili je zamijenjen novim modelom, postaje e-otpad (Europska komisija, 2013.; Osibanjo & Nnorom, 2007.; Schiller et al., 2016). Niz različitih predmeta klasifikuje se kao e-otpad, od kućanskih i kuhinjskih aparata do konzola za igrice, mobilnih telefona i personalnih kompjutera. Približno 53,6 miliona tona e-otpada generisano je 2019, a neki procjenjuju da će se ta količina udvostručiti do 2050. (Forti et al., 2020.).

Glavni problem je što proizvodimo više e-otpada nego što možemo reciklirati. Forti i sur. (2020) upozoravaju da je samo 17,4% svih otpadnih elektronskih uređaja zvanično prikupljeno i reciklirano. Ne znamo što se događa s preostalih 82,6%, iako je vjerovatno odloženo, prodato ili reciklirano na ekološki štetan način. Nedostatak informacija o prikupljanju i recikliranju e-otpada pokazuje da se većinom tog otpada rukuje izvan zvaničnog sistema prikupljanja otpada i šalje u zemlje u razvoju. Ovo je oblik organizovanog ekološkog kriminala koji je u porastu u posljednjoj deceniji. E-otpad sadrži i opasne materije, najčešće teške metale kao što su olovo, živa, kadmijum i druge otrovne hemikalije koje imaju nepovoljan učinak (bioakumulacija) na okolinu i zdravlje ljudi (Forti i sur., 2020.).

Rožnik (2020) je sprovela istraživanje u kojem je istakla problem e-otpada u Sloveniji. U svojoj studiji o 28 slučajeva nezakonitih pošiljki e-otpada, otkrila je da je Slovenija zbog geografskog položaja pretežno tranzitna zemlja za e-otpad (nezakoniti prevoz e-otpada u susjedne zemlje). Nalazi su pokazali da su slovenske kompanije nezakonito izvozile e-otpad u inostranstvo ili primale pošiljke e-otpada. E-otpad se prevozio s manjkavom dokumentacijom ili bez ikakve, kao i s netačnim klasifikacijskim oznakama.

E-otpad se uopšteno dijeli u šest kategorija zavisno od veličine i namjene (Forti et al., 2020.): oprema za izmjenu temperature (zamrzivači, frižideri, klima uređaji i toplotne pumpe), zasloni i monitori, svetiljke, velika oprema (mašine za pranje veša, mašine za pranje posuđa i sl.), sitna oprema (tosteri, vage, kuvala za vodu i sl.), te mala informatička i telekomunikaciona oprema. Iako sav e-otpad ne sadrži osjetljive podatke, ovaj se dokument usredsređuje na dvije kategorije e-otpada: „mala informatička i telekomunikaciona oprema", koja uključuje mobilne telefone i personalne kompjutere, te „zaslone i monitore", što uključuje prenosive računare i tablete. Ove vrste e-otpada sadrže trajno pohranjene podatke, tvrde diskove (HDD), čvrste diskove (SSD) i memoriju samo za čitanje (ROM) (Hartwig, 2016; Hovav & Ferdani Putri, 2016).

Nedostatak regulative u globalnoj industriji e-otpada predstavlja brojne prijetnje. Uz prijetnje okolini i zdravlju, pojavila se nova prijetnja s prodajom, recikliranjem i popravkom e-otpada: preuzimanje ličnih i poslovnih podataka na uređajima koji su odloženi (Chen et al., 2021.; Debnath i sur., 2020.).

Personalni kompjuteri, prenosivi računari, pametni telefoni i drugi uređaji omogavaju nam da pri ruci imamo značajne količine podataka. Tehnološki napredak znači da su naši uređaji postali sposobniji i da nam mogu pružiti širok izbor usluga i funkcija; međutim, to takođe znači da naši uređaji akumuliraju značajnije količine podataka (Zingerle & Kronman, 2019.). Zbog brzine tehnološkog razvoja i sve većeg kapaciteta za skladištenje podataka, naši uređaji sadrže više poslovnih, ličnih i finansijskih podataka nego ikad (Hartwig, 2016; Schafer, 2014). Mediji za skladištenje podataka sve se više dizajniraju za sprečavanje gubitka podataka, što je korisno za oporavak podataka koje je korisnik možda slučajno izbrisao (Ceci et al., 2021.).

Često se koriste nepouzdane metode za uklanjanje podataka, poput ručnog brisanja, formatiranja ili vraćanja na fabrička podešavanja (Ceci et al., 2021.). U većini slučajeva ove metode ne uklanjaju u potpunosti podatke s uređaja; samo uklanjaju vezu između naziva datoteke i mjesta na uređaju (kopije metapodataka) gdje se datoteka fizički nalazi. Uređaji koji više ne rade, možda zato što je baterija ili napajanje pokvareno su takođe problematični, korisnici se ne odlučuju na popravku uređaja, a istovremeno ne sprovode nikakvo brisanje podataka (AVAST, 2014; Blancco, 2017). Problem predstavlja i korišćenje uređaja u lične i poslovne svrhe. Istraživanje Markelja i Zgage (2018.) na uzorku od 277 je pokazalo da je izbrisana granica između lične i poslovne upotrebe; ovo donosi nove prijetnje i postavlja pitanja u vezi s koracima koje treba preduzeti s uređajem koji je došao do kraja svog životnog vijeka, jer takvi uređaji sadrže poslovne, ali i lične podatke (Mihai, n.d.).

Uređaji koji se odlažu ili prodaju mogu sadržati različite podatke, datoteke i informacije koje otkrivaju lične i poslovne detalje (Wakolbinger et al., 2014.). Mogući-

nost da takve informacije dobiju i koriste neovlašćene treće strane predstavlja rizik za privatnost i bezbjednost korisnika i organizacija (Debnath, 2020; Forti et al., 2020). Podaci na elektronskim uređajima mogu se koristiti za iznudu, krađu identiteta, duboko lažno snimanje, društveni inženjering, podsticanje na preuzimanje ili otvaranje zlonamjernog softvera i tako dalje. (ENISA, 2021b). Kibernetički kriminal može imati direktne ili indirektne finansijske posljedice (Romanosky, 2016; Smith et al., 2019). Pretpostavimo da krši odredbe Opšte uredbe o zaštiti podataka (GDPR). U tom slučaju organizacija može biti kažnjena s 20 miliona eura ili 4% svog godišnjeg prometa u cijelom svijetu u prethodnoj fiskalnoj godini (Opšta uredba o zaštiti podataka, 2016.). Kibernetički kriminal takođe može prouzrokovati tehnički kvar i štetu reputaciji (Candiwan & Zafira, 2020; ENISA, 2021a; Roškot et al., 2020; Verizon, 2019).

Sa aspekta informacione bezbjednost, e-otpad nije dobio pažnju koju zaslužuje. Kako bi se osigurala informaciona sigurnost za pojedince, to je tema koju je potrebno detaljnije analizirati, proučiti i razjasniti. Ovaj rad je imao za cilj saznati, na osnovu istraživanja sprovedenog u Sloveniji, kako su korisnici postupali sa svojim e-otpadom, zašto su prodali, zbrinuli ili dali postojeće uređaje te koje su mjere preduzeli prije nego što je uređaj napustio njihov posjed. Takođe smo ispitali jesu li pojedinačni činioci, kao što su svijest o prijetnjama povezanim s prodajom uređaja, prošlo iskustvo s kibernetičkim kriminalom ili svijest o ograničenjima procesa brisanja podataka uticali na njihovu odluku da uklone podatke sa svojih elektronskih uređaja. I pored toga, ova pitanja kibernetičkog kriminala i kriminala protiv okoline mogu predstavljati nove izazove za policiju. U zaključku autori raspravljaju o prijetnjama informacionoj bezbijednosti pojedinaca u Sloveniji, te mogućim mjerama i poboljšanjima koja bi se mogla uvesti za poboljšanje zaštite.

PRETHODNA ISTRAŽIVANJA

U poređenju s prije nekoliko decenija, kada su neki uređaji trajali više od deset godina, tehnološke promjene i potražnja potrošača doveli su do toga da će malo koji uređaj u današnje vrijeme njihov vlasnik zadržati duže od nekoliko godina. Vlasnici uređaja odlučuju se prodati, pokloniti, odložiti i reciklirati svoje postojeće uređaje iz različitih razloga (Evropska komisija, 2013.; Osibanjo & Nnorom, 2007.; Schiller et al., 2016.). Stalna poboljšanja pametnih uređaja dovela su do brže zamjene starijih i zastarjelih verzija uređaja onima koji nude veću brzinu, više prostora i novi dizajn. Posljedično, stari uređaji koji korisniku više nemaju nikakvu vrijednost poklanjaju se, prodaju ili čak bacaju u kantu za smeće (Tan i sur., 2018.).

U studiji sprovedenoj u Nigeriji, Miner, Rampedi, Ifegbesan i Machete (2020.) ispitali su kako korisnici postupaju s e-otpadom (veličina uzorka od 228). Otkrili su da su

razlozi zbog kojih su ispitanici prestali koristiti određeni elektronski uređaj sljedeći: uređaj više ne radi (35,1%), željeli su nadograditi svoj postojeći uređaj (32,9%), uređaj im je ukraden (26,33%) a na tržište je stigao novi dizajn (25,4%). Rezultati istraživanja takođe su pokazali da je 27,6% ispitanika uređaj držalo kod kuće, 25% ih je odložilo u uobičajeni kućni otpad, 17% je uređaj prodalo, 8% poklonilo uređaj, a 7% ih je dalo uređaj posredniku za recikliražu otpada. U sličnoj studiji u Saudijskoj Arabiji, Almulhim (2022) na uzorku od 523 je utvrdio da su ispitanici promijenili svoje elektronske uređaje iz sljedećih razloga: uređaj je bio pokvaren (50,1%), željeli su nadograditi svoj uređaj (38,2%), željeli su kupiti novi model (36,54%) i uređaj im je ukraden (32,3%).

U kanadskoj studiji Ceci i sur. (2021.) su posmatrali kako se ljudi nose sa svojim e-otpadom na kraju životnog vijeka. Utvrđeno je da je oko 73% svih ispitanika (veličina uzorka od 131, moguće više odgovora) zadržalo svoje elektronske uređaje (pametne telefone, prenosive računare, tablete, diskove), 44% ih je poklonilo, 41% prodalo, 25% recikliralo , 11% ih je vratilo trgovcu, a 10% ih je odložilo u uobičajeni kućni otpad. Studija provedena u Gani i Kagbetoru (2022.) otkrila je da je 39% korisnika prodalo svoj e-otpad, 31% ga je zadržalo, 24,5% dalo, a 5,5% spalilo (veličina uzorka od 200). Osim što pojedinac radi sa svojim uređajem kada ga više ne koristi, važno je razmotriti što radi s njim prije nego što ga baci, proda ili pokloni. Studija Ceci i sur. (2021.) je otkrila da je 62% od 131 ispitanika formatiralo uređaj, 25% ručno izbrisalo podatke, a 5% sigurno izbrisalo podatke.

Očekivalo se da će se pronaći slučajevi osetljivih podataka koji ostaju na korišćenom uređaju (Hartwig, 2016.). U svojoj studiji organizacije Blancco Technology Group i Kroll Ontrack (2015.) pokušale su utvrditi koliko se podataka može dobiti sa korišćenih uređaja kupljenih na eBayu, Amazonu i Gazelle.com. Za potrebe istraživanja kupili su 122 artikla korištene opreme, uključujući mobilne telefone, tvrde diskove i SSD-ove. Nalazi su pokazali da su se pokušali obrisati podaci ili formatirati uređaj na 57% mobilnih telefona i 75% tvrdih diskova i SSD-ova. Pronašli su izbrisane podatke ili tragove podataka na 48% tvrdih diskova i SSD-ova i vratili hiljade poruka e-pošte, poziva, tekstualnih poruka, fotografija i video snimaka na 35% mobilnih telefona koje su kupili.

U sličnoj studiji, AVAST (2014) je nabavio 20 korišćenih mobilnih telefona na američkoj stranici eBay. Otkrili su da su, iako su podaci izbrisani na svim uređajima, uspjeli dohvatiti 40.000 ličnih fotografija, uključujući porodične fotografije, fotografije djece i golišave fotografije, uz pomoć javno dostupnog softvera. Takođe su otkrili 750 tekstualnih e-mailova i poruka, imena kontakata i e-mail adrese, te 1000 upita za pretraživanje, a takođe su uspjeli identifikovati četiri prethodna vlasnika uređaja. Za potrebe svoje studije, Zingerle i Kronman (2019) posjetili su jedno od najvećih svjetskih odlagališta e-otpada, Agbogbloshie, u glavnom gradu Gane. Kupili su 22 tvrda diska od različitih subjekata koji su nabavili i reciklirali tvrde diskove sa desktop

i laptop računara. Po povratku kući, hard diskove su poslali na analizu. Spasili su 85 GB podataka sa šest od 20 tvrdih diskova koji još rade. Ovi diskovi sadržavali su lične fotografije, snimke, dokumente, kopije pasoša, zaposlenje i druge podatke za kontakt.

U sličnoj studiji sprovedenoj 2011. studenti novinarstva sa Univerziteta British Columbia kupili su velik broj tvrdih diskova na tržnicama na otvorenom u Agbogbloshieu u Gani. Utvrdili su da podaci nisu izbrisani s tih diskova. Na jednom od diskova pronašli su osjetljive finansijske podatke i ugovore. Disk je pripadao organizaciji koja je sarađivala s Nacionalnom upravom za vazduhoplovstvo i svemir (NASA), Obavještajnom agencijom za odbranu (DIA) i Odjeljenjem nacionalne bezbjednosti (DHS) (Bennion, n.d.).

Svaki put kada prodamo, poklanjamo ili zbrinemo uređaj, postoji mogućnost da neki podaci ostanu na njemu. Pražnjenje koša za smeće, formatiranje tvrdog diska i ponovno instaliranje operativnog sistema ne obezbjeđuje potpuno brisanje podataka. Umjesto brisanja ili brisanja podataka, korisnik ih označava kao dostupne za pisanje ako tvrdi disk zahtijeva prostor (Yusof et al., 2019). Ako uređaj padne u pogrešne ruke, mogao bi ugroziti pojedince ili organizacije. To znači da su mogućnosti za različite oblike kibernetičkog kriminala zapravo širom otvorene, što znači dodatni posao za policijske istražitelje. Nadalje, korišćeni elektronski uređaji često završe nezakonito odloženi, što predstavlja ekološki zločin i otvara drugi zadatak za policiju.

PROPISI, STANDARDI I SMJERNICE ZA PODATKE SADRŽANE U E-OTPADU

Postoje mnoge preporuke i standardi koji se odnose na rukovanje uređajima i izvođenje dezinfekcije podataka kada se uređaj više ne koristi ili mu je došao kraj životnog vijeka. Uređaji poput računara i telefona mogu sadržavati lične podatke. Opšta uredba o zaštiti podataka (GDPR) utvrđuje pravila o zaštiti ličnih podataka i pokriva cijeli životni ciklus podataka organizacije (Opća uredba o zaštiti podataka, 2016.). IT odjeli često brišu podatke s elektronskih uređaja i sklapaju ugovor s preduzećem za uklanjanje i recikliranje uređaja. Kompanije u EU i organizacije van EU koje nude robu ili usluge kupcima ili kompanijama u EU dužne su štititi podatke u skladu s odredbama GDPR-a. Uređaji moraju biti zaštićeni u istoj mjeri nakon odlaganja, kao i tokom upotrebe (Opšta uredba o zaštiti podataka, 2016.). Međunarodna norma ISO 27001 definiše sistem upravljanja informacionom sigurnošću i cijeli životni ciklus upravljanja imovinom (ili elektronskim uređajima) unutar organizacije: inventar imovine, vlasništvo nad medijima, klasifikacija informacija i tako dalje (ISO/IEC, 2013a). ISO 27001 pruža okvir koji pomaže organizacijama bilo koje veličine ili djelatnosti da sistematski i ekonomično zaštite svoje informacije. Uopšteno, norme ISO 27001 i 27002 određuju kako treba postupati s medijima na kraju upotrebe ili životnog ciklu-

sa uređaja, ali ne definišu posebno metode i postupke za dezinfekciju medija kako bi se osigurala bezbjednost informacija.

NIST 800-88 ('Guidelines for Media Sanitization') jedinstveni je dokument američke vlade koji pruža metodička uputstva za brisanje podataka s elektronskih medija za pohranu. Smjernice se ne odnose na sve vrste medija jer se ti mediji stalno mijenjaju i razvijaju. Smjernice su osmišljene tako da se univerzalno primjenjuju na različite vrste medija, uključujući one koji možda nisu izmišljeni (Ayers et al., 2014.). NIST 800-88 postavlja tri osnovna načela 'Clear, Purge and Destroy" ("očisti, pročisti i uništi"), koja se mogu primijeniti na tvrde diskove, SSD-ove, memoriju i druge tehnologije pohrane (npr. USB ključeve).

Da bi se medij ispravno očistio, prvo je potrebno identifikovati vrstu medija, kojih ima mnogo (tvrdi diskovi, SSD-ovi, USB ključevi, mobilni uređaji itd.). Drugi kritični činilac je da li sadrži medij osjetljive informacije, tj. informacije koje bi se, ako budu otkrivene, mogle koristiti u svrhu krađe, iznude, pristupa kritičnim informacijama ili izvršenja bilo koje druge vrste kibernetičkog kriminala. Metoda čisćenja takođe će zavisti od toga hoće li se uređaj ponovo upotrebljavati, prodati, pokloniti ili reciklirati, tj. hoće li medij napustiti vlasnikov posjed. Pri ispravnom "čišćenju" takođe se moraju uzeti u obzir vremenski (sigurno uklanjanje podataka sa medija može trajati nekoliko sati ili dana) i ekološki činioci (ako se uređaj može ponovo upotrebljivati, ne treba ga uništiti) (ISO/IEC, 2013b; ISO/IEC, 2013a ; Kissel i sur., 2014).

Nakon što se identifikuju činioci, mogu se primijeniti različite tehnike bezbjednog ukalnjanja podataka. Vrsta sanitizacije uveliko zavisi o vrsti medija koji se koristi. NIST 800-88 spominje tri principa brisanja. Najprije se podaci s medija moraju ručno izbrisati, prebrisati i formatirati ili se uređaj mora vratiti na fabričke postavke. To obezbjeđuje da podaci nisu slobodno dostupni na uređaju i zaštićeni su od neinvazivnih tehnika preuzimanja podataka. Drugo načelo uključuje metode kao što su brisanje podataka s fiksnim uzorkovanjem bitova, brisanje blokova, kripto brisanje i demagnetiziranje. Ove metode čine podatke nepovratnima, čak i uz korišćenje laboratorijskih tehnika. Treće načelo (usitnjavanje, dezintegracija, usitnjavanje ili spaljivanje) primjenjuje se kako bi se osigurala potpuna nepovratnost podataka ili ako se prvi i drugi princip ne mogu primijeniti (Kissel et al., 2014.).

Nakon sanitizacije slijedi verifikacija kako bi se osiguralo da su svi podaci uklonjeni sa svih lokacija medija i da je dezinfekcija bila uspješna (Ceci et al., 2021; Kissel et al., 2014). Nakon obavljene provjere izrađuje se dokument ili potvrda o sanitizaciji medija. Trebao bi sadržati sve ključne informacije, npr. izvor medija, vrstu medija, serijski broj, vrstu sanitizacije, odredište nakon sanitizacije i druge pojedinosti. Ovaj dokument predstavlja revizijski trag. Osim ako sanitizacija nije potvrdila i dokumentovala odgovorna osoba, ne postoji način da se sazna jesu li sve informacije s elektronskog uređaja ili medija izbrisane na odgovarajući način (Cullipher, 2019; Kissel i sur., 2014).

STUDIJA

Studija je uz pomoć online upitnika željela ispitati kako su korisnici elektronskih uređaja u Sloveniji postupali sa svojim uređajima nakon što ih više nisu koristili i koji su činioci uticali na njihovu svijest o mjerama zaštite elektronskih uređaja.

Ciljna populacija istraživanja su bili korisnici društvenih mreža (Facebook, Twitter, LinkedIn) i korisnici aplikacija za razmjenu poruka (Messenger, WhatsApp, Viber). Podaci su prikupljeni uz pomoć anonimne ankete sprovedene između maja i juna 2022. pomoću online alata 1ka za objavu na društvenim mrežama i aplikacijama za razmjenu poruka, sa uzorkovanjem bez vjerovatnoće primjenom metode sniježne grudve. Upitnik se sastojao od 27 pitanja podijeljenih u pet setova. Pitanja su uglavnom bila zatvorenog tipa i raspoređena na Likertovoj skali od pet tačaka od 1 do 5, gdje 1 znači „uopšte se ne slažem", a 5 „u potpunosti se slažem". Prvi skup pitanja utvrđuje razloge ispitanika za odlaganje, prodaju ili poklanjanje svojih elektronskih uređaja. Uz pomoć osam varijabli, drugi set provjeravala se svijest ispitanika o prijetnjama povezanim s odlaganjem, prodajom ili poklanjanjem elektronskih uređaja. Treći skup, koji je sadržao pet varijabli, posmatrao je iskustva ispitanika s kibernetičkim kriminalom. Za usporedbu, četvrta (pet varijabli) osmišljena da utvrdi svijest ispitanika o zaštitnim mjerama koje treba preduzeti prije nego što se uređaj odloži, proda ili pokloni. Peti dio upitnika (četiri varijable) sadržao je pitanja koja su trebala provjeriti u kojoj su mjeri ispitanici upoznati s ograničenjima procesa brisanja datoteka, dok su šesti i posljednji dio činila demografska pitanja, uključujući pol, dob i obrazovanje.

Kako uzorak ankete nije bio slučajan, ne možemo bez rezerve ekstrapolirati rezultate na cjelokupnu populaciju; umjesto toga, rezultate bismo trebali uzeti samo kao preliminarne pokazatelje kako se ljudi ponašaju u odnosu na prijetnje njihovoj informacionoj bezbjednosti, koje nastaju kao posljedica nepravilnog rukovanja nekim vrstama e-otpada u Sloveniji.

Uzorak se sastojao od 132 (61,4%) ispitanica i 83 (38,4%) ispitanika. Prosječna dob ispitanika bila je 33 godine (najmlađi 19, najstariji 72). Ispitanici uglavnom imaju završeno više, visoko ili visoko obrazovanje (64,8%), zatim srednje obrazovanje (27,1%) te strukovno ili tehničko obrazovanje (8,1%).

U prvom dijelu upitnika pokušali smo utvrditi zašto su se ljudi odlučili prodati, odložiti ili pokloniti svoje elektronske uređaje. Od 216 ispitanika, njih 172 (80%) reklo je da je to učinilo jer je uređaj bio pokvaren, a 118 (55%) reklo je da želi nadograditi svoj postojeći uređaj jer je novi brži, ima više prostora i bolju kameru. Sedamnaest ispitanika (8%) izjavilo je da im je uređaj ukraden, a osam (4%) da su zamijenili postojeći uređaj jer je onaj koji su naknadno kupili imao novi dizajn.

Takođe smo pokušali utvrditi što su korisnici radili s uređajima koje više ne koriste. Dvije trećine (66%, ili 143 ispitanika) reklo je da uređaj drži kod kuće, 47% (101) je uređaj poklonilo, 35% (75) prodalo uređaj, 25% (54) odnijelo uređaj u centar za prikupljanje otpada, a 7% (15) odložilo je uređaj u uobičajeni kućni otpad.

U tabeli 1 prikazane su varijable pomoću kojih smo ispitivali u kojoj su mjeri korisnici bili svjesni prijetnji povezanih s e-otpadom, jesu li bili žrtve cyber kriminala u prošlosti i bili svjesni ograničenja procesa brisanja podataka s elektronskih uređaja. Koristeći faktorizaciju, formulisali smo četiri faktora: 'Svijest o prijetnjama povezanim s odlaganjem, prodajom ili poklanjanjem elektronskih uređaja', 'Iskustvo cyber kriminala', 'Svijest o mjerama zaštite uređaja' i 'Svijest o ograničenjima proces brisanja podataka'. Ovi faktori korišteni su za potrebe daljnje analize.

Tabela 1 Opis varijabli.

Varijable	FW*	M	CK*	CS*	SD
Svijest o prijetnjama povezanim s odlaganjem, prodajom ili poklanjanjem elektronskih uređaja					
α = 0,95 | KMO = 0,91 | promjenljivo = 69,67%	0.77	4.09	-1.13	1.24	0.93
Lični podaci (ime i prezime, adresa) moguće je dobiti s elektronskih uređaja	0.80	3.81	-0.95	0.34	1.07
Moguće je dobiti korisničke podatke (korisničko ime, lozinka) s elektronskih uređaja	0.83	3.63	-0.69	-0.30	1.11
Moguće je dobiti podatke o platnoj kartici s elektronskih uređaja	0.77	4.00	-1.29	1.48	0.99
Moguće je dobiti istoriju preglednika s elektronskih uređaja	0.88	3.94	-1.15	1.05	1.03
Podaci s elektronskih uređaja mogu se koristiti za stvaranje zlonamjernih poruka e-pošte (phishing).	0.91	4.03	-1,30	1.53	1.01
Podaci s elektronskih uređaja mogu se koristiti u svrhu iznude.	0.84	3.96	-1.12	0.83	1.03
Podaci s elektronskih uređaja mogu se koristiti za krađu identiteta.	0.86	3.95	-1.20	1.20	1.03
Iskustvo sajber kriminala α = 0.72 | KMO = 0.73 | var = 35.45%					
Bio sam žrtva zloupotrebe platnih kartica prilikom kupovine putem interneta	0.51	2.00	-0.011	1.15	1.33
Ukradena mi je lozinka ili drugi korisnički podaci	0.71	2.47	-1.05	0.58	1.39

Moj računar je zaražen zlonamjernim softverom (virusom)	0.49	3.23	-1.30	-0.35	1.43
Doživio sam iznudu putem e-pošte ili društvenih i drugih medija	0.66	2.31	-1.14	0.55	1.35
Primio sam e-poruku od nepoznate osobe koja traži lične podatke, podatke o platnoj kartici ili plaćanje (phishing)	0.58	3.19	-1.43	-0.29	1.50
Svijest o mjerama zaštite uređaja α = 0.73 | KMO = 0.69 | var = 43.63%					
Brišem podatke (fotografije, snimke, dokumente) prije zbrinjavanja/prodaje/poklanjanja uređaja.	/	4.50	-1.89	4.46	0.76
Formatiram/izvodim vraćanje na fabričke postavke prije odlaganja/prodaje/poklanjanja uređaja	0.58	4.25	-1.46	1.45	1.05
Koristim sigurne alate za brisanje podataka (CCleaner, BCWipe, MobiWIPE, itd.) prije odlaganja/prodaje/poklanjanja uređaja	0.49	2.93	0.10	-1.31	1.42
Odjavljujem se sa svih korisničkih računa (Gmail, Facebook, Outlook) prije odlaganja/prodaje/poklanjanja uređaja	0.65	4.15	-1.40	1.07	1.14
Brišem istoriju preglednika i kolačiće prije odlaganja/prodaje/poklanjanja uređaja	0.86	3.76	-0.71	-0.90	1.36
Svijest o ograničenjima procesa brisanja podataka α = 0.80 | KMO = 0.77 | var = 51.15%					
Nakon što se elektronski uređaj formatira ili vrati na fabričke postavke, i dalje je moguće oporaviti izbrisane podatke	0.72	3.36	-0.08	-0.79	1.09
Nakon što se datoteke (fotografije, snimke, dokumenti) ručno izbrišu s uređaja, i dalje je moguće vratiti obrisane podatke	0.76	3.76	-0.49	-0.32	0.95
Ručnim brisanjem datoteka u sistemu Windows/Android ne brišem cijelu datoteku već samo podatke koji pokazuju lokaciju datoteke	0.80	3.70	-0.13	-0.59	0.90
Sigurno brisanje podataka znači da se podaci na uređaju brišu, što sprječava njihovu rekonstrukciju	0.56	3.76	-0.13	-0.48	0.85

FW* = Težina faktora
CK* = Koeficijent ekcesa
CS* = Koeficijent asimetrije

Koristeći višestruku regresiju, pokušali smo utvrditi jesu li faktori kao što su svijest o kibernetičkim prijetnjama, iskustvo kibernetičkog kriminala i svijest o ograničenjima procesa brisanja podataka odredili jesu li preduzeli korake za brisanje podataka sa svojih uređaja.

Prije izvođenja višestruke regresije provjerili smo karakteristike procijenjenog regresijskog modela (ANOVA). Kako je p-vrijednost manja od 0,05 (tablica 2), regresijski model je bio statistički značajan, što znači da smo mogli odbaciti nultu hipotezu da su regresijski koeficijenti jednaki nuli (Šifrer & Erčulj, 2020.). Tabela 2 prikazuje R-kvadrat od 0,14 (14%), što znači da možemo koristiti prediktorske varijable (svijest o ograničenjima procesa brisanja podataka, iskustvo cyber kriminala i svijest o prijetnjama povezanim s odlaganjem, prodajom ili poklanjanjem elektronskih uređaja) kako bi se objasnila varijabilnost od 14% zavisne varijable 'Svijest o mjerama zaštite koje treba preduzeti prije nego što se uređaj odloži, proda ili poklanja'. Ostatak se može pripisati drugim činiocima koji nisu dio naše analize.

Tabela 2: Procjena koeficijenata regresije

Model	N.C.*		S.C.*	t	p
	B	S.D.	Beta		
Konstantno*	2.77	0.35		7.97	0.00
Svijest o prijetnjama povezanim sa odlaganjem, prodajom ili davanjem elektronskih uređaja	0.10	0.12	0.10	0.78	0.44
Iskustvo sajber kriminala	0.19	0.07	0.18	2.63	0.01
Svijest o ograničenjima procesa brisanja podataka	0.35	0.10	0.27	3.44	0.00
R^2 = 14 % | ANOVA: F = 6.26 p-value = 0.00					

N.C.* = Nestandardizovani koeficijent
S.C.* = Standardizovani koeficijent
Konstantno* = Svijest o zaštitnim mjerama koje treba preduzeti prije nego što se uređaj odloži, proda ili pokloni

Tabela 2 pokazuje da su dvije od tri prediktorske varijable („Iskustvo cyber kriminala" i „Svijest o ograničenjima procesa brisanja podataka") statistički značajne (p-vrijednost < 0,05). Kompozitna varijabla „Svijest o prijetnjama povezanim s odlaganjem, prodajom ili poklanjanjem elektronskih uređaja" nema statistički značajan učinak na zavisnu varijablu (p-vrijednost = 0,44).

Koeficijent regresije je pozitivan u statistički značajnim kompozitnim varijablama „Iskustvo cyber kriminala" (b = 0,19) i „Svijest o ograničenjima procesa brisanja podataka" (b = 0,35). Ako vrijednost gore navedenih kompozitnih varijabli raste u skladu s izjavom ispitanika, zavisna varijabla, 'Svijest o mjerama zaštite koje treba poduzeti prije nego što se uređaj odloži, proda ili pokloni', također raste ako drugi nezavisne varijable se ne mijenjaju.

Koristeći se višestrukom regresijom, otkrili smo da što bolje korisnik poznaje ograničenja procesa brisanja podataka, veća je upotreba mjera za brisanje podataka, što dovodi do smanjenja vjerovatnosti pojave kibernetičkih prijetnji. Isto se odnosi i na faktor 'Iskustvo cyber kriminala'. Korisnici s prošlim iskustvom u kibernetičkom kriminalu bili su oprezniji nakon što je uređaj napustio njihov posjed.

DISKUSIJA

Kako se količina e-otpada povećava iz godine u godinu (Forti i sur., 2020.), ključno je utvrditi prodaju li korisnici elektronskih uređaja, poklanjaju ili odlažu te uređaje, te koji je razlog njihove odluke. Studija pokazuje da je glavni razlog zašto su ispitanici zamijenili svoj uređaj taj što više ne radi (80%), zatim nadogradnja uređaja (55%), krađa (8%) i novi dizajn (4%). Do sličnih otkrića došli su Miner i sur. (2020.) i Almulhim (2022.), a glavni razlozi zamjene uređaja su činjenica da uređaj više ne radi i želja za nadogradnjom postojećeg uređaja. Bitno je istaknuti da uređaj koji ne radi (najčešće zbog neispravne baterije) može biti najranjivija vrsta uređaja jer korisnik nije izvršio nikakvo brisanje podataka (AVAST, 2014; Blancco, 2017). Napredak pametnih uređaja također podstiče korisnike da radne uređaje zamijene novim, bržim i ljepšim uređajima, što doprinosi globalnom porastu e-otpada (Tan et al., 2018.).

S povećanom količinom e-otpada u svijetu dolazi do povećanja prijetnji informacionoj bezbijednosti (Forgor et al., 2019; Forti et al., 2020). Elektronski uređaji sadrže velike količine ličnih i poslovnih podataka koji se mogu koristiti za izvršenje različitih oblika cyber kriminala (phishing e-pošte, krađe identiteta, društvenog inženjeringa itd.). To može dovesti do finansijske štete, tehničkog kvara i narušavanja ugleda. Osim ako se podaci na elektroničkom uređaju ne izbrišu ili medij uništi (tehnike NIST 800-88 'Clear, Purge and Destroy') i provjere jesu li podaci na odgovarajući način izbrisani, nemoguće je reći jesu li podaci stvarno i uklonjeni.

Studija je također pokazala da se slovenska populacija ne razlikuje značajno od ostalih populacija kada je u pitanju rukovanje e-otpadom. U više navrata se elektronski uređaji premještaju iz sigurnog okruženja u manje sigurno bez prethodnog uklanjanja podataka s tog uređaja (Alghazo et al., 2018; Chen et al., 2021). Najviše ispitanika (66%) uređaj drži kod kuće, 47% ga poklanja, 35% prodaje, 25% nosi u centa za sku-

pljanje otpada, a 7% ga odlaže u zajednički kućni otpad. Slični su rezultati dobijeni u studijama Ceci et al. (2021) i Dzah et al. (2022), odnosno da većina korisnika prodaje svoje elektronske uređaje. Neuspjeh pravilnog uklanjanja podataka s elektronslog uređaja koji se prodaje, poklanja ili odlaže ili koji na drugi način ostaje u posjedu korisnika može dovesti do ranjivosti (ISO/IEC, 2013a; Kissel et al., 2014).

Što se tiče informacione bezbjednosti, vrlo su važni koraci koje korisnici poduzimaju prije nego što odlože, prodaju ili predaju svoj e-otpad. Rezultati ankete pokazuju da korisnici preduzimaju korake poput vraćanja na fabričke postavke, formatiranja, ručnog brisanja podataka i odjave s korisničkih računa kada prestanu koristiti uređaj. Međutim, preduzima se manje koraka za sigurno brisanje ili brisanje podataka s uređaja. Ceci i sur. (2021) dali su slične nalaze u svojoj studiji, s najmanjim brojem korisnika koji su se odlučili za metode koje sigurno uklanjaju podatke. Naši nalazi, kao i oni Ceci et al. (2021), u skladu sa nalazima organizacija Blancco Technology Group i Kroll Ontrack (2015). Kupili su korištene elektronske uređaje, pregledali ih i ustanovili da su većinu uređaja bivši korisnici formatirali ili na njima ručno izbrisali podatke. To je ranjivost sa stanovišta informacione bezbjednosti.

Ovaj se rad nadovezuje na postojeće studije sprovedene u Sloveniji. Osim ispitivanja načina na koji su ljudi postupali sa svojim e-otpadom i koje su mjere preduzeli prije prodaje, odlaganja ili poklanjanja uređaja, utvrđeno je da činioci kao što su prošlo lično iskustvo cyber kriminala i svijest o ograničenjima podataka- proces brisanja pozitivno je uticao na samozaštitno ponašanje korisnika elektronskih uređaja. Nasuprot tome, svijest o prijetnjama nije imala nikakav uticaj. U svojoj studiji, koja je imala uzorak od 309, Markelj i Završnik (2016) otkrili su da svijest o prijetnjama sama po sebi ne diktira način na koji korisnik rukuje svojim mobilnim uređajem; umjesto toga, rukovanje uređajem zavisilo je o stavu/motivaciji korisnika. Direktiva NIS2 istakla je činjenicu da je broj kibernetičkih napada porastao posljednjih godina, te da postaju sve sofisticiraniji, ciljani i prikriveniji (Negreiro, 2022.). Rezultati istraživanja pokazuju da način na koji korisnici trenutno postupaju s e-otpadom ne osigurava odgovarajuću bezbjednost jer su podaci u memoriji uređaja podložni preuzimanju od trećih strana. Uz sve veću prijetnju kibernetičkoj bezbjednosti i privatnosti korisnika, ključno je da se korisnici edukuju i budu svjesni kako ispravno i sigurno postupati sa svojim elektronskim uređajima i e-otpadom. Time bi se smanjila verovatnoća da će se podaci preuzeti iz e-otpada i da se ti podaci koriste u izvršenju sajber kriminala. Od vitalne je važnosti da se informaciona bezbjednost ojača u cijelosti, od trenutka kada se uređaj počne koristiti do trenutka kada se prestane koristiti, tj. kada postane e-otpad koji se prodaje, poklanja ili odlaže.

Količina e-otpada iz godine u godinu raste, kao i količina podataka o elektronskim uređajima. Što se tiče informacione bezbjednosti, način na koji korisnici postupaju s e-otpadom predstavlja rizik, budući da se neadekvatne tehnike primarno koriste za

brisanje podataka. Korisnici se moraju edukovati i upoznati s nedostacima ručnog brisanja i formatiranja podataka, kao i mogućim posljedicama. Uopšteno, korisnici elektronskih uređaja trebaju biti svjesni kako sigurno koristiti uređaje i ukloniti podatke s uređaja. Ako nisu, njihovi su uređaji ranjivi na treće strane koje žele pristupiti finansijskim podacima, informacijama o članovima porodice i poslovnim podacima koji bi se zatim mogli koristiti za izvršenje jednog od brojnih oblika kibernetičkog kriminala. Kao što je već spomenuto, ova (nova) pitanja kibernetičkog i ekološkog kriminala predstavljaju nove izazove za policiju.

LITRATURA

1. J. Alghazo, O. K. M. Ouda, A. E. Hassan, E-waste environmental and information security threat: GCC countries vulnerabilities, Euro-Mediterranean Journal for Environmental Integration 3 (1) (2018) 1–10. https://doi.org/10.1007/s41207-018-0050-4.
2. A. I. Almulhim, Household's awareness and participation in sustainable electronic waste management practices in Saudi Arabia. Ain Shams Engineering Journal, 13 (1) (2022) 1-16. https://doi.org/101729. 10.1016/j.asej.2022.101729.
3. AVAST, Avast demonstrates the risk of selling used smartphones – recovers 40,000 personal photos and emails from phones bought online. (2014) https://press.avast.com/avast-demonstrates-risk-of-selling-used-smartphones-recovers-40000-personal-photos-and-emails-from-phones-bought-online.
4. R. Ayers, W. Jansen, S. Brothers, Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1). NIST Special Publication, 1 (1) (2014) 85. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf.
5. J. Bennion, Drowning in Electronics: Where the Law Stands on E-Waste, (n.d.) https://www.pbs.org/frontlineworld/stories/ghana804/resources/ewaste.html. accessed: 2023-02-08
6. Blancco, What is cryptographic erasure. (2017) https://www.blancco.com/resources/article-what-is-cryptographic-erasure/. accessed: 2023-08-02
7. Blancco Technology Group, and Kroll Ontrack, Blancco Technology Group and Kroll Ontrack Study Finds Lingering Data After Used Electronics Are Resold Online Blancco. (2015) https://www.blancco.com/blancco-technology-group-and-kroll-ontrack-study-finds-lingering-data-after-used-electronics-are-resold-online/. accessed: 2023-04-05
8. B. Markelj, A. Završnik, Kibernetska korporativna varnost mobilnih naprav: zavedanje uporabnikov v Sloveniji. Revija za kriminalistiko in kriminologijo, 67 (1) (2016) 44-60.
9. B. Markelj, S. Zgaga, Kibernetska varnost in kibernetska kriminaliteta uporabnikov mobilnih naprav v Sloveniji. Revija za kriminalistiko in kriminologijo, 69

(1) (2018) 15-29.
10. Candiwan, N. H. Zafira An information security awareness investigation of E-commerce users: A case study of Traveloka. International Journal of Advanced Trends in Computer Science and Engineering, 9 (2) (2020) 1422–1429. https://doi.org/10.30534/ijatcse/2020/79922020.
11. J. Ceci, H. Khan, U. Hengartner, D. Vogel, Concerned but ineffective: user perceptions, methods, and challenges when sanitizing old devices for disposal. Proceedings of the 17th Symposium on Usable Privacy and Security, SOUPS 2021, 8 (10) (2021) 455–473. https://www.usenix.org/system/files/soups2021-ceci.pdf.
12. H. Chen, O. Turel, Y. Yuan, E-waste information security protection motivation: the role of optimism bias. Information Technology in People, 1 (1) (2021) 1–33. https://doi.org/10.1108/ITP-09-2019-0458.
13. V. Cullipher, What is NIST 800-88, and what Does "media sanitization" really mean. Blancco (2019) https://www.blancco.com/resources/blog-what-is-nist-800-88-media-sanitization/. accessed: 2023-11-12
14. B. Debnath, J. M. Alghazo, G. Latif, R. Roychoudhuri, S. K. Ghosh, Sustainable waste management: policies and case studies. Sustainable Waste Management: Policies and Case Studies, 1 (1) (2020) 403-419. https://doi.org/10.1007/978-981-13-7071-7.
15. C. Dzah, J. Agyapong, M. Apprey, K. Agbevanu, P. Kagbetor, Assessment of perceptions and practices of electronic waste management among commercial consumers in Ho, Ghana. Cogent Environmental Science, 8 (1) (2020) 1-16. https://doi.org/10.1080/27658511.2022.2048465.
16. ENISA, Cybersecurity challenges and recommendations (2021a) https://doi.org/10.2824/7703522 accessed: 2023-08-02
17. ENISA, Threat landscape 2021 (2021b) https://doi.org/10.2824/324797. accessed: 2023-08-02
18. European Commission, Equivalent conditions for waste electrical and electronic equipment (WEEE) recycling operations taking place outside the European Union (2013) https://ec.europa.eu/environment/pdf/waste/weee/Final report_EC S.pdf. accessed: 2023-08-03
19. V. Forti, C. P. Baldé, R. Kuehr, G. Bel, The global e-waste monitor 2020 (2020) http://ewastemonitor.info/wp-content/uploads/2020/12/GEM_2020_def_dec_2020-1.pdf. accessed: 2023-08-03
20. K. Hartwig, Digital waste in cyber crime: examining the relationship (2016) https://doi.org/10.13140/RG.2.2.32774.37445. accessed: 2023-08-04
21. A. Hovav, F. Ferdani Putri, This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy, Pervasive and Mobile Computing, 32 (2016) 35-49. https://doi.org/10.1016/j.pmcj.2016.06.007.
22. ISO/IEC, Information technology – security techniques – information security management systems – requirements (2013a) https://eldritchdata.neocities.org/PDF/CS/SecManagmentSystemsReq.pdf. accessed: 2023-08-03

23. ISO/IEC, Information technology — security techniques — code of practice for information security control (2013b) from https://trofisecurity.com/assets/img/ISO-IEC_27002-.pdf. accessed: 2023-08-03
24. R. Kissel, A. Regenscheid, M. Scholl, K. Stine, NIST special publication 800-88 (revision 1) guidelines for media sanitization. NIST Special Publication 800-88, 1(1) (2014) 1–64. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf.
25. A. Mihai, Hacking E-waste is the "greatest little secret" of cyber-security, and it's worth paying attention. Heidelberg Laureate Forum Foundation (n.d.). https://www.newsroom.hlf-foundation.org/blog/article.html?tx_news_pi1%5Baction%5D=detail&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Bnews%5D=285&cHash=d96c53bc9cc7dab1e56315d944f49c9d. accessed: 2023-11-12
26. K. J. Miner, I. T. Rampedi, A. P. Ifegbesan, F. Machete, Survey on Household Awareness and Willingness to Participate in E-Waste Management in Jos, Plateau State, Nigeria. Sustainability, 12 (3) (2020) 1047. from https://doi.org/10.3390/su12031047.
27. M. Negreiro, The NIS2 Directive A high common level of cybersecurity in the EU (2022) https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf. accessed: 2023-12-12
28. O. Osibanjo, I. C. Nnorom, The challenge of electronic waste (e-waste) management in developing countries. Waste Management and Research, 25 (6) (2007) 489–501. https://doi.org/10.1177/0734242X07082028.
29. S. Romanosky, Examining the costs and causes of cyber incidents. Journal of Cybersecurity, 2 (2) (2016) 121–135. https://doi.org/10.1093/cybsec/tyw001.
30. M. Roškot, I. Wanasika, Z. Kreckova Kroupova, Cybercrime in Europe: surprising results of an expensive lapse. Journal of Business Strategy, 42 (2) (2020) 91–98. https://doi.org/10.1108/JBS-12-2019-0235.
31. A. Rožnik, Situacijska prevencija nezakonite trgovine z električnimi in elektronskimi odpadki [Doctoral dissertation]. Faculty of Criminal Justice and Security (2020) https://dk.um.si/IzpisGradiva.php?id=76573&lang=slv&prip=rul:8311585:d2. accessed: 2023-11-12
32. S. Schiller, J. Merhout, R. Sandlin, Enterprise IT asset disposition: an overview and tutorial. Journal of the Midwest Association for Information Systems, 2016 (2) 27–42. https://doi.org/10.17705/3jmwa.00019.
33. B. Schafer, D-waste: Data disposal as challenge for waste management in the Internet of Things. The International Review of Information Ethics, 22 (12) (2014) 101–107. https://doi.org/10.29173/irie131.
34. K. T. Smith, A. Jones, L. Johnson, L.M. Smith, Examination of cybercrime and its effects on corporate stock value. Journal of Information, Communication and Ethics in Society, 17 (1) (2019) 42–60. https://doi.org/10.1108/JICES-02-2018-0010.

35. Q. Tan, H. Duan, L. Liu, J. Yang, J. Li, Rethinking residential consumers' behavior in discarding obsolete mobile phones in China. Journal of Cleaner Production, 195 (1) (2018) 1228–1236. https://doi.org/10.1016/j.jclepro.2018.05.244.
36. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, OJ L 119, 4.5.2016 (p. 1–88)
37. Verizon, 2019 data breach investigations report (2019) https://www.phishingbox.com/assets/files/images/Verizon-Data-Breach-Investigations-Report-DBIR-2019.pdf. accessed: 2023-11-12
38. T. Wakolbinger, F. Toyasaki, T. Nowak, A. Nagurney, When and for whom would e-waste be a treasure trove? Insights from a network equilibrium model of e-waste flows. International Journal of Production Economics, 154 (1) (2014) 263–273. https://doi.org/10.1016/j.ijpe.2014.04.025.
39. N. A. B. Yusof, S. N. H. B. S. Abdullah, M. F. E. bin M. Senan, N. Z. binti Z. Abidin, M. B. Sahri, Data sanitization framework for computer hard disk drive: A case study in Malaysia. International Journal of Advanced Computer Science and Applications, 10 (11) (2019) 398–406. https://doi.org/10.14569/IJACSA.2019.0101155.
40. A. Zingerle, L. Kronman, Information diving on an e-waste dump global data breach. In M. Verdicchio, M. Carvalhais, L. Ribas and A. Rangel (ed.), Conference on Computation, Communication, Aesthetics in X (2019) (pp. 164–176). https://2019.xcoax.org/xCoAx2019.pdf

UDK 343.98:623.4

FORENZIČKI ODGOVOR NA KRIMINALITET U VEZI SA ZLOUPOTREBOM VATRENOG ORUŽJA, MUNICIJE I EKSPLOZIVA

FORENSIC RESPONSE TO CRIME RELATED TO THE MISUSE OF FIREARMS, AMMUNITION AND EXPLOSIVES

Lazar Nešić

Apstrakt

U ovom radu je objašnjena uloga forenzike u obezbeđivanju materijalnih dokaza za procesuiranje krivičnih dela u vezi sa vatrenim oružjem, municijom i eksplozivom (VOME). Na Zapadnom Balkanu ova vrsta kriminala je posebno izražena zbog prisustva velike količine VOME u nelegalnom posedu građana, pre svega kao posledica oružanih konflikata krajem prošlog veka. Pored podsticanja nasilnog kriminala u regionu, značajne količine VOME koje su van efektivne kontrole vlada predstavljaju izvor za njihovo krijumčarenje u zapadne i severne delove Evrope. Forenzika je jedno od sredstava koja su na raspolaganju organima za sprovođenje zakona i pravosudnim organima u suzbijanju kriminala u vezi sa VOME. Aspekti kako državni forenzički sistem obezbeđuje informacije za istrage i dokaze za krivično gonjenje ove vrste zločina, kako na nacionalnom tako i na međunarodnom nivou, objašnjeni su u narednim poglavljima.

Ključne reči: *forenzika, kriminalitet, VOME (vatreno oružje, municija i eksploziv), akreditacija, ENFSI (Evropska mreža forenzičkih instituta), FOMD (forenzička obrada mesta događaja),l GSR čestice, IEN (improvizovana eksplozivna naprava)*

Abstract

This paper explains the role of forensics in providing material evidence for the prosecution of firearms, ammunition and explosives (FAME) crimes. In the Western Balkans, this type of crime is particularly pronounced due to the presence of large quantities of FAME in illegal possession by citizens, primarily as a result of armed conflicts at the end of the last century. In addition to fueling violent crime in the region, significant quantities of FAME that are beyond the effective control of governments represent a source for their smuggling into Western and Northern Europe. Forensics is one of the tools available to law enforcement and judicial authorities in combating FAME crimes. Aspects of how the state forensic system provides information for investigations and evidence for the prosecution of this type of crime, both at the national and international levels, are explained in the following chapters.
Keywords: *forensics, crime, VOME (firearms, ammunition and explosives), accreditation, ENFSI (European Network of Forensic Institutes), FOMD (Forensic Scene Processing), GSR particles, IED (Improvised Explosive Device)*

UVOD – SLOŽENOST FENOMENA ZLOUPOTREBE VOME

Zloupotreba vatrenog oružja, municije i eksploziva može se razmatrati i analizirati sa različitih aspekata pošto mnoga krivična dela i prekršaji uključuju ova sredstva. Prema Interpolu, upotreba vatrenog oružja od strane lica iz kriminogene sredine ugrožava bezbednost građana u svim zemljama sveta. Pored istaknute upotrebe u oružanim pljačkama i ubistvima, ova sredstva su takođe povezana sa širokim spektrom drugih krivičnih dela. To uključuje korupciju, ekološki kriminal, trgovinu ljudima, pomorsku pirateriju, organizovani kriminal i terorističke aktivnosti.[1]

Mnogi relevantni subjekti, kao što je na primer Globalna inicijativa protiv transnacionalnog organizovanog kriminala, naglašavaju problem nezakonite trgovine vatrenim oružjem. U njihovoj brošuri (Policy Brief) izdatoj 2022. godine, nedozvoljena trgovina vatrenim oružjem je definisana kao pretnja održivom razvoju, miru i bezbednosti jer njeno širenje ne samo da podstiče eskaliranje sukoba, već i podržava druge kriminalne aktivnosti.[2] Europol-ovi izveštaji SOCTA[3] uvek predstavljaju trgovinu vatrenim oružjem u odvojenom poglavlju kao posebnu kategoriju kriminala. Kako navodi UNODC, nezakonita trgovina i zloupotreba vatrenog oružja su suštinski povezane sa kriminalnim organizacijama i mrežama: kao sredstvo koje pomaže

1 https://www.interpol.int/Crimes/Firearms-trafficking
2 https://globalinitiative.net/wp-content/uploads/2022/08/GI-TOC-policy-brief_Arms-trafficking-web-1.pdf
3 Serious and Organized Crime Threat Assessment: https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021

izvršenju krivičnih dela sa elementima nasilja, kao sredstvo za ispoljavanje moći i kao unosna roba za krijumčarenje koja podstiče oružane sukobe, kriminal i nesigurnost. Različiti oblici kriminala, kao što su trgovina ljudima, vatrenim oružjem i drogom, često se prepliću.[4] Malo i lako oružje kriminalci jednostavno sakrivaju i transportuju, tako da je trgovina vatrenim oružjem unosan posao koji, zauzvrat, podstiče i finansira druge vrste teških krivičnih dela.

S druge strane, razne protivzakonite delatnosti, pre svega krivična dela, uključuju zloupotrebu VOME. Pored krijumčarenja (vatrenog oružja i municije),[5] Krivični zakonik Crne Gore[6] prepoznaje i mnoga krivična dela koja obavezno ili opciono uključuju zloupotrebu VOME: Ubistvo (različite vrste),[7] Teška tjelesna povreda,[8] Nedozvoljeno držanje i nošenje oružja i eksplozivnih materija,[9] Izrađivanje i nabavljanje oružja i sredstava namijenjenih za izvršenje krivičnog djela,[10] Razbojništvo,[11] Terorizam,[12] Nedozvoljeno postupanje sa eksplozivnim i zapaljivim materijama[13], Nasilje u porodici ili u porodičnoj zajednici,[14] itd. Dok je obim žrtava u oružanim sukobima dobro poznat pojam, manje očigledna, ali još dramatičnija je činjenica da se više života izgubi širom sveta upotrebom vatrenog oružja van ratnih događaja, nego u ratovima koji su u toku.[15] Problemi u vezi sa nasiljem uz upotrebu vatrenog oružja pokrivaju čitav spektar ugrožavanja bezbednosti ljudi: od visokog nivoa individualne fizičke nesigurnosti (nasilje u porodici, na javnom mestu i od stane kriminalnih bandi) sa teškim ekonomskim i socijalnim posledicama po društvo, do ozbiljnog kriminala, terorizma, oružanih sukoba itd.

Takođe, prema Amnesty International-u, samo prisustvo vatrenog oružja može učiniti da se ljudi osećaju ugroženo i uplašeno za svoje živote, sa teškim i dugoročnim psihološkim posledicama po pojedince i čitave zajednice.[16] U kontekstu nasilja u porodici, vatreno oružje predstavlja vanredno otežavajuću okolnost za žrtvu nasilja i njeno preduzimanje bilo kakve akcije sa ciljem da se nasilje okonča, ali i instrument kojim se održavaju tradicionalni obrasci ponašanja i podela uloga u okviru domaćinstva.[17]

4 UNODC article "A Global Problem: Illicit Trafficking and Misuse of Firearms as a Threat to Global Security": https://www.unodc.org/unodc/en/firearms-protocol/index.html
5 Član 265(2) KZ
6 https://www.gov.me/dokumenta/c4dcee51-ee88-430f-a8db-de91f38eadc4
7 Chapter XIV, Criminal Offenses Against Life and Body, Čl. 143-145, 147, 148
8 Čl. 151
9 Čl. 403
10 Čl. 402
11 Čl. 242
12 Čl. 447
13 Čl. 335
14 Čl. 220
15 UNODC article "A Global Problem: Illicit Trafficking and Misuse of Firearms as a Threat to Global Security": https://www.unodc.org/unodc/en/firearms-protocol/index.html
16 https://www.amnesty.org/en/what-we-do/arms-control/gun-violence/
17 dr Danijela Spasić, Marina Tadić, „Zloupotreba oružja i rodno zasnovano nasilje", Centar za istraživanje javnih politika, Beograd, 2016: https://publicpolicy.rs/documents/302291386e5a5a15d9d9c25a697f116addabe382.pdf

ULOGA FORENZIKE U PROCESUIRANJU KRIVIČNIH DELA, A POSEBNO ONIH KOJA SE ODNOSI NA VOME

Problemi povezani sa kriminalom i vatrenim oružjem su tako složene prirode da njihovo suzbijanje zahteva usklađeno dejstvo koje uključuju odgovarajuće intervencije krivično-istražnog i procesnog sistema u smislu prevencije, istrage i procesuiranja krivičnih dela.4 Primena forenzičkih metoda je neophodna za efikasno rasvetljavanje i procesuiranje većine krivičnih dela navedenih u prethodnom odeljku. Forenzički dokazi se pribavljaju i koriste u krivičnom postupku kao konačni ishod forenzičkog procesa. Istovremeno, mnogi forenzički rezultati pomažu sprovođenje krivičnih istraga i služe kao jedino ili barem ključno sredstvo za rasvetljavanje dela, posebno u sadejstvu sa forenzičkim bazama podataka. U sistemu krivične istrage sa dobro razvijenom forenzičkom infrastrukturom danas je čest slučaj da se, na osnovu otiska prsta ili DNK profila dobijenog sa lica mesta, krivično delo (počev od lakog, pa do najtežeg) brzo rasvetli. Istovremeno se obezbeđuju dokazi sa najvećom upotrebnom vrednošću. Takođe, imajući u vidu transnacionalnu i organizovanu dimenziju teškog kriminala danas, ciljajući ovde prvenstveno na nezakonitu trgovinu i zloupotrebu vatrenog oružja, municije i eksploziva, izuzetno je važna konstruktivna međunarodna razmena forenzičkih dokaza i obaveštajnih podataka.

Naučne metode i tehnike su generalno iznele forenziku u prvi plan krivično-istražnog postupka i pravosudnog sistema. Za istragu i krivično gonjenje mnogih vrsta krivičnih dela, ključni dokazi se, po pravilu, pribavljaju forenzičkim veštačenjima, uključujući različite forenzičke obrade. U svakoj zemlji dnevno se obrađuju desetine i stotine lica mesta izvršenja krivičnih dela. Veliki broj tragova koji su obezbeđeni na mestu izvršenja krivičnog događaja se ispituju u forenzičkim laboratorijama, proveravaju se baze podataka i sačinjavaju izveštaji (zapisnici) o veštačenju, čime se obezbeđuju dokazi za krivični postupak koji je u toku.

Forenzički dokazi i druge informacije, kao ishodi različitih forenzičkih postupaka, predstavljaju skoro uvek bitne komponente krivičnih istraga i postupaka kod krivičnih dela u vezi sa vatrenim oružjem, municijom i eksplozivima. Sve vrste forenzičkih ispitivanja i dokaza mogu biti i obično jesu uključene u ove procese. Balistički tragovi (tragovi ispaljenja na projektilima i čaurama) upotrebljavaju se za identifikaciju vatrenog oružja koje je korišćeno u izvršenju ili je u vezi sa krivičnim delom, za povezivanje dva ili više krivičnih dela (koristeći balističku zbirku nerešenih krivičnih dela (ZND)), za utvrđivanje marke i modela nepoznatog vatrenog oružja itd. Informacije dobijene forenzičkom analizom vatrenog oružja, improvizovane eksplozivne naprave (IEN) i njenih delova i komponenti mogu biti od pomoći za praćenje i utvrđivanje njihovog porekla. Forenzičkim veštačenjem utvrđuju se različiti atributi vatrenog oružja važni za krivični postupak, kao npr. da li predmet predstavlja vatreno oruž-

je prema zakonu,[18] da li je oružje funkcionalno ispravno, kojoj kategoriji pripada,[19] itd. Forenzički se ispituju funkcionalne karakteristike IEN. Istovremeno, vrsta i profil eksploziva (bilo da je aktiviran ili neaktiviran) i vrsta prekursora se određuju u forenzičkim laboratorijama korišćenjem različitih forenzičkih hemijskih analitičkih metoda. Učinioci svih vrsta krivičnih dela u vezi sa vatrenim oružjem, municijom i eksplozivima identifikuju se prvenstveno uz pomoć biometrijskih metoda (otisci prstiju, DNK, identifikacija na osnovu lica itd.), ali i korišćenjem drugih forenzičkih tehnika. Generalno, praktično da ne postoji forenzička metoda koja se ne može koristiti u rešavanju slučajeva vezanih za vatreno oružje, municiju i eksplozive ili obezbeđivanju materijalnih dokaza za procesuiranje takvih krivičnih dela.

FORENZIČKA OBRADA MESTA DOGAĐAJA

Većina dokaza koje forenzički sistem obezbeđuje u okviru krivičnog postupka potiče sa uviđaja, konkretnije sa forenzičke obrade mesta događaja (FOMD). Stoga se kredibilitet svakog dokaza inicijalno zasniva na ukupnom kvalitetu sprovođenja FOMD. Sledeće vrste dokaza su samo primeri onoga što se obično pronalazi na mestu događaja gde je korišćeno vatreno oružje ili eksploziv, ili pak na žrtvi ili osumnjičenom licu: projektili i čaure od metaka ispaljenih iz vatrenog oružja, komadi municije, fragmenti projektila, ispaljene sačmene kuglice, čepovi, tragovi rikošeta na površinama i drugi tragovi dejstva projektila vatrenog oružja, vatreno oružje i njegovi delovi, odeća žrtve, tragovi pucanja iz vatrenog oružja (GSR), potencijalni tragovi eksploziva (brisevi, materijal izuzet iz kratera eksplozije itd.), delovi i fragmenti eksplozivnih naprava, neeksplodirano eksplozivno sredstvo (formacijsko ili IEN), eksploziv, ali i sve druge „standardne“ vrste tragova, kao što su tragovi papilarnih linija, tragovi obuće ili pneumatika, DNK brisevi, tragovi krvi, morfološki tragovi prskotina krvi, staklo, vlakna i drugi mikrotragovi itd. Takođe, u slučajevima nedozvoljenog posedovanja, trgovine i krijumčarenja vatrenog oružja, njegovih delova, eksploziva, prekursora i sl, u procesuiranju slučajeva nedozvoljene proizvodnje, modifikacije ili konverzije vatrenog oružja, po pravilu se vrše pretresi i uviđaji uz podršku ili od strane timova forenzičara za uviđaje. U takvim prilikama se pribavljaju i forenzički dokazi, na isti način kao i prilikom obrade „klasičnih“ nasilnih slučajeva u kojima je korišćeno vatreno oružje ili eksploziv.

Uzimajući u obzir ove činjenice, postaje razumljivo u kojoj meri je FOMD neophodna za procesuiranje svih krivičnih dela u vezi sa VOME, za obezbeđivanje forenzičkih dokaza i drugih podataka, i koliko je ista od suštinskog značaja za istragu i krivične postupke na nacionalnom i međunarodnom nivou. Imajući u vidu sofisticirane i izuzetno osetljive, naučno zasnovane metode koje se koriste u forenzičkim laboratorija-

18 Zakon o oružju: https://www.katalogpropisa.me/propisi-crne-gore/zakon-o-oruzju-2/
19 Čl. 4 Zakona o oružju

ma za obradu samih dokaznih predmeta dobijenih sa mesta događaja, postaje jasno u kojoj meri je neophodno imati odgovarajuće kapacitete za FOMD. Takvi kapaciteti podrazumevaju posedovanje kompetentnog osoblja i rukovanje adekvatnom opremom, korišćenje savremenih metoda i odgovarajućih mera za sprečavanje gubitka, degradacije i kontaminacije dokaza, njihovu slučajnu zamenu, neovlašćeno postupanje, itd., tokom izvođenja FOMD i nakon toga, tokom transporta, prvobitne obrade, i čuvanje dokaza.

BALISTIČKA VEŠTAČENJA

Forenzički dokazi koji su od primarnog značaja za krivične postupke u vezi sa VOME koje je dostavio nacionalni forenzički sistem su oni dobijeni u balističkim laboratorijama. Shodno tome, dokazna snaga materijala koji je predočen sudu od strane tužioca, ali i kredibilitet informacija koje se koriste u krivičnim istragama na nacionalnom i međunarodnom nivou, u velikoj meri se oslanjaju na ukupan kvalitet metodologije koja stoji iza rezultata balističkih veštačenja. Kao rezultati balističkih ispitivanja daju se sledeći dokazi i informacije: identifikacija vatrenog oružja korišćenog u izvršenju krivičnih dela na osnovu balističkih tragova na projektilima i čaurama, povezivanje različitih krivičnih dela u kojima je korišćeno isto vatreno oružje, utvrđivanje (ili procena) marke i modela vatrenog oružja korišćenog u krivičnim predmetima, izazivanje uništenih identifikacionih oznaka vatrenog oružja (važno za praćenje oružja), procena daljine pucanja, utvrđivanje funkcionalne ispravnosti, kategorije i potkategorije vatrenog oružja (od značaja za pravnu kvalifikaciju krivičnih dela), utvrđivanje putanje projektila i rekonstrukcija događaja sa upotrebom vatrenog oružja itd. Na ovaj i druge slične načine, dokazi i informacije se obezbeđuju ne samo za procesuiranje slučajeva u kojima je upotrebljeno vatreno oružje (uglavnom nasilni slučajevi sa upotrebom VOMA), već i za slučajeve nedozvoljenog posedovanja i trgovina vatrenim oružjem i njegovim delovima i nezakonite proizvodnje, modifikacije ili konverzije vatrenog oružja. Materijal iz ovakvih slučajeva koji se dostavlja balističkim laboratorijama, a prethodno je sakupljen tokom pretresa, mora da se fiksira uz primenu adekvatnih forenzičkih mera što se najbolje ostvaruje kada se u pretrese uključe forenzički (FOMD) timovi.

Iz navedenog je vidljivo koliko su kvalitet i ispravnost balističkih veštačenja bitni za procesuiranje svih krivičnih dela počinjenih uz korišćenje oružja, te za obezbjeđivanje forenzičkih dokaza i drugih podataka i koliko su oni važni za istrage i krivične postupke na nacionalnom i međunarodnom nivou. Uzimajući u obzir dokazni efekat naučnih metoda koje se koriste u balističkim laboratorijama za krivično procesuiranje dela u vezi sa vatrenim oružjem, postaje jasno u kojoj meri je od suštinske važnosti imati odgovarajuće i standardizovane balističke kapacitete. Ovo poslednje podrazumeva (slično gore navedenom) dobru opremu i osoblje, korišćenje savremenih

metoda i potpunu primenu standarda ISO/IEC 17025 što rezultira odgovarajućom akreditacijom.

VEŠTAČENJE EKSPLOZIVA, EKSPLOZIVNIH SREDSTAVA, I EKSPLOZIJA

Sve vrste zloupotreba eksploziva, posebno ako se posmatraju iz perspektive kriminaliteta, predstavljaju značajnu društvenu opasnost i postavljaju izazove za suzbijanje istih. Postoje mnoga sredstva forenzičkog odgovora u ovoj oblasti, koja se kreću od aktivnosti na mestu eksplozije do različitih laboratorijskih metoda koje imaju za cilj utvrđivanje vrste eksploziva i upotrebljenog sredstva (formacijskog ili improvizovanog), utvrđivanje modusa operandi, identifikaciju učinilaca itd.

Fizička ispitivanja

U oblasti veštačenja eksploziva/eksplozija, fizička ispitivanja se vrše kako na mestu događaja tako i u laboratoriji. Veštačenje nakon eksplozije ima za cilj utvrđivanje uzroka eksplozije i obavlja se uporedo sa uviđajem odnosno FOMD. Tragovi pronađeni i prikupljeni tokom ovih aktivnosti dalje se obrađuju u forenzičkim laboratorijama kako bi se razjasnile relevantne okolnosti, utvrdila vrsta eksploziva i identifikovali učinioci. Određivanje tipa eksplozivne naprave i mehanizma aktiviranja na osnovu tragova nakon eksplozije spada u fizička ispitivanja, kao i ispitivanja fizičkih karakteristika eksploziva (npr. brzina detonacije), eksplozivnih sredstava (improvizovanih i formacijskih), sredstava za iniciranje itd.

Hemijska ispitivanja

Pored mnoštva drugih forenzičkih primena, hemijske analitičke tehnike se koriste da bi se utvrdilo da li nepoznata (privremeno oduzeta) supstanca predstavlja eksploziv, zatim za utvrđivanje vrste eksploziva ili prekursora, i (potencijalno) porekla eksploziva, kao i da bi se pribavile važne informacije koje se mogu koristiti u praćenju tokova ilegalnih eksploziva. S druge strane, povećanje osetljivosti analitičkih instrumenata i odgovarajućih tehnika omogućava sve uspešniju identifikaciju vrste eksploziva iz tragova prikupljenih sa mesta eksplozije, u okviru veštačenja nakon eksplozije.

GSR ANALIZA

Za ispitivanje GSR čestica (tragovi pucanja iz vatrenog oružja) koriste se različite analitičke tehnike kojima se analiziraju ili testiraju tragovi prikupljeni od osumnjičenih lica (uglavnom sa šaka) i sa drugih predmeta i površina od interesa. Metak ispaljen iz vatrenog oružja oslobađa sitne čestice u oblaku dima koje se talože na susedne

predmete, uključujući i šake strelca. Pored organskih jedinjenja (koja potiču npr. od baruta ili maziva), ove čestice sadrže i neorganska (npr. iz inicijalne kapisle ili čaure). Kada se neorganski tragovi sastoje od čestica koje sadrže olovo (Pb), barijum (Ba) i antimon (Sb), to ukazuje da je korišćeno vatreno oružje, jer ovi hemijski elementi potiču po pravilu iz inicijalne kapisle metka. Osnovno eksplozivno jedinjenje u kapisli je uobičajeno olovo stifnat, dok se oksidaciona i redukciona jedinjenja koja se koriste sastoje od antimon sulfata i barijum nitrata.

Činjenica da su prisutne GSR čestice služi kao potvrda pucanja iz vatrenog oružja, ali se njihova analiza može proširiti i dalje od same potvrde. Forenzičkim analizama se može, na primer proceniti ili čak odrediti broj ispaljenih hitaca i rastojanje između vatrenog oružja i (potencijalne) mete. Proučavanjem obrazaca distribucije, GSR analiza može povezati lica ili objekte sa aktivnostima koje uključuju transfer GSR čestica. Informacije koje mogu proizaći iz ispitivanja ove specifične vrste tragova su od vitalnog značaja za identifikaciju potencijalnih učinilaca, rekonstrukciju događaja sa upotrebom vatrenog oružja i potvrđivanje ili pobijanje verzija događaja.

Kada je u pitanju analiza uzoraka radi traženja i otkrivanja GSR čestica, primarni metod izbora danas je skenirajuća elektronska mikroskopija u kombinaciji sa energetskom disperzivnom spektroskopijom (SEM/EDS).

AKREDITACIJA U FORENZICI I IZAZOVI U AKREDITOVANJU POSLOVA FOMD

Standardizacija i akreditacija forenzičkih aktivnosti, kako onih na mestu krivičnog događaja, tako i onih u forenzičkim laboratorijama, međunarodno su prepoznate kao sredstvo za postizanje visokog nivoa kvaliteta FOMD (i laboratorijskih ispitivanja), kao što je gore objašnjeno. U Evropi, ovaj stav se najbolje odražava u Politici o akreditaciji[20] ENFSI.[21] Ovaj dokument predviđa da ENFSI „želi da promoviše dosledne i pouzdane naučne dokaze kroz ceo forenzički proces od mesta događaja do suda“ na različite načine, od kojih onaj koji se tiče FOMD uključuje implementaciju međunarodnog standarda ISO/IEC 17020 za postizanje akreditacije, dok se za laboratorijske metode primenjuje ISO/IEC 17025. Pošto ENFSI okuplja 73 forenzičke institucije – članice iz 39 evropskih zemalja[22] koje zajedno rade na harmonizaciji i standardizaciji u forenzici, pored ostalog, kreiranjem najboljih praksi,[23] standardizacija i akreditacija forenzičkih metoda i tehnika generalno odražava je-

20 http://enfsi.eu/wp-content/uploads/2017/06/BRD-ACR-001_Policy-on-Accreditation.pdf
21 Evropska mreža forenzičkih instituta (engl. the European Network of Forensic Science Institutes): https://enfsi.eu/
22 https://enfsi.eu/about-enfsi/members/
23 ENFSI Politika najboljih praksi: https://enfsi.eu/wp-content/uploads/2017/01/Policy-on-creation-of-Best-Practice-Manuals-within-ENFSI-1.pdf

dan od najvažnijih aspekata stava vlada u Evropi u pogledu napora za unapređenje krivične istrage i krivičnog gonjenja.

Pored unapređenja kvaliteta forenzičkih dokaza, primena istih sveukupno priznatih međunarodnih standarda u obezbeđivanju forenzičkih dokaza olakšava njihovu međunarodnu razmenu i transparentnu primenu u pravosudnim sistemima različitih zemalja. Osnovna korist i razlog za usklađivanje politike standardizacije i akreditacije u oblasti forenzike na globalnom, a posebno na evropskom nivou, jeste mogućnost trenutnog i efektivnog korišćenja forenzičkih rezultata/dokaza dobijenih u jednoj zemlji u krivičnoj istrazi i pravnim postupcima u drugoj zemlji.

Praktična iskustva pokazuju da je mnogo lakše i izvodljivije akreditovati forenzičke laboratorijske metode (u skladu sa standardom ISO/IEC 17025) nego akreditovati aktivnosti koje nisu deo testiranja u forenzičkom procesu. Pored nepostojanja potpuno prilagođenog i adekvatnog standarda,[24] ovo je tako zbog složenosti tih procesa, sa nizom nepredviđenih problema na koje se može naići, na primer na mestu krivičnog događaja, ili tokom veštačenja akcidenata (požara, eksplozija), zatim zbog strogih zahteva vezanih za prostorije, opremu i potrošni materijal, ogromne količine dokumentacije neophodne za akreditaciju i drugih faktora. Različita nacionalna zakonodavna rešenja mogu nametnuti dodatne probleme, kao što su nejasne i preklapajuće nadležnosti.

Iz svih ovih razloga, akreditacija forenzičkih aktivnosti u skladu sa standardom ISO/IEC 17020 odvija se veoma sporo. Na primer, kada je u pitanju FOMD, osim nekoliko „pilot" jedinica akreditovanih u skladu sa ISO/IEC 17020, u Evropi praktično ne postoji do sada akreditovana nacionalna CSI infrastruktura. Prema UKAS-u,[25] poseban napredak u ovoj oblasti je postignut u poslednje vreme u Ujedinjenom Kraljevstvu.[26]

ZAKLJUČAK

Postoji niz krivičnih dela koja uključuju zloupotrebu vatrenog oružja, municije i eksploziva. Osim kod nasilnih, VOME može igrati značajnu ulogu u mnogim drugim vrstama krivičnih dela, kao što su nedozvoljena trgovina, krijumčarenje, nelegalno posedovanje, proizvodnja, modifikacija ili konverzija vatrenog oružja, ali i korupcija, ekološki kriminal, trgovina ljudima itd. Izražena je zabrinutost u vezi sa upotrebom vatrenog i eksplozivnog oružja u nasilju u porodici. Samo prisustvo pištolja ili bombe u domaćinstvu može izazvati ozbiljne negativne psihološke efekte na žrtvu nasilja u porodici, koja je na taj način sprečena da preduzme bilo kakvu aktivnost da zaustavi nasilje.

24 ISO/IEC 17020 standard je dizajniran i sadrži zahteve za rad različitih vrsta kontrolnih tela.
25 Nacionalno akreditaciono telo Ujedinjenog Kraljevstva: https://www.ukas.com/
26 https://www.ukas.com/find-an-organisation/?q=police&type%5B%5D=280

Forenzika može igrati značajnu ulogu u borbi protiv svih vrsta kriminala u vezi sa VOME. Objektivna priroda forenzičkih disciplina doprinosi željenom ishodu sudskih postupaka svih vrsta krivičnih dela, posebno onih vezanih za upotrebu nasilja i VOME, da nevini budu oslobođeni sumnji i optužbi, a da krivci odgovaraju. Zahvaljujući forenzici, istina može prevladati u ambijentu dvosmislenosti, bez obzira na mogući bočni uticaj bilo koje vrste društvene nepravde ili pristrasnosti.

LITERATURA:

1. del Mercado, Guillermo Vázquez, 2022, Arms Trafficking and Organized Crime – Global trade, local impact, Geneva, Global Initiative Against Transnational Organized Crime.
2. 2021, European Union Serious and Organized Crime Threat Assessment, The Hague, European Union Agency for Law Enforcement Cooperation.
3. 2012, ISO/IEC 17020:2012 Conformity assessment — Requirements for the operation of various types of bodies performing inspection, Geneva, International Organization for Standardization, International Electrotechnical Commission.
4. 2023, Krivični zakonik Crne Gore, Podgorica, Skupština Crne Gore.
5. 2019, Policy on Accreditation, The Hague, European Network of Forensic Science Institutes.
6. 2016, Policy on Creation of Best Pratice Manuals Within ENFSI, The Hague, European Network of Forensic Science Institutes.
7. 2015, Zakon o oružju, Podgorica, Skupština Crne Gore.
8. Spasić, Danijela, Tadić, Marina, 2016, Zloupotreba oružja i rodno zasnovano nasilje, Beograd, Centar za istraživanje javnih politika.

UDK 343.132:343.352

ULOGA FINANSIJSKIH ISTRAGA U SUZBIJANJU KRIVIČNIH DJELA SA ELEMENTIMA KORUPCIJE

THE ROLE OF FINANCIAL INVESTIGATIONS IN COMBATING CRIMINAL OFFENCES WITH ELEMENTS OF CORRUPTION

Dr Aleksandra Rakočević
Saradnica u nastavi na Pravnom fakultetu UCG, Podgorica
e-mail: rakocevic.a@ucg.ac.me

Apstarkt

Korupciju kao socijalno patološku pojavu, odnosno protivpravno i amoralno ponašanje možemo proučavati sa različitih aspekata pri čemu krivično pravna dimenzija ima poseban značaj. Ukoliko analiziramo dostupne definicije ovog kriminalnog fenomena možemo konstatovati da su pretežno parcijalne i da ne determinišu korupciju na sveobuhvatan način, već ističu njene pojedine karakteristike. U krivično pravnom smislu korupcija je inkriminisana djelatnost čiji akteri ostvaruju protivpravnu imovinsku korist. Krivična djela sa elementima korupcije pretežno su svrstana u grupe krivičnih djela protiv službene dužnosti i platnog prometa i privrednog poslovanja. Nosioci organizovanog kriminaliteta koriste korupciju u vršenju delikata podmićivanjem, zloupotrebom, nezakonitim uticajem i slično i na taj način jačaju svoje pozicije i stvaraju uslove za nesmetano djelovanje sa akcentom na kreiranje efikasne zaštite od otkrivanja i procesuiranja. Korupciju karakteriše permanentna dinamičnost i brojna fenomenologija koja je vrlo heterogena i kreće se od individualnog podmićivanja do vrlo sofisticiranih situacija sukoba interesa. U ovom rada dat je prikaz jednog broja krivičnih djela sa elementima korupcije u

crnogorskom zakonodavstvu i izvršena analiza relevantnih međunarodnih dokumenata u ovoj oblasti. U borbi protiv korupcije tradicionalni metodi djelovanja nadležnih organa odavno su postali anahroni. Jedna od savremenih metoda koja ima nesporan značaj u suprotstavljanju korupciji je finansijska istraga koja u osnovi obuhvata oblik kriminalističkog istraživanja u čijem je fokusu imovina nosilaca kriminalnih aktivnosti. Nezakonito stečena imovina je ključ za otkrivanje krivičnih djela i učinilaca, a njena identifikacija omogućava ulaženje u trag izvršiocima krivičnih djela prateći najčešće tokove novca. U ovom radu dat je prikaz zakonske regulative finansijskih istraga u Crnoj Gori kao i statističkih podataka o broju finansijskih istraga i na osnovu njih trajno oduzete imovinske korsti za period 2018-2023. godina.
Ključne riječi: *korupcija, nezakonito stečena imovina, finansijske istrage, otkrivanje, suzbijanje.*

Abstract

Corruption as a socially pathological phenomenon, i.e. illegal and immoral behavior can be studied from different aspects, where the criminal legal dimension has a special importance. If we analyze the available definitions of this criminal phenomenon, we can state that they are mostly partial and that they do not determine corruption in a comprehensive way, but emphasize its individual characteristics. In the sense of criminal law, corruption is an incriminated activity whose actors create illegal property benefits. Criminal offences with elements of corruption are mainly classified into the groups of criminal offences against official duty and payment transactions and economic operations. The leaders of organized crime use corruption in the commission of offences by bribery, abuse, illegal influence et cetera and thus strengthen their positions and create conditions for unhindered operation with an emphasis on creating effective protection against detection and prosecution. Corruption is characterized by permanent dynamism and numerous phenomenology that is very heterogeneous and ranges from individual bribery to very sophisticated situations of conflicts of interest. This paper presents a number of criminal offences with elements of corruption in Montenegrin legislation and analyzes relevant international documents in this area. In the fight against corruption, the traditional methods of action of competent authorities have become anachronistic a long time ago. One of the modern methods that is of great importance in combating corruption is the financial investigation, which basically includes a form of criminal investigation, in whose focus is the property of the perpetrators of criminal activities. Illegally acquired property is the key to uncovering criminal acts and perpetrators, and its identification enables tracking down the perpetrators

of criminal acts by following the most common cash flows. This paper presents the legal regulation of financial investigations in Montenegro, as well as statistical data on the number of financial investigations and, based on them, permanently confiscated property benefits for the period 2016-2022. year.
Keywords: *corruption, illegally acquired property, financial investigation, detection, suppression.*

UVOD

Razvoj ljudskog društva od nastanka do danas pratile su brojne socijalne patologije. Korupcija kao jedna od njih je vjerni pratilac svih društveno ekonomskih formacija i može se posmatrati kao konstanta od prvih pisanih izvora postojanja čovjeka, koja uništava zdravo tkivo i vitalne vrijednosti društvene zajednice. Ona posebno pogađa društva u tranziciji koja ne uspijevaju da ostvare vladavinu prava. Visok stepen korupcije u bilo kojoj državi direktno urušava sistem vrijednosti i predstavlja krupnu prepreku ukupnom progresu. Paralelno sa razvojem društva korupcija je dobijala na intenzitetu naročito u odnosu na korišćenje službenog položaja ili društvenog uticaja za sticanje protivpravne koristi. Pošto je korupcija pronalazila mogućnosti upliva u sve strukture društva poseglo se za krivičnopravnom reakcijom kao poslednjim sredstvom u borbi civilizovanog društva protiv korupcije. I pored prijetnje krivičnim sankcijama korupcija se širila do toga nivoa da se danas smatra opštom i globalnom negativnom društvenom pojavom. Svakodnevno smo svjedoci brojnih koruptivnih delikata u mnogim državama svijeta bilo da su nerazvijene, srednje ili visoko razvijene demokratske države. Etimološko značenje riječi corruptio (lat.) znači pokvarenost i odslikava na najbolji način ovaj kriminalni fenomen koji se sastoji u zloupotrebi službene dužnosti i podmićivanju radi lične koristi.

Crna Gora ima ozbiljne probleme sa korupcijom, a procesuirani slučajevi najviših sudskih, tužilačkih, policijskih i drugih zvaničnika za krivična djela sa elementima korupcije dovoljno govore o raširenosti ove vrste kriminaliteta u javnom i privatnom sektoru. Iako je Crna Gora nakon dugih pregovora sa EU konačno dobila završna mjerila i ušla u fazu zatvaranja pregovaračkih poglavlja, nedavni izvještaj GRECO ukazuje na veoma ograničen napredak u borbi protiv korupcije i vrlo skromne rezultate u suprotstavljanju ovoj pojavi. Izvještaj za prethodni period bavio se procjenom mjera koje su preduzele crnogorske vlasti u dijelu realizacije preporuka iz Izvještaja o usaglašenosti za CG za 2022. godinu, koji je obuhvatio 22 preporuke. Konstatovano je da je država zadovoljavajuće ispunila samo tri od dvadeset dvije preporuke, da je jedanaest djelimično ispunjeno, a da čak osam nije ispunjeno. Istaknuto je da iako postoje značajne zakonodavne inicijative u vezi sa licima na najvišim izvršnim funkcijama napredak je vrlo limitiran. Kao jedan od nedostataka navodi se nepostojanje koordinisane strategije za prevenciju korupcije u vrhu vlasti na osnovu odgovarajućih procjena rizika. Nakon de-

taljne analize crnogorskog Zakona o sprječavanju korupcije utvrdili su da pravni okvir nije korigovan kako bi se obezbijedila njegova efikasnost i koherentnost. U izvještaju se između ostalog preporučuje da bi pravila o imunitetu koja se pružaju članovima izvršne vlasti trebalo revidirati na način da se eksplicitno isključe sva koruptivna krivična djela. Podsjetili su da je neophodno ostvariti dalji napredak kako bi se postigao adekvatan nivo usaglašenosti sa preporukama iz 2022. godine.[1]

Imajući u vidu kompleksnost krivičnih djela sa elementima korupcije evidentno je da se tradicionalnim metodima kriminalistike ovi delikti ne mogu efikasno suzbijati. Riječ je o vrsti krivičnih djela sa ekspanzijom novih pojavnih oblika koji predstavljaju veliki izazov za oficijelne strukture. Stoga je otkrivanje i procesuiranje ovih delikata nezamislivo bez finansijskih istraga kao ključnog sredstva za oduzimanje imovine stečene krivičnim djelom. Fokus kompletnih istraga u ovoj oblasti mora biti na istraživanju imovine nosilaca kriminalnih aktivnosti i detekciji njenog porijekla.

KRIVIČNA DJELA SA ELEMENTIMA KORUPCIJE I FINANSIJSKE ISTRAGE U MEĐUNARODNIM DOKUMENTIMA

Međunarodna zajednica ulaže značajne napore u cilju efikasnog suzbijanja krivičnih djela sa elementima korupcije kreiranjem adekvatne normativne osnove za suzbijanje ove vrste kriminaliteta sa akcentom na sveobuhvatnu međudržavnu saradnju. U dokumentima od međunarodnog značaja su vrlo precizno definisane procedure istrage i krivičnog gonjenja korupcije, zamrzavanje, konfiskacija i povraćaj imovine stečene kriminalnom djelatnošću. Izuzetno važan dokument u suprotstavljanju korupciji je Konvencija UN protiv korupcije[2] usvojena u Njujorku 2003. godine, koja je ukazala na težinu problema koje generiše korupcija ugrožavajući vladavinu prava, održivi razvoj i druge vitalne vrijednosti modernog društva. U preambuli ovog akta naglašeno je da korupcija predstavlja transnacionalnu pojavu, da je povezana sa različitim oblicima privrednog i organizovanog kriminaliteta i da je radi efikasnog suzbijanja neophodan sveobuhvatan multidisciplinarni pristup. Posebno je ukazano na nezakonito sticanje ličnog bogatstva koje prouzrokuje negativne posledice po demokratiju i pravnu državu. Njen doprinos je i u tome što je definisala ključne pojmove kao što su javni funkcioner, imovina, sredstva stečena izvršenjem krivičnog djela, zamrzavanje ili zaplena, predikatno krivično djelo i kontrolisana isporuka, otklanjajući na taj način brojne dileme i otvorena pitanja u vezi konotacije naznačenih termina. Značajno poglavlje u konvenciji odnosi se na mjere za sprječavanje korupcije koje

1 Na 97 plenarnoj sjednici GRECO, održanoj od 17-21. juna u Strazburu usvojen je Izvještaj o usaglašenosti za CG u okviru petog kruga evaluacije na temu „ Prevencija korupcije u odnosu na najviše nivoe izvršne vlasti i policiju“
GRECO-Montenegro –Publication of the 5th Round Compilance Report,
https://www.coe.int/en/web/greco/home/-/asset_publisher/lxOP5Yph48Zi/content/montenegro-publication-of-the-5th-round-compliance pristup: 10.08.2024.

2 Konvencija UN protiv korupcije Sl.list SCG-Međunarodni ugovori, br. 12/2005.

uključuju obavezu država potpisnica da ustanove sveobuhvatni unutrašnji regulatorni i nadzorni režim banaka i nebankarskih finansijskih institucija, koje pružaju usluge za prenos novca ili vrijednosti kako bi se spriječilo pranje novca. U poglavlju III propisana su krivična djela sa elementima korupcije i to: podmićivanje domaćih javnih funkcionera, podmićivanje stranih javnih funkcionera i funkcionera javnih međunarodnih organizacija, pronevjera, zloupotreba ili drugo nelegitimno korišćenje imovine od strane javnog funkcionera, zloupotreba uticaja, zloupotreba funkcija, nezakonito bogaćenje, podmićivanje u privatnom sektoru, pronevjera imovine u privatnom sektoru, pranje sredstava stečenih izvršenjem krivičnog djela, prikrivanje i ometanje pravde. Sve naznačene inkriminacije je propisalo crnogorsko zakonodavstvo, osim krivičnog djela nazakonito bogaćenje pravdajući to činjenicom da je ono obuhvaćeno drugim krivičnim djelima. U čl. 31 propisane su mjere zamrzavanja, zaplene i konfiskacije imovine, odnosno sredstava stečenih vršenjem koruptivnih krivičnih djela, imovine, opreme i drugih sredstava koja se koriste ili su namijenjena za izvršenje krivičnih djela. U stavu 2 predviđena je obaveza država da preduzmu mjere, koje omogućuju identifikaciju, traganje, zamrzavanje i zaplenu sredstava stečenih krivičnim djelom. U slučaju da su nezakonito stečena sredstva transformisana ili zamijenjena u drugu imovinu, ta imovina se takođe oduzima, kao i nezakonito stečena imovina sjedinjena sa imovinom stečenom iz zakonitih izvora. Predviđeno je i da prihodi koji proisteknu iz sredstava stečenih kriminalnom djelatnošću takođe podliježu konfiskaciji.

Krivičnopravna konvencija SE o korupciji usvojena je 1999. godine u Strazburu[3] u cilju zaštite društva od korupcije koja predstavlja prijetnju demokratiji i ljudskim pravima. Ovaj dokument je propisao sljedeća krivična djela sa elementima korupcije: aktivno podmićivanje domaćih državnih službenika, pasivno podmićivanje domaćih državnih službenika, podmićivanje članova porodice domaćih javnih skupština, podmićivanje stranih državnih službenika, podmićivanje članova domaćih javnih skupština, podmićivanje stranih državnih službenika, podmićivanje članova stranih javnih skupština, aktivno podmićivanje u privatnom sektoru, pasivno podmićivanje u privatnom sektoru, podmićivanje službenika međunarodnih organizacija, podmićivanje članova međunarodnih parlamentarnih skupština, podmićivanje sudija i službenika međunarodnih sudova, trgovina uticajem, pranje novca koji je dobit od krivičnih djela korupcije i krivična djela u računovodstvu. U dijelu sankcija i mjera ovaj akt predviđa usvajanje zakonodavnih mjera koje omogućuju konfiskaciju i druge načine lišavanja prava svojine na sredstvima i prihodima od krivičnih djela korupcije ili na imovini čija vrijednost odgovara tim prihodima. Od mjera kojima se olakšava prikupljanje dokaza i konfiskacija dobiti predviđene su specijalne istražne tehnike radi identifikacije, ulaženja u trag, zamrzavanja i zaplene dobiti od korupcije ili imovine čija vrijednost odgovara toj dobiti.

3 Zakon o potvrđivanju Krivičnopravne konvencije o korupciji, Sl. list SRJ- međunarodni ugovori, br. 2/2022 i 18/2005.

Konvencija UN protiv nezakonitog prometa opojnih droga i psihotropnih supstanci iz 1988. godine[4] predstavlja prvi dokument koji sadrži solidnu normativnu osnovu za napad na ekonomske aspekte ilegalne trgovine drogom i ukidanje finansijskih podsticaja za vršenje krivičnih djela iz oblasti zloupotrebe droge sa akcentom na oduzimanja prihoda stečenih nezakonitim prometom droge.[5] U članu 1 koji definiše osnovne pojmove iz ove oblasti zaplena podrazumijeva trajno lišenje svojine shodno odluci suda ili drugog državnog organa u svim slučajevima kada se ova mjera može implementirati. Osim toga predviđen je još jedan vrlo značajan instrument u borbi protiv ovih krivičnih djela, a to je zamrzavanje ili oduzimanje što uključuje privremenu zabranu transfera, konverzije, korišćenja i raspolaganja svojinom i preduzimanje nadzora nad svojinom za koju postoji sumnja da je pribavljena izvršenjem predikatnog krivičnog djela. U članu 3 kao posebni oblik krivičnog djela predviđena je konverzija ili transfer svojine u cilju prikrivanje nezakonitog porijekla i prikrivanja prave prirode svojine stečene izvršenjem ovih delikata. Konvencija naglašava značaj međunarodne saradnje kao preduslova za suzbijanje naznačenih delinkventnih aktivnosti.

Konvencija UN protiv transnacionalnog organizovanog kriminaliteta poznata kao Palermo konvencija iz 2000. godine sa dodatnim protokolima predstavlja najvažniji međunarodni pravni akt koji reguliše oblast suzbijanja krivičnih djela izvršenih na organizovan način.[6] U uvodnim odredbama ovog dokumenta se dobit od kriminala definiše kao imovina koja je proistekla ili je nastala neposredno ili posredno izvršenjem zločina, dok konfiskacija obuhvata trajno lišavanje prava svojine na imovini na osnovu odluke nadležnog organa. Konfiskaciju i zaplenu predviđa član 12 ovog dokumenta kao obavezu država potpisnica da izvrše oduzimanje dobiti stečene izvršenjem teških krivičnih djela, odnosno imovine čija vrijednost odgovara vrijednosti nezakonito ostvarene dobiti. U tom cilju neophodna je identifikacija, zamrzavanje i zaplena dobiti, odnosno imovine i u slučajevima kada je došlo do transformacije u drugu imovinu ili je spojena sa legalnom imovinom, takva imovina je podložna konfiskaciji do procijenjene vrijednosti pomiješanih sredstava od izvršenja krivičnih djela. Oduzimanju podliježu i svi prihodi proistekli iz dobiti od kriminala ili imovine u koju je nelegalna dobit transformisana. Poseban značaj imaju odredbe člana 7 u kojima su predviđene mjere za sprječavanje pranja novca, odnosno legalizacije nezakonitih aktivnosti.

Konvencija EU o pranju, traženju, zapleni i oduzimanju prihoda nastalih izvršenjem krivičnih djela donijeta je u Strazburu 1990. godine.[7] Polazeći od činjenice da krivično

4 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988. Zakon o ratifikaciji konvencije UN protiv nezakonitog prometa opojnih droga i psihotropnih supstanci, Sl. list SRJ-Međunarodni ugovori, br. 14/90.

5 Gurule J. (1998). The 1988 U.N. Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances –A Ten Year Perspective: Is International Cooperation Merely Illusory? Fordham International Law Journal Volume 22, Issue 1 1998 Article 2 p.74.

6 United Nations Convention Against Transnational Organized Crime, (Zakon o potvrđivanju Konvencije Ujedinjenih nacija protiv transnacionalnog organizovanog kriminaliteta, Sl. list SRJ, br. 6/21).

7 Zakon o potvrđivanju Konvencije o pranju, traženju, zapleni i konfiskaciji prihoda stečenih kriminalom, "Sl. list SRJ-Međunarodni ugovori", br.7/2002; 18/2005.

djelo pranje novca nije vezano samo za oblast zloupotrebe opojnih droga i psihotropnih supstanci, već da obuhvata više drugih predikatnih krivičnih djela, Savjet Evrope je zauzeo stanovište da je jedna od ključnih metoda za suprotstavljanje teškim oblicima kriminaliteta oduzimanje prihoda stečenih kriminalom nosiocima kriminalne aktivnosti.[8] Negativne posledice pranja novca najviše pogađaju države čija tržišta nijesu razvijena, a finansijski sistemi pokazuju brojne nedostatke.[9] U članu 1 prihod je označen kao svaka ekonomska korist od izvršenja krivičnih djela koji se može sastojati od bilo koje imovine. U istom članu imovina je definisana kao materijalna, nematerijalna, pokretna ili nepokretna imovina, uključujući i pravnu dokumentaciju ili instrumente za dokazivanje vlasništva ili interesa u odnosu na imovinu. Pod sredstvima se podrazumijeva svaka imovina koja se koristi ili postoji namjera da se koristi na različite načine za kriminalnu djelatnost. Prema autorima ovog dokumenta pod konfiskacijom se podrazimijeva svaka kazna ili mjera izrečena od strane suda nakon sprovedenog krivičnog postupka čija je posledica konačno oduzimanje imovine. Pod predikatnim krivičnim djelom ovaj dokument podrazumijeva svaki oblik protivpravne i protivzakonite aktivnosti koja uzrokuje sticanje prihoda koji mogu biti predmet krivičnog djela pranje novca. U sljedećem članu su predviđene mjere konfiskacije kao obaveza država da usvoje zakone koji će omogućiti da se oduzmu sredstva, prihodi ili imovina stečena kriminalnom djelatnošću. Naglašava se obaveza država da kroz odgovarajuća zakonska rješenja omoguće da se utvrdi nezakonito stečena imovina, kao i da se spriječi raspolaganje imovinom, pa je u tom cilju potrebno primijeniti specijalna istražna ovlašćenja i tehnike. To podrazumijeva stavljanje na raspolaganje bankarske, finansijske i komercijalne dokumentacije istražnim organima i korišćenje praćenja, osmatranja, prisluškivanja i drugih specijalnih istražnih metoda. Citirani dokument predviđa četiri oblika krivičnog djela pranje novca sa više alternativno postavljenih radnji izvršenja.[10] U odjeljku 3, članovima 11-18 regulisane su privremene mjere, odnosno zamrzavanje i zaplena u cilju sprječavanja prenosa ili raspolaganja imovinom. U pogledu izvršenja konfiskacije predviđena je obaveza država potpisnica da na zahtjev druge države molilje izvrše nalog za konfiskaciju, koji je izdao sud, koji može obuhvatiti i plaćanje novčanog iznosa, koji odgovara vrijednosti prihoda ako se imovina nalazi u zamoljenoj državi. Predviđeno je da svakom imovinom koju konfiskuje zamoljena država raspolaže država molilja u skladu sa svojim zakonodavstvom.

U svrhu efikasnijeg suzbijanja pranja novca na međunarodnom nivou, formirana je Grupa za finansijske akcije[11] koja je u toku 1990. godine donijela dokument "Četrdeset preporuka za borbu protiv pranja novca" koji sadrže strateški važne elemente i upućuju na bazične pravce u suzbijanju pranja novca. Zbog toga je od velike važnosti

8 Jovanović A. (2022). Suzbijanje pranja novca i finansiranja terorizma u crnogorskom i evropskom krivičnom zakonodavstvu i praksi, Podgorica, str.58.

9 Budimir N. (2020). Pranje novca kao savremeni fenomen-pojam, faze i sprječavanje pranja novca, Naučne publikacije Državnog univerziteta u Novom Pazaru, Vol 3 / 1, str. 64.

10 Jovanović A., op.cit. str.60

11 Međunarodno tijelo koje postavlja standarde u suzbijanju pranja novca, finansiranja terorizma i finansiranja širenja oružja za masovno uništenje.

pratiti preporuke i težiti unapređenjima na zakonodavnom nivou u smislu boljih i efikasnijih normativnih rješenja.[12] Prva direktiva EU o sprječavanju korišćenja finansijskog sistema u svrhu pranja novca[13] istakla je potrebu inkriminisanja pranja novca kao tipologiju najtežih delikata koji ugrožavaju nacionalne i međunarodne interese. Evidentno je da se inkriminacija pranje novca vezuje za visokoprofitabilne transakcije i da se u velikom broju slučajeva ne evidentiraju u oficijelnim statistikama.[14] Zbog toga je tamna brojka kod ovog oblika kriminaliteta vrlo visoka. Obim implementacije ovog dokumenta je proširen u smislu da pod udar krivičnog gonjenja mogu doći sva novčana sredstva, materijalna ili nematerijalna, pokretna ili nepokretna imovina, dokumenta i sredstva koja upućuju na postojanje vlasništva ili ekonomskog interesa na takvoj imovini. Značaj direktive se ogleda i u tome što ona predviđa da pranje novca kao krivično djelo egzistira i u slučaju ako su aktivnosti preduzete u cilju pranja novca na teritoriji država članica EU, kao i na teritoriji drugih država. Proširen je broj nosilaca kriminalnih aktivnosti koji pored fizičkih lica obuhvata i kreditne i finansijske institucije, odnosno pravna lica. Na ovaj način EU je inkorporirala opšte krivično pravne standarde za suzbijanje pranja novca, ali i proširila implementaciju na značajan broj krivičnih djela.[15] Druga Direktiva Savjeta Evrope o preveniranju korišćenja finansijskog sistema u cilju pranja novca[16] iz 2001. godine, proširila je broj predikatnih krivičnih djela i profesija, koje su povezane sa pranjem novca saglasno preporukama FATF i Konvencije UN iz 2000. godine. Direktivom 2015/849 EU[17] o promjeni akta (EU) br. 648/2012 EP i SE i o stavljanju van pravne snage Direktive 2005/60 EZ EP i SE i Direktive Komisije 2006/70 EZ, kreiran je djelotvoran pravni mehanizam za rješavanje problema prikupljanja novca ili imovine u terorističke svrhe budući da se od država članica zahtijevalo da detektuju i reduciraju riziko faktore povezane sa pranjem novca i finansiranjem terorizma. Naglašeno je da krivična djela sa elementima pranja novca, zatim, finansiranja terorizma i organizovanog kriminalnog ispoljavanja predstavljaju veliki problem EU zbog čega je potrebno razvijati krivičnopravni sistem i preduzeti preventivne mjere u ovoj oblasti.[18] Pojedini autori ističu da proces pranja novca obuhvata produženo krivično djelo koje ga je i kreiralo.[19] Propisano je pet oblika krivičnog djela pranje novca, a krivično djelo finansiranje terorizma obuhvata obezbjeđenje ili pribavljanje novčanih sredstava bilo kojim putem, direktno ili indirektno sa intencijom da se ta sredstva koriste i uz postojanje svijesti i volje da su ona namijenjena eksploataciji u cjelini ili djelimično za izvršenje inkriminacija sa

12 Iljkić D.(2015). Pranje novca u domaćem i stranom zakonodavstvu, Finansije i pravo, Vol.3, No.1 str.37.
13 Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, (1991) OJ L 166/77.
14 Rička Ž.(2011). Uloga računovođa u sprečavanju pranja novca, Reviconov zbornik (Međunarodni simpozijum ubrzane reforme u funkciji održivog razvoja, 303-317.
15 Crumbley, L., Heitger, L.,Stivenson, S. (2007). Forensic and Investigative Accounting. Chicago:CCH Business Valuation Guide, p.7011
16 Directive 2001/97/EC of the European Parliament and the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, Official Journal, L 244, 28 January 2001.
17 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 .
18 Jovanović A. op.cit. str. 63.
19 Carlson J. (2010). Suprotstavljanje mitu i korupciji, Zagreb: Oksimoron,d.o.o. str.110.

elementima terorizma.[20] Ovdje se radi o tzv. teleološkom modelu koji je baziran na različitim ciljevima pranja novca, odnosno u ovom slučaju finansiranja terorizma.[21] Direktiva EU 2018/843 EP i SE o izmjeni Direktive 2015/849 o preveniranju korišćenja finansijskog mehanizma u cilju pranja novca ili finansiranja terorizma i o inoviranju direktiva 2009/138 EZ i 2013/36 EU[22] je proširila oblast implementacije Direktive 2015/849 na ponuđače usluga razmjenjivanja kripto valuta, maskiranjem translacije ili eksploatacijom anonimnosti na pojedinim mrežama. Stoga je od velike važnosti pribavljanje kriminalistički relevantnih informacija na osnovu kojih se mogu povezati adrese virtuelne valute sa pravnim i fizičkim identitetom vlasnika kripto valute što je moguće operacionalizovati korišćenjem finansijsko obavještajnih i operativnih podataka oficijelnih organa. S pravom se ističe da virtuelne valute ne treba identifikovati sa elektronskim novčanim sredstvima, kao ni sa valutama elektronskih igara.

Ključni cilj citiranih dokumenata je unapređenje zakonodavstva koje će onemogućiti ulazak ilegalnog novca u legalni monetarni sistem sa fokusom na eleminaciju izvora nelegalnog novca. U poslednjoj fazi pranja novca (integracija) nosioci kriminalnih aktivnosti reinvestiraju novac u reproduktivni ciklus odnosno u zakonite djelatnosti. U tu svrhu osnivaju neimenovane firme u državama gdje je konspirativnost garantovana, dostavljaju fiktivne uvozno izvozne račune, vrše transportovanje iz jedne finansijske institucije u drugu i slično.[23] Budući razvoj evropskog krivičnog prava u oblasti procesuiranja osoba zbog izvršenja krivičnog djela pranje novca povjeren je posebno formiranom Kontakt tijelu koje konstituišu predstavnici država članica EU. Zadatak ovog tijela je preduzimanje aktivnosti na implementaciji citiranih akata kroz oficijelne konsultacije o pragmatičnim problemima koji se pojavljuju u implementaciji. Osim toga, predviđene su i permanentne konsultacije između država članica EU radi razmatranja pitanja iz ove oblasti.[24]

KRIVIČNA DJELA SA ELEMENTIMA KORUPCIJE U CRNOGORSKOM ZAKONODAVSTVU

Korupcija i privredni kriminalitet generišu višestruke negativne posledice po kompletno društvo u svim njegovim djelovima.[25] U Crnoj Gori je Zakon o sprječavanju

20 Direktiva 2015/849 Evropske unije, član 1 tač.5.

21 Mitsilegas V. (2003). Money Laundering Counter-measures in the European Union: A New Paradigm of Security Governance Versus Fundamental Legal principles, Hague, Kluwer Law International, p.25.

22 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

23 Jergović-Katušić S. (2007). Pranje novca (pojam, karakteristike, pravna regulativa i pragmatični problemi), Hrvatski ljetopis za kazneno pravo i praksu, p.619.

24 Jovanović A., op.cit. str. 89.

25 Simović M, Šikman M. (2017). Krivičnopravno reagovanje na teške oblike kriminaliteta, Banja Luka: Pravni fakultet Univerziteta u Banjoj Luci. str.271.

korupcije stupio na snagu početkom 2016. godine.[26] Na osnovu ovog akta formirana je Agencija za sprječavanje korupcije Crne Gore. Ovim zakonom je definisana korupcija kao zloupotreba službenog, poslovnog i društvenog položaja ili uticaja u cilju sticanja lične koristi ili koristi za drugog. Takođe je definisan pojam zviždača i modeli njegove zaštite. Agencija je ovlašćena da vodi administrativne istrage kroz postupak za utvrđivanje sukoba interesa.

U crnogorskom Krivičnom zakoniku krivična djela sa elementima korupcije svrstana su u dvije glave KZ. U prvoj brojnijoj tipologiji delikata protiv platnog prometa i privrednog poslovanja propisana su sljedeća krivična djela sa elementima korupcije: pranje novca, povreda ravnopravnosti u vršenju privredne djelatnosti, zloupotreba monopolističkog položaja, zloupotreba položaja u privrednom poslovanju, prouzrokovanje stečaja, prouzrokovanje lažnog stečaja, zloupotreba ovlašćenja u privredi, lažni bilans, zloupotreba procjene, odavanje poslovne tajne, odavanje i korišćenje berzanske tajne, primanje mita u privrednom poslovanju, davanje mita u privrednom poslovanju, navođenje na protivzakoniti uticaj, manipulacija na tržištu hartija od vrijednosti ili drugih finansijskih instrumenata, kao i krivična djela zloupotreba u vezi sa javnom nabavkom, zloupotreba u postupku privatizacije i primanje i davanje mita u postupku stečaja, propisana Zakonom o izmjenama i dopunama KZ iz decembra 2023. godine. U grupi krivičnih djela protiv službene dužnosti propisana su sljedeća krivična djela sa elementima korupcije: zloupotreba službenog položaja, protivzakoniti uticaj, navođenje na protivzakoniti uticaj, primanje mita i davanje mita. U nastavku izlaganja ukazaćemo na osnovne karakteristike jednog broja krivičnih djela iz ove oblasti imajući u vidu dozvoljeni obim rada.

Krivično djelo pranje novca potiče iz aktivnosti kriminalnih organizacija da operu ilegalni novac putem perionica sa intenzivnim gotovinskim pranjem koje su kontrolisale akvizicije kompanija ili poslovne formacije. U poslednje vrijeme postoji očigledna tendencija zloupotrebe interneta u cilju preduzimanja nezakonitih transakcija u formi onlajn bankarstva, sajber novca i elektronske torbice.[27] Pranje novca je proces kojim velika količina nezakonito stečenog novca od trgovine drogom, terorističkih aktivnosti i drugih teških zločina dobija izgled da potiče od legitimnog izvora sa vrlo negativnim posledicama po ekonomiju i političku stabilnost države.[28] U KZ CG[29] krivično djelo pranje novca propisano je u čl. 268 i sadrži šest pojavnih oblika. Osnovni oblik obuhvata više alternativno postavljenih radnji izvršenja, odnosno konverziju ili prenosa novca ili druge imovinske koristi sa znanjem da su pribavljeni kriminalnom djelatnošću u namjeri prikrivanja ili lažnog prikazivanja porijekla novca ili druge imovine, zatim skrivanje,

26 Zakon o sprječavanju korupcije, Službeni list Crne Gore, br. 53/2014.

27 Schneider F.G, Niederlander U. (2008). Money Laundering: Some Facts, European Journal of Law and Economics, 26(3)387-404. DOI:10.1007/s10657-008-9070-x.

28 Kumar V.A. (2012). Money Laundering: Concept, Significance and its Impact, European Journal of Business and Menagement, Vol. 4, No. 2. p. 113.

29 Krivični zakonik RCG, sl. list RCG, 70/23 i Službeni list CG br. 40/2008..110/2023.

držanje ili korišćenje novca ili druge imovine sa znanjem da potiču od krivičnog djela ili prikrivanje ili lažno prikazivanje činjenica o prirodi, porijeklu, mjestu deponovanja, kretanja, raspolaganja ili vlasništva novca ili druge imovine za koju učinilac zna da je pribavljena kriminalnom djelatnošću. Poseban oblik obuhvata vršenje pranja novca u svojstvu izvršioca i saučesnika u krivičnom djelu kojim je pribavljen novac ili imovina. Kažnjava se i lice koje pomogne učiniocu radi izbjegavanja krivične odgovornosti ili preduzme radnje prikrivanja porijekla nezakonito stečenog novca. Teži oblici postoje ako je pranje novca izvršeno na organizovan način, odnosno ako iznos novca ili imovine prelazi 40000 eura. Privilegovani oblici postoje ako je djelo izvršeno od strane učinioca koji je postupao iz nehata kao i odgovorno lice u pravnom licu. Propisana je mjera oduzimanja novca i imovine.[30] Osnovni oblik krivičnog djela povreda ravnopravnosti u vršenju privredne djelatnosti obuhvata četiri alternativno postavljene radnje izvršenja, odnosno zloupotrebu službenog položaja ili ovlašćenja ograničavanjem slobodnog i samostalnog povezivanja privrednog društva ili drugog subjekta privrednog poslovanja u obavljanju privredne djelatnosti što čini prvi vid osnovnog oblika. Drugi oblik radnje izvršenja obuhvata uskraćivanje ili ograničavanje prava privrednom društvu da na određenom području obavlja privrednu djelatnost. Treći oblik radnje sadrži stavljanje u neravnopravan položaj privrednog subjekta prema drugim subjektima privrednog poslovanja u pogledu uslova privređivanja, dok četvrti oblik obuhvata ograničavanje slobodnog obavljanja privredne aktivnosti. Poseban oblik ovog delikta postoji ukoliko učinilac zloupotrijebi svoj društveni položaj ili uticaj za izvršenje naznačenog krivičnog djela (čl. 269 KZ CG). Ovo krivično djelo ne može biti u idealnom sticaju sa krivičnim djelom zloupotreba službenog položaja budući da se radi o radnji izvršenja ove inkriminacije.[31] Krivično djelo zloupotreba monopolističkog položaja iz člana 270 KZ CG obuhvata zaključenje monopolističkog sporazuma kojim se izaziva poremećaj na tržištu ili se privredni subjekt dovodi u povlašćen položaj u odnosu na druge od strane odgovornog lica ostvarujući imovinsku korist za taj ili drugi subjekt ili se nanosi šteta drugim akterima privrednog poslovanja, potrošačima ili korisnicima usluga. U svakoj modernoj državi zabranjene su sve aktivnosti kojima se kreira ili podstiče monopolski položaj i sprječava tržišna utakmica.[32] Osnovni oblik kod zloupotreba položaja u privrednom poslovanju obuhvata zloupotrebu položaja ili povjerenja u pogledu raspolaganja tuđom imovinom, prekoračenjem granica ovlašćenja ili neizvršenjem dužnosti i na taj način pribavi sebi ili drugom protivpravnu imovinsku korist ili drugom nanese imovinsku štetu odgovorno lice u privrednom društvu, drugom subjektu privrednog poslovanja ili drugom pravnom licu. Drugi oblik ovog delikta ima elemente krivičnog djela pronevjere budući da obuhvata prisvajanje novca, hartija od vrijednosti i drugih pokretnih stvari koje su učiniocu povjerene na radu u privrednom društvu ili drugom subjektu privrednog poslovanja, u namjeri da se sebi ili drugom pribavi

30 Brojni međunarodni i evropski dokumenti propisuju ovo krivično djelo radi jednistvenog krivično pravnog odgovora od kojih se posebno izdvaja Konvencija o pranju, traženju, zapleni i konfiskaciji prihoda stečenih kriminalom iz 1990. godine

31 Lazarević Lj. Vučković B. Vučković V. (2004). Komentar Krivičnog zakonika Crne Gore, Cetinje, str. 670.

32 Rakočević V. (2010). Krivična djela sa elementima korupcije, Podgorica, str. 312.

protivpravna imovinska korist. Teži oblik postoji ako je izvršenjem ovog delikta pribavljena imovinska korist preko 40000 eura (čl. 272 KZ CG). Radi se o supsidijarnom krivičnom djelu koje postoji samo ukoliko radnjom izvršenja nije ostvareno biće drugog delikta.[33] Krivično djelo zloupotreba u vezi sa javnom nabavkom spada u novija krivična djela protiv platnog prometa i privrednog poslovanja sa elementima korupcije. Saglasno pozitivnim propisima država je u obavezi da za svoje potrebe i potrebe firmi u njenom većinskom vlasništvu u svrhu nabavke robe, pružanja usluga i realizacije javnih radova iznad određenog novčanog iznosa raspisuje tender koji bi garantovao transparentnost i zakonitost. Inkriminacija iz člana 272c sadrži sedam oblika. Osnovni oblik čini ono lice koje u vezi sa javnom nabavkom podnese ponudu zasnovanu na lažnim podacima ili se suprotno zakonu dogovara sa ostalim ponuđačima ili preduzme druge protivpravne radnje u namjeri da time utiče na donošenje odluka naručioca javne nabavke. Drugi oblik zloupotrebe u vezi sa javnom nabavkom obuhvata vršenje krivičnog djela zloupotreba službenog položaja od strane lica koje kod naručioca javne nabavke krši zakon i druge propise o javnim nabavkama i time prouzrokuje štetu javnim sredstvima. Treći oblik ovog krivičnog djela vrši učinilac koji nekom subjektu prilagođava uslove javne nabavke ili sklapa ugovor sa ponuđačem čija je ponuda u suprotnosti sa uslovima iz dokumentacije za nadmetanje. Četvrti oblik ovog delikta obuhvata iskorišćavanja položaja ili ovlašćenja, prekoračenje granica ovlašćenja ili nevršenje dužnosti od strane učinioca koji daje, preuzima ili ugovara poslove za svoju djelatnost ili djelatnost osobe u odnosu na koju postoji sukob interesa. Teži oblik postoji ukoliko je ovo krivično djelo učinjeno u vezi sa javnom nabavkom čija vrijednost prelazi iznos od sto hiljada eura i on je određen isključivo vrijednošću u novčanom ekvivalentu javne nabavke. Poseban oblik postoji ukoliko je zloupotreba u vezi sa javnom nabavkom izvršena na štetu finansijskih interesa Evropske unije. U stavu 7 člana 272c propisan je privilegovani oblik koji postoji ukoliko učinilac ovog krivičnog djela dobrovoljno otkrije da se ponuda bazira na lažnim podacima ili na nedozvoljenom dogovoru sa ostalim ponuđačima ili da je preduzeo druge radnje u namjeri da utiče na donošenje odluke naručioca prije nego što se zaključi ugovor o javnoj nabavci. Zloupotreba u postupku privatizacije iz čl.272d KZ CG inkriminisana je sa velikim zakašnjenjem budući da je kroz ovaj postupak veliki broj zaposlenih otišao na biro rada, a država zakinuta za značajna finansijska sredstva. Djelo ima dva osnovna i jedan teži oblik. Prvi oblik delikta obuhvata podnošenje ponude u postupku privatizacije zasnovane na lažnim podacima ili protivpravno dogovaranje sa drugim učesnicima u postupku ili preduzimanje druge protivpravne radnje kojom se utiče na tok postupka ili donošenje odluke organa za realizaciju privatizacije. Drugi oblik obuhvata sve tri radnje zloupotrebe službenog položaja ili ovlašćenja kojima se krši zakon ili drugi propisi o privatizaciji prouzrokujući štetu kapitalu ili dolazi do umanjenja imovine koja je predmet privatizacije. Teži oblik postoji ako je djelo učinjeno u vezi sa privatizacijom čija procijenjena vrijednost prelazi iznos od milion eura. Prouzrokovanje stečaja iz čl. 273 KZ CG sadrži osnovni i privilegovani oblik. Osnovni oblik čija je radnja izvršenja postavljana putem posledične dis-

33 Jovašević D. (2017). Krivično pravo-Posebni deo, Dosije studio, Beograd, str.154.

pozicije[34] se sastoji u neracionalnom trošenju sredstava ili njihovom otuđenju u bescijenje, prekomjernom zaduživanju, preuzimanju nesrazmjernih obaveza, lakomislenom zaključivanju ugovora sa osobama nesposobnim za plaćanje, propuštanju blagovremenog ostvarivanja potraživanja, uništenju ili prikrivanju imovine od strane odgovornog lica u privrednom društvu ili drugom privrednom subjektu koje nesavjesnim poslovanjem prouzrokuje stečaj nanoseći drugom štetu. Privilegovani oblik postoji ukoliko je delikt izvršen iz nehata. Prouzrokovanje lažnog stečaja čini odgovorno lice u privrednom društvu u namjeri da taj subjekt izbjegne plaćanje obaveza prouzrokujući stečaj prividnim ili stvarnim umanjenjem njegove imovine na jedan od sljedećih načina: cijelu ili dio imovine privrednog subjekta prikrije, prividno proda, proda ispod tržišne vriejdnosti ili besplatno ustupi; zaključi fiktivne ugovore o dugu ili prizna nepostojeća potraživanja; poslovne knjige prikrije, uništi ili tako preinači da se iz njih ne mogu sagledati poslovni rezultati ili stanje sredstava ili obaveza ili ovo stanje sačinjavanjem lažnih isprava prikaže takvim da se na osnovu njega može otvoriti stečaj. Teži oblik postoji ako su usljed izvršenja ove inkiminacije nastupile teške posledice za povjerioca (čl. 274 KZ CG). Zloupotreba ovlašćenja u privredi (čl.276 KZ CG) ima osnovni i kvalifikovani oblik a može se izvršiti alternativno postavljenim radnjama izvršenja kao što su stvaranje ili držanje nedozvoljenih novčanih, robnih ili drugih vrijednosti u zemlji ili inostranstvu, neistinitim prikazivanjem stanja u privrednom subjektu, kretanja sredstava ili rezultata poslovanja ili korišćenjem sredstava protivno njihovoj namjeni. Teži oblik postoji ako je pribavljena imovinska korist preko 40000 eura. Propisivanjem ovog krivičnog djela štiti se pravilno privredno poslovanje.[35] Primanje mita u privrednom poslovanju (čl.276a), davanje mita u privrednom poslovanju (čl. 276b) i primanje i davanje mita u postupku stečaja (čl.276c) su klasična koruptivna krivična djela sa aktivnim ili pasivnim podmićivanjem, odnosno zahtijevanje ili primanje mita ili prihvatanje obećanja mita da se zaključi ugovor ili postigne poslovni dogovor ili pruži usluga i slično, odnosno davanje, nuđenje ili obećanje mita odgovornom licu da za sebe ili drugog zaključi ugovor itd.

Krivična djela protiv službene dužnosti su izvorno koruptivni delikti kojima se ostvaruje protivpravna imovinska korist za učinioca ili drugo lice. Shodno svojstvu učinioca u teoriji krivičnog prava ove inkriminacije se dijele na prava i neprava krivična djela protiv normalnog i zakonitog funkcionisanja službe. Prema tome prava krivična djela protiv službene dužnosti su ona izvršena od strane službenog lica. Neprava krivična djela protiv službene dužnosti mogu biti izvršena od strane bilo koje osobe, a dobijaju teži oblik ukoliko su izvršena od strane službenog lica. Krivično djelo zloupotreba službenog položaja predstavlja opšte krivično djelo protiv službene dužnosti, a u slučaju da su ostvareni elementi nekog drugog krivičnog djela iz ove tipologije postojaće samo drugo krivično djelo pošto se radi o prividnom idealnom sticaju.[36] Ovo krivično djelo iz čl. 416 KZ CG ima osnovni, teži i najteži oblik. Osnovni oblik

34 Jovašević D. op.cit. str.157.
35 Petrović Mrvić N. (2015), Krivično pravo posebni deo, Službeni glasnik, Beograd, str.238.
36 Stojanović Z. Delić N. (2015). Krivično pravo-posebni deo, Pravna knjiga, Beograd, str.291.

se sastoji u protivpravnom iskorišćavanju službenog položaja ili ovlašćenja, prekoračenju granica službenog ovlašćenja ili nevršenju službene dužnosti kojom prilikom učinilac sebi ili drugom pribavi protivpravnu imovinsku korist, drugom nanese štetu ili teže povrijedi prava drugog. Teži i najteži oblici postoje ako je izvršenjem ovog krivičnog djela pribavljena imovinska korist u iznosu preko tri, odnosno trideset hiljada eura.

Krivično djelo primanje mita ima tri oblika i to pravo pasivno podmićivanje, nepravo pasivno podmićivanje i naknadno podmićivanje.[37] Crnogorsko zakonodavstvo poznaje pet oblika ovog delikta (čl. 423 KZ CG). Prvi oblik postoji kad službeno lice neposredno ili posredno zahtijeva ili primi mito ili prihvati obećanje mita za sebe ili drugoga da izvrši službenu ili drugu radnju koju ne bi smjelo izvršiti ili da ne izvrši službenu ili drugu radnju koju bi moralo izvršiti. Drugi oblik postoji kad službeno lice neposredno ili posredno zahtijeva ili primi mito ili prihvati obećanje mita za sebe ili drugog da izvrši službenu ili drugu radnju koju bi moralo izvršiti ili da ne izvrši službenu ili drugu radnju koju ne bi smjelo izvršiti. Treći teži oblik postoji ako službeno lice izvrši ovo krivično djelo u vezi sa otkrivanjem krivičnih djela, pokretanjem ili vođenjem krivičnog postupka izricanjem ili izvršenjem krivične sankcije. Četvrti oblik obuhvata naknadno podmićivanje u onim slučajevima kada službeno lice nakon izvršenja ili neizvršenja službene radnje zahtijeva ili primi mito. Peti oblik obuhvata izvršenje ovog krivičnog djela od strane odgovornog ili drugog lica u ustanovi ili drugom subjektu koji se bavi privrednim poslovanjem. Propisana je mjera oduzimanja primljenog mita. Krivično djelo davanje mita iz člana 424 KZ CG obuhvata četiri oblika. Prvi oblik se sastoji u pravom aktivnom podmićivanju kojom prilikom učinilac službenom licu neposredno ili posredno da, ponudi ili obeća mito za njega ili drugog da službeno lice izvrši službenu ili drugu radnju koju ne bi smjelo izvršiti ili da ne izvrši službenu ili drugu radnju koju bi moralo izvršiti ili ko posreduje u ovakvom davanju mita službenom licu. Drugi obliki sadrži nepravo aktivno podmićivanje od strane učinioca koji službenom licu neposredno ili posredno da, ponudi ili obeća mito za njega ili drugog da službeno lice izvrši službenu ili drugu radnju koju bi moralo izvršiti ili da ne izvrši službenu ili drugu radnju koju ne bi smjelo izvršiti ili ko posreduje u ovakvom davanju mita službenom licu. Blaži oblik je predviđen u slučaju da učinilac prijavi djelo prije nego što je saznao da je ono otkriveno kada se može osloboditi od kazne. Četvrti oblik se sastoji u davanju, nuđenju ili obećanju mita odgovornom ili drugom licu u ustanovi ili drugom subjektu koji se ne bavi privrednim poslovanjem. Imajući u vidu broj krivičnih djela sa elementima korupcije ostala nećemo navoditi shodno dozvoljenom obimu rada.

37 Jovašević D. op.cit. str.329.

ULOGA FINANSIJSKIH ISTRAGA U SUZBIJANJU KORUPTIVNIH KRIVIČNIH DJELA

Danas se argumentovano može reći da su finansijske istrage izuzetno važno sredstvo za otkrivanje krivičnih djela sa elementima korupcije. Njihova uloga je u tome da detektuju tragove novca i druge imovine stečene kriminalnom aktivnošću što direktno razotkriva kriminalne mreže obezbjeđujući kredibilne dokaze za krivično gonjenje. Osim toga, ključna uloga finansijskih istraga je u identifikaciji, a kasnije i konfiskaciji imovine nezakonitog porijekla. Polazeći od činjenice da postoji visok rizik od prodora nosilaca kriminalnih aktivnosti u legalne poslovne tokove, finansijske istrage su nezaobilazno i vrlo efikasno sredstvo odgovora države na kriminalne prijetnje, izazove i rizike. Stoga je krucijalno važno da se poboljšaju finansijske istrage u cilju oduzimanja kriminalnog profita i sprječavanja njegovog ulaska u legalnu ekonomiju. Krajem prošlog i u prvim decenijama XXI vijeka suzbijanje najtežih formi kriminalnog ispoljavanja u značajnoj mjeri je usmjereno na konfiskaciju sredstava stečenih kriminalom i sprječavanje da nelegalna imovina bude inkorporirana u zakonitu imovinu. To znači da bi oduzimanje nezakonite imovine dovelo do demotivacije učinilaca ukoliko bi im se jasno stavilo do znanja da će im nezakoniti prihodi biti oduzeti. Veoma je važno da se nelegalno stečena imovina oduzme jer se na taj način sprječava vršenje drugih krivičnih djela.[38] Brojna istraživanja pokazuju blisku vezu između korupcije i pranja novca. Nosioci kriminalnih aktivnosti moraju da legalizuju prihode stečene kriminalom. Kompletan postupak oduzimanja imovine stečene kriminalnom djelatnošću nazamisliv je bez finansijske istrage kojom se otkriva nezakonito stečena imovina i njeno porijeklo, bez čijeg efikasnog sprovođenja nijedan postupak oduzimanja nelegalne imovine ne može imati uspješan epilog. Ona potiče od postupaka poreskih službi koji su imali cilj da utvrde neprijavljene prihode i izbjegavanje plaćanja poreza. Finansijska istraga obuhvata dokazne radnje koje se preduzimaju radi pronalaska i utvrđivanja nezakonito stečene imovine, što uključuje i sredstva pranja novca, koju treba obezbijediti radi oduzimanja ako je stečena krivičnim djelom.[39] Finansijska istraga sadrži istraživanje imovine stečene kriminalom kroz prikupljanje dokaza o imovini u cilju utvrđivanja nesrazmjere sa zakonitim prihodima i privremenog oduzimanja radi osiguranja trajnog oduzimanja.[40] Pojedini autori s pravom smatraju da oduzimanje nezakonito stečene imovine predstavlja ključni instrument modernih strategija suzbijanja zločina budući da omogućava identifikovanja tragova novca, njegovo praćenje i lociranje.[41] Njena ključna uloga je u istraživanju i utvrđivanju tokova novca kroz opservaciju tragova novca i ona je obavezna faza u postupku oduzimanja nezakonite imovine.

38 Naylor, R.T. (1999). A critique of follow-the money methods in crime control policy. Crime, Law and Social Change, Springer, Vol.32 p.11.

39 Lukić T.(2009).Oduzimanje imovine stečene krivičnim delima, Zbornik Pravnog fakulteta u Novom Sadu, 2/2009. str.386.

40 Lajić O. (2011). Institut oduzimanja imovinske koristi stečene krivičnim delom, Pravni fakultet Univerziteta u Novom Sadu, Novi Sad, str. 97.

41 Luigu Gay (2014). Italijansko zakonodavstvo i iskustvo sa ocjenom o konfiskaciji i ponovnoj upotrebi dobara dobijenih organizovanim kriminalom i ostali kriminološki fenomeni, Strani pravni život, (1) 11-30 str.27

Oduzimanje nelegalno pribavljene imovine započinje istražnom fazom, odnosno finansijskom istragom u kojoj se utvrđuje prihod stečen kriminalnom djelatnošću i obezbjeđuju podaci o imovini vlasnika zbog čega se smatra jednom od najznačajnijih etapa u ovom postupku.[42] U poglavlju II a i III Zakona o oduzimanju imovine stečene kriminalnom djelatnošću CG[43] definisani su finansijski izviđaj i istraga. Budući da je izviđaj u osnovi policijska ili kriminalistička djelatnost, slično kao i u drugim slučajevima otkrivanja krivičnih djela i učinioca, ovaj državni organ postupajući po sopstvenoj inicijativi ili zahtjevu državnog tužioca preduzima radnje za otkrivanje i identifikaciju protivzakonito stečene imovine u svrhu utvrđivanja dovoljnog kvantuma sumnje koja ukazuje na imovinsku korist stečenu kriminalnom djelatnošću. Predviđeno je da se dokazi pribavljeni finansijskim izviđajem mogu koristiti u krivičnim postupku. U skladu sa članom 11 citiranog akta finansijska istraga se pokreće naredbom državnog tužioca ukoliko su kumulativno ispunjena dva uslova. Prvi je postojanje osnova sumnje da je imovina stečena kriminalnom djelatnošću, a drugi da postoji osnovana sumnja da je izvršeno jedno ili više krivičnih djela za koja se finansijska istraga može pokrenuti. Ova vrsta istrage treba da prikupi podatke o imovini, prihodima i troškovima života imaoca radi donošenja zahtjeva za trajno oduzimanje imovine, pri čemu se posebna pažnja poklanja odnosu između prihoda i imovine imaoca, odnosno podacima i dokazima o imovini koja je prenesena na treće osobe ili je prešla na pravnog sljedbenika. Relevantan je i način sticanja i prenošenja imovine. Obaveza je kreditne ili finansijske instutucije da državnom tužiocu dostavi podatke potrebne za otkrivanje imovinske koristi koja je stečena protivpravno. Za potrebe finansijske istrage državni tužilac formira finansijski istražni tim koji ima obavezu da sačini izvještaj i uz dokaze dostavi državnom tužiocu. Finansijska istraga se sprovodi u skladu sa ZKP, a podaci na ovaj način prikupljeni su klasifikovani, odnosno obuhvaćeni stepenom tajnosti. Proces identifikovanja pojavnih oblika imovine realizuje se putem operativnog i obavještajnog rada i provjerom preko državnih institucija, da bi se nakon toga najčešće koristile metoda čiste vrijednosti i metoda rashoda u procesu dokazivanja. Propisano je proširenje finansijske istrage ako dokazi ukazuju da je imovinska korist prenesena na lice koje nije obuhvaćeno naredbom za sprovođenje istrage. Finansijska istraga se završava naredbom državnog tužioca kad utvrdi da je slučaj dovoljno razjašnjen za podnošenje zahtjeva za trajno oduzimanje imovinske koristi ili za obustavljanje finansijske istrage, a najkasnije u roku od jedne godine po pravosnažnosti presude. Ukoliko se u toku finansijske istrage utvrdi da ne postoje uslovi za podnošenje zahtjeva za trajno oduzimanje imovine državni tužilac naredbom obustavlja finansijsku istragu.

Smatra se da su najveći izazovi u procesuiranju krivičnih djela sa elementima korupcije obezbjeđenje dokaza koji dovode u vezu imovinu sa kriminalnom djelatnošću. Zbog

42 Simović M. Šikman M. (2018). Krivičnoprocesne radnje u suzbijanju teških oblika kriminaliteta, Revija za kriminologiju i krivično pravo, Vol. 56/1 str.9-33.

43 Zakon o oduzimanju imovine stečene kriminalnom djelatnošću CG, Sl. list CG br. 58/2015,47/2019 i Zakon o izmjenama i dopunama Zakona o oduzimanju imovinske koristi stečene kriminalnom djelatnošću, Sl. list CG br.54/2024.

toga je krucijalno važno utvrditi iznos koristi stečene krivičnim djelom što je oduzimanje zasnovano na vrijednosti. Da bi se u tome uspjelo neophodno je ući u trag imovini praćenjem kretanja novca radi utvrđivanja veze sa krivičnim djelom i lociranja imovine. Kriminalne organizacije koriste različite finansijske transakcije da bi prikrile porijeklo imovine. Zbog toga je neophodno korišćenje visokosofisticiranih istražnih metoda za praćenje imovine i analizu finansijskih podataka radi osiguranja kredibilnih dokaza za potrebe krivičnog postupka. Dokazivanje na osnovu neto vrijednosti bazira se na informacijama koje obuhvataju finansijske transakcije nosilaca kriminalnih aktivnosti koji za kratak vremenski period pribavljaju veliku imovinsku korist sumnjivog porijekla. Primjenom ove tehnike prati se promjena vrijednosti imovine osobe pod istragom. Dokazivanje na osnovu troškova započinje utvrđivanjem početne neto vrijednosti imovine osumnjičenog da bi se u sljedećoj fazi utvrdio izvor viška sredstava.[44] Shodno konceptu izviđaja i istrage informacije uključuju kompletnu imovinu i obaveze, kao i prihode i rashode. Kriminalistički relevantne informacije mogu biti prikupljene iz različitih javnih i drugih izvora od finansijskih institucija do poslovne konkurencije. Jedan od najvažnijih izvora podataka je Izvještaj FATF.

STATISTIČKI PRIKAZ FINANSIJSKIH ISTRAGA U CRNOJ GORI ZA PERIOD OD 2018. DO 2023. GODINE

Nedostatak finansijskih istraga pojačava korupcije, a oduzimanje imovine stečene kriminalnom djelatnošću više pogađa nosioce kriminalnih aktivnosti čak i od kazne zatvora. U tabeli se nalaze podaci o broju pokrenutih finansijskih istraga i istraga okončanih oduzimanjem imovinske koristi stečene kriminalnom djelatnošću za sedmogodišnji perod.

Tabela 1[45]

Godina	*Pokrenute istrage*	*Istrage završene oduzimanjem imovinske koristi stečene kriminalnom djelatnošću*
2018	7	0
2019	15	1
2020	11	0
2021	25	0
2022	12	1
Ukupno	70	2

44 Bošković G. Marinković D.(2010).Metodi finansijske istrage u suzbijanju organizovanog kriminala, Žurnal za kriminalistiku i pravo, KPA , Beograd, str. 87-100.

45 Godišnji izvještaj o radu Državnog tužilaštva i Tužilačkog savjeta za 2019. godinu, Podgorica, 2020. Godišnji izvještaj o radu Državnog tužilaštva i Tužilačkog savjeta za 2020. godinu, Podgorica, 2021. Godišnji izvještaj o radu Državnog tužilaštva i Tužilačkog savjeta za 2021. godinu, Podgorica, 2022. Godišnji izvještaj o radu Državnog tužilaštva i Tužilačkog savjeta za 2022. godinu, Podgorica, 2023.

U posmatranom periodu oduzeta su dva stana površine 193 i 53 m2, zatim 3.063 metra kvadratna zemljišta i 805,00 eura. Pokrenuto je 70 finansijskih istraga, a samo su dvije uspješno okončane. Na loše rezultate u ovoj oblasti pored nespremnosti nadležnih organa utiču i nepostojanje objedinjenog registra bankovnih računa, nedostupnost podataka o stvarnim vlasnicima, neažurirani podaci u katastru, kao i spora i otežana međunarodna saradnja.

ZAKLJUČAK

Krivična djela sa elementima korupcije predstavljaju svojevrsnu „etičku gangrenu" koja direktno ugrožava bazične postulate razvoja društvenog organizma. U suprotstavljanju ovom kriminalnom fenomenu krivično pravno reagovanje države može biti efikasno samo ako je na optimalan način podržano i drugim instrumentima reagovanja javnog i privatnog sektora, zbog čega borba protiv korupcije mora biti multisektorska. Finansijska istraga se s pravom smatra jednom od najvažnijih metoda suprotstavljanja korupciji. Međutim, u ovom slučaju ona je shodno vrlo lošim rezultatima na planu trajnog oduzimanja imovine stečene kriminalnom djelatnošću očigledno najslabija karika u suzbijanju korupcije. Neki od razloga za nezadovoljavajuće stanje u ovoj oblasti su nepostojanje Suda za borbu protiv korupcije i organizovanog kriminaliteta u Crnoj Gori, kao i nedostatak specijalne kriminalističke agencije koja bi igrala ključnu ulogu u obezbjeđenju dokaza. U svim godišnjim izvještajima EK o napretku Crne Gore u pristupanju EU se naglašava veliki problem nedostatka finansijskih istraga. Stoga bi za poboljšanje stanja u ovoj oblasti makar za početak bilo potrebno formiranje Odjeljenja za finansijske istrage u okviru Specijalnog državnog tužilaštva CG.

LITERATURA

1. Bošković G. Marinković D. (2010).Metodi finansijske istrage u suzbijanju organizovanog kriminala, Žurnal za kriminalistiku i pravo,KPA, Beograd.
2. Budimir N. (2020). Pranje novca kao savremeni fenomen-pojam, faze i sprečavanje pranja novca, Naučne publikacije Državnog univerziteta u Novom Pazaru, Vol 3 / 1.
3. Gay L. (2014). Italijansko zakonodavstvo i iskustvo sa ocjenom o konfiskaciji i ponovnoj upotrebi dobara dobijenih organizovanim kriminalom i ostali kriminološki fenomeni, Strani pravni život, (1) 11-30.
4. Godišnji izvještaj o radu Državnog tužilaštva i Tužilačkog savjeta za 2019. godinu, Podgorica, 2020.
5. Godišnji izvještaj o radu Državnog tužilaštva i Tužilačkog savjeta za 2020. godinu, Podgorica, 2021.

6. Godišnji izvještaj o radu Državnog tužilaštva i Tužilačkog savjeta za 2021. godinu, Podgorica, 2022.
7. Godišnji izvještaj o radu Državnog tužilaštva i Tužilačkog savjeta za 2022. godinu, Podgorica, 2023.
8. Gurule J. (1998). The 1988 U.N. Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances –A Ten Year Perspective: Is International Cooperation Merely Illusory? Fordham International Law Journal Vol. 22, Issue 1, Article 2.
9. Directive 2001/97/EC of the European Parliament and the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, Official Journal,L 244, 28 January 2001.
10. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.
11. Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 .
12. Zakon o potvrđivanju Krivičnopravne konvencije o korupciji, Sl. list SRJ- Međunarodni ugovori, br. 2/2022 i 18/2005.
13. Zakon o ratifikaciji konvencije UN protiv nezakonitog prometa opojnih droga i psihotropnih supstanci, Sl. list SRJ-Međunarodni ugovori, br. 14/90.
14. Zakon o potvrđivanju Konvencije o pranju, traženju, zapleni i konfiskaciji prihoda stečenih kriminalom, "Sl.list SRJ-Međunarodni ugovori", br.7/2002; 18/2005.
15. Zakon o oduzimanju imovine stečene kriminalnom djelatnošću CG, Sl. list CG br. 58/2015,47/2019 i Zakon o izmjenama i dopunama Zakona o oduzimanju imovinske koristi stečene kriminalnom djelatnošću, Sl. list CG br.54/2024.
16. Zakon o sprječavanju korupcije, Službeni list Crne Gore, br. 53/2014.
17. Iljkić D.(2015). Pranje novca u domaćem i stranom zakonodavstvu, Finansije i pravo, Vol.3, No.1.
18. Jergović-Katušić S. (2007). Pranje novca (pojam, karakteristike, pravna regulativa i pragmatični problemi), Hrvatski ljetopis za kazneno pravo i praksu, 1/2007.
19. Jovanović A. (2022). Suzbijanje pranja novca i finansiranja terorizma u crnogorskom i evropskom krivičnom zakonodavstvu i praksi, Podgorica.
20. Jovašević D. (2017). Krivično pravo-Posebni deo, Dosije studio, Beograd.
21. Konvencija UN protiv korupcije Sl.list SCG-Međunarodni ugovori, br. 12/2005.
22. Konvencije UN protiv transnacionalnog organizovanog kriminaliteta, Sl. list SRJ, br. 6/21.
23. Krivični zakonik RCG, Sl. list RCG, 70/23 i Službeni list CG br. 40/2008..110/2023.
24. Kumar V.A. (2012). Money Laundering: Concept, Significance and its Impact, European Journal of Business and Menagement, Vol. 4, No. 2.
25. Lazarević LJ. Vučković B. Vučković V. (2004). Komentar Krivičnog zakonika

Crne Gore, Cetinje.
26. Lajić O. (2011). Institut oduzimanja imovinske koristi stečene krivičnim delom, Pravni fakultet Univerziteta u Novom Sadu, Novi Sad, str. 97.
27. Lukić T. (2009).Oduzimanje imovine stečene krivičnim delima, Zbornik Pravnog fakulteta u Novom Sadu, 2/2009.
28. Mitsilegas V. (2003). Money Laundering Counter-measures in the European Union: A New Paradigm of Security Governance Versus Fundamental Legal principles, Hague, Kluwer Law International.
29. Naylor, R.T. (1999). A critique of follow-the money methods in crime control policy. Crime, Law and Social Change, Springer, Vol.32 p-1-58.
30. Petrović Mrvić N. (2015), Krivično pravo posebni deo, Službeni glasnik, Beograd.
31. Rakočević V. (2010). Krivična djela sa elementima korupcije, Podgorica.
32. Rička Ž.(2011). Uloga računovođa u sprečavanju pranja novca, Reviconov zbornik (Međunarodni simpozijum ubrzane reforme u funkciji održivog razvoja, 303-317.
33. Simović M. Šikman M. (2018). Krivičnoprocesne radnje u suzbijanju teških oblika kriminaliteta, Revija za kriminologiju i krivično pravo, Vol. 56/1 str.9-33.
34. Simović M, Šikman M. (2017). Krivičnopravno reagovanje na teške oblike kriminaliteta, Banja Luka: Pravni fakultet Univerziteta u Banjoj Luci.
35. Stojanović Z. Delić N. (2015). Krivično pravo-posebni deo, Pravna knjiga, Beograd.
36. Schneider F.G, Niederlander U. (2008). Money Laundering: Some Facts, European Journal of Law and Economics, 26(3)387-404. DOI:10.1007/s10657-008-9070-x.
37. Carlson J. (2010). Suprotstavljanje mitu i korupciji, Zagreb: Oksimoron,d.o.o.
38. Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, (1991) OJ L 166/77.
39. Crumbley, L., Heitger, L.,Stivenson, S. (2007). Forensic and Investigative Accounting. Chicago:CCHBusiness Valuation Guide.

UDK 343.61: 343.98.06(497.16)

RASPODJELA VRSTA MOTIVA KOD KD UBISTVA U CRNOJ GORI I ZNAČAJ DNK ANALIZA

DISTRIBUTION OF TYPES OF MOTIVES IN THE CRIMINAL OFFENCE OF MURDER IN MONTENEGRO AND THE IMPORTANCE OF DNA ANALYSIS

Dr Jelena Jovanović
Forenzički centar Crne Gore
e-mail: jelena.jovanovic@policija.me

Apstarkt

U skorijoj istoriji se traga za alatkom koja bi mogla razriješavati krivična djela ubistva, nešto kao „srebreni metak", odnosno tehnika koja može apsolutno identifikovati izvršioca krivičnog djela iz materijalnih tragova ostavljenih na mjestu krivičnog djela a koja će omogućiti nadzor osumnjičenih. DNK analiza je potencijalno jedna od tih tehnika. Interesovanje pravne nauke, sudija, advokata i tužilaca je ogromno, bitno je približiti značaj DNK vještačenja. Pravna teorija zahtijeva sigurnost, dok nauka dopušta sumnju. Motivi predstavljaju odgovor na pitanje zašto je došlo do nekog krivičnog djela. Najčešći motivi krivičnih djela ubistva u ovoj studiji su razvrstani u dvije kategorije: kriminalni motiv i interpersonalni (mržnja, psihopatološki, porodični, ljubomora, itd.). Na osnovu dostupne naučne i stručne literature i rezultata ovog istraživanja može se zaključiti da se motivi mogu razvrstati u odnosu na poznate i nepoznate izvršioce. Utvrđena raspodjela vrste motiva je očekivana. Izdvajanjem kriminalnog motiva od ukupnog broja ubistava, obu-

hvaćenih ovim radom 29,1% je s motivom pripadnosti kriminalu. Statistički značajnu razliku uočavamo kod nepoznatih izvršilaca i poznatih izvršilaca u motivima mržnje, psihopatoloških i ljubomore. Sve tri ove skupine motiva možemo stoga grupisati u interpersonalne motive. Interpersonalni motivi su slabije zastupljeniji kod nepoznatih izvršilaca.
Ključne riječi: *mjesto zločina, motiv, DNK, dokazi, ubistvo*

Abstract

In recent history, there has been a search for a tool that could solve murder crimes, something like a "silver bullet", that is, a technique that can absolutely identify the perpetrator of the crime from physical evidence left at the scene of the crime. Also, this tool could enable the surveillance of criminals. DNA analysis is potentially one of these techniques. The interest of jurisprudesce, judges, lawyers and prosecutors is huge, it is important to approximate the importance of DNA expertice. Legal theory requires certainty, while science allows doubt. Motives represent the answer to the question of why a criminal offense occurred. The most common motives for criminal acts of murder in this paper are classified into two categories: criminal motive and interpersonal (hate, psychopathological, family, jealousy, etc.). By consulting a large number of literature, sources, as well as the data obtained in this work, it can be concluded that motives can be classified in relation to known and unknown perpetrators. The established distribution of motive types is expected. By extracting the criminal motive from the total number of murders covered by this work, 29.1% are with the motive of belonging to crime. We observe a statistically significant difference in the motives of hatred, psychopathology and jealousy among unknown perpetrators and known perpetrators. All three of these groups of motives can therefore be grouped into interpersonal motives. Interpersonal motives are less prevalent in unknown perpetrators.
Keywords: *crime scene, motive, DNA, evidence, murder.*

UVOD

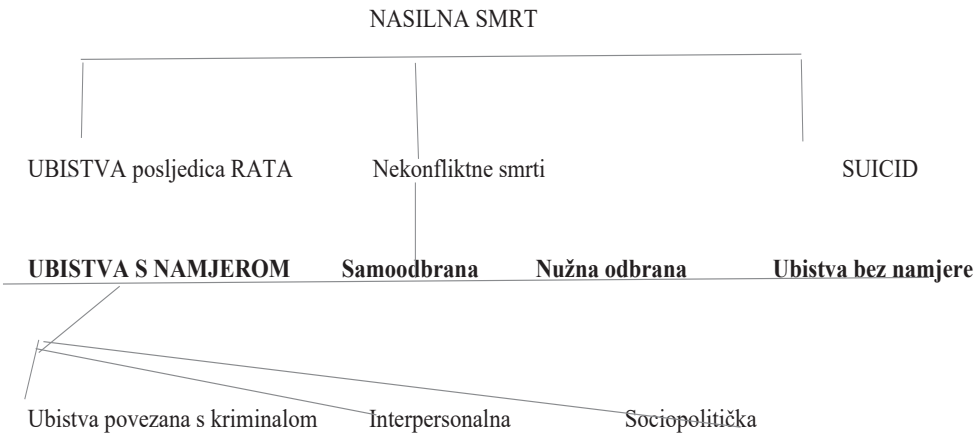
U skorijoj istoriji se traga za alatkom koja bi mogla razriješavati krivična djela ubistva, nešto kao „srebreni metak", odnosno tehnika koja može apsolutno identifikovati izvršioca krivičnog djela iz materijalnih tragova ostavljenih na mjestu krivičnog djela, a takođe bi mogao omogućiti nadzor osumnjičenih. Može se postaviti pitanje da li je DNK analiza ta tehnika. Forenzička izrada DNK profila nosi sa sobom najmanje dva političko-etička problema, jedan povezan s individualnim slobodama (tjelesni integritet), a drugi povezan s više zakonski principom (presumpcija nevinosti, teret

dokazivanja) (Toom, 2012). Inovacije s forenzičkim DNK analizama i bazama podataka su uveliko doprinijele otkrivanju i osuđivanju osumnjičenih za krivična djela, a samim tim i prihvatanju naučnog DNK dokaza od organa za provođenje pravde. Proporcionalnost obično se usvaja razmatranjem „razumnosti" koju sud treba postići; odnosno prosuđivati odgovarajuću ravnotežu između pojedinačnog prava i kolektivnog ili društvenog prava. Ravnoteža između individualnog i kolektivog dobra kao što je to vrhovni sudac i donio u presudi"Minnesot v. Carter" jeste nešto čega se treba pridržavati prilkom upotrebe DNK analiza[1].

U svim periodima društvenog razvoja postojala je potreba za zaštitom života i tjelesnog integriteta čovjeka. Osnovne ljudske vrijednosti predstavljaju život i ljudski integritet (Ivanović i Ivanović, 2013). Opšti, zajednički interes društva pored individualnog interesa za očuvanje života i ljudskog integriteta. Stoga svaki napad na život i ljudski integritet zahtjeva reakciju društva. Ubistva predstavljaju povrede najvećeg ljudskog dobra. „Krivična djela protiv života i tijela prema zaštitnom objektu mogu se podijeliti na: 1. djela kojim se štiti život i 2. djela kojim se štiti tjelesni integritet" (Korajlić, 2012, str. 537). Ubistvo u širem smislu podrazumijeva uništenje života, s aspekta krivičnog prava podrazumijeva se potivpravno lišenje života nekom ljudskom radnjom (Korajlić, 2012).

U izvještaju Global Study of Homicide, United office on Drugs and Crime (UNODC) za 2019. godinu, podjele ubistava su prikazane u ilustraciji 1.

Ilustracija 1.



1 Neki pravnici i eksperti primjećuje cirkularnost definicije Četvrtog amandmana "razumnost" vidjeti e.g., Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring). Međutim, takve kritike još nisu natjerale Sud da preispita svoj test, osim možda za usku kategoriju interijera domova, za koju je Sud utvrdio gotovo automatski razumno očekivanje privatnosti na temelju privatnosti koja ima "korijene" duboko u običajnom pravu." Vidi Kyllo protiv Sjedinjenih Država, 533 U.S. 27, 34 (2001).

Global Study of Homicide (UNODC, 2019) definiše ubistva s namjerom prema Internacionalnoj klasifikaciji ubistva za statističku svrhu (ICCS)[2], i definicija glasi: „Nezakonska smrt je prouzrokovana od strane druge osobe sa posledicom smrti ili teških povreda." Istim izvještajem se određuju tri bitna elementa za definisanje ubistva s namjerom, a to su: ubistvo od druge osobe, namjera izvršioca da prouzrokuje smrt ili ozbiljne tjelesne povrede i nezakonito ubijanje (Global study of Homicide, 2019). Definicija ubistva u engleskom Law Dictionary (2006) glasi: „Protivpravno ubijanje ljudskog bića, a da smrt nastupi u roku od godinu dana."

DNK analize su zasnovana na tehnikama forenzičke DNK analize, na tehnikama molekularne biologije, te uključuju izolaciju molekula DNK, reakciju lanca polimeraze (PCR), kapilarnu elektroforezu i populaciono genetički model zasnovan na principima i zakonima nasljeđivanja po Mendelu i Hardy-Weinbergovoj ravnoteži. Značaj DNK analiza za dokazivanje krivičnih djela ubistava jeste neminovan, a ukazivanje na taj značaj zahtijeva ozbiljan pristup. Većina javnosti u Crnoj Gori DNK vještačenja povezuje sa CSI televizijskim serijama (CSI-efekat), dok se savremeni sudski postupci s obiljem biološkog materijala ne mogu zamisliti bez DNK vještačenja. Interesovanje pravne nauke, sudija, advokata i tužilaca je ogromno, bitno je približiti značaj DNK vještačenja. Pravna teorija zahtijeva sigurnost, dok nauka dopušta sumnju. Također, obični građani će se osjećati sigurnije kada znaju za doprinos DNK dokaza za rješavanje krivičnih djela.

U ovom radu akcenat će biti na motivima vezanim za krivična djela ubistva sa poznatim i nepoznatim izvršiocima. Povlačenje paralele između rasvjetljavanja krivičnog djela ubistva s poznatim izvršiocem odnosno nepoznatim izvršiocem, uz pomoć DNK dokaza a uvezano sa motivima krivičnih djela ubistava. Postoji li razlika u raspodjeli motiva kod krivičnog djela Ubistva po poznatom inepoznatom izvršiocu.

Predmet istraživanja jesu kriminalistički i forenzički aspekti ubistva, raspodjela motiva kod poznatih inepoznatih izvršilaca krivičnog djela Ubistva. Kriminalistički i forenzički aspekti ubistva se mogu analizirati pomoću DNK dokaza.

Cilj istraživanja

DNK dokaz je neoboriv dokaz koji omogućava rasvjetljavanje krivičnog djela. Pravilno dopremanje predmeta, odnosno izuzetih tragova s predmeta do laboratorije, što vjerniji prikaz lica mjesta u laboratoriji, prvi je i najbitniji korak. Opravdano je postaviti pitanje relevantnosti DNK dokaza, a zatim i da li postoji neki sled motiva kod poznatih i nepoznatih izvršilaca krvičnih djela ubistava.

2 UNODC, International Classification of Crime for Statistical Purposes (ICCS): Version 1.0 (Vienna, 2015), s. 33

Cilj istraživanja jeste raspodejla vrste motiva u krivičnim djelima ubistava razmatranim u Crnoj Gori u odnosu na nepoznatog i poznatog izvršioca. Različito ponašanje poznatih i nepoznatih izvršilaa ubistava i odgovor na pitanje zašto se dogodilo neko krivično djelo. Motiv predstavlja odovor na pitanje zašto je došlo do nekog krivičnog dela.

Hipoteza

Ponašanje i karakteristike poznatih i nepoznatih izvršilaca kod krivičnog djela ubistva, se razlikuju. Krivična djela ubistva po poznatom izvršiocu uspješnije se rješavaju kada postoje svjedoci na mjestu događaja koji bi mogli identifikovati žrtvu, osumnjičenog. Hipoteza koju postavljamo u ovom radu jeste u odnosu na motiv kod krivičnih djela ubistava.

• 1. Raspodjela vrste motiva krivičnog djela ubistva se razlikuje kod poznatih i nepoznatih izvršilaca.

DNK analiza sa pravnog i naučnog aspekta

Veoma je raširena ideja da DNK profili mogu rasvijetliti krivična djela na nivou cijele Evropske unije. Jako je važno da se definišu pravni standardi, s jedne strane za prikupljanje i analizu DNK dokaza, a s druge da razmjena DNK profila između zemalja bude definisana. Prikupljanje i čuvanje bioloških uzoraka izvodi se u skladu sa zakonima određene zemlje. Također, potrebno je definisanje kada i od koga i pod kojim uslovima mogu da se izuzmu uzorci za DNK analizu. Nacionalna legislativa zemalja oko prikupljanja i skladištenja uzoraka za DNK analizu se razlikuje (Belfiore, 2011). DNK tehnike profiliranja su prepoznate uglavnom zajedničkim standardima.

U skorijoj istoriji preduzeto je nekoliko projekata usmjerenih na standardizaciju tehnika profiliranja DNK, prvo izvan pravnog okvira EU[3], a zatim i unutar njega. Krajem osamdesetih godina, *Europe DNA profiling Group* EDNAP[4], Evropska grupa za profiliranje DNK, uspostavila je postupke koji se temelje na zajedničkim standardima u metodologiji i nomenklaturi, kako bi se olakšala razmjena podataka o DNK u Evropi. Evropska grupa DNK profiliranja *Europe DNA profiling Group* (EDNAP) zahtijeva standardizaciju Forenzičkog rada svih DNK laboratorija. Standardizacija se tiče tehničkog i proceduralnog standarda. Tehnički standard obuhvata genetičku nomenklaturu lokusa, statističku interpretaciju i evaluaciju dokaza. Proceduralni

3 Pravni okvir EU nadležnosti u oblasti DNK analiza obuhvata Rezoluciju Vijeća Evrope R(92)1992.

4 U skladu s informacijama dostupnim na internetu EDNAP, www.isfg.org/EDNAP, ukupno 17 zemalja članica grupe. Godine 1991. EDNAP je zvanično postao radna grupa Internacionalnog društva forenzičkih hemogenetičara, današnji ISFG - Internacionalno udruženje forenzičkih genetičara, međunarodna organizacija koja promoviše analiziranje genetskih markera za potrebe forenzike.

standard se odnosi na akreditaciju laboratorija, rad laboratorija, licenciranje osoblja i učestvovanje u profišensi[5] testovima.

DNK profil predstavlja uređeni numerički niz koji predstavlja skup identifikacionih karakteristika nekodirajućeg dijela DNK uzorka dobijen analizom DNK markera (Zakon o izmjenama i dopunama Zakona o DNK registru, Crne Gore, 2014). DNK marker predstavlja genetski lokus u molekulu i predstavlja određeni dio molekula DNK (Zakon o izmjenama i dopunama Zakona o DNK registru, 2014). Crna Gora ima uređenu legislativu, odnosno Zakon o DNK registru još od 2011. godine. Unos, odnosno arhiviranje podataka u Crnoj Gori zavisi od dužine kazne. Zakonom o izmjenama i dopunama Zakona o DNK registru su napravljene izmjene koje su u skladu s Prumskom regulativom, sa ESS, odnosno Evropskim standardnim setom lokusa, ukupno 16 genskih lokusa, i u skladu s evropskim rezolucijama. S obzirom na osjetljivost podataka i potrebu njihovog zakonitog korištenja i obrade prema svrsi koja je određena, legislativa mora biti uređena po EU legislativi. DNK baze podataka značajno obogaćuju policijsku evidenciju o krivičnim djelima, mogućim povezivanjima i čak predstavljaju značajniju alatku od policijskih baza podataka o izvršiocima. Postojanje baza podataka omogućava lakše identitikovanje povratnika nekih krivičnih djela, zatim povezivanja različitih lica sa jednim licem mjesta događaja, kao i povezivanje više lica mjesta sa jednim licem. Staley (2005, str. 38.) navodi: „Baza podataka koja uključuje ljude koji će najvjerojatnije ponoviti prekršaj, olakšava njihovo identifikovanje ako opet učine prekršaj. To bi zahtijevala NDNAD (Nacionalna baza podataka DNA Ujedinjenog Kraljevstva) kako bi se odrazilo bolje na razumijevanje uzoraka počinitelja krvičnog djela i vjerovatnoću ponovnog počinjenja krivičnog djela ". Kada poredimo navedenu tvrdnju sa zakonskim rješenjima u Crnoj Gori, jasno je da se ne radi o prekršajima već o krivičnim djelima kao najtežim oblicima protivpravnog ponašanja[6].

KRIVIČNO DJELO UBISTVO U REPUBLICI CRNOJ GORI

Prema Krivičnom zakonu Crne Gore (2009), kvalifikovano je: obično ubistvo[7], teško ubistvo[8], lakši slučaj kao ubistvo na mah[9], ubistvo iz nehata[10] i ubistvo djeteta pri poro-

5 Proficiency test GEDNAP (German DNA Profiling), organizovan od „Stain Commission", koji je oformilo njemačko udruženje instituta za sudsku medicinu 1980. godine. GEDNAP test je međunarodno priznat proficiency test čijim se uspješnim provođenjem verifikuje ispravnost rada forenzičkih DNK laboratorija.

6 Krivični zakonik CG "Sl. list RCG", br. 70/2003, 13/2004 - ispr. i 47/2006 i "Sl. list CG", br. 40/2008, 25/2010, 32/2011, 64/2011)

7 Odredba čl. 143, obično ubistvo, Krivični zakonik CG („Službeni list Crne Gore", br. 70/2003, 13/2004 - ispr. i 47/2006 i „Sl. list CG", br. 40/2008, 25/2010, 32/2011, 64/2011).

8 Odredba čl. 144. Krivičnog zakonika CG („Službeni list Crne Gore", br. 70/2003, 13/2004 - ispr. i 47/2006 i „Sl. list CG", br. 40/2008, 25/2010, 32/2011, 64/2011).

9 Odredba član 145. Krivičnog zakonika CG („Službeni list Crne Gore", br. 70/2003, 13/2004 - ispr. i 47/2006 i „Sl. list CG", br. 40/2008, 25/2010, 32/2011, 64/2011).

10 Član 148. Krivičnog zakonika CG („Službeni list Crne Gore", br. 70/2003, 13/2004 - ispr. i 47/2006 i „Sl. list CG", br. 40/2008, 25/2010, 32/2011, 64/2011).

đaju[11] (Krivični zakonik CG). Krivični zakon Federacije Bosne i Hercegovine propisuje Krivično Djelo ubistva[12], propisuje zatim ubistvo na mah[13], prouzrokovanje smrti iz nehata[14], zatim odredbom Krivičnog zakona Federacije Bosne i Hercegovine, čedomorstvo[15], učestvovanje u samoubistvu[16], protivpravni prekid trudnoće[17]. Uočavaju se razlike u nepostojanju krivično-pravne kvalifikacije teško ubistvo u Krivičnom zakonu Federacije Bosne i Hercegovine. Također, postojanja kvalifikacije protivpravni prekid trudnoće i učestvovanje u samoubistvu u Krivičnom zakonu Federacije Bosne i Hercegovine. Kazneni zakon Republike Hrvatske propisuje kvalifikaciju ubistva[18] i teškog ubistva[19], usmrćenje[20], prouzrokovanje smrti iz nehata[21], sudjelovanje u samoubistvu[22], protivpravni prekid trudnoće[23]. Kada se uporede krivičnopravne kvalifikacije krivičnog djela ubistva u Kaznenom zakonu Hrvatske i Krivičnom zakoniku Crne Gore i Federacije Bosne i Hercegovine, vidi se njihovu sličnost i s jednim i s drugim, i njihov presjek u krivičnopravnim rješenjima Republike Hrvatske. Naime, u kaznenom zakonu Hrvatske postoji kvalifikacija ubistva i teškog ubistva kao u Krivičnom zakoniku Crne Gore, a postoji i protivpravni prekid trudnoće i učestvovanje u samoubistvu kao kod Krivičnog zakona Federacije Bosne i Hercegovine. Krivični zakonik Republike Srbije propisuje ubistvo[24], teško ubistvo[25], ubistvo na mah[26], ubistvo deteta pri porođaju[27], lišenje života

11 Član 146. Krivičnog zakonika CG („Službeni list Crne Gore", br. 70/2003, 13/2004 - ispr. i 47/2006 i „Sl. list CG", br. 40/2008, 25/2010, 32/2011, 64/2011).
12 Odredba člana 166. Krivičnog zakona Federacije Bosne i Hercegovine („Službene novine FBiH", br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017)
13 Odredba člana 167. Krivičnog zakona Federacije Bosne i Hercegovine („Službene novine FBiH", br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017)
14 Odredba člana 168. Krivičnog zakona Federacije Bosne i Hercegovine („Službene novine FBiH", br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017)
15 Odredba člana 169. Krivičnog zakona Federacije Bosne i Hercegovine („Službene novine FBiH", br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017)
16 Odredba člana 170. Krivičnog zakona Federacije Bosne i Hercegovine („Službene novine FBiH", br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017)
17 Odredba člana 171 Krivičnog zakona Federacije Bosne i Hercegovine („Službene novine FBiH", br. 36/2003, 21/2004 - ispr., 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016 i 75/2017)
18 Odredba člana 110. Kaznenog zakonika Republike Hrvatske (Nacionalne novine, 25/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22)
19 Odredba člana 111. Kaznenog zakonika Republike Hrvatske (Nacionalne novine, 25/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22)
20 Odredba člana 112. Kaznenog zakonika Republike Hrvatske (Nacionalne novine, 25/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22)
21 Odredba člana 113. Kaznenog zakonika Republike Hrvatske (Nacionalne novine, 25/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22)
22 Odredba člana 114. Kaznenog zakonika Republike Hrvatske (Nacionalne novine, 25/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22)
23 Odredba člana 115. Kaznenog zakonika Republike Hrvatske (Nacionalne novine, 25/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22)
24 Odredba člana 113. Krivičnog zakonika („Službeni glasnik Republike Srbije", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019)
25 Odredba člana 114. Krivičnog zakonika („Službeni glasnik Republike Srbije", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019).
26 Odredba člana 115. Krivičnog zakonika („Službeni glasnik Republike Srbije", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019).
27 Odredba člana 116. Krivičnog zakonika („Službeni glasnik Republike Srbije", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019).

iz samilosti[28], nehatno lišenje života[29], navođenje na samoubistvo[30] i nedozvoljen prekid trudnoće[31]. Uočavamo veliku sličnost između krivično-pravnih kvalifikacija krivičnih djela ubistva u Kaznenom zakonu Hrvatske i Krivičnom zakoniku Republike Srbije. Način izvršenja ubistva su sve radnje koje izvršilac preduzima da bi oduzeo nečiji život (Korajlić, 2012). Posljedica krivičnog djela ubistva jeste smrt neke osobe, ako je smrt izvedena na nedozvoljen način. Interes društvene zajednice jeste da se ispita način smrti. Smrt jednog lica treba da bude prouzrokovana radnjom drugog lica i da postoji uzročna veza između te dvije radnje (Korajlić, 2012). Pored krivično-pravne kvalifikacije krivičnog djela ubistva, s aspekta kriminalistike, ubistva mogu se kvalifikovati prema različitim kriterijima. Prema sredstvima izvršenja, mogu se podijeliti na ubistva izvršena (Ivanović i sur., 2013):

a. fizičkim sredstvima i
b. psihičkim sredstvima.

Sredstva izvršenja su razna i mogu biti najčešće: vatreno oružje, hladno oružje, ručne bombe, eksplozivne naprave, razni alati, hemijske otrovne materije, saobraćajno sredstvo, strangulacijska sredstva, drugi predmet, električna energija i sl. (Korajlić, 2012).

Podjela na profesionalna i neprofesionalna ubistva je naročito značajna. Aleksić, Škulić i Žarković (2004) navode karakteristike profesionalno izvedenih ubistava:

a. visok stepen organizovanosti,
b. ubistvo obično vrši više učesnika, uz prethodno obezbijeđenu logističku podršku, prije i tokom izvršenja te nakon izvršenja krivičnog djela,
c. djelo se vrši radi ostvarivanja određenih ranije isplaniranih ciljeva, ponekad se određeni elementi izvršenja uvježbavaju, a postoji i formiranje timova za izvršenje djela,
d. ubistvo izvršavaju oni koji to čine za određenu naknadu, materijalnu ili drugu korist,
e. žrtva određenog ubistva je obično neko istaknuto lice, bilo da se radi o licu iz kriminalne sredine ili je to važan pripadnik državnih organa,
f. ubistvo se vrši uz posebne mjere opreza, ali i vještine, kao i specifične obučenosti izvršilaca koji predstavljaju jedan obrazac realizacije ovakvih krivičnih djela,
g. zatim druga upotrijebljena sredstva kao što su automobili, noviji i skuplji modeli, obično prethodno ukradeni i s lažnim tablicama, koji efikasno uklanjaju ili skrivaju paljenjem.

28 Odredba člana 117. Krivičnog zakonika („Službeni glasnik Republike Srbije", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019).

29 Odredba člana 118. Krivičnog zakonika („Službeni glasnik Republike Srbije", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019).

30 Odredba člana 119. Krivičnog zakonika („Službeni glasnik Republike Srbije", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019).

31 Odredba člana 120. Krivičnog zakonika („Službeni glasnik Republike Srbije", br. 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019).

Koriste se i druga sredstva, kao naprimjer mobilni telefoni za jednokratnu upotrebu i dr.

Različiti su motivi za izvršavanje krivičnog djela ubistva. Ivanović et al. (2013) navode različite motive krivičnog djela ubistva: osveta, mržnja, ljubomora, sujevjerje, prikrivanje drugih krivičnih djela, patološka sujeta, motivi duševno bolesnih osoba, politički i ekonomski motivi i dr.

Najčešći trag žrtve na licu mjesta jeste trag krvi. Također, mogu se naći i drugi tragovi biološkog porijekla, kao i daktiloskopski tragovi.

U bližoj prošlosti podaci za krivična djela ubistva su bili po poznatom izvršiocu. Bolje su se rješavala kada postoje svjedoci na mjestu događaja koji bi mogli identifikovati žrtvu, osumnjičenog. Ubistva su se dosta shvatala kao zločin iz strasti, gdje su bili uključeni članovi porodice ili bliski poznanici. Takve društvene okolnosti su olakšavale identifikaciju navodnih izvršilaca. U novije vrijeme ubistva su češća između stranaca, odnosno po nepoznatom izvršiocu. Krivično djelo ubistvo po poznatom izvršiocu je kada postoje svjedoci koji su izvršioca vidjeli na licu mjesta ili ga oštećeni poznaje ili su u pitanju rođačke veze, bez obzira na to je li izvršilac lišen slobode ili ne. Istragom se kasnije otkriva izvršilac ako je krivično djelo ubistvo u početku bilo po nepoznatom. Ako se ne otkrije istragom, krivično djelo ostaje neriješeno, a izvršilac nepoznat.

U ovom radu razmatrat će se krivična djela ubistva u odnosu na momenat izvršenja krivičnog djela, tj. je li izvršilac bio poznat u momentu izvršenja krivičnog djela. S aspekta forenzike, izvršilac je nepoznat sve dok se tragovima s mjesta izvršenja ne dokaže suprotno.

Za uspješno otkrivanje izvršilaca krivičnih djela ubistava bitno je načelo brzine i operativnosti, koje se ogleda u hitnom preuzimanju operativno-taktičkih radnji i brzom izlasku na lice mjesta radi obezbjeđenja relevantnih materijalnih tragova (Korajlić, 2012).

Implementacija naučnih metoda u utvrđivanju činjenica od značaja za potrebe kriminalistike i pravnih postupaka, više se ne može zamisliti bez uključivanja vještačenja bioloških tragova analizom molekula DNK. Jedna od najznačajnijih alatki u pronalasku i identifikovanju izvršilaca uz pomoć DNK analiza jeste CODIS (Combined DNA Indexing System) sistem odnosno DNK registar. Uvijek se vrši poređenje sa DNK profilima osumnjičenih lica, a ako su osumnjičena lica nedostupna organu krivičnog gonjenja poređenje se vrši sa bazom DNK registra.

U ovom radu ukazaćemo na postojanje jednog slijeda motiva, prikazivanjem uz pomoć poznatih i nepoznatih uzvršilaca, šire slike u objašnjavanju krivičnih djela

ubistava u Crnoj Gori. Poseban akcenat će biti stavljen na analizu DNK profila, ukazujući na značaj korišćenja DNK analiza u problemima krivičnih djela ubistava kod poznatih i nepoznatih izvršilaca. Etnografski i zvanični podaci su korišćeni iz serijala "Put osvete" autorke Svetlane Đokić u produkciji TV Vijesti, projekat koji je podržan i od strane ambasade Sjedinjenih Američkih država (Put osvete, 2020).

Početkom 2015 godine, jedinstveni Kotorski klan se rascjepljuje na dva suprostavljena klana Škaljarski i Kavački klan. Razlog njihovog rascjepljenja jeste podjela dobiti, koja je započela na teritoriji Zapadne Evrope (Put osvete, 2020; Zapadni Balkan: Meka organizovanog kriminala, DW, 2019). Cijela serija ubistava i postavljanja eksplozivnih naprava započinje od tada u Crnoj Gori. Kriminalni klanovi su bili dosta brži od policije, koja je prilično kasnila i zbog Krivičnog zakonika Crne Gore[32] koji nije dozvoljavao mjere tajnog nadzora do 2004. godine. Ekspanzija prodaje kokaina nastaje tih godine. Kriminalni klanovi su distribuirali kokain kontenjerima, prema operativnim podacima. Modus operandi karakterističan za Crnu Goru jesu mornari koji su korišćeni za distribuciju kokaina (Put osvete, 2020). U tekstu DW dio izvještaja Civilne observatorije za borbu protiv organizovanog kriminala u jugoistočnoj Evropi koja je dio Globalne inicijative protiv transnacionalno organizovanog kriminala (Zapadni Balkan: Meka organizovanog kriminala, DW, 2019, Global initiative new, 2019). U Valensiji u Španiji, koja je osnovna baza za distribuciju kokaina, nestaje 200 kg kokaina G. R. u njegovom "štek stanu"[33]. Glavni okidač za razbijanje do tada jedinstvenog Kotorskog klana na dva klana jeste upravo nestanak tog kokaina. Kum G.R. i najbliži saradnik G.Đ. biva ranjen u Španiji (Put osvete, 2020). Izvori iz medija (Britanci traže istragu protiv dva klana, 2017) navode da Italijanska GDF i Američka DEA predpostavljaju da Crnogorske kriminalne organizacije kupuju kokain od revolucionarnih oružanih snaga Kolumbije FARK. Pojačavaju se kontrole nadležnih službi nad brodovima u Crnoj Gori, i u drugim zemljama koje predstavljaju usputne stanice u krijumčarenju kokaina. Isti izvor navodi i podatak da je crnogorski klan povezan s kalabrijskom N`drangetom, koja se smatra najopasnijom kriminalnom organizacijom u Evropi (Britanci traže istragu protiv dva klana, 2017).

REZULTATI

Pravni osnov za procjenu broja stanovništva Crne Gore regulisan je Zakonom o zvaničnoj statistici i sistemu zvanične statistike[34]. Prema podacima Monstata (Statistički

32 (Zakonik o krivičnom postupku "Sl. list Crne Gore", br. 057/09 od 18.08.2009, 049/10 od 13.08.2010, 047/14 od 07.11.2014, 002/15 od 16.01.2015, 035/15 od 07.07.2015, 058/15 od 09.10.2015)

33 Štek stan se koristi kao ulični govor -sleng koji koriste kriminalne grupe, a predstavlja stan odnosno prostor za stanovanje osmišljen za skrivanje ljudi ili predmeta. Vrlo često mijenjanje stanova bez opažanja, a nije isključeno da kriminalna grupa iznajmi nekoliko takvih stanova, pa ih mijenjaju kako ne bi bili uočeni, tako da im se vrlo teško ulazi u trag.

34 Zakon o zvaničnoj statistici i sistemu zvanične statistike („Službeni list Crne Gore", 18/12 i 47/19).

zavod Crne Gore), 1. januara 2022. godine u Crnoj Gori živjela su 618.683 stanovnika. U studiji Grde i Lukovočkića (2019) za države bivše Jugoslavije prikazana je godišnja stopa ubistava za 2017. godinu, te je tako stopa ubistava 2,4 u Crnoj Gori, 1,5 u Sjevernoj Makedoniji, 1,1 u Srbiji i Hrvatskoj, te 0,9 u Sloveniji (Gurda i Lukovčkić, 2019). U izvještaju Global Study of Homicide, prema podacima United Office on Drugs and Crime (UNODC) za 2019. godinu, ukupna stopa ubistava na nivou Crne Gore bila je 2,71 za 2015. godinu, 4,46 za 2016. godinu i 2,37 za 2017. godinu (Global Study on Homicide, 2019).

Krivičnih djela ubistava u Crnoj Gori, prema zvaničnim podacima MUP-a, u 2009. godini bilo je 24, u 2010. godini 15, u 2011. godini 21, u 2012. godini 16, u 2013. godini 9, u 2014. godini 17, u 2015. godini 17 i u 2016. godini 24.

Tabela 1. Krivična djela ubistva prikazana po godinama; prikaz vještačenih u odnosu na ukupan broj

Godine	2009	2010	2011	2012	2013	2014	2015	2016	Ukupno
KD ubistva	24	15	21	16	9	17	17	24	143
Nerazriješena KD ubistva	4	1	2	1	2	2	3	7	22
Ukupno	11	10	18	8	12	10	15	12	96

Tabela 2. Krivična djela ubistva, vještačena u DNK laboratoriji, prikazana po godinama

Godine	2009	2010	2011	2012	2013	2014	2015	2016	Ukupno
KD ubistva po poznatom izvršiocu	5	9	11	7	8	4	8	5	57
KD ubistva po nepoznatom izvršiocu	6(2)	1	7(3)	1	4(1)	6(1)	7 (3)	7 (2)	39
Ukupno	11	10	18	8	12	10	15	12	96

Kada uporedimo tabele 1. i 2, odnosno broj krivičnih djela ubistava registrovan po godinama u kojima se vrši istraživanje, vidimo jedino u 2013. godini manji broj registrovanih krivičnih djela ubistava nego što je vještačeno u DNK laboratoriji, usljed različitih datuma vještačenja početkom i krajem 2013. godine. U svi ostalim godinama, naročito 2009, uočavamo znatnu razliku u broju vještačenih i broju registrovanih ubistava. Krivičnih djela ubistava u Crnoj Gori, prema zvaničnim podacima MUP-a,

jeste: 2009 (N= 24); 2010 (N= 15); 2011(N=21); 2012 (N=16); 2013 (N= 9); 2014 (N=17); 2015 (N=17); 2016 (N=24). Ukupan broj ubistava u Crnoj Gori od 2009. do 2016. godine (N=143). Ukupan broj krivičnih djela ubistava DNK vještačenih u Forenzičkom centru (N=96). Prikazano po godinama, 2009 (N= 11); 2010 (N= 10); 2011 (N=18); 2012 (N=11); 2013(N= 9); 2014 (N=10); 2015 (N=15); 2016 (N=15). Opisna statistika za procenat vještačenih u odnosu na ukupan broj krivičnih djela ubistava iznosi 2009 (45%); 2010 (66%); 2011 (85%); 2012 (68%); 2013 (100%); 2014 (58%); 2015 (88%); 2016 (62%).

Tabela 3. Krivična djela ubistva, vještačena u DNK laboratoriji, prikazana po godinama

Godine	2009	2010	2011	2012	2013	2014	2015	2016	Ukupno
KD ubistva IZVRŠENA	24	15	21	16	9	17	17	24	143
KD ubistva VJEŠTAČENA	11	10	18	8	12	10	15	12	96
PROCENAT %	45	66	85	68	100	58	88	62	96

U prvoj godini DNK vještačenja nisu imala dominantnu ulogu usljed pripremanja DNK laboratorije i osposobljavanja za vještačenje. 2009 godine procenat vještačenja je 45%, što ako uporedimo sa radom Shroeder 2009. godine koji provodi studiju o značaju DNK dokaza za razrješavanje krivičnog djela ubistva u policiji Njujork. Shroeder (2009) govori o korištenju DNK dokaza u istraživanju krivičnog djela ubistva. Naime, u samo 40% slučajeva koji su razmatrani u periodu od 1999. do 2003. godine, DNK dokaz je upotrijebljen. U tih 40% slučajeva dobijena je stopa rasvjetljavanja krivičnog djela ubistva 28%, što je relativno niska stopa. Podaci se slažu sa procentom korišćenja DNK analiza prvih godina u Crnoj Gori (45%). Shroeder objašnjava dobijene rezultate studije: otpor detektiva prema DNK dokazu, troškovi samog DNK dokaza, neophodno znanje iz oblasti DNK analiza. Zaključuje da su detektivi posezali za upotrebom DNK kao dokaza samo u krajnjem slučaju, kada tradicionalne metode istrage zakažu. Ako posmatramo hronološki, od 2009 godine (45%) do 2016 godine (62%), to ukazuje na značaj DNK analiza i porast njihovog korišćenja.

Raspodjela motiva KD ubistva

Motiv predstavlja odgovor na pitanje zašto, kao jedno od zlatnih pitanja kriminalistike (Korajlić, 2012). Svako krivično djelo, osim u nehatu, učinjeno je s nekim motivom. Traženje motiva pri analizi krivičnog djela predstavlja retrospektivan osvrt na učinjeno krivično djelo, odnosno misaonu rekonstrukciju djela (Modly, 1998). Pomoću motiva se i razjašnjava pitanje postojanje umišljaja i nehata, analizom sva-

ke izolovane činjenice kao sastavnog dijela posljedice. Motiv se može smatrati kao podsticaj, povod kao unutrašnja kategorija, a kao spoljašnja kategorija razlog, djeluje na karakter, nagone, osjećaje (Korajlić, 2012). Motivi mogu biti različiti, ekonomske, psihološke prirode. Također mogu biti pospješujući i sprečavajući, altruistički i egoistični. Motivi kod poznatog i nepoznatog izvršioca krivičnog djela se utvrđuju na osnovu rezultata uviđaja (Korajlić, 2012). Motiv je veoma tijesno vezan sa sačinjavanjem profila izvršioca. Motivi za ubistva su uglavnom kategorizovani kao agresija, osveta, mržnja, ljubomora, mentalna bolest, povezanost s novcem, povezanost s bandom, povezanost s drogom, neslaganje, svađe ukućana, ljubavne svađe. Pripisano ubistvima mogu biti kategorizovani kao interpersonalni odnosi, poslovni, kriminalni, poznanstvo. Ubistva s namjerom se dijele na kriminalna, sociopolitička i interpersonalna (Globa study of Homicide, 2019). U poređenju s motivima prikazanim u tabeli 14. vidi se da bi se podjela KD mogla svrstati u tri kategorije: kriminalnu (pripadnost klanovima), interpersonalnu (mržnja, psihopatološki, porodični, ljubomora) i sociopolitičku.

Tabela 4. Prikaz najčešćih motiva kod KD ubistva u odnosu na poznatog i nepoznatog izvršioca

	Koristoljublje	Pripadnost klanovima	Mržnja, fizički sukob	Psihopatološki, porodični	Ljubomora	Majka novorođenče	Nehat
n.i	10	18	4	0	1	0	
p.i	6	10	17	16	10	2	2
Ukupno	16	28	21	16	11	2	2

Najčešći motivi krivičnih djela ubistva u ovoj disertaciji su razvrstani u dvije kategorije: kriminalni motiv i interpersonalni (mržnja, psihopatološki, porodični, ljubomora, itd.). Opisna statistika motiva krivičnih djela ubistva je predstavljena u tabeli 4. Procenat krivičnih djela ubistva s kriminalnim motivom je 15,8% u slučaju poznatog izvršioca i 54,5% u slučaju nepoznatog izvršioca. Na osnovu rezultata $\chi 2$ testa homogenosti (test statistika $\chi 2 = 28.484$, $df = 1$, $p<0.001$), može se zaključiti da se raspodjela vrste motiva krivičnih djela ubistva razlikuje kod poznatih i nepoznatih izvršilaca. Kriminalni motivi su znatno češće zastupljeni kod nepoznatih izvršilaca, odnosno interpersonalni motivi kod poznatih izvršilaca ubistva.

Tabela 5. Opisna statistika vrste motiva KD ubistva

Izvršilac	Kriminalni motivi (%)	Interpersonalni motivi (%)
Poznat	10 (15,8%)	47 (74.6%)
Nepoznat	18 (54.5%)	5 (15.2%)

U odnosu na lice mjesta, varijable su prikazane u tabeli. 6. Procenat zastupljenosti za stan oštećenog iznosi 37,5%. Slična zastupljenost jeste za otvoreni prostor 34,3%. Zastupljenost izvršenja krivičnih djela za automobile i za kafane iznosi isto 9,3%. Značajno manja zastupljenost je za stan osumnjičenog 2%, a ista je i za hotel, kao i zapaljeni automobil i ZIKS (Zavod za izvršenje krivičnih sankcija). Samo je jedan slučaj fabrike kao mjesta izvršenja. U odnosu na lice mjesta, vidimo procentualno podjednaku zastupljenost za stan oštećenog i za otvoreni prostor. Značajno manja zastupljenost jesu kafane, fabrike, stan oštećenog, srednja vrijednost zastupljenosti za automobile i kafane. U tabeli 7. je opisna statistika u odnosu na lice mjesta.

Tabela 6. Prikaz varijabli u odnosu na lice mjesta

	Stan oštećenog	Stan osumnjičenog	Hotel	Otvoreni prostor	Automobil	Kafana	Zapaljen automobil	Fabrika	ZIKS
2009.	7		1	3	**1**				
2010.	5			3		3			
2011.	6	1		6	1	1	1		
2012.	3	1		4	2				
2013.	2		1	5		2		1	
2014.	2			2		2	1		1
2015.	8			4	2	1			
2016.	3			6	3				1
Ukupno	36	2	2	33	9	9	2	1	2

U tabeli 7. je opisna statistika u odnosu na lice mjesta.

Tabela 7. Opisna statistika lica mjesta KD ubistva

Lice mjesta za KD ubistva	Broj (%)
Stan izvršioca	36 (37.5%)
Otvoreno lice mjesta	33 (34.3%)

DISKUSIJA

Najveći broj ubistava razmatranih u ovom radu kao motiv ima pripadnost klanovima. Jedan od ciljeva ovog istraživanja jeste istražiti razliku motiva kod krivičnog djela ubistva čiji je izvršilac poznat i nije poznat. Imajući to u vidu, rezultate dobijene u ovoj studiji detaljnije analiziramo. Broj krivičnih djela ubistava koja ima kriminalni motiv iznosi (N=28 (96)). Izdvajanjem kriminalnog motiva od ukupnog broja ubistava, 96, koja su obuhvaćena ovom studijom, ukupno 28, odnosno 29,1% je s motivom pripadnosti kriminalu. Te rezultate potvrđuje naučna teorija koja kaže da pripadnost kriminalu inače povećava vjerovatnoću da će isti ljudi biti uključeni u ubistva (Dobrin, 2001). Analogno tome, i izdvajanje kriminalnog motiva kod krivičnih djela ubistava s poznatim izvršiocem (N= 10) i (N=18) kod krivičnog djela ubistva s nepoznatim izvršiocem. Procenat KD ubistava s kriminalnim motivom je 15,8% u slučaju poznatog izvršioca i 54,5% u slučaju nepoznatog izvršioca. Statistički rezultati testa homogenosti upućuju da se raspodjela vrste motiva KD ubistva razlikuje kod poznatih i nepoznatih izvršilaca.

Samo u periodu 2015. i 2016. godine u Crnoj Gori, s elementima organizovanog kriminala, bilo je ukupno devet ubistava (Jovanović, 2022). Kriminalni motivi su znatno češće zastupljeni kod nepoznatih izvršilaca. Nosioci organizovanog kriminala u Crnoj Gori su organizovane kriminalne grupe – klanovi. Nazive dobijaju prema dijelu grada koji kontrolišu (Put osvete, 2020). Kriminalni motivi su znatno češće zastupljeni kod nepoznatih izvršilaca. O tačnom broju kriminalnih klanova koji djeluju u Crnoj Gori ne može se sa sigurnošću govoriti. Početkom 2000. godine počinje ekspanzija kokaina u Evropi. Kokain se sve više krijumčari iz zemalja Južne Amerike. U posao su se uključili brojni kriminalci, tako da država ima pune ruke posla. Specijalno državno tužilaštvo Crne Gore radi u pravcu njihovog otkrivanja. Može biti zadovoljno brojem optuženih i brojem osuđujućih presuda u krivičnim djelima protiv života i tijela i u pravcu trgovine drogom i cigaretama.

Do 2004. godine crnogorska policija nije imala zakonske mogućnosti za provođenje mjera tajnog nadzora. Prilikom prikupljanja dokaza za rasvjetljavanje kriminala, jedna od značajnijih alatki jeste upravo provođenje mjera tajnog nadzora. Godine 2004.

doneseno je zakonsko rješenje o provođenju mjera tajnog nadzora - Krivični zakonik Crne Gore[35].

Osim rezultata za kriminalni motiv, rezultati istraživanja su utvrdili da je kod poznatog izvršioca broj krivičnih djela ubistava koji za motiv imaju mržnju (N=17); psihopatološki motiv kod poznatog izvršioca (N=16); ljubomora (N=10). Kod nepoznatog izvršioca rezultati istraživanja su pokazali da je kao motiv mržnja (N=4); psihopatološki (N=0); ljubomora (N=1). Statistički značajnu razliku uočavamo kod nepoznatih izvršilaca i poznatih izvršilaca u motivima mržnje, psihopatoloških i ljubomore. Sve tri ove skupine motiva možemo stoga grupisati u interpersonalne motive. Interpersonalni motivi su slabije zastupljeniji kod nepoznatih izvršilaca ubistva. Utvrđena raspodjela vrste motiva je očekivana. Upravo motiv se utvrđuje rekonstrukcijom krivičnog djela. Vrlo često postoje svjedoci, radi se o porodičnim odnosima, ljubomori, svađama, unutrašnjim nagonima. Očekivanije je da se utvrdi izvršilac krivičnog djela, upravo usljed vrste motiva i profilisanja krivičnog djela.

Najčešći motivi KD ubistva u ovom radu su razvrstani u dvije kategorije: kriminalni motiv i interpersonalni (mržnja, psihopatološki, porodični, ljubomora itd.). Opisna statistika motiva KD ubistva je predstavljena u tabeli 4. Procenat KD ubistva s kriminalnim motivom je 15,8% u slučaju poznatog izvršioca i 54,5% u slučaju nepoznatog izvršioca.

Navedeni rezultati se dalje mogu analizirati s varijablom lica mjesta. U odnosu na lice mjesta, kao varijablu imamo procenat zastupljenosti, za stan oštećenog iznosi 37,5%. Slična zastupljenost jeste za otvoreni prostor, 34,3%. Zastupljenost izvršenja krivičnih djela za automobile i za kafane iznosi isto 9,3%. Značajno manja zastupljenost je za stan osumnjičenog 2%, a ista je i za hotel, kao i zapaljeni automobil i ZIKS (Zavod za izvršenje krivičnih sankcija). Samo je jedan slučaj fabrike kao mjesta izvršenja. U odnosu na lice mjesta, vidimo procentualno podjednaku zastupljenost za stan oštećenog i za otvoreni prostor. Značajno manja zastupljenost jesu kafane, fabrike, stan oštećenog. Zastupljenosti za automobile i kafane je osrednja.

Obezbjeđivanje lica mjesta ima za cilj da se otkriju lokacije potencijalnih činjenica koje mogu poslužiti kao dokaz (Korajlić, 2012). Otvoreni prostor je dosta nepogodniji za DNK dokaze, usljed izloženosti fizičkim agensima, kao što je vjetar i kiša koji utiču na gubitak biološkog materijala. Zatvorena lica mjesta su dosta pogodnija u odnosu na utvrđivanje prisustva biološkog materijala. Postojanost biološkog materijala na predmetima zavisi od lica mjesta, odnosno da li je zaštićeno ili ne. Reymond et al. (2009) izveli su studiju o perzistentnosti, odnosno postojanosti biološkog materijala i utvrdili su da na otvorenom licu mjesta značajno opada količina pronađenog bio-

35 Krivični zakonik Crne Gore. Mjere tajnog nadzora. Vrste mjera tajnog nadzora i uslovi za njihovu primjenu. Član 157. („Službeni list Crne Gore", br. 70/2003, 13/2004 - ispr. i 47/2006 i „Službeni list Crne Gore", br. 40/2008, 25/2010, 32/2011, 64/2011)

loškog materijala nakon dvije nedjelje, dok je količina biološkog materijala u zatvorenom prostoru značajna, mada postoji varijabilnost i u tome. Tip lica mjesta dosta utiče na same materijalne dokaze i pronalaženje istih. Praksa prepoznaje nekoliko metoda pretraživanja lica mjesta. Jako je bitno imati u vidu da spor i metodičan pristup licu mjesta jesu preduslovi uspjeha na mjestu događaja (Korajlić, 2012). Pretraga lica mjesta uvijek je usmjerena na pronalazak bitnih činjenica od značaja.

Implikacija navedenih rezultata istraživanja mogla bi da ukazuje da je češća zastupljenost otvorenog lica mjesta kod profesionalnih izvršenja krivičnih djela. Fizički agensi iz spoljašnje sredine negativno utiču na biološki materijal. Paljenje automobila nakon izvršenja krivičnog djela imamo u dva slučaja (N=2), što je dosta mala učestalost u odnosu na ukupan broj krivičnih djela ubistava. Prilikom paljenja automobila i eksplozija razvijaju se visoke temperature, što uništava biološki materijal na licu mjesta.

Priručnik Best Practice Manual (ENFSI, 2022)[36] navodi faktore koji su od značaja za rezultate DNK analiza, na licu mjesta: istraga lica mjesta; izbjegavanje kontaminacije; istraga i otkrivanje; pravilno uzorkovanje; pakovanje, označavanje i čuvanja materijalnih tragova i predmeta; učestvovanje u ispravnom lancu nadzora.

Svaki od navedenih faktora je izuzetno bitan. DNK laboratorija Forenzičkog centra je akreditovana laboratorija po ISO 17025 standardu za akreditaciju laboratorija. Pravilno obilježavanje, označavanje, čuvanje i transport fizičkih tragova s lica mjesta je od izuzetne važnosti. Kriminalistički tehničari na licu mjesta moraju biti pravilno obučeni i moraju se pridržavati svih mjera za pravilno postupanje s tragovima i prevencija za sprečavanje kontaminacije.

Postojanje DNK baza je od velikog značaja za razrješavanje krivičnih djela. Baze podataka mogu da pruže daljnju vezu. Učinkovite baze podataka jesu specifična legislativa i ograničenja koja zakon nameće snagama zakona prilikom korištenja baza. Neadekvatna legislativa može ograničiti potencijal DNK baze podataka.

ZAKLJUČAK

Na osnovu dostupne naučne i stručne literature kao i podataka dobijenih u ovom radu može se zaključiti da se motivi mogu razvrstati u odnosu na poznate i nepoznate izvršioce. Utvrđena raspodjela vrste motiva je očekivana. Izdvajanjem kriminalnog motiva od ukupnog broja ubistava, obuhvaćenih ovim radom 29,1% je s motivom pripadnosti kriminalu. Rezultate potvrđuje naučna teorija da pripadnost kriminalu inače povećava vjerovatnoću da će isti ljudi biti uključeni u ubistva.

36 Best Practice Manual for Human Forensic Biology and DNA Profiling. (2022). ENFSI Board. ISBN Identifier 978-3—949994-06-7

Kriminalistički aspekt oblasti DNK istraživanja jeste u obradi lica mjesta, u pravilnom pronalaženju, obilježavanju, pakovanju i dopremanju tragova i predmeta s lica mjesta. Sprečavanje kontaminacije, s lica na predmet, a i s predmeta na predmet, zaštita lica mjesta i odgovarajuće kriminalističke procedure neophodno je provesti na licu mjesta. Lanac formiranja dokaza je neophodno ispoštovati, uz pravilno dokumentovanje, fotografisanje svih neophodnih koraka. DNK laboratorija Forenzičkog centra jeste akreditovana laboratorija po ISO 17025 standardu za laboratorije. Jedan od primarnih razloga za izraženu zainteresovanost naučne javnosti za ovu oblast ogleda se upravo u DNK analizi i njenoj upotrebi za kazivanje istine, odnosno utvrđivanje istine.

Implikacija navedenih rezultata istraživanja mogla bi da ukazuje da je češća zastupljenost otvorenog lica mjesta kod profesionalnih izvršenja krivičnih djela. Fizički agensi iz spoljašnje sredine negativno utiču na biološki materijal.

Najčešći motivi KD ubistva u ovom radu su razvrstani u dvije kategorije: kriminalni motiv i interpersonalni. Statistički značajnu razliku uočavamo kod nepoznatih izvršilaca i poznatih izvršilaca. Grupisanjem skupine motiva u interpersonalne motive koji su slabije zastupljeni kod neoznatih izvršilaca krivičnog djela.

LITERATURA

1. Aleksić, Ž., Škulić, M., Žarković, M, 2004. Leksikon kriminalistike, Smederevska Palanka
2. Belfiore, Rossana, 2011. Collection, analysis and exgange of DNA data in the European Union, New Journal of European Criminal Law, 2(3), 317-337.
3. Bojanić, Nebojša. 2011. Primjenjena forenzika, Fakultet za kriminalistiku, kriminologiju i siguronosne studije, Sarajevo.
4. Council of Europe:Recommendation No. R (92) 1Of The Committee of Ministers to Member States on The Use of analysis of deoxyribonucleic Acid (DNA) within The framework of the Criminal Justice System, 1992. (Adopted by the Committee of Ministers on 10 February 1992 at the 470th meeting of the Ministers' Deputies)
5. Council resolution of 30 November 2009 on the exchange of DNAanalysis results, OJ C 296 of 5 December 2009, p. 1. Already in 1997, the Council invited Member States to establish national DNAdatabases in accordance with the same standards and in a compatible manner (Council resolution of 9 June 1997 on the exchange of DNAanalysis results, OJ C 193 of 24 June 1997, p. 2).
6. COUNCIL DECISION 2008/615/JHA of 23 June 2008 ('Prüm Decisions') on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

7. Gurda, Vedad. & Lukovockić, Amar, 2019. Neke fenomenološke karakteristike krivičnih djela ubistava I sankcionisanje njihovih učinitelja, Zbornik radova Pravnog fakulteta u Tuzli, 5(1),
8. Global Study on Homicide: Executive Summary, United Nations Office on Drugs and Cime, Viena, 2019.
9. DNA database management review and recommendation.(2017). ENFSI DNA Working group https://enfsi.eu/wp-content/uploads/2017/09/DNA-database-management-review-and-recommendatations-april-2017.pdf
10. Dobrin, A. 2001. The risk of offending on homicide victimization: A case control study, Journal of Research in Crime of Delinquency, 38(2) 154 – 173.
11. Fondavila, M., Phillips, C., Navaren, N,. Cerezo, M,. Rodrigez, A.Colia, R., Fernandez, L.M., Carracedo, A. & Laveu, M.V,2008. Challenging DNA: Assesment of a range of genotyping approaches for highly degraded forensic samples.FSI Genetics, 2(1) ,212-218.
12. House of Lords European Union Committee. 2007. Prüm: An Effective Weapon Against Terrorism and Crime? HL Paper 90. London: The Stationery Office.
13. House of Lords European Union Committee. 2008. Europol: coordinating the fight against serious and organised crime,HL Paper 183. London: The Stationery Office.
14. INTERPOL.(2009). INTERPOL handbook on DNA data exchange and practice (2nd ed). Lyon: INTERPOL.
15. INTERPOL. Forensics: DNA, INTERPOL. (2018) (pristupljneo 2021 februar 12). https://www.interpol.int/INTERPOL-expertise/Forensics/DNA
16. Ivanović, Aleksandar &Ivanović, Aleksandar A. 2013. Kriminalističke procedure, Policijska akademija, Danilovgrad.
17. Jovanović, Jelena, 2022. DNK analiza i CODIS u borbi protiv organizovanog kriminala u Crnoj Gori, Kriminalističke teme, 22 (2), 1-19.
18. Korajlić, Nenad,2012. Istraživanje krivičnih djela. Sarajevo: Pravni fakultet.
19. Lee, H. C.,1996. Materijalni tragovi. Zagreb.
20. National Research Council,1996. The Evaluation of Forensic DNA Evidence (1sted,). National Academies press.
21. Newton, M.,2008. The Encyclopedia of Crime Scene Investigation. NewYork:Checmarks Books.
22. McCortney, I.C., Wilson, J. T., & Wiliams, R. 2011. Transnational Exgange of Forensic DNA: Viability, Legitimacy and Acceptibility. EUR J Crim Policy Res ,17(1), 305-322.
23. Modly, D.,1998. Priručnik - kriminalistički leksikon. Sarajevo: Fakultet kriminalstičkih nauka.
24. Modly, D. i Mršić, G.,2014. Forenzika suvremene kriminalističke teorije. Split: Sveučilište u Splitu.
25. Primorac, D., Primorac, D., Butorac, S. & Adamović, S..,2009. Analiza DNK u sudskoj medicini. Hrvatski ljetopis za kazneno pravo i praksu. Zagreb; 16 (1), 3-26.

26. Raymond, JJ, (2009). Trace evidence characteristics of DNA: A preliminary investigation of the persistence of DNA at crime scene. Forensic Sci.Int Genete (4) 26-33.
27. Staley, K, 2005. The Police National DNA Database: Balancing Crime Detection, Human Rights and Privacy. Retrieved from http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/NationalDNADatabase.pdf
28. Shroeder, D.A ,2007. DNA and Homicide Clearance: What' s Really going on ?. Criminal Justice, University of New Heaven.7, 279-98.
29. Schroeder, A.D., i White, D.M.,2009. Exploring the Use of DNA Evidance in Homicide Investigation:Implications for Detective Work and Case Clearance. Police Quarterly, 12,3, 319-342.
30. Toom, V. 2012. Forensic DNA databases in England and the Netherlands:governance, structure and performance compared. Northumbria University Centre for Forensic scene Newcastle, 31,3 ,311-322.
31. Wilis, S. M., McKenna, L., McDermott, S., O'Donell, G., Barrett, A., Rasmusson, B.,Nordgar, A.,Begeur, C.F.H., Sjerps, M.J., Lucena-Malina, J., Zadora, G.,Aitken, C., Lovelock, T., Lunt, L., Champod, C., Biedermann, A., Hicks. T.N., & Taroni, F. (2015). ENFSI guideline for evaluating reporting in forensic science, Strengthening the Evaluuation of Forensic results across Europe (STEOFRAE) http://enfsi.eu/sites/default/files/documents/external_publication/m1_guidelines-pdf(2015)

Zakoni

32. Zakonik o krivičnom postupku ("Sl. list Crne Gore", br. 057/09 od 18.08.2009, 049/10 od 13.08.2010, 047/14 od 07.11.2014, 002/15 od 16.01.2015, 035/15 od 07.07.2015, 058/15 od 09.10.2015)
33. Krivični zakonik Crne Gore ("Sl. list RCG", br. 70/2003, 13/2004 - ispr. i 47/2006 i "Sl. list CG", br. 40/2008, 25/2010, 32/2011, 64/2011)
34. Zakon o DNK registru. (2011). Službeni list CG, broj 39/11
35. Zakon o Izmjenama i dopunama Zakona o DNK registru. (2014). Službeni list Crne Gore, broj
36. Zakon o zaštiti podatak o ličnosti ("Službeni list Crne Gore", br. 079/08 od 23.12.2008, 070/09 od 21.10.2009, 044/12 od 09.08.2012)

Članci, internet izvori

37. Aprcović, M., Policija otkrila ko je osumnjičeni za ubistvo Đuričkoviča: traži se nalogodavac, Antena M, 06.09.2017, https://www.antenam.net/drustvo/49675-djurickovic
38. Britanci traže istragu protiv dva klana, Dan,2017-04-19, https://www.dan.co.me/?nivo=3&datum=2016-07-13&rubrika=Hronika&najdatum=2017-04-19&clanak=595152

39. Pogledajteputosvete,Vijesti,02.12.2020.,https://www.vijesti.me/tv/emisije/482813/pogledajte-put-osvete-kako-je-poceo-rat-crnogorskih-kriminalnih-klanova
40. Zapadni Balkan: Meka organizovanog kriminala, DW, 20.05.2019.https://www.dw.com/bs/zapadni-balkan-meka-organizovanog-kriminala/a-48805544#
41. Hot spot of Organized Crime in Western Balkan, Global initiative new, 20.05.2019, https://globalinitiative.net/analysis/oc-western-balkans/

UDK343.61(497.16)

POJAM I ELEMENTI OSNOVNOG OBLIKA UBISTVA U CRNOGORSKOM KRIVIČNOM ZAKONODAVSTVU

CONCEPT AND ELEMENTS OF THE BASIC FORM OF MURDER IN THE MONTENEGRO CRIMINAL LEGISLATION

Prof. dr Velimir Rakočević
Pravni fakultet, Univerzitet Crne Gore
e-mail: veljorakocevic@yahoo.com

Dr Aleksandra Rakočević
Pravni fakultet, Univerzitet Crne Gore
e-mail: aleksandrajovanovic417@gmail.com

Apstrakt

Pravo na život je vrhovno ljudsko pravo i najveća civilizacijska vrijednost i to je razlog zbog čega je čovjekov život na prvom mjestu skale vrijednosti. Budući da se radi o najznačajnijem pravu čovjeka sve države putem krivičnog zakonodavstva štite pravo na život koje u modernom društvu ima univerzalni karakter. Ovaj vid krivičnopravne zaštite života je integralan i primaran i za razliku od drugih tipologija inkriminacija isključuje fragmentarnu, akcesornu i supsidijarnu prirodu krivičnog prava. Protivpravno lišenje života druge osobe može se izvršiti na različite načine, različitim sredstvima i u vrlo heterogenim okolnostima. Osnovni oblik ubistva shodno zakonskoj definiciji, obuhvata lišavanje života drugog lica ili

preciznije protivpravno lišenje života druge osobe sa umišljajem s obzirom da kod ovog oblika ubistva ne postoje kvalifikovani oblici, privilegovani oblici i posebni slučajevi koji karakterišu druge vidove ove inkriminacije. Biće osnovnog oblika ubistva sadrži šest ključnih segmenata. Prvi je radnja koja obuhvata brojne aktivnosti fokusirane na lišenje života druge osobe. Drugi segment je nastupanje smrti kao posledica inkriminisanih djelatnosti učinioca. Treći segment obuhvata objektivnu uzročnu vezu između radnje i posledice. Protivpravnost lišenja života druge osobe je četvrti segment bića osnovnog oblika ubistva. Peti segment obuhvata živo ljudsko biće kao objekt krivičnopravne zaštite. Šesti konstitutivni element obuhvata umišljaj kao subjektivno obilježje. Radnja, posledica, objekt radnje, objektivna uzročna veza između radnje i posledice i protivpravost su objektivna obilježja, dok je krivica subjektivno obilježje. Postojanje objektivnih i subjektivnog obilježja potrebno je utvrditi u svakom konkretnom slučaju da bi se radilo o krivičnom djelu iz člana 143 KZ CG.
Ključne riječi: *pravo na život, krivično pravna zaštita života, osnovni oblik ubistva, objektivni elementi ubistva, subjektivni element ubistva.*

Abstract

The right to life is the supreme human right and the greatest civilizational value, and this is the reason why human life is at the top of the value scale. Since it is the most important human right, all states protect the right to life through criminal legislation, which in modern society has a universal character. This type of criminal law protection of life is integral and primary, and unlike other typologies of incrimination, it excludes the fragmentary, accessory and subsidiary nature of criminal law. Unlawful deprivation of another person's life can be carried out in different ways, by different means and in very heterogeneous circumstances. The basic form of murder, according to the legal definition, includes taking the life of another person or, more precisely, unlawfully taking the life of another person with intent, given that this form of murder does not have qualified forms, privileged forms and special cases that characterize other types of this incrimination. The essence of the basic form of murder contains six key segments. The first is an action that includes numerous activities focused on taking another person's life. The second segment is the occurrence of death as a consequence of the incriminated activities of the perpetrator. The third segment includes the objective causal connection between the action and the consequence. The illegality of taking the life of another person is the fourth segment of essence of the basic form of murder. The fifth segment includes a living human being as an object of criminal protection. The sixth constitutive element includes intention as a subjective characteristic. Action, consequence,

object of action, objective causal connection between action and consequence and illegality are objective features, while guilt is a subjective feature. The existence of objective and subjective characteristics must be determined in each specific case in order to be considered a criminal offence under Article 143 of the Criminal Code of Montenegro.
Keywords: *right to life, criminal law protection of life, basic form of murder, objective elements of murder, subjective element of murder.*

UVOD

Život je najveći imetak koji čovjek posjeduje i jedinstveni momenat ljudskog egzistiranja. Pravo na život je univerzalno ljudsko pravo iz koga nastaju druga prava čovjeka i ovo pravo ima prednost u odnosu na sva druga ljudska prava. Čovjeka ga stiče rođenjem a fundirano je još u periodu procvata antičke kulture i Rimskog prava a posebno u djelima Cicerona i Hipokrata. Sadržano je u brojnim nacionalnim, evropskim i međunarodnim dokumentima a konstitucionalizacija prava čovjeka započela je krajem XVIII vijeka u SAD i Francuskoj. Život i tijelo su ubjedljivo najznačajnije ljudske vrijednosti kojima su podređene sve druge bitnosti zbog čega zauzimaju dominantno prvo mjesto u sistemu značajnosti. Pravo na život i tjelesni integritet su bazična prava čovjeka međusobno tijesno povezana budući da povredi života prethodi povreda tjelesnog integriteta.

Pravo na život garantovano je brojnim međunarodnim dokumentima. U članu 3 Univerzalne deklaracije o ljudskim pravima naznačeno je da svako ima pravo na život, slobodu i bezbjednost ličnosti.[1] Radi se o najvišem standardu u oblasti ljudskih prava čija sadržina predstavlja osnovu međunarodnih ugovora o ljudskim pravima. Takav je slučaj sa Međunarodnim paktom o građanskim i političkim pravima koji u članu 6 utvrđuje da je pravo na život neodvojivo od ličnosti čovjeka i mora biti zaštićeno zakonom. Iz toga proizilazi da ni jedna osoba ne može biti lišena života arbitrerno.[2] Konvencija za zaštitu ljudskih prava i osnovnih sloboda u članu 2 garantuje pravo na život. U stavu 1 predmetnog člana navedeno je da je pravo na život svake osobe zakonom zaštićeno. Posebno je naglašeno da niko ne smije biti namjerno lišen života, osim prilikom izvršenja sudske presude kojom je lice osuđeno za krivično djelo za koje je zakonom predviđena smrtna kazna. U sljedećem stavu naznačeni su izuzeci od ovog pravila kada se oduzimanje života ne smatra nezakonitim. To su slučajevi korišćenja apsolutno nužne sile radi odbrane osobe od nezakonitog nasilja, radi zakonitog lišenja slobode ili sprječavanja bjekstva osobe koja je u skladu sa za-

1 Universal declaration of Human Rights (Univerzalna deklaracija o ljudskim pravima), usvojena od strane Generalne skupštine Ujedinjenih nacija (A/RES/217, 1948. Pariz.

2 Međunarodni pakt o građanskim i političkim pravima, usvojen rezolucijom Generalne skupštine 2200 A (XXI) od 16. decembra 1966, stupio na snagu 23 marta 1976.

konom lišena slobode kao i prilikom preduzimanja aktivnosti radi suzbijanja nereda ili pobune većeg obima.[3]

Ne može se ograničiti pravo na život, propisano je u članu 25 st.4 Ustava Crne Gore.[4] Najviši pravni akt u državi zabranjuje smrtnu kaznu kao i kloniranje ljudskih bića i jemči nepovredivost fizičkog i psihičkog integriteta čovjeka. Ljudski život je neprikosnoven, on se mora poštovati kao i ličnost u cjelini. Stoga je ključni zadatak modernog društva ostvarenje prava na život dostojan čovjeka.

ZAJEDNIČKI ELEMENTI KRIVIČNIH DJELA PROTIV ŽIVOTA I TIJELA

Krivična djela protiv života i tijela obuhvataju različite forme violentnog kriminaliteta kojima se povređuje, odnosno ugrožava fizički i psihički integritet ljudskog bića. Kod ovih krivičnih djela objekt krivično pravne zaštite je život i tijelo živog čovjeka, determinisan kao dvočlani koncept vrijednosti koji konstituiše ličnost i sadrži život, odnosno pravo na život kao i tjelesnu konstituciju čovjeka, uključujući i pravo na nepovredivost tjelesnog integriteta. U osnovi radi se o deliktima agresije koji egzistiraju pod uobičajenim nazivom *criminal violence* pri čemu se pravi razlika između fizičkog, psihičkog i ekonomskog nasilja kao i između instrumentalnog i impulsivnog oblika nasilja.

Krivično pravna zaštita života i tijela je autonomna, integralna i izvorna, zbog čega su za ovu tipologiju kriminaliteta isključena sporedna, segmentarna i pomoćna obilježja krivičnog prava što je apsolutno razumljivo imajući u vidu univerzalno značenje prava na život. Najdjelotvornija i najznačajnija dimenzija zaštite života i tijela je krivično pravna i ključna je baza zaštite ostalih prava čovjeka. Pravo na život i tijelo garantuje se svakoj osobi u svim uslovima i ne može biti derogirano. Objekt krivično pravne zaštite kod ove tipologije delikata je dvostruk i obuhvata život i tijelo kao esencijalne vrijednosti. Naznačene vrijednosti zaštićene su od momenta rađanja do trenutka nastupanja smrti uz postojanje izuzetka kod krivičnog djela povrede ploda koje je specifično po tome što se život štiti od začeća, odnosno intrauterino. Radnja izvršenja kod krivičnih djela protiv života i tijela pretežno je određena putem posledične norme, odnosno aktivnim preduzimanjem radnje ili propuštanjem što uključuje svaku podobnu aktivnost da prouzrokuje posledicu na objektu radnje. Posledica sadrži povredu u smislu uništenja ljudskog života ili ploda ili nanošenja nekog od oblika tjelesne povrede ili ugrožavanja života ili tijela putem izazivanja konkretne opasnosti po ove vitalne vrijednosti. Treba istaći da ovi delikti mogu biti izvršeni isključivo protiv tuđeg života ili tijela jer autoagresija nije sankcionisana kada je riječ o suicidu. Samopovreda u određenim slučajevima može imati obilježja krivičnog djela. Takav je slučaj kod krivičnog djela

3 European Convention on Human Rights (Evropska konvencija o ljudskim pravima) Rim, 1950.
4 Ustav Crne Gore, „Sl.list CG", br. 1/2007 i 38/2013-Amandmani I-XVI).

zloupotreba prava iz socijalnog osiguranja kojom prilikom učinilac nanosi sebi tjelesne povrede usljed kojih nastupa privremena ili trajna nesposobnost za rad, da bi ostvario neko pravo iz socijalnog osuguranja koje mu ne pripada. Ista je situacija kada se radi o krivičnom djelu izbjegavanje vojne službe onesposobljavanjem ili obmanom iz grupe krivičnih djela protiv Vojske Crne Gore. Radnja ovog krivičnog djela sastoji se u samoozljedi učinioca u namjeri da izbjegne vojnu službu.

Žrtva krivičnih djela protiv života i tijela jeste ljudsko biće u svim fazama života bez obzira da li je dobrog zdravstvenog stanje ili je oboljelo, da li je novorođenče ili osoba u poznim godinama života. To znači da se život štiti svakom čovjeku bez izuzetka. Najveći broj krivičnih djela iz ove grupe u pogledu oblika krivice sadrži umišljaj, osim kod krivičnih djela nehatnog lišenja života i teške tjelesne povrede iz nehata kod kojih se kažnjava i za nehat. Učinilac ovih delikata može biti svaka osoba sa izuzetkom krivičnog djela ubistva djeteta pri porođaju gdje izvršilac može biti samo majka djeteta. Život i tijelo čovjeka zaštićeni su i jednim brojem inkriminacija propisanim u drugim grupama krivičnih djela. Tako npr. krivično djelo ubistvo najviših predstavnika Crne Gore kao protivpravno lišenje života drugog lica u namjeri ugrožavanja ustavnog uređenja i bezbjednosti države, odnosno političko ubustvo, pripada grupi krivičnih djela protiv ustavnog uređenja i bezbjednosti Crne Gore. Slična je situacija i sa jednim brojem krivičnih djela propisanim u tipologijama inkriminacija protiv čovječnosti i drugih dobara zaštićenih međunarodnim pravom, protiv Vojske Crne Gore, protiv opšte sigurnosti ljudi i imovine i slično, shodno dominantnom objektu zaštite koji nije život i tjelesni integritet.

OSNOVNI OBLIK UBISTVA U CRNOGORSKOJ KRIVIČNO PRAVNOJ TRADICIJI

Nastanak krivičnog prava u Crnoj Gori podudara se sa nastankom moderne crnogorske države, odnosno početkom razvoja kapitalizma na starom kontinentu (Jovanović J. 1995:25). Pisano krivično zakonodavstvo u Crnoj Gori vezuje se za vladavinu Pertra I svetog (1782-1820) normirano u odredbama Stege (1796) i Zakonika obščeg crnogorskog i brdskog (1798-1803). Stega je prvi pisani zakon na teritoriji stare Crne Gore koji je napisao vladika Petar I Petrović Njegoš u namjeri da ojača vezu između Crnogoraca i Brđana (Stojanović P. 1982:10). Ovaj pravni akt krivičnog i ustavnog karaktera ima šest članova i predstavlja normiranje borbe za slobodu. Njegove odredbe su prožete etičkom dimenzijom budući da potencira najveće crnogorske vrijednosti kao što su čast i savjest zbog čega propisuje samo etičke sankcije. Posebno se naglašava osuda izdaje a izdajniku se prijeti prokletstvom i on ostaje bez časti i potencira neophodnost pomaganja u slučajevima ugroženostii plemena od okupatora (Milićević J. Rakočević N.1986:58). U zakonu se poziva na njegovo poštovanje i obavezuju crkva i nahije da čuvaju tekst zakona (Jevtić D. Popović D. 1977:30).

Zakonik Petra I ima 33 člana i gotovo u cjelosti tretira krivična djela (Petrović R.1929:18). U njemu je obrađena većina krivično pravnih instituta u osnovnoj ili početnoj formi. Termini kojima se u ovom pravnom aktu označavaju krivična djela, učinioci i sankcije su neodređeni i različiti (Dragović M.1985:3). Interesantno je istaći da su sinonimi za krivično djelo u ovom pravnom dokumentu bili zločinstvo, krvoproliće, zlo, bezakonje, lupeština, kavga, pohara, grabiteljstvo i slično. Od sinonima za učinioca krivičnog djela u zakoniku se navode: zločinac, ubica, izdajnik, krvnik, lupež, poharnik, rukostavnik i td. Krivična djela se sankcionišu od strane države koja štiti pojedinca i zabranjuje samovlašće. U fokusu zakonika je suzbijanje krvne osvete, privatnog kažnjavanja i ukidanje imovinske naknade. Jedna od prvih krivično pravnih tipologija izražena je u odredbama koje regulišu izdaju otadžbine i krivična djela protiv sudstva s jedne strane i krivična djela protiv privatne imovine, s druge strane. Odredbe člana 14 predviđaju oslobađanje od krivične odgovornosti za krađu djeteta koje nema čiste svijesti i pameti, što je preteča savremene koncepcije o nepostojanju krivične odgovrnosti djece. Zakonik isključuje zastarjelost apsolutnu i relativnu kao osnov gašenja prava države da goni učinioca zločina ili izvrši kaznu, što i nije iznenađenje budući da je ovaj institute novijeg datuma. To se posebno odnosi na najteža krivična djela kao što su izdaja i ubistvo. Zakonik predviđa kažnjavanje za pokušaj krivičnog djela sa elementima korupcije sudija ali ipak ostavlja ovaj institute nedovršenim zbog toga što ne normira elemente pokušaja, zatim krivična djela za koja je pokušaj kažnjiv, nema odredbi o dovršenom i nedovršenom pokušaju kao i o apsolutno i relativno nepodobnom pokušaju (Marinović S. 2007:129-131).

Kao olakšavajuće okolnosti Zakonik predviđa: nehotično izvršeno ubistvo i poharu, ubistvo zbog uvrede časti (čl. 8), ubistvo u nužnoj odbrani (čl. 10), ubistvo lopova u krađi (čl. 13). Otežavajuće okolnosti predviđene su u članu 2, 7 i 17 (ubistvo, udarac "od sile i opačine" i krađa u povratu). Kvalifikatorne okolnosti prilikom izricanja kazne smatrane su krvno srodstvo, kumstvo, pobratimstvo, zatim mjesto zločina, sredstvo kojim je krivično djelo izvršeno, odnos zločinac –žrtva i lična svojstva žrtve.

Predviđeno je kažnjavanje za saučesništvo pa shodno tome će se kazniti zločinci koji zločince brane. Međutim, saučesništvo nije definisano na integralan način niti zakonodavac poznaje pojam podstrekača i pomagača. U tom periodu postojala je izražena plemenska solidarnost pa su učinioci teških krivičnih djela izbjegli kaznu zaštićeni od rođaka i susjeda. Tradicionalno gostoprimstvo Crnogoraca (pravo utoka) bilo je sastavni dio duha naroda da je bilo neprihvatljivo da se ne pruži utočište i najvećem kriminalcu (Marinović S.2007:31). Po prvi put u ovom pravnom aktu propisana je kazna za svakog ko brani ili krije ubicu ili izdajnika.

U pogledu subjektivnog bića krivičnog djela Zakonik ne determiniše oblike krivice iako su sudovi imali u vidu subjektivne elemente prilikom odlučivanja o sankciji uči-

niocu. O umišljaju i nehatu riječ je samo kod krvnih delikata. U zakoniku se ubistvo izvršeno sa direktnim umišljajem definiše ubistvom od sile i opačine, a za nehatno lišenje života koristi se termin ne kteći.

Ovaj pravni akt predviđa tri vrste ubistva: hotimično (čl. 2), nehotimično (čl. 9) i ubistvo u nužnoj odbrani (čl.10). Za hotimično ubistvo tj. u slučaju da Crnogorac ubije brata Crnogorca ili Brđanina i suprotno, bez ikakve krivice i nužde, takav ubica se ne može osloboditi i za njega je propisana smrtna kazna koja se izvršavala strijeljanjem, kamenovanjem ili vješanjem. Nehotično ubistvo bilo je predviđeno u slučaju da se nekome puška omakne ili kojim drugim načinom da ne kteći čojka rani ili ubije.

Zakonik definiše tri uslova za postojanje nužne odbrane. Oni se odnose na zaštitu fizičkog integriteta ličnosti, zaštitu dostojanstva i zaštitu imovine. Ubistvo u nužnoj odbrani postojalo je ako koji ubije čojka napastnika vrhu sebe braneći se i zaklinjući ga Bogom, da se ot njega prođe, a on ne ustupi nego prego toga pogine. Ubistvo lopova u krađi, odnosno ko učinioca krađe zatekne na djelu i liši života ne povlači kažnjavnje tog lica (čl.13). Citirani akt predviđao je smrtnu kaznu za najteža krivična djela, zatim kaznu zatvora, progonstvo, konfiskaciju imovine i novčanu kaznu.

Zakonik Danila I knjaza i gospodara slobodne Crne Gore i Brdah[5] sadrži pretežno odredbe krivično pravnog karaktera kao i drugih grana prava kao što su ustavno i građansko sadržanih u 95 članova ovog pravnog akta. S pravom se ističe da je ovaj zakon doprinio evropeizaciji crnogorskog prava u smislu prevazilaženja patrijarhalnog društvenog uređenja i načina života, oduzimanja samostalnosti plemenima i jačanja vlasti države (Bojović J.1982:18). U preambuli zakonika navedeno je da ni jedna država ne može biti srećna, prosperitetna i uvažena ako nema zakonika koji garantuje ostvarivanje pravde i zaštite građana. Svaki Crnogorac i Brđanin jednak je pred sudom propisano je u prvom članu ovog akta. Knjaz je uživao pojačanu krivično pravnu zaštitu imajući u vidu da je za povredu člana 4 (vrijeđanje ličnosti ili dostojanstva Gospodara) propisano sankcionisanje kao za ubistvo. Knjaz je imao pravo pomilovanja lica osuđenih na smrt od strane najviše sudske instance, predviđeno je u članu 5. Odbrana države od neprijatelja bila je kao i uvijek kroz istoriju najvažnija obaveza. Ona je podrazumijevala da u slučaju napada na teritoriju države svaki građanin ustane na oružje i brani otadžbinu, a ukoliko neki građanin to ne učini njemu se oduzima oružje i to trajno. Propisano je da se izdajnicima pripaše ženska opregljača, da se zna da muškog srca nemaju (čl.18). U slučaju pojave opasnosti po državu starješine su bile u obavezi stati na čelo naroda i povesti borbu, a ukoliko bi se starješina oglušio o tu svetu obavezu bio bi osuđen na smrt. Ukoliko se prilikom potjere za učiniocem krivičnog djela pronađu lica koja krivca brane oni bi bili lišeni slobode i privedeni nadležnom sudu. Ako bi te osobe potegle oružje na one koji gone krivca bile bi lišene života ukoliko se odmah ne predaju i polože oružje. Pojedine zakonske odredbe (čl.

5 Zakonik Danila I knjaza i gospodara slobodne Crne Gore i Brdah (1855), Cetinje.

24) predviđaju obavezu održavanja dobrosusjedskih odnosa sa pograničnim državama što uključuje zabranu vršenja imovinskih delikata na štetu interesa tih država a sankcije su ekvivalentne onima koje se izriču učiniocima koji su zločine izvršili na štetu Crnogoraca ili Brđana. Za ubistvo brata Crnogorca ili Brđaniina bez krivice i bez nužde nad učiniocem se izvršavala smrtna kazna bez mogućnosti otkupa, a ukoliko bi učinilac izvršio bjekstvo njegova imovina i prihodi su oduzimani i polagani u državnu kasu. Tim osobama je bio zabranjen povratak u domovinu a građanin koji je tog učinioca primio ili branio nakon saznanja šta je učinio, bio je kažnjen kao i učinilac (čl.29). Učiniocu koji žrtvu povrijedi upotrebom puške ili noža i koji je prvi započeo svađu propisano je stavljanje u tavnicu ili plaćanje zemaljske globe, a učinilac koji korišćenjem oružja ili drveta bez povoda povrijedi drugog sankcionisan je kaznom u dvostrukom iznosu. Ukoliko lice ostane invalid prilikom povrede zavisno od stepena krivice predviđena je novčana kazna u različitom iznosu. Ukoliko je žrtva udarena nogom ili kamišem bez povoda predviđena je takođe novčana kazna a ukoliko napadnuti u afektu liši života učinioca nakon što bude udaren za njega pogovora nije koliko ni za lupeža koji u krađi pogine (čl.34). Međutim, ako napadnuti nakon jednog sata ili drugi dan nakon što je udaren liši života napadača biće sankcionisan kao da je samovoljno ubio čoeka, što i danas predstavlja dilemu kada se radi o ubistvu na mah. U članu 37 propisano je nehatno lišenje života koje postoji u slučaju da se nekome puška omakne ne kteći da čoeka rani ili ubije, to lice treba da plati troškove liječenja. Osnov isključenja protivpravnosti predviđen je u članu 38 koji predviđa ubistvo u nužnoj odbrani. Ukoliko se liši života napasnik vrhu sebe braneći se, za toga pogovora nema, napadač se može lišiti života a da na sudu ništa ne odgovara. Zakon zabranjuje krvnu osvetu izvan krivca i krvnika, tj. na prvom bratu njegovom zbog čega će taj učinilac biti osuđen na smrt. Može se lišiti života samo krvnik ali ne i brat ili rođak učinioca koji nijesu krivi. Propisano je da megdan mogu megdandžije dijeliti same a ako im neko drugi pomogne taj će biti novčano kažnjen. Ukoliko učinilac nekom zapali kuću od njega bi se naplatila odšteta a vlasnik je ovlašćen da učinioca liši života. Iz prethodno citiranih odredbi može se zaključiti da su običaji imali ključnu ulogu u regulisanju društvenih odnosa u tom period razvoja naše države.

U dijelu sankcija Zakonik je predviđao smrtnu kaznu, tjelesnu (batinanje), oduzimanje oružja i pripasivanje ženske opregljače, progonstvo, zatvor, globu i lišenje glavarskog ili svešteničkog čina ili zvanja. Kamenovanje koje je propisivao Zakonik Petra I nije kao sankcija previđeno u ovom aktu. Šibikanje kao tjelesna kazna je izvršavano javno na pazarima i skupovima kao bi se ostvarila generalna prevencija. Oduzimanje oružja i pripasivanje ženske opregljače kao moralne kazne bile su propisane za neodazivanje pozivu za borbu za slobodu. Progonstvo je najčešće izricano kumulativno sa konfiskacijom imovine a kazna lišavanja glavarskog ili svešteničkog čina izricala se za povredu službene dužnosti kao glavna ili sporedna kazna uz novčanu kaznu. Zakonik je značajno doprinio obogaćivanju crnogorske krivično pravne tradicije.

U periodu od 1810. do 1906. godine uslijedila je intenzivna zakonodavna aktivnost u krivično pravnoj oblasti kada su u Evropi donijeti značajni krivični zakoni kao što su Code penal u Francuskoj 1810. godine, Krivični zakonik Bavarske 1813. godine, Krivični zakonik Pruske 1851. godine, koji je bio osnova za donošenje Krivičnog zakonika Sjevernonjemačkog saveza 1871. godine, zatim Kazniteljni zakonik za Knjaževstvo Srbiju 1860. godine i slično. Krivični zakonik za Knjaževinu Crnu Goru[6] u dijelu opštih odredbi klasifikuje krivična djela trodiobno prema težini na zločine, prijestupe i istupe. Zločini kao najteži oblici kriminaliteta sankcionisani su najtežim kaznama, dok su za ostale oblike inkriminisane aktivnosti propisane blaže sankcije. Zakonik propisuje načelo zakonitosti u krivičnom pravu (nullum crimen, nulla poena sine lege) na način kako su ovaj princip definisali predstavnici Klasične krivično pravne škole kao civilizacijsku tekovinu koja po svom značaju daleko nadilazi granice krivičnog prava. Krivičnim pravom štite se najveće vrijednosti društva propisivanjem krivičnih djela i krivičnih sankcija za učinioce. Usvojen je teritorijalni princip važenja zakonika za svakog ko učini zločin na crnogorskoj teritoriji bilo da je u pitanju državljanin ili stranac, kao i u slučaju da Crnogorac djelo učini u inostranstvu. Saučesnik (čl.46-52) se kažnjava kao i učinilac zločina a pokušaj (čl. 42-45) se određuje kao početak preduzimanja radnje izvršenja na objektu zaštite i kažnjva se samo onda kad to KZ propisuje za zločine, dok se za prekršaje pokušaj ne kažnjava. Prihvaćena je biološka koncepcija neuračunljivosti a druga međustanja svijesti ovim pravnim aktom nijesu predviđena. U pogledu donje grancie krivične odgovornosti Zakonik je propisuje na 12 godina života, što znači da djeca koja nijesu navršila 12 godina života u vrijeme izvršenja delikta nijesu krivično odgovorna, a sa navršenih 12 godiina života za ova lica je bila predviđena kazna zatvora. Olakšavajuće i otežavajuće okolnosti predviđene su u čl.59-67 citiranog akta. Olakšavajuće okolnosti su sljedeće: 1) ako je učinilac na zlo naveden nevoljom, prevarom ili prijetnjom, 2) ako nije razumio koliko zlo može proizaći iz njegovog djela i kakve će poslediice po njega imati, 3) ako je delikt izvršio usljed osjećaja humanosti ili razdražen uvredom lica prema kome je zlo učinio, 4) ako se prije izvršenja zločina dobro vladao, 5) ako je vršeći krivično djelo imao priliku učiniti veću štetu ali je nije učinio, 6) ako se sam prijavi i prizna krivicu (čl. 59). U čl. 60 predviđeno je da priznanje kao najvažnija olakšavajuća okolnost kod najtežih krivičnih djela, učiniocu umjesto smrtne kazne omogućava izricanje robije ili zatočenja. Zakonik prepoznaje otežavne i osobito otežavne okolnosti. Ukoliko je učinilac planirao izvršenje krivičnog djela, za njega se pripremao i zrelije razmišljao je otežavna okolnost. Takođe je otežavna okolnost ako je učinilac nanio veću štetu izvršenim krivičnim djelom, ako je više dužnosti zločinom ili prijestupom povrijeđeno i ako je veća opasnost nastupila izvršenjem zločina. Kao osobito otežavne okolnosti smatrane su recidivizam (ako je krivac za drugi zločin ili prijestup već bio kažnjen) i ako je u izvršenju krivičnog djela učestvovalo više osoba, pri čemu je krivac bio u ulozi kolovođe ili podstrekača. U glavi VI definisani su idealni i realni sticaj. Idealni sticaj postiji kad lice jednom radnjom izvrši više

6 Krivični zakonik za Knjaževinu Crnu Goru (1906). Cetinje.

zločina ili prijestupa a kazniće se onom kaznom koju zakonik za najteže od njih predviđa. Realni sticaj postoji kad učinilac sa više samostalnih radnji izvrši više zločina ili prijestupa, pa se za sva ta djela zajedno sudi, osudiće se na sve što zakon predviđa. U glavi VIII (čl.74-82) propisan je institut zastarjelosti. Rok zastarjelosti za zločin za koji zakon donosi smrt ili doživotni zatvor nastupa ukoliko protekne 30 godina od dana izvršenja (čl. 74). Zločin za koji zakon predviđa robiju ili zatočenje više od 10 godina zastariće ako protekne 20 godina od vremena izvršenja, a svaki drugi zločin zastarijeva kad protekne 10 godina od vremena izvršenja. U pogledu rokova ista je situacija i sa zastarjelošću izvršenja kazne.

Posebni dio krivičnog prava obrađen je u glavama IX-XXXII pod nazivom O kaznenju zločina i prijestupa ponaosob u kojima je izvršena konkretizacija zločina i prijestupa. U glavi IX obrađeni su zločini i prijestupi protiv Otadžbine, Vladaoca i Ustava. Shodno današnjoj tipologiji to je naziv za grupu krivičnih djela protiv ustavnog uređenja i bezbjednosti Crne Gore. Interesantno je istaći da se kod ovih krivičnih djela po prvi put pomjera zona kažnjivost na pripremne radnje, što je obilježje ovih krivičnih djela i danas. Zakonodavci su polazili od važnosti objekta zaštite zbog čega su propisali kažnjavanje u što ranijoj fazi, odnosno prije nastupanja posledice. Radi se pretežno o deliktima izdaje otadžbine, ubistva vladara i slično, za koje je zaprijećena smrtna kazna bez alternative. Posebno težak delikt biio je otmica djevojke i taj problem je u dužem vremenskom periodu bio aktuelan. Smatran je velikom sramotom u porodici djevojke i širem bratstvu zbog čega je dolazilo do osvete i krvavog rata (Marinović S. 2007:210).

Ubistvo kao najteži zločin protiv života obrađen je u glavi XV. Za razliku od važeće determinacije osnovnog oblika ubistva (lišavanje života drugog) zakonik pod ubistvom podrazumijeva svako nedozvoljeno djelo usljed kojeg kakav čovjek život izgubi, ne gledajući na način i sredstva kojima je to učinjeno (čl.154). Upravo način izvršenja predstavlja kvalifikatornu okolnost kao i okolnosti izvršenja, pobude izvšenja, svojstva žrtve i težina posledice što ubistvo kvalifikuje kao teško ubistvo u modernom krivičnom pravu. Zakonik uočava razliku ubistava prema stepenu krivice, pa ubistvo sa predumišljajem i hotimično ubistvo sankcioniše smrtnom kaznom, dok za hotimično ubistvo bez predumišljaja predviđa kaznu zatvora od 20 godina. Od privilegovanih ubistava zakonik poznaje ubistvo na mah i nehatno ubistvo. Ubistvo djece a naročito vanbračne djece propisano je u glavi XVI zakonika. Ubistvo bračnog djeteta strože je sankcionisano u odnosu na ubistvo vanbračnog djeteta. Abortus je sankcionisan u glavi XVIII a učinilac osim majke može biti i lice koje vrši pobačaj, daje uputstva za pobačaj ili pomaže prilikom pobačaja. Za izvršenje ovog krivičnog djela sa smrtnom posledicom propisana je vječita robija kao i u slučajevima kad se pobačaj obavlja bez pristanka brmenite žene. Glava XVIII sadrži odredbe o odbacivanju djece i slabomoćnih. Propisana je kazna zatvora ilii robija do pet godina za ostavljanje bez pomoći djeteta do sedam godina ili slaboumnog lica. Majka koja

svoje vanbračno dijete odbaci u namjeri da ga se oslobodi kažnjava se zatvorom do dvije godine, a ukoliko nastupi smrtna posledica kazna je robija od dvije do dvanaest godina. Danas se ova krivična djela nalaze u podgrupi krivičnih djela odbacivanja u okviru tipologije protiv života i tijela. U glavi XIX propisane su tjelesne povrede. Zakonik nije sistematizovano tjelesne povrede prema kriterijumima savremenog krivičnog prava što ne umanjuje njegovu vrijednost budući da definiše pojedine oblike ovog krivičnog djela. Shodno principima prve krivično pravne teorije naglašeno je da težina kazne zavisi od težine povrede. Stoga je za nanošenje tjelesne povrede zbog koje je žrtva postala invalid bila predviđena kazna od 15 godina robije. Zanimljiva je formulacija teške tjelesne povrede prema načinu izvršenja koju ne propisuje moderno zakonodavstvo. Ukoliko je ovaj delikt izvršen na podmukao način učinilac će pored kazne zatvora, odnosno robije biti osuđen i na gubitak građanske časti, a ako se radi o vojniku proći će kroz redove čete, odnosno šibikanje. Krivo se zakleti u Crnoj Gori nekada je za posledicu imalo moralnu ekskomunikaciju iz ljudskog roda (Marinović S. 2007:201). Prokletstvo je imalo bezvremenu dimenziju i predstavljalo je gubitak duhovnog identiteta. Krivokletstvo u građanskim postupcima bilo je sankcionisano robijom u trajanju do 8 godina. U krivičnim postupcima se pravila razlika u odnosu na to da li je lažno zaklinjanje bilo u korist ili na štetu optuženog, kao i da li je u vezi toga obećana ili dobijena nagrada. Shodno tome, ukoliko je neko usljed lažnog svjedočenja od strane krivokletnika na smrt bio osuđen ali kazna nije izvršena, ona se sastojala u robiji od namjanje 10 godina uz izricanje gubitka građanske časti. Ukoliko je neka osoba usljed krivokletstva osuđena važili su određeni principi. Krivokletnik se kažnjava istom kaznom na koju je bilo osuđeno nevino lice ako je kazna nad tim licem bila u cjelosti ili djelimično izvršena. Ukoliko je optuženi zbog lažnog svjedočenja lica koje se zaklelo osuđen na težu kaznu, lice koje se krivo zaklelo će se osuditi na zasluženu kaznu kao i na višak koji je osuđeni usljed njegovog lažnog svjedočenja nepravedno pretrpio. Krivokletnik je kažnjavan smrću ako je svjesno lažno svjedočio u namjeri da nevino optuženi bude osuđen na smrt i pogubljen. Ako analiziramo 23 tipologije i podtipologije krivičnih djela koje je propisivao Krivični zakonik za Knjaževinu Crnu Goru u odnosu na 24 tipologije važećeg KZ CG vidjećemo da je krivično pravo posebni dio bilo izuzetno razvijeno u odnosu na ondašnji nivo društvenog razvoja.

Zakonik je propisivao 12 vrsta sankcija za učinioce zločina i prijestupa. Najteža kazna bila je osuda na smrt za najteže zločine i izvršavana je strijeljanjem. Osuda na robiju propisana je kao vječita ili u trajanju od 2-20 godina. Robija u okovima propisana je učiniocu zbog izvršenog zločina za koji je predviđena smrtna kazna i za beščasteće delikte. Kazna zatočenja je izricana u trajanju od 2-20 godina, a osuđenik nije imao radnu obavezu. Zatvor se izricao na period od 30 dana do 5 godina uz radnu obavezu. Za 12 mjeseci zatvora moglo se izreći 8 mjeseci robije ili zatočenja. Zakonik nije određivao gornju grancu novčane kazne dok je njen minimum bio 2 perpera. Ona se mogla zamijeniti zatvorom, ukoliko se žrtva nije mogla obeštetiti u naturi. Imovinski

delinkventi (lupeži) sankcionisani su gubitkom građanske časti i istovremeno nijesu smjeli nositi oružje. Ostale kazne propisane u zakoniku bile su lišenje zvanja, prolazak kroz redove čete, oduzimanje određene stvari, zabrana izvjesnih radnji, potjera i policijski nadzor (Marinović S.2007:187).

OSNOVNI OBLIK UBISTVA U SAVREMENOM CRNOGORSKOM KRIVIČNOM ZAKONODAVSTVU

Pojam

Osnovni oblik ubistva shodno zakonskoj definiciji *ko drugog liši života, kazniće se zatvorom od pet do petnaest godina* (član 143 KZ CG)[7], obuhvata lišavanje života drugog lica ili preciznije protivpravno lišenje života druge osobe sa umišljajem s obzirom da kod ovog oblika ubistva ne postoje kvalifikovani oblici, privilegovani oblici i posebni slučajevi koji karakterišu druge vidove ove inkriminacije. Biće osnovnog oblika ubistva sadrži šest ključnih segmenata. Prvi je radnja koja obuhvata brojne aktivnosti fokusirane na lišenje života druge osobe. Drugi segment je nastupanje smrti kao posledica inkriminisanih djelatnosti učinioca. Treći segment obuhvata objektivnu uzročnu vezu između radnje i posledice. Protivpravnost lišenje života druge osobe je četvrti segment bića osnovnog oblika ubistva. Peti segment obuhvata živo ljudsko biće kao objekt krivičnopravne zaštite. Šesti konstitutivni element obuhvata umišljaj kao subjektivno obilježje. Radnja, posledica, objekt radnje, objektivna uzročna veza između radnje i posledice i protivpravost su objektivna obilježja, dok je krivica subjektivno obilježje. Postojanje objektivnih i subjektivnog obilježja potrebno je utvrditi u svakom konkretnom slučaju da bi se radilo o krivičnom djelu iz člana 143 KZ CG. Iako se radi o klasičnom i drevnom deliktu poznatom od nastanka ljudskog društva, ovo krivično djelo i danas zaokuplja pažnju naučne i šire javnosti kako zbog svog značaja tako i usljed novih formi i pojačane dinamike ispoljavanja. Iako je nepovredivost života ustavni princip, treba istaći da krivičnopravna zaštita života nije apsolutna kategorija. Postoje odstupanja koja predviđaju dozvoljenost povrede prava na život koja ne sadrže element protivpravnosti koja može biti isključena po opštem i posebnom osnovu. Opšti osnovi se odnose na ubistvo izvršeno u nužnoj odbrani ili ubistvo izvršeno u krajnjoj nuždi. Posebni osnovi tiču se izvršenja smrtne kazne, primjene službenog ovlašćenja i slično. Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda u članu 2 stav 1 predviđa da ni jedno lice ne smije biti namjerno lišeno života osim u slučaju izvršenja smrtne kazne. U sljedećem stavu ovaj dokument propisuje da se lišenje života drugog lica ne smatra protivpravnim ako proizilazi iz upotrebe apsloutno nužne sile radi odbrane određene osobe od nezakonitog nasilja (nasilje je uvijek zloupotreba sile), zatim u cilju izvršenja zakonitog lišenja slobode

7 Krivični zakonik Crne Gore („Sl. List RCG“, br. 70/2003,13/2004 i 47/2006 i „Sl.list CG“, br. 40/2008,25/2010,32/2011, 64/2011, 40/2013, 56/2013,14/2015, 42/2015,44/2017,49/2018 i 3/2020.

ili sprječavanja bjekstva osobe koja je u skladu sa zakonom lišena slobode i tokom preduzimanja legalnih aktivnosti u svrhu suzbijanja nereda ili pobune EKLJP, čl.2).[8]

OBJEKT ZAŠTITE

Objekt zaštite je čovjekov život, odnosno pravo na život kao esencijalno ljudsko pravo, dok je objekt napada živ čovjek čiji život se štiti od trenutka rađanja do trenutka nastupanja smrti i lišenje života u smislu ovog krivičnog djela mora biti izvršeno u tom vremenskom intervalu. U tom kontekstu od fundamentalne važnosti je utvrđivanje započinjanja života i nastupanja smrtnog ishoda jer od toga zavisi postojanje bitnih elemenata ovog delikta. U vezi početka krivičnopravne zaštite života postoji više mišljenja, odnosno različitih stavova (Jovanović Lj. Jovašević D. 1995:111). Shodno ranijim stavovima krivičnopravna zaštita života otpočinje procesom rađanja djeteta, odnosno početkom porođaja (Stojanović Z. 2008:382), prirodnim ili hirurškim putem (Mrvić, Petrović N.2015:19). Ne postoji jedinstven stav po pitanju vrste porođajnih bolova, odnosno da li se radi o bolovima generisanim pritiskom novorođenčeta koje prolazi kroz porođajni kanal što su bolovi napona ili su u pitanju bolovi otvaranja koji se javljaju prije bolova napona (Mrvić Petrović N. 2015:19). Savremena medicinska shvatanja ukazuju na relevantnost bolova otvaranja nezavisno od toga da li su izazvani prirodno ili vještački koji mogu trajati kraći vremenski period u rasponu od nekoliko sati do više dana (Kolarić D. 2008:159). Ovo shvatanje podrazumijeva da dijete još uvijek nije odvojeno od majke jer za trenutak započinjanja rađanja to nije potrebno (Lazarević Lj.Vučković B. Vučković V 2004:340). Procesom odvajanja djeteta od tijela majke započinje krivičnopravna zaštita života (Jovašević D.2017:13).

Relevantne odredbe člana 146 Krivičnog zakonika Crne Gore koje se odnose na krivično djelo ubistvo djeteta pri porođaju upućuju na zaključak da je prihvaćen koncept krivičnopravne zaštite djeteta dok porođaj traje, odnosno prije odvajanja od majke. Iz prethodnog proizilazi da porođaj započinje pojavom porođajnih bolova i kontrakcija kada se radi o porođaju prirodnim putem, a ukoliko je u pitanju carski rez kao hirurška intervencija tada se momenat započinjanja porođaja smatra otvaranje materice (Schonke A. Schroder H. Lenckner T. 2012:118). Shodno stavovima pojedinih autora krivičnopravna zaštita života započinje trenutkom djelimičnog ili potpunog izlaska djeteta iz utrobe majke i da je proces radjanja djeteta otpočeo. Egzistiraju i mišljenja po kojima krivičnopravna zaštita života započnje momentom uspostavljnja plućnog disanja novorođenčeta, nakon prestanka posteljičnog disanja. Za relevantnost krivičnopravne zaštite neophodno je da se novorođenče rađa živo, odnosno da je živo rođeno ukoliko je proces rađanja okončan. U krivičnopravnom

8 Evropska konvencija o ljudskim pravima-EKLJP (European Convention on Human Rights-ECHR),potpisana je u Rimu 1950. godine a stupila je na snagu 1953. godine i danas se smatra najefikasnijim i najstarijim aktom zaštite ljudskih prava na globalnom nivou.

smislu nije relevantna sposobnost za život novorođenčeta. Krivičnopravna zaštita pruža se i djeci koja nemaju izgleda da prežive usljed odstupanja u razvoju jednog tkiva ili dijela organizma što izaziva kasnije defekte na organima čovjeka. Zaštita života ploda u utrobi majke ostvaruje se inkriminacijom nedozvoljeni prekid trudnoće u slučajevima nasilnog uništenja fetusa koji nije sposoban za život. Ukoliko je usljed prekida trudnoće došlo do prijevremenog porođaja i lišenja života novorođenčeta treba riješiti problem razgraničenja najtežih krvnih delikata u odnosu na povredu ploda. U slučaju da je dijete rođeno živo usljed prekida trudnoće a nakon toga usmrćeno kvalifikuje se kao ubistvo (Stojanović Z. 2008:382). U tom slučaju radilo bi se o krivičnom djelu iz člana 144 st.1 tač.6 KZ CG, odnosno ubistvu djeteta kao oblik teškog ubistva.

Kao prestanak života ili određivanje momenta smrti u smislu krivičnopravne zaštite života smatra se cerebralna ili moždana smrt koja podrazumijeva prestanak svih funkcija mozga. U pitanju je biloška smrt kao ireverzibilan proces i od tog trenutka prestaje krivičnopravna zaštita života. Utvrđivanje momenta smrti vrši se primjenom „Harvardskog kriterijuma" prema kojem elektroencefalogram mora najmanje deset minuta pokazivati prestanak električne aktivnosti mozga i da u tom periodu ne postoje druge reakcije (Rakočević V. 2014:34). Entitet moždane smrti fundiran je na sveobuhvatnoj kliničkoj studiji početkom osamdesetih godina prošlog vijeka. Moždane ćelije su najosjetljivije i umiru za samo nekoliko minuta, što nije slučaj sa drugim ćelijama koje mogu biti vitalne i više dana nakon tjelesne smrti. Moždana smrt znači smrt moždanog stabla i kore velikog mozga. To podrazumijeva nepovratni prestanak rada centralnog nervnog sistema kao i kardiovaskularnog i respiratornog sistema. Radi se o biološkoj smrti koja je apsolutna i kada nastupi ni jedan organ čovjeka ne vrši životnu funkciju. Cerebralna smrt podrazumijeva prekid priliva kiseonika u mozak što generiše trajno oštećenje mozga i izumiranja moždanih ćelija. Prema ranijim medicinskim shvatanjima kriterijum gašenja života bila je klinička smrt koja nastaje prestankom rada srca, prestankom disanja i prestankom funkcionisanja krvotoka. Nastupanje kliničke smrti postalo je sporno nakon razvoja savremenih metoda reanimacije koje omogućavaju vještačko održavanje vitalnih životnih funkcija. Prestanak disanja ili srčane aktivnosti kao trenutak smrti pokazao se spornim u smislu sprječavanja transplatacije organa koji moraju vršiti funkciju u momentu presađivanja. Zbog toga je pitanje određivanja trenutka smrti vrlo značajno kako iz ugla krivičnog prava, tako i kada se radi o kadaveričnim transplantacijama organa ili djelova tijela. Presađivanje se može vršiti samo kada je nastupila moždana smrt.

RADNJA

Radnja izvršenja osnovnog oblika ubistva sastoji se u raznovrsnim djelatnostima činjenja ili nečinjenja koje su podesne ili neophodne da prouzrokuju smrt druge osobe

kao posledicu. Zakonodavac je determinisao radnju prema posledici bez kazuističkog pristupa jer bi u slučaju nabrajanja brojnih oblika radnje postojala mogućnost da neka radnja bude izostavljena iz opisa elemenata bića ovog zločina. To je razlog nepostojanja egzaktnog određenja radnje koja nije zakonski determinisana nego putem posledične dispozicije ko drugog liši života, odnosno svaka aktivnost kojom se druga osoba lišava života. Ovaj zločin se najčešće izvršava činjenjem. Najčešći oblici aktivnog djelovanja učinioca su: pucanje, udaranje, zadavljenje, trovanje, spaljivanje, bacanje i slično. Ubistvo nečinjenjem postoji ukoliko je smrt druge osobe generisana propuštanjem dužnog činjenja sa smrtnom posledicom. U pitanju su najčešće delikti nečinjenja kao što su nedavanje hrane nemoćnoj osobi ili uskraćivanje lijeka bolesnoj osobi od strane osoba koje su u obavezi da se o njima staraju što je prouzrokovalo smrt. Ovaj vid ubistva nečinjenjem postoji i kada učinilac sa umišljajem dovede u opasnost žrtvu koja je zbog nepružanja pomoći smrtno stradala, zatim u drugim slučajevima neuklanjanja opasnih stvari, materija ili prepreka od strane osoba čija je to radna obaveza ili službena dužnost. Za sve slučajeve nečinjenja bitan je garantni odnos između učinioca i žrtve koji se sastoji u obavezi učinioca da spriječi nastupanje smrti. Sredstva korišćena prilikom ubistva mogu biti fizička i psihička koja se kombinuju sa različitim načinima izvršenja. U fizička sredstva spadaju kratkocijevno i dugocijevno vatreno oružje, hladno oružje, eksplozivne naprave, oruđa, otrovi, bakteriološka i hemijska sredstva. Fizičkim prouzrokovanje smrti korišćenjem prethodno naznačenih sredstava djeluje se na život i tijelo žrtve. Psihičko prouzrokovanje smrti obuhvata lišenje života izazivanjem izuzetno jakih emocija kod žrtve u vidu ekstremno intenzivnog bola, straha, žalosti ili psihičkog mučenja usljed čega je nastupila smrt kao posledica nastanka šoka koji blokira vitalne životne funkcije. U ovim slučajevima ključno je dokazati kauzalnu vezu između emocija visokog intenziteta i nastupanja smrti. Dokazivanje je otežano i u odnosu na umišljaj kod učinioca ovog delikta (Aleksić Ž. Škulić M. 2004:269). Ubistva se većinom izvršavaju direktnim dejstvom učinioca radnjama činjenja ili propuštanja. U neposredna lišenja života spadaju : pucanje u žrtvu, ubadanje hladnim oružjem, davanje otrova, davljenje, guranje u provaliju i slično. Posredno lišenje života drugog lica obuhvata korišćenje određenog sredstva, odnosno mehanizma uz prethodnu radnju učinioca što prouzrokuje smrtnu posledicu. Ovaj način izvršenja podrazumijeva i lišenje života drugog lica posredovanjem druge osobe ili žrtve. Najčešći primjer ovog načina izvršenja jeste postavljanje eksplozivne naprave na, u ili ispod prevoznog sredstva žrtve koja se aktivira nakon ulaska u vozilo ili nakon stavljanja u pogon vozila. To može biti i kvarenje kočionog ili upravljačkog sistema u vozilu žrtve što usljed saobraćajne nesreće prouzrokuje smrtnu posledicu, zatim podmetanje otrova umjesto lijeka koji žrtva kasnije konzumira, upućivanje paketa ili pisama sa eksplozivnim ili toksičnom sadržinom sa aktiviranjem nakon otvaranja pošiljke i slično. Kao što je prethodno naglašeno protivpravnost radnje ubistva mora da postoji imajući u vidu da ovaj zločin ne postoji ukoliko je do oduzimanja života došlo shodno opštim ili posebim osnovima isključenja protivpravnosti.

POSLEDICA

Posledica osnovnog oblika ubistva je uništenje života, odnosno nastupanje smrti žrtve protiv koje je preduzeta radnja izvršenja ili propuštena radnja sprječavanja smrtne posledice u biološkom smislu. Smrtna posledica može nastupiti odmah nakon izvršenja prve radnje učinioca fokusirane na oduzimanje života druge osobe ili kasnije nakon kraćeg ili dužeg perioda vremena. Važno je istaći da za postojanje ovog krivičnog djela između radnje i posledice mora da postoji objektiva uzročna veza. Iako vrijeme nastupanja smrti nije krivičnopravno relavantno za ovo krivično djelo, ipak, treba naglasiti da ukoliko posledica nastupi kasnije kauzalitet je teže utvrditi.[9] Ukoliko je postojala teška bolest, naknadne povrede ili infekcije sve to može uzrokovati smrtnu posledicu ili ubrzati njen nastanak, a ako bi ovi činioci bili smrtonosni tada se prekida uzročni niz (Jovanović Lj. Jovašević D. 1995:113). Vrlo često smrtnu posledicu može da generiše više činilaca. U slučaju izostanka smrtne posledice djelo se kvalifikuje kao ubistvo u pokušaju pod uslovom da je nesporan subjektivni element, odnosno umišljaj.

KAUZALITET

Od brojnih teorija uzročnosti za utvrđivanje uzročne veze između radnje i posledice referentne su teorija ekvivalencije, teorija adekvatne uzročnosti i teorija objektivnog uračunavanja. Teorija ekvivalencije ili jednakosti uslova se smatra jednom od najznačajnijih u evropskom krivičnom pravu i podrazumijeva da svi uslovi posledice koje nije moguće saznajno eliminisati bez nastupanja posledice su jednaki u vrijednosti zbog čega je svaki od uslova uslov konkretne posledice (Condicio sine qua non). To znači da je kauzalan svaki uslov koji se ne može ignorisati a da posledica ne otpadne (Kühl K.2002:26). Roxin uzročnost interpretira putem zbira svih uslova posledice. Shopdno tome svaki pojedinačni uslov je uzrok posledice bez obzira što je do realizacije posledice došlo njihovim udruženim dejstvom (Roxin C. 1997:294). Prema teoriji adekvatne uzročnosti razmatra se da li određeno ponašanje može dosvesti do krivično pravne posledice pri redovnom slijedu događaja. Iz toga proizilazi da svi događaji koji od toga odstupaju neće se smatrati uzrocima posledice, pri čemu se analizira da li je nastanak posledice statistički moguć (C.von Bar.2000:413). Prema teoriji objektivnog uračunavanja kauzalitet je neophodna pretpostavka da bi se neki delikt mogao objektivno pripisati učiniocu. U prvoj etapi se utvrđuje faktička veza između radnje i posledice, u drugoj etapi se

9 Tokom razvoja ljudskog društva uzročnost je zaokupljala mnoge mislioce od kojih treba posebno istaći jednog od najvećih umova civilizacije stare Grčke Aristotela koji je tvrdio da su uzroci zločina loše imovno stanje, zločinačke pubude i navike kao i društveno uređenje. Ukazivao je na siromaštvo i bogatstvo kao na uzroke koji posredstvom volje i osjećanja vode u kriminalnu aktivnost. Iz ugla krivičnopravne nauke najveće zasluge za eksplikaciju problema uzročnosti pripadaju bez simnje Anselmu Feuerbachu koji je između ostalog formulisao osnovno načelo krivičnog prava-nulum crimen, nula poene sine lege.

utvrđuje normativna veza između ova dva elementa a u trećoj realizovan uzrok u vidu posledice krivičnog djela.

Predstavnici empirizma smatrali su da je uzročnost derivat prirodne nužnosti kao ishod prethodnih događaja. Racionalistički pravac predvođen Descrtesom i Humeom smatrao je uzročnost kompleksnim pitanjem od posebne važnosti. Za jednog od najznačajnijih predstavnika klasične filozofije Immanuela Kanta kauzalitet je a priori sintetički sud i ne izvodi se iz empirije (De Pierris, G. Friedman, M. 2008:58). Autori koji su za osnovu uzimali kauzalni deteminizam koji je polazio od uzročnog niza smatrali su da svaki proces sa istim startnim uslovima dovodi do istog rezultata što je osporeno pojavom kvantne fizike. To je dovelo do pojave probabilističkog koncepta kauzaliteta baziranog na subatomskom indeterminizmu (Martinović I. 2012/77). Koncept kvantne fizike polazi od postojanja neizvjesnosti u univerzumu i determinisanosti saznajnih kapaciteta čovjeka.[10] Postoje tri funkcije uzročnosti u pravu i to atributivna, eksplanatorna i prediktivna (Hart H.L.A., Honoré, A.M., 1956:398). Prediktivna funkcija (forward-looking function) kauzaliteta sadrži predikciju u vezi budućih dešavanja ukoliko su ispunjeni određeni uslovi. Imajući u vidu da je krivično pravo fokusirano na izvršeno krivično djelo prediktivna funkcija nije primarna. Eksplanatorna funkcija kauzaliteta (backward-looking function) sastoji se u analizi koji prethodni događaj egzaktno pojašnjava kasniji događaj u vezi određenja šta se desilo kao i načina i motiva izvršenja. Ova funkcija se ostvaruje implementacijom naučnih pravila prilikom utvrđivanja činjenica na koje se oslanja krivično pravo putem principa i procedura kreirajući pravno dejstvo. U literaturi se često ističe primjer vozača automobila koji prelazi preko pješaka koji leži na putu a ekspertizom se ne može utvrditi je li lice bilo živo u momentu gaženja. Slična je situacija i kada je u pitanju korišćenje lijeka za spavanje tokom trudnoće što može generisati probleme u embrionu ploda. U tim slučajevima se primjenjuje princip in dubio pro reo, odnosno da kauzalitet ne postoji. Iz ugla krivičnog prava najznačajnija je atributivna funkcija uzročnosti koja promjene u spoljašnjem svijetu pripisuje određenom licu jer događaje tretira kao ishod uticaja pojedinca i sastavni je dio procesa vrednovanja. Radi se o shvatanjima njemačke krivičnopravne teorije koja zastupa odvojenost normativnog ocjenjivanja od empirijski saznatog sadržaja. Uzročnost se dijeli na učenje o kauzalnoj vezi (die Lehre von Kausalzusammenghang) i objektivno uračunavanje. Evidentno je da se kauzalitet svodi na formulu condicio sine qua non a doktrina o uzročnoj vezi na formuli nužnog uslova.(Roxin, C. 2006:354).

10 Teorija determinističkog haosa polazi od senzitivnosti linearnih sistema na startne uslove. To znači da čak i minimalna razlika u startnim uslovima prouzrokuje divergenciju dva i više sistema, odnosno minimalna razlika u početnim uslovima generiše značajno drugačiji rezultat. Edward Lorenz je to definisao kao butterfl y effect (učinak leptira), a radi se o metafori shodno kojoj mahanje krilima ovog insekta u Brazilu može dosvesti do uragana u Teksasu.

KRIVICA

Subjektiva dimenzija ovog zločina je vrlo kompleksna budući da pored umišljaja i nehata sadrži namjeru i motiv. U pogledu krivice za ostvarenje krivičnog djela ubistva potreban je umišljaj direktni ili eventualni, odnosno da je učinilac bio svjestan da lišava života drugu osobu i hoće izvršenje ubistva ili kada je bio svjestan da može izvršiti ubistvo pa je na to pristao. U zavisnosti od stepena svijesti i stepena volje kod učinioca u odnosu na krivično djelo ubistvo krivica će se reflektovati u vidu direktnog ili eventualnog umišljaja. Ukoliko se utvrdi da nema umišljaja djelo će se kvalifikovati kao nehatno lišenje života, odnosno privilegovano ubistvo. Imajući u vidu da je ovo krivično djelo koncipirano putem posljedične norme postojanje umišljaja se utvrđuje na osnovu objektivnih elemenata. U svakom konkretnom slučaju se utvrđuju sve relevantne okolnosti sa akcentom na radnju izvršenja, koja treba da je slobodno preduzeta tj.bez prinude, shodno vlastitoj volji uračunljive osobe. Krivica mora postojati u vrijeme preduzimanja radnje, odnosno kada je trebalo preduzeti radnju pri čemu je irelevantno vrijeme nastupanja posledice. Povrede vitalnih organa kao što su srce i mozak, zatim način i sredstva izvršenja i druge okolnosti cijene se prilikom utvrđivanja umišljaja. U praksi nije sporno da postoji direktni umišljaj ako učinilac iz neposredne blizine iz vatrenog oružja puca u glavu žrtve, dok bi eventualni umišljaj postojao ukoliko učinilac pristane na nastupanje posledice, kao npr. ako učinilac tupim predmetom zada udarac u glavu žrtvi svjestan da je može usmrtiti i pristaje na nastupanje posledice. Učinilac je predvidio mogućnost nastajanja posledice budući da krivica sadrži tri elementa i to radnju, posledicu i kauzalni odnos. Direktni umišljaj je teži oblik krivice koje se manifestuje u jačem stepenu volje u odnosu na eventualni. Umišljajne djelatnosti nema bez motivacije kao baze svake voljne ljudske radnje. Motiv je akter koji generise radnju i fokusira je prema cilju (Jovanović Lj. 1972:65). Prema stavu sudske prakse namjera da se neka osoba liši života nije subjektivni element ovog zločina jer je za njegovo postojanje dovoljno da egizistira umišljaj. Motiv nije zakonsko obilježje ubistva ali je značajan kako za rješavanje zločina izvršenog od strane nepoznatog lica tako i za odmjeravanje kazne učiniocu. Imajući u vidu da direktni umišljaj predstavlja viši stepen krivice u odnosu na eventualni to može biti značajno iz ugla učinioca zbog uticaja na visinu kazne.

Na sadržaj umišljaja kod osnovnog oblika ubistva utiču namjera, cilj i motiv iako to ne proizilazi iz zakonske definicije ovog oblika krivice. Namjera usmjerava djelovanje učinioca delikta prema ostvarenju cilja koji namjerava postići zbog čega između ova dva subjektivna elementa postoji povezanost. Treba naglasiti da cilj koji učinilac želi ostvariti može da nadilazi smrtnu posledicu kao prethodnu fazu za postizanje glavnog cilja kao što je slučaj kod ostvarivanja naslednih prava. Stoga namjera može biti okolnost koja je značajna za odmjeravanje kazne učiniocu bez obzira na činjenicu da nije bitan element osnovnog oblika ubistva. Pojedini autori smatraju da je cilj objektivni fenomen koji se reflektuje u svijesti osobe Srzentić N. Stajić A. Lazarević

Lj. 1997:266). Cilj može biti krivično pravno relevantan kod pojedinih oblika teškog ubistva u odnosu na pobude, dok se kod osnovnog oblika ove inkriminacije uzima u obzir prilikom odmjeravanja kazne. Između motiva i pobuda ne postoji razlika osim u nazivu imajući u vidu da pobude obuhvataju motiv izvršenja objašnjavajući razloge izvršenja ubistva (Delić N. 1988:75). Motiv ima ogroman značaj za rasvjetljavanje krivičnog djela iako nije njegovo obilježje a ukoliko motiv nije moguće utvrditi to nema uticaja na postojanje ovog zločina. On se javlja kao privilegujuća ili kvalifikatorna okolnost. Može imati krivično pravni značaj ali ne i da bude integralni dio kvalifikacije krivičnog djela (Kolarić D.,2012:290). U okviru opštih pravila o odmjeravanju kazne ovo subjektivno obilježje može biti od značaja što je propisano u članu 42 KZ CG koji predviđa da će sud učiniocu krivičnog djela odmjeriti kaznu u zakonskim granicama polazeći od svrhe kažnjavanja i otežavajućih i olakšavajućih okolnosti a naročito stepena krivice, pobuda iz kojih je djelo učinjeno i slično.

OSTALI ELEMENTI

Osnovni oblik krivičnog djela ubistva je dovršen nastupanjem smrti kod druge osobe. Ukoliko nije nastupila smrtna posledica djelo se kvalifikuje kao ubistvo u pokušaju koje je kažnjivo iako posledica nije nastupila. Ukoliko je prilikom ubistva u pokušaju ostvaren kvalifikovani pokušaj može se raditi o idealnom sticaju sa ubistvom u pokušaju i prividnom idealnom sticaju u vidu konsumpcije kao što je u slučaju povrede tijela pri čemu učinilac odgovara za težu kvalifikaciju a tjelesna povreda utiče na visinu kazne.

U vezi dejstva stvarne zablude o licu u situacijama kada je umišljaj usmjeren na lišenje života jednog lica a došlo je do smrtne posledice u odnosu na drugu osobu treba istaći da je ova vrsta zablude krivično pravno irelevantna iz ugla umišljaja.

Ovaj oblik krivičnog djela postoji samo ako je ostvaren protivpravno. Protivpravnost ne postoji ukoliko je postupano u nužnoj oedbrani, krajnjoj nuždi, prilikom izvršenja smrtne kazne ili korišćenja sredstava prinude od strane ovlašćenih lica.

Učinilac osnovnog oblika ubistva može biti svaka osoba. Za ovo krivično djelo predviđena je kazna zatvora od pet do petnaest godina.

ZAKLJUČAK

Pravo na život je temeljno ljudsko pravo i najveća vrijednost moderne civilizacije. U svim savremenim državama ono se štiti najvišim pravnim aktima kao najznačajnije ljudsko pravo. Krivično pravo upravo ovoj najvećoj vrijednosti pruža primarnu

i suverenu krivično pravnu zaštitu. Ubistvo kao protivpravno lišenje života drugog lica ljudskom radnjom manifestuje se u vrlo različitim formama. Objekt radnje je živ čovjek od početka rađanja do trenutka nastupanja smrti kada može biti izvršeno ovo krivično djelo. Radnja izvršenja nije precizno određena imajući u vidu brojne mogućnosti lišenje života. Iz toga proizilazi da to može biti svaka svaka radnja podobna da prouzrokuje smrt druge osobe. Posledica obuhvata nastupanje smrti osobe protiv koje je preduzeta inkriminisana aktivnost, odnosno propuštena dužnost preveniranja nastupanja smrtne posledice. Kauzalitet kod ovog krivičnog djela zahtijeva utvrđivanje objektivne uzročne veze. Pokušaj je kažnjiv i postoji kada posledica nije nastupila. U pogledu krivice kod osnovnog oblika ubistva moguć je direktni i eventualni umišljaj.

LITERATURA

1. Aleksić Ž. Škulić M. (2004). Kriminalistika, Dosije, Beograd.
2. Bojović J. (1982). Zakonik knjaza Danila, Titograd.
3. Dragović M. (1895). Spomenik XXI: Materijal za istoriju Crne Gore, SKA, Beograd.
4. Delić N. (1988). Kvalifikovana/teška ubistva (motiv-pobude), Zbornik radova Ubistva i samoubista u Jugoslaviji, Srpsko udruženje za krivično pravo, Kopaonik.
5. De Pierris, G. i Friedman, M.,(2008). Kant and Hume on Causality, The Stanford Encyclopedia of Philosophy.
6. Evropska konvencija o ljudskim pravima-EKLJP (European Convention on Human Rights-ECHR),1950. Rim.
7. Zakonik Danila I knjaza i gospodara slobodne Crne Gore i Brdah,1855. Cetinje.
8. Jevtić D. Popović D. (1997).Narodna pravna istorija, Beograd.
9. Jovanović J. (1995) Istorija Crne Gore, Podgorica.
10. Jovanović Ljubiša (1972). Motiv i vinost, Zbornik Pravnog fakulteta u Nišu.
11. Jovanović Ljubiša, Jovašević Dragan, (1995). Krivično pravo II posebni deo, Beograd.
12. Jovašević D. (2017). Krivična dela ubistva, Institut za kriminološka i sociološka istraživanja, Beograd.
13. Kolarić D. (2008). Krivično delo ubistva, Službeni glasnik, Beograd.
14. Kolarić D. (2012). Biće krivičnog dela ubistva, Pravni život, br. 8/12.
15. Kühl, Kristian: Strafrecht. Allgemeiner Teil, IV, Verlag Franz Vahlen, München, 2002.
16. Krivični zakonik za Knjaževinu Crnu Goru, 1906. Cetinje.
17. Krivični zakonik Crne Gore „Sl. List RCG“, br. 70/2003,13/2004 i 47/2006 i „Sl. list CG“, br.40/2008,25/2010,32/2011,64/2011,40/2013,56/2013,14/2015,42/2015,44/2017,49/2018 i 3/2020.

18. Lazarević Lj. Vučković B. Vučković V. (2004). Komentar krivičnog zakonika Crne Gore, Obod, Cetinje.
19. Marinović S. (2007). Kaznena istorija Crne Gore, Podgorica.
20. Martinović I. (2012). Problem uzročnosti u kaznenom pravu, Hrvatski ljetopis za kazneno pravo i praksu (Zagreb), vol. 19, broj 1/2012.
21. Milićević J. Rakočević N. (1986). Crna Gora od 1735-1797, Beograd.
22. Mrvić, Petrović N. (2015). Krivično pravo Posebni deo, Pravni fakultet Univerziteta Union u Beogradu i Javno preduzeće Službeni glasnik, Beograd.
23. Universal declaration of Human Rights (Univerzalna deklaracija o ljudskim pravima), usvojena od strane Generalne skupštine Ujedinjenih nacija (A/RES/217, 1948, Pariz.
24. Međunarodni pakt o građanskim i političkim pravima, usvojen rezolucijom Generalne skupštine 2200 A (XXI) od 16. decembra 1966, stupio na snagu 23 marta 1976.
25. Petrović R. (1929). Zakonik Petra I vladike crnogorskog, Istorijsko-pravna rasprava, Cetinje.
26. Rakočević V. (2014). Krivična djela sa elementima organizovanog kriminaliteta, Podgorica.
27. Roxin, C. (1997). Strafrecht. Allgemeiner Teil. Band I. Grundlagen. Der Aufbau der Verbrechenslehre, III, C. H. Beck´sche Verlagsbuchhandlung, München.
28. Roxin, C.,(2006). Strafrecht – Allgemeiner Teil, sv. I., Verlag C. H. Beck, München.
29. Stega crnogorska i brdska, 1796. Cetinje.
30. Srzentić N. , Stajić A. Lazarević Lj. (1997). Krivično pravo-opšti deo, Beograd.
31. Stojanović P. (1982). Zakonik vladike Petra I i Danilov zakonik, Istorijsko-pravna studija, Cetinje, str.1-30.
32. Stojanović Z. (2008). Krivično pravo, CID, Podgorica.
33. Schonke, A., Schroder, H., Lenckner, T., et. al. (2012) Strafgesetzbuch StGB. Munchen: Deutscher Taschenbuch Verlag, 50. Auflage, p.118.
34. Ustav Crne Gore, „Sl.list CG“, br. 1/2007 i 38/2013-Amandmani I-XVI).
35. Hart, H.L.A., and Honoré, A.M., (1956), "Causation in the Law", Law Quarterly Review, 72(1): 58–90, 72(2): 260–281, 72(3): 398–417. 1959, Causation in the Law, Oxford: Oxford University Press.1985, Causation in the Law, second edition, Oxford: Oxford University Press. doi:10.1093/acprof:oso/9780198254744.001.0001
36. C. von Bar,(2000). The Common European Law of Torts, Volume Two, Claredon Press, Oxford.

UDK 343.98:004.8

MOŽE LI VJEŠTAČKA INTELIGENCIJA ZAMIJENITI RAD FORENZIČARA?

CAN ARTIFICIAL INTELLIGENCE REPLACE THE WORK OF A FORENSIC SCIENTIST?

Prof. dr Aleksandar B. Ivanović
Uprava policije Crne Gore

Dr Nikola Terzić
Ministarstvo unutrašnjih poslova Crne Gore

Apstrakt

U ovom radu će biti pokrenuto pitanje: može li vještačka inteligencija zamijeniti rad sudskog vještaka-forenzičara? Biće prezentovani pozitivni aspekti primjeni vještačke inteligencije u jednoj veoma važnoj oblasti kao što je angažman sudskog vještaka-forenzičara u pravosudnom postupku. Osim pomenutog u radu će biti dat i osvrt na oprezan pristup primjene vještačke inteligencije u radu forenzičara, a to se najviše i uglavnom odnosi na njen etički aspect. Dalje, ovaj rad sadrži u sebi i jedan jedinstven predlog, a isti se odnosi na uvođenje u sudsku praksu instituciju-Forenzičar vještačke inteligencije! Na kraju rada je dat i jedan konkretan primjer iz prakse autora, koji se odnosi na mogućnost primjene vještačke inteligencije kod vještačenja tragova vatrenog oružja.
Ključne riječi: *vještačka inteligencija, forenzičke nauke, forenzičar vještačke inteligencije*

Abstract

In this paper, the question will be raised: can artificial intelligence replace the work of a court expert-forensic expert? The positive aspects of the application of artificial intelligence in a very important area such as the involvement of a court expert-forensic expert in judicial proceedings will be presented. In addition to the aforementioned, the paper will also review the cautious approach to the application of artificial intelligence in the work of forensics, and this mostly and mainly refers to its ethical aspect. Furthermore, this paper also contains a unique proposal, and it refers to the introduction into court practice of the institution - Forensic Artificial Intelligence! At the end of the paper, a concrete example from the author's practice is given, which refers to the possibility of applying artificial intelligence in the examination of traces of firearms.
Keywords: artificial intelligence, forensic science, artificial intelligence forensic scientist.

UVOD

Opšte je poznata uloga i značaj forenzike i forenzičkih nauka u društvu. Svako savremeno društvo teži da se zasniva na pravdi, bezbjednosti i slobodi. Svaki od navedenih segmenata društvene vrijednosti zasniva se na nezavisnom i modernom pravosuđu. Savremeno pravosuđe podrazumeva primjenu sofisticiranih forenzičkih tehnika i tehnologija. Sva tri navedena segmenta naprednog demokratskog društva zavise od kvaliteta primjene forenzičkih nauka u pravosuđu. Nema pravde, bezbednosti, a pogotovo slobode građana, ako im društvo ne obezbijedi pravosudni sistem na kome se dokazi i činjenice zasnivaju na ponovljivim, proverljivim i međunarodno usaglašenim forenzičkim analizama, ispitivanjima i vještačenjima. Rad na vještačenju i upoređivanje otisaka prstiju, rukopisa, tragova vatrenog oružja (čaura, projektila...), tragova obuće, tragova stakla, fotografija i video snimaka sa mjesta zločina i raznih forenzičkih tragova, zahtijeva dugo, često iscrpljujući i zahtjevan angažman sudskog vještaka, pa se ponekad (ne)opravdano postavlja pitanje da li tako dugotrajan, iscrpljujući rad može dovesti do grešaka usled umora i/ili drugih okolnosti? Pogotovo kada se primenjuju subjektivne forenzičke metode, da li je moguće posumnjati da je forenzičar bio umoran, pristrasan, emotivan i/ili pod bilo kojom vrstom predrasuda, tokom forenzičkih analiza, ispitivanja i vještačenja? Tu dolazimo do jednog (ne)opravdanog pitanja, da li bi se otklanjanje ove vrste (ne)opravdanih nedoumica primjene forenzičkih nauka u pravosuđu, riješilo primjenom vještačke inteligencije!

U savremenom svijetu, vještačka inteligencija nije samo tehnološki trend ili savremeni hir, već je to pojam koji nezadrživo ulazi u sve sfere društvenog živora i po

mišljenju autora ovog rada, vještačka inteligencija predstavlja napredak u budućnosti čovječanstva.

Prilikom definisanja pojma vještačke inteligencije prva je reagovala Evropska unija, pa su stručnjaci Evropske komisije to definisali kao: „Sistemi vještačke inteligencije su softverski (i eventualno hardverski) sistemi koje su razvili ljudi, a imaju složen cilj da delovanje u fizičkoj ili digitalnoj dimenziji, prikupljanje podataka o životnoj sredini, tumačenje prikupljenih i sistematizovanih ili nesistematizovanih podataka o obliku zaključivanja na osnovu prethodno stečenog znanja, odnosno rezultata obrade novih informacija i sposobnosti donošenja odluka na najbolji način. delovanja u odnosu na postizanje cilja koji je ta osoba postavila. Ovakvi sistemi vještačke inteligencije mogu da prate pravila koja je postavio programer, da konstruišu digitalni model određenog procesa ili pojave, a mogu i da menjaju sopstveno ponašanje, prilagođavajući ga okruženju. uslovi koji su se promenili kao rezultat prethodno savršenih radnji"[1].

Vještačka inteligencija u forenzičkim naukama može se primijeniti za obradu i analizu velikih količina podataka, a akcenat je na interpretaciji podataka. Vještačka inteligencija pomaže da se prevaziđu nedostaci forenzičke istrage i ljudske greške, ali prvenstveno da se unaprijedi, ubrza i olakša istraga (Ahmed Alaa El-Din, 2022; Budić, 2022; Budić, 2023; Gupta, Sharma i Johri, 2020; Jadhav, Sankhla i Kumar, 2020). Forenzičke nauke zahtijevaju analizu velike količine složenih podataka, dok vještačka inteligencija nudi rješavanje problema u realnom vremenu i prostoru, štedeći vrijeme forenzičara, a istovremeno i sudske postupke u pojedinačnim slučajevima. Iako bi se vještačka inteligencija u forenzičkim naukama koristila u svim forenzičkim disciplinama, njena primjena bi najviše i uglavnom bila zastupljena prilikom rekonstrukcije mjesta zločina, upotrebe 3D skenera, a zatim i u analizi DNK dokaza, analizi otisaka prstiju (daktiloskopija), forenzička odontologija, forenzička balistika i otkrivanje tragova vatrenog oružja, toksikologija i analiza narkotika (Ahmed Alaa El-Din, 2022, str. 24-26).

PRIMJENA VJEŠTAČKE INTELIGENCIJE U FORENZIČKIM NAUKAMA

Jedan od ciljeva forenzičkih analiziranja, ispitivanja i vještačenja bi bio da se pri radu forenzičara, bilo kakva vrsta greške svede na najmanju moguću mjeru. Tu se najviše i uglavnom misli na "ljudske greške", koje mogu biti izazvane umorom i/ili gubitkom koncentracije kod forenzičara. U vezi pomenutog, a obzirom da se vještačka inteligencija kao oblast veoma intenzivno razvija i nalazi primjenu u svim domenima savremenog života, smatra se da ista može naći veliku primjenu u forenzičkim nau-

1 Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). Adopted on: 22/05/2019. Amended on: 08/11/2023. OECD, 2024. URL: https://legalinstruments. oecd.org/en/instruments/oecd-legal-0449

kama kao "nepristrasni saradnik"[2] te osim eliminisanja eventualnih greški i gubitka koncentracije pri radu forenzičara, vještačka inteligencija isključuje svaku vrstu pristrasnosti i predrasuda!

Osnova primjene vještačke inteligencije u forenzičkim naukama je digitalna forenzika koja se zasniva na kompleksnoj analizi baza podataka. Koliko je kompleksna primjena digitalne tehnike i tehnologije pri analizi forenzičkih podataka, vidimo na primeru DNK baze podataka Velike Britanije, koja sadrži preko 4,5 miliona uzoraka, kako osuđenih, tako i nevinih lica koja su osumnjičena[3]. Međutim, osim pomenutog vještačka inteligencija ima (ili može imati) primjenu prilikom:

- Otisaka prstiju; Prednosti vještačke inteligencije čine je prikladnom za različite zadatke u sistemima automatske identifikacije i klasifikacije otiska prsta. Takođe, ovi automatizovani sistemi temeljeni na vještačkoj inteligenciji mogu značajno smanjiti broj poređenja i vrijeme identifikovanja s visokom točnošću. Dalje, pomoću latentnih otisaka prstiju, forenzički istraživači su razvili sistem vještačke inteligencije pomoću kojeg, između ostalog mogu razlikovati i klasifikovati uzorke otisaka prstiju i odrediti dob, pol i druga antropološka obilježja kroz komponente znoja[4].
- Forenzičko medicinskih vještačenja; Mogućnosti veštačke inteligencije u forenzičkoj medicini mogu naći primjenu u polju prepoznavanja lica, analize otisaka prstiju, ali i analizi autopsije putem slika, gde bi se od sistema očekivao doprinos pri utvrđivanju uzroka smrti. Između ostalog bi primjena vještačke inteligencije u medicinskoj forenzici imala mogućnost utvrđivanja starosti putem analize zuba, kostiju i/ili lica i drugih segmenata medicinske forenzike[5].
- Analiziranja rukopisa; Vještačka inteligencija može da se koristi za prepoznavanje i upoređivanje različitih slika uzoraka potpisa ili rukopisa. Neki algoritmi prepoznavanja uzoraka i modeli neuronskih mreža AI pomažu stručnjacima da prepoznaju pol skriptora (autora rukopisa)[6].
- Balističkih analiza; Vještačka neuronska mreža može biti od pomoći forenzičkim ekspertima u slučajevima analiziranja i upoređivanja tragova barutnih čestica, tragova na čaurama, zatim kod upoređivanja tragova projektila, identifikacije vatrenog oružja i drugih balističkih dokaza iz same baze podataka uz pomoć obrade

2 M. Janković, R. Radovanović, Milica Janković (2024). Prilog analizi upotrebe vještačke inteligencije u forenzici. LXVIII Konferencija ETRAN, Niš 2024.

3 M. Andrejević (2012). Značaj forenzičke DNK analize u pravosudnom sistemu. Strani pravni život 2/2012.

4 Zhou, Z. & Zare, R. N. (2017). Personal information from latent fingerprints using desorption electrospray ionization mass spectrometry and machine learning. Analytical Chemistry, 89(2), 1369–1372. https://doi.org/10.1021/acs.analchem.6b04498

5 M.Vodanović, M. Subašić, D.Milošević, I. Galić, H. Brkić, „.Artificialintelligence in forensic medicine and forensic dentistry" J ForensicOdontostomatol. 2023 Aug 27;41(2):30-41. PMID: 37634174; PMCID:PMC10473456.

6 Kulik, S. D. (2015). NEURAL NETWORK MODEL OF ARTIFICIAL INTELLIGENCE FOR HANDWRITING RECOGNITION. Journal of Theoretical & Applied Information Technology, 73(2).

slike u kom slučaju bi se izbjegle subjektivne metode[7].

- Obrade slike i analize video zapisa; Veliki broj forenzičkih istraživača je razvio algoritme koji pomoću vještačke inteligencije obavljaju prepoznavanje lica pomoću analize fotografija i video zapisa[8].
- Prepoznavanje odjeće; Prepoznavanje odjeće je metoda koja se može koristiti u slučajevima kada nemamo na raspolaganju metode identifikacije lica i druge biometrijske dokaze. Identifikacijom pomoću odjevnih predmeta možemo doći do podataka koji obično odražavaju pol, dob i društveni status. U cilju pomenutog istraživanja koristi se DCNN (Deep Convolutional Neural Network) koji posjeduje mogućnost da klasifikuje snimke odjeće na osnovu kvaliteta i razlikovanja specifičnih karakteristika kao što su logotipi I slično[9].
- Forenzička toksikologija; Širenje hemijskih baza podataka i potreba za širenjem obima pretraživanja predstavlja izazov prilikom istraživanja zloupotrebe opojnih droga i nelegalnih supstanci. Automatizovana hemikalija analiza je omogućila identifikaciju jedinjenja i dostupnost dotada nezamislive količine informacija. Do 2020. Chemical Abstract Service (CAS) imao je više od 160 miliona organskih i neorganskih jedinjenja u svojim bazama podataka. Istraživanje ovako velike količine podataka zahtijeva primjenu vještačke inteligencije sa ciljem preciznosti, tačnosti i blagovremenosti prilikom poređenja i identifikacije[10].
- Analiza raznih vrsta forenzičkih baza podataka; Konvencionalni i ručni pristupi za pretraživanje i ispitivanje raznih vrsta forenzičkih podataka teško da mogu biti kompetentni, operativni, efektni i efikasni. Primjena vještačke inteligencije u cilju analiziranja i povezivanja podataka iz forenzičkih baza, smanjuju količinu podataka koje treba forenzičar lično da analizira i u realnom vremenu daju podskup koji će istražiteljima biti od koristi za traženu identifikaciju[11] (Hoelz et. al., 2009.).
- Forenzički 3D; Rekonstrukcija izrađena pomoću 3D metode je nova praktična metoda u forenzičkiom naukama koja podrazumijeva intedisciplinarnu saradnju i može naći primjenu u razrješavanju u rasvjetljavanju raznih vrsta krivičnih djela. Primjena 3D tehnologije i vještačke inteligencije može da se, između ostalog koristi za pojedine faze forenzičke vizualizacije. Takođe, pomoću vještačke inteligencije možemo automatski kreirati 3D grafičke modele i animacije kako bi omogućili interaktivnost rekonstruisanih situacija u stvarnom vremenu. Simulacija virtualne stvarnosti u forenzičkom procesu uključuje grafičko modeliranje 3D virtualnih objekata i ljudi na osnovu mjerenja i fotografija te vrši animaciju mo-

7 Swapnil R. Kamdar and Astha Pandey, "The Scope of Artificial Intelligence in Forensic Science", The Indian Police Journal, July-September, 2011, Vol. -58 Issue-3

8 Kasar, M. M., Bhattacharyya, D., & Kim, T. H. (2016). Face recognition using neural network: a review. International Journal of Security and Its Applications, 10(3), 81-100.

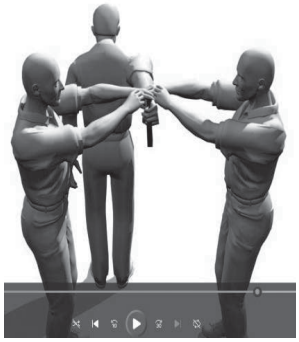
9 Bedeli, M., Geradts, Z. & van Eijk, E. (2018). Clothing identification via deep learning: forensic applications. Forensic Sciences Research, 3(3), 219–229.

10 Gasteiger, J. (2020). Chemistry in times of artificial intelligence. Chemphyschem: a European journal of chemical physics and physical chemistry, 21(20), 2233–2242. https://doi.org/10.1002/ cphc.202000518

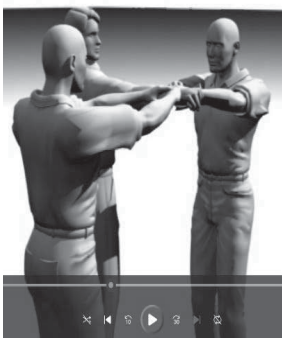
11 Hoelz, B. W., Ralha, C. G., & Geeverghese, R. (2009, March). Artificial intelligence applied to computer forensics. In Proceedings of the 2009 ACM symposium on Applied Computing (pp. 883-888).

dela za ponovno rekonstruisanje lica mjesta krivičnog djela[12]. U cilju pomenute primjene 3D tehnologije i vještačke inteligencije za pojedine faze forenzičke vizuelizacije, navešćemo jedan primjer iz prakse autora ovog rada. Naime, prije skoro 15-ak godina (!) u jednom krivičnom djelu zloupotrebe vatrenog oružja gdje je jedan od koautora ovog rada bio angažovan u svojstvu sudskog vještaka da na odjevnom predmetu lica koje je izvršilo krivično djelo ubistvo iz vatrenog oružja, izvrši vještačenje prisustva barutnih čestica. Nakon tog ispitivanja, naredbom od strane sude je traženo od istog vještaka da se izjasni da li se detektovani tragovi barutnih čestica nalaze sa prednje il isa zadnje strane odjevnog predmeta lica koje je izvršilo ovo teško krivično djelo iz vatrenog oružja. Ta konstatacija bi bila od velike važnosti za razrješavanje predmetnog slučaja iz razloga što se osumnjičeni u ovom slučaju branio izjavom da su ga dva lica tom kritičnom prilikom, povlačili za ruku u kojoj je držao vatreno oružje (pištolj) i da je iz tog razloga ispaljenje projektila izvršio kada mu je ruka bila iza leđa i da samim tim nije mogao vidjeti žrtvu niti imati namjeru da izvrši krivično djelo ubistvo! Pomenuta lica koja su se sa osumnjičenog povlačili za ruku u kojoj je držao vatreno oružje (pištolj) izjavljivali su suprotno: da je osumnjičeni izvršio ispaljenje projektila sa ispruženom rukom ispred sebe i da je jasno mogao da vidi žrtvu u koju je pucao! Kako se, nakon završenog vještačenja, prikaz nalaza barutnih čestica na odjevnom predmetu osumnjičenog za izvršenje krivičnog djela izvršenog ispaljenjem projektila iz vatrenog oružja ne bi mogao precizno i korektno predstaviti u 2D formi iz razloga što su se dokazane barutne čestice najviše i uglavnom nalazile sa desne bočne strane (ispaljenje je izvšeno desnom rukom) to se ne bi moglo u mišljenju predmetnog vještačenja sa preciznošću konstatovati da su barutne čestice nađene sa prednje, a takođe ni sa zadnje strane. Da bi sa korektnošću i preciznošću odgovorio na naredbu suda i da bi pružio što veći doprinos rasvjetljavanja predmetnog krivičnog djela, koautor ovog rada je kao sudski vještak u ovom predmetu izradio 3D prezentaciju nalaza detektovanih barutnih čestica na odjevnom predmetu osumnjičenom. Nakon toga je vještak izvršio probna opaljenja koja su podrazumijevala situaciju kada je opaljenje izvršeno sa rukom ispruženom prema predjelu leđa (po izjavi osumnjičenog) i kada je opaljenje izvršeno sa rukom ispruženom sa prednje strane strane tijela udesno (po izjavama lica koja su se povlačila sa rukom osumnjičenog). Na osnovu prezentovanih, nađenih barutnih čestica na odjevnim predmetima u obije situacije nakon izvršenih probnih ispaljenja i upoređivanjem njihove disperzije (rasipanja i rasporeda) sa izazvanim barutnim česticama na odjevnom predmetu osumnjičenog, sud je mogao da uz druge dokaze u ovom predmetu dođe do pravog i preciznog zaključak. Na sledećim slikama je prikazan dio pomenutog nalaza uz napomenu da format ovog rada ne može da prikaže 3D animacije koje je sudski vještak, kao prilog Izvještaja o vještačenju, predao sudu na CD disku u formi video sadržaja.

12 Ma M, Zheng H, Lallie H. Virtual reality and 3D animation in forensic visualization. J Forensic Sci. 2010 Sep;55(5):1227-31. doi: 10.1111/j.1556-4029.2010.01453.x. Epub 2010 Jun 8. PMID: 20533989.

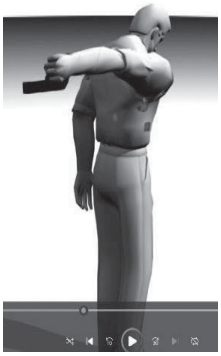


Slika broj 1



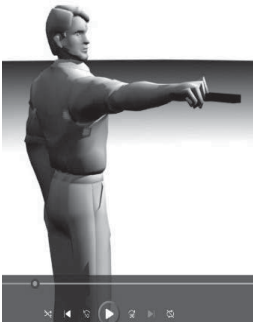
Slika broj 2

Slika broj 3



Slika broj 4

Slika broj 5



Slika broj 6

Na slici broj 1 je prikazana situacija ispaljenja projektila po izjavi osumnjičenog, dok je na slici broj 2, prikazana situacija po izjavi svjedoka. Slika broj 3, predstavlja položaj na kojem su nađene barutne čestice na ruci prilikom ispaljenja projektila nakon situacije predstavljene na slici broj 1. Slika broj 4, predstavlja položaj na kojem su nađene barutne čestice na tijelu prilikom ispaljenja projektila nakon situacije predstavljene na slici broj 1. Slika broj 5, predstavlja položaj na kojem su nađene barutne čestice na ruci prilikom ispaljenja projektila nakon situacije predstavljene na slici broj 2. Slika broj 6, predstavlja položaj na kojem su nađene barutne čestice na tijelu prilikom ispaljenja projektila nakon situacije predstavljene na slici broj 2.

Nakon gore prezentovanog primjera, predlog za primjenu vještačke inteligencije bio bio da se u ovakvim i sličnim slučajevima pristupi izradi baze podataka koja bi sadržavala raspored barutnih čestica na odjevnim predmetima prilikom raznoraznih situacija koje bi mogle da se dese u praksi i da nakon upoređivanja sa disperznim rasporedom barutnih čestica u konkretnom slučaju daju odgovore na pitanja koja bi bila od koristi za rasvjetljavanje ovih i sličnih krivičnih djela izvršenih vatrenim oružjem.

Osim pomenutih forenzičkih disciplina, vještačka inteligencija može naći primjenu i kod analiziranja tragova obuće, dlake i kose, tragova vlakana, ali i prilikom analize samih tragova. Analiza tragova je dugotrajan, subjektivan proces i zavisi od ljudskog faktora. Prilikom analiziranja tragova, forenzičari se najviše i uglavnom oslanjaju na svoju stručnost i iskustvo. Primjenom vještačke inteligencije, umnogome bi se unaprijedio rad na analizi tragova. Kao primjer vještačke inteligencije u analizi tragova možemo navesti analizu krvnih mrlji koji su nastali usled izvršenja nekog krivičnog djela. Pomoću primjene vještačke inteligencije možemo da analiziramo veličinu, oblik i disperziju krvnih mrlji koje su nastale kao posledica nekog krivičnog djela i pomoću te analize da odredimo njihov način nastanka što će nam dati odgovore na pitanja kako se desio kritični događaj?

PREDLOG UVOĐENJA INSTITUCIJE FORENZIČAR VJEŠTAČKE INTELIGENCIJE (FAI)

Jedna od obaveza vještaka-forenzičara da prati sve stručne i naučne novitete, sva objavljena istraživanja iz oblasti kojom se bavi. Bilo bi (možda) preambiciozno očekivati da vještak bude upoznat sa baš svakom vrstom naučnog i stručnog napretka i istraživanja u njegovoj forenzičkoj disciplini u svijetu! Međutim, učesnici u sudskom postupku imaju pravo da od vještaka zahtevaju da im iznese sve mogućnosti koje mogu uticati na njegov nalaz i mišljenje u vezi sa analizom predmetnog materijalnog traga. U vezi sa prevazilaženjem pomenutog problema, predlog bi bio uvođenje u sudski postupak Instituta - Forenzičar vještačke inteligencije!

Forenzičar vještačka inteligencija (FAI) bi bila softverski sistem koji se sastojao i od hardvera i od softvera. Bio bi dostupan učesnicima sudskog postupka (sudije, tužioci, advokati) i mogao bi da bude „angažovan" na sudskim raspravama kao i svi sudski vještaci koje sud angažuje, izabrani iz nacionalnog registra sudskih veštaka. FAI hardver bi bio nosilac vještačke inteligencije, odnosno elektronskih i mehaničkih delova koji čine sistem. Softver bi sadržao programe koji se koriste za upravljanje sistemom. FAI bi prikupljao sve podatke iz određene forenzičke discipline, koji su dostupni na svim vrstama naučnih i stručnih mreža. Na ovaj način, preko FAI-a, svi podaci, koji mogu biti korisni i koje bi svaka strana u sudskom postupku zatražila, bili bi dostupni svim učesnicima u sudskom postupku i bili bi dostupni u realnom vremenu i prostoru. Takođe, FAI bi mogao da sprovede meta-analizu podataka izvučenih iz svih naučnih i stručnih baza podataka (monografije, udžbenici, časopisi, studije...), a pomenuti metapodaci bi mogli da se transformišu u razumljiv i pojednostavljen format u vidu korisnih informacija (koje bi zahtijevali sudije, tužioci, advokati) u veoma kratkom roku. Prikupljanje i čuvanje velike količine informacija i podataka za forenzičare je veoma težak, obiman proces koji zahtijeva dugo vremena. Međutim, FAI ovaj problem rješava velikim kapacitetom svoje baze podataka koju koristi za prikupljanje i skladištenje forenzičkih podataka, nji-

hovih svojstava, istraživanja i rezultata. Prikupljanjem i analizom velike količine podataka, FAI bi bila od velike koristi prilikom prihvatanja ili odbacivanja određenih dokaza na sudu, a samim tim i prilikom istrage raznih vrsta krivičnih djela.

Primjena FAI bi takođe imala značajnu ulogu i u kriminalističkim istragama, koja bi dovela do poboljšavanja tačnosti i efikasnosti u radu istražnih organa. Dalje, FAI bi imao mogućnost da obrađuje ogromne količine podataka i to brzinom koja je nodostižna kriminalističkim analitičarima, smanjivao bi vrijeme potrebno za istragu, a dragocjeno za operativni sastav da pravovremeno i u zakonskom roku preduzima radnje i mjere u cilju rasvjetljavanja krivičnih djela i identifikovanja njihovih počinilaca. Upotreba FAI u kriminalističko-forenzičkim istragama imaće uticaj na efikasnost i efektivnost prilikom primjene specijalnih istražnih metoda, a naročito primjenom na poslovima pretrage baza podataka (DNK profila, otisaka prstiju, tragova vatrenog oružja i sl.), pomažući na taj način da se kriminalisti zaduženi za pojedine predmete mogu fokusirati na složenije i interpretativne aspekte istrage!

ZAKLJUČAK

Primjena vještačke inteligencije u forenzičkim naukama nije stvar izbora već neminovnost, ali čija upotreba donosi mnoge izazove i tom procesu treba ozbiljno pristupiti. Opšte prihvaćen stav bi bio da uvođenje vještačke inteligencije u forenzičkim naukama isključuje svaku vrstu pristrasnosti, predrasuda, grešaka izazvanih umorom, gubitkom koncentracije kod forenzičara i slično. Pristupačnost velikom broju podataka i informacija, koji se mogu koristiti prilikom forenzičkih analiza, ispitivanja i vještačenja, dalja ušteda vremena tokom forenzičkih istraga, tačnost, preciznost, kompetentnost, sve su to argumenti koji ukazuju da bi primjena vještačke inteligencije u velikoj mjeri osavremenila i unapredila rad i angažovanje forenzičara, a samim tim i pravosuđa u celini! Međutim, osim pomenutog optimizma, postoji i (ne)opravdana opreznost? Ovo se najviše i uglavnom odnosi na to koja bi prava i obaveze imao digitalni sistem u ovom članku nazvan – Forenzičar veštačke inteligencije (FAI). Pored obaveze da FAI mora da poštuje ljudska prava u cilju zaštite podataka o ličnosti (DNK profili, otisci prstiju i druge forenzičke informacije, koji su tretirani zakonom o zaštiti podataka o ličnosti građana), FAI bi trebalo da ima i etičku odgovornost. Najvažniji aspekt rada FAI-a je etika, a zatim slijede bezbjednost, transparentnost, nepristrasnost, zaštita privatnosti. U primjeni forenzičkih nauka u pravosuđu, ali i društvu uopšte, razvoj FAI ne bi trebalo da bude primaran u odnosu na etiku, naprotiv, trebalo bi na početku definisati čija, šta i kolika je etička odgovornost u radu FAI, a zatim odgovornost za bilo kakve greške u radu FAI? Međutim, pored navedenih obaveza, potrebno je definisati koja bi prava imala FAI? Kao i svaki forenzički ekspert, FAI treba da ima prava da zaštiti svoj integritet. Na ovaj način, primjenom vještačke inteligencije u pravosuđu, FAI bi se priznalo da pored forenzičkih podataka ima svijest i savjest!

LITERATURA

1. Ahmed Alaa El-Din, E. (2022) Artificial intelligence in Forensic Science: invasion or revolution? Egyptian Society of Clinical Toxicology Journal, 10(2), 20-32.
2. B. Vučkovič, Vesna Vučković (2023). Vještačka inteligencija izazov za sudske postupke. Čovječanstvo pred izazovom vještačke inteligencije. Zbornik radova sa XI međunarodnog naučnog skupa. Evropski univerzitet u Brčkom.
3. Bedeli, M., Geradts, Z. & van Eijk, E. (2018). Clothing identification via deep learning: forensic applications. Forensic Sciences Research, 3(3), 219–229.
4. Budić, M. Š. (2023) Etičke dileme i stavovi prema primeni veštačke inteligencije1. Kritika: časopis za filozofiju i teoriju društva, 4(1), 49-65.
5. Donnelly, S. (2012) Forensic science in a human rights framework. Australian Journal of Forensic Sciences, 44(1), 93-103.
6. Elkins, K. M., & Fambegbe, I. (2020) Case studies and methods for teaching professional ethics for forensic science students. The Journal of Forensic Science Education, 2(1).
7. Gasteiger, J. (2020). Chemistry in times of artificial intelligence. Chemphyschem: a European journal of chemical physics and physical chemistry, 21(20), 2233–2242. https://doi.org/10.1002/ cphc.202000518
8. Gupta, S., Sharma, M. V. i Johri, P. (2020). Artificial intelligence in forensic science. International Research Journal of Engineering and Technology, 7(5), 7181-7184.
9. Hoelz, B. W., Ralha, C. G., & Geeverghese, R. (2009, March). Artificial intelligence applied to computer forensics. In Proceedings of the 2009 ACM symposium on Applied Computing (pp. 883-888).
10. International Criminal Police Organization (Interpol), Disaster victim identi®cation guide, 1998, pp. 1±66.
11. Jadhav, E. B., Sankhla, M. S., i Kumar, R. (2020) Artificial intelligence: Advancing automation in forensic science & criminal investigation. Journal of Seybold Report ISSN NO, 1533, 9211.
12. Jasuja, O.P. (2001) Ethics In Forensic Science. Anil Aggrawal's Internet Journal of Forensic Medicine and Toxicology, Vol. 2, No. 2.
13. Kasar, M. M., Bhattacharyya, D., & Kim, T. H. (2016). Face recognition using neural network: a review. International Journal of Security and Its Applications, 10(3), 81-100.
14. Kulik, S. D. (2015). NEURAL NETWORK MODEL OF ARTIFICIAL INTELLIGENCE FOR HANDWRITING RECOGNITION. Journal of Theoretical & Applied Information Technology, 73(2).
15. M. Andrejević (2012). Značaj forenzičke DNK analize u pravosudnom sistemu. Strani pravni život 2/2012.
16. M. Janković, R. Radovanović, Milica Jankovič (2024). Prilog analizi upotrebe vještačke inteligencije u forenzici. LXVIII Konferencija ETRAN, Niš 2024.

17. M.Vodanović, M. Subašić, D.Milošević, I. Galić, H. Brkić, „.Artificialintelligence in forensic medicine and forensic dentistry“ J ForensicOdontostomatol. 2023 Aug 27;41(2):30-41. PMID: 37634174; PMCID:PMC10473456.
18. Ma M, Zheng H, Lallie H. Virtual reality and 3D animation in forensic visualization. J Forensic Sci. 2010 Sep;55(5):1227-31. doi: 10.1111/j.1556-4029.2010.01453.x. Epub 2010 Jun 8. PMID: 20533989.
19. Natalia Filipenko, S. Lukashevych, Olena Andrieieva, A. Ivanović (2024). Application of Artificial Intelligence and Information and Communication Technologies: Socio-Ethical Problems (Review Article). Theory and Practice of Forensic Science and Criminalistics Research Paper Collection, No. 34 for 2024.
20. Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449). Adopted on: 22/05/2019. Amended on: 08/11/2023. OECD, 2024. URL: https://legalinstruments. oecd.org/en/instruments/oecd-legal-0449
21. Sanela Andrić, A. Ivanović (2023). Forenzičke nauke i etika u eri primjene vještačke inteligencije. Kriminalističke teme. Godina XXIII, br. 3-4, 2023, str 95-102.
22. Siau, K., & Wang, W. (2020) Artificial intelligence (AI) ethics: ethics of AI and ethical AI. Journal of Database Management (JDM), 31(2), 74-87.
23. Stevanović, A. (2022). Uloga veštačke inteligencije u kontroli kriminaliteta, U: Digitalizacija u kaznenom pravu i pravosuđu, Kostić, J. & Matić Bošković, M. (ur.), VII Međunarodni naučni skup, Tematski zbornik radova međunarodnog karaktera, Beograd: Institut za uporedno parvo, 343-363.
24. Swapnil R. Kamdar and Astha Pandey, “The Scope of Artificial Intelligence in Forensic Science”, The Indian Police Journal, July-September, 2011, Vol. -58 Issue-3
25. United Nations, Of®ce of legal affairs: guidelines for the conduct of United Nations inquiries into allegations of massacres, 1995, pp. 1±108.
26. World Health Organization, International statistical classi®- cation of diseases and related health problems, 10th Revision, Geneva, 1992.
27. Yadav, P. K. (2017) Ethical issues across different fields of forensic science. Egyptian journal of forensic sciences, 7: 10, 1-6.
28. Zhou, Z. & Zare, R. N. (2017). Personal information from latent fingerprints using desorption electrospray ionization mass spectrometry and machine learning. Analytical Chemistry, 89(2), 1369–1372. https://doi.org/10.1021/acs.analchem.6b04498

UDK 343.51(497.16)

KRIVIČNO DJELO FALSIFIKOVANJE NOVCA U CRNOJ GORI

THE CRIMINAL OFFENSE OF FORGERYING MONEY IN MONTENEGRO

mr Branka Sekulić
Ministarstvo unutrašnjih poslova Crne Gore
e-mail: brankasekuliceva@gmail.com

Slaven Medenica
Uprava policije Crne Gore
e-mail: privreda.slaven@yahoo.com

Apstrakt

Falsifikovanja novca je stara pojava, ali je tehnika falsifikovanja dostigla zavidan stepen usavršenosti tek u naše vrijeme. Falsifikovanje se vrši u takvim razmjerama da može negativno da se odrazi na ekonomski sistem zemlje i da izazove poremećaje u monetarnoj politici. Posebna pažnja posvećena je definisanju krivičnog djela u našem zakonodavstvu, metodama ispoljavanja i falsifikovanja novca, načinima stavljanja falsifikovanog novca u opticaj, razotkrivanju falsifikovanog novca od strane policije i dokazivanju ovog krivičnog djela. Osim toga osvrnuli smo se na usklađenost propisa u odnosu na međunarodne instrumente i evropsko zakonodavstvo.
Ključne riječi: *falsifikovanje novca, metodi falsifikovanja, pravni aspekt, otkrivanje, dokazivanje, statistika.*

Abstract

Counterfeiting money is an old phenomenon, but the technique of forgery has reached an enviable level of perfection only in our time. Counterfeiting is carried out on such a scale that it can have a negative impact on the country's economic system and cause disruptions in monetary policy. Special attention is paid to the definition of the criminal offense in our legislation, the methods of manifestation and counterfeiting of money, the ways of putting counterfeit money into circulation, the detection of counterfeit money by the police and the proof of this criminal offense. In addition, we referred to international instruments and European legislation, and the harmonization of regulations.
Key words: *counterfeiting of money, methods of counterfeiting, legal aspect, detection, proof, statistics.*

UVOD

Različiti napadi na privredni sistem ili pojedine oblasti privrede inkriminisani su, u najvećem broju drzava, bilo u okviru opšteg krivičnog zakonodavstva ili donošenjem posebnih privrednih kaznenih zakona. Krivična djela protiv privrede i platnog prometa su mnogobrojna i sadržajno različita ali posebno ćemo obraditi krivično djelo falsifikovanja novca koje je inkriminisano Krivičnim Zakonikom Crne Gore (član 258).

Novac kao mjerilo vrijednosti i sredstvo plaćanja u razmjeni roba i drugih dobara, ima višestruk značaj za privredu svake zemlje. Istorija falsifikovanja novca vremenski se poklapa sa nastankom novca. Dok emitenti novca usavršavaju tehnike izrade i zaštite novca, falsifikatori, koristeći naučno-tehnička dostignuća, pokušavaju da što vjernije imitiraju zaštitne elemente novca kako bi lažni novac pustili u opticaj i tako stekli materijalnu korist.

POJAM FALSIFIKOVANJA NOVCA

Falsifikovanje ili krivotvorenje je imitiranje, oponašanje, koje je obično napravljeno sa namjerom prevare, odnosno da se proslijedi nekome, kao da je original. Shodno tome, lažni novac je valuta koja je nelegalno napravljena, bez odobrenja vlade ili države. Novac ima različite vrste zaštite od krivotvorenja, vidljive i skrivene. Krivotvoreni novac može se otkriti istragom različitih karakteristika.

Falsifikovanje novca je stara pojava, ali je tehnika falsifikovanja dostigla zavidan stepen usavršenosti tek u naše vrijeme. Falsifikovanje se vrši u takvim razmjerama da

može negativno da se odrazi na ekonomski sistem zemlje i da izazove poremećaje u monetarnoj politici. Osnovni motivi i ciljevi falsifikovanja novca su ekonomski i politički.

Sve moderne novčanice sadrže više zaštita protiv falsifikovanja. Posebno novčanice visokih apoena, mogu imati čak pedeset takvih elemenata, od čega su neki očigledni i vidljivi, a neki su tajni. Oni se kreću od više abecednih fontova, različitih veličina i oblika za slova i cifre u serijskim brojevima, specijalnim bojama koje se vide samo pod ultraljubičastim ili infracrvenim svetlom.

KRIVIČNO PRAVNI ASPEKT FALSIFIKOVANJA NOVCA

Lažnim novcem smatra se novac izrađen na način i od materijala kao pravi novac, suprotno propisima kojima se uređuje izrada novca.

Krivično djelo falsifikovnja novca inkriminisano je Krivičnim Zakonikom Crne Gore članom 258. a ispoljava se u sledećim krivično-pravnim oblicima;

1. Ko napravi lažan novac u namjeri da ga stavi u opticaj kao pravi ili ko u istoj namjeri preinači pravi novac, kazniće se zatvorom od dvije do dvanaest godina.
2. Ko pribavlja, drži, prenosi, unosi ili iznosi lažan novac u namjeri da ga stavi u opticaj kao pravi ili ko lažan novac stavlja u opticaj, kazniće se zatvorom od dvije do deset godina.
3. Ako je djelom iz st. 1 i 2 ovog člana napravljen, preinačen, stavljen u promet ili pribavljen lažan novac u iznosu koji prelazi petnaest hiljada eura, odnosno odgovarajući iznos u stvarnom novcu, učinilac će se kazniti zatvorom od pet do petnaest godina.
4. Ko lažan novac koji je primio kao pravi, pa saznavši da je lažan, stavi u opticaj ili ko zna da je načinjen lažan novac ili da je lažan novac stavljen u opticaj, pa to ne prijavi, kazniće se novčanom kaznom ili zatvorom do jedne godine." (Krivični zakonik Crne Gore ("Službeni list RCG", broj 070/03, 013/04, 047/06, "Službeni list CG" 040/08, 025/10, 073/10, 032/11, 064/11, 040/13, 056/13, 014/15, 042/15, 058/15, 044/17, 049/18, 003/20, 026/21, 144/21, 145/21, 110/23.).

Shodno tome, zakon inkriminiše nekoliko oblika ovog krivičnog djela:

1. Falsifikovanje novca je pravljenje lažnog novca ili preinačenje pravog novca u namjeri da se stavi u opticaj kao pravi

Pravljenje je stvaranje lažnog novca od nekog predmeta koji ne znači novac, ali se stvara predmet koji po formi liči na novac koji je u upotrebi, te mogućnost da se za

pravljenje novca koriste i novčanice koje više nijesu u upotrebi. Preinačenje, znači prepravljanje pravog novca; vršeći izmjene na novcu koji je u upotrebi u našoj ili stranoj zemlji u promjeni njegove vrijednosti. Pravljenje i preinačenje pravog novca predstavlja krivično djelo samo kada postoji namjera da se lažni novac upotrijebi kao pravi, pa se ta namjera mora utvrđivati u svakom konkretnom slučaju.

2. Upotreba falsifikovanog novca je stavljanje u opticaj lažnog novca ili preinačenog pravnog novca

Falsifikovani novac je stavljen u opticaj kada je upotrijebljen, i kada je omogućena njegova dalja upotreba, što se najčešće ostvaruje njegovom predajom drugom licu, a najčešće: plaćanjem roba ili usluga, davanjem u zajam, razmjenom novčanica, otplatom duga i slično.

Zakonik razlikuje dva oblika ovog krivičnog djela.

- Prvi je kada se u opticaj stavlja novac za koji se unaprijed zna da je falsifikovan, od strane lica koje je falsifikovalo ili preinačilo novac, ili od strane lica koje je prilikom primanja novca znalo da je preinačen ili falsifikovan.
- Drugi, lakši oblik, postoji kada se u opticaj stavlja lažni novac koji je primljen kao pravi. U ovom slučaju učinilac prilikom prijema nije znao da je novac lažni već je do tog saznanja došao kasnije, pa isti novac stavlja u opticaj da bi se obeštetio ili da bi se istog oslobodio.

3. Pribavljanje falsifikovanog novca je nabavljanje ovakvog novca u namjeri da se stavi u opticaj kao pravi

Kod ovog oblika krivičnog djela nije važno na koji način je pribavljen lažni novac (npr. razmjenom novca, kupovinom, krađom i sl.). Djelo je završeno pribavljanjem lažnog novca u namjeri da se stavi u opticaj kao pravi. Moguć je i pokušaj ovog krivičnog djela a on bi postojao kad su preuzete aktivnosti da se nabavi lažni novac iako još nije nabavljen.

4. Neprijavljivanje falsifikovanog novca ili njegove upotrebe

Djelo čini onaj ko zna da je napravljen lažni novac ili da je lažni novac stavljen u opticaj, a to ne prijavi. Radnja krivičnog djela je nečinjenje odnosno propuštanje da se nadležni organ obavijeti o pravljenju ili pojavi lažnog novca. Krivično djelo je svršeno kada je učinilac saznao za postojanje lažnog novca i kada je bio u mogućnosti da to prijavi nadležnim organima. Izvršilac kod svih oblika krivičnog djela može biti bilo koje lice, dok je u pogledu vinosti potreban umišljaj. Sadržina umišljaja je različita prema pojedinim oblicima krivičnog djela, tako kod falsifikovanja novca i

pribavljanja falsifikovanog novca treba da postoji umišljaj i namjera da se lažni novac stavi u opticaj kao pravi.

Lažni novac nastao izvršenjem ovog krivičnog djela obavezno se oduzima. Teži oblik ovog krivičnog djela postoji kada je pribavljen lažni novac u iznosu većem od petnaest hiljada eura, odnosno taj iznos u stvarnom novcu.

ORGANIZACIJA I NAČINI FALSIFIKOVANJA

Polazeći od činjenice da ovaj „zanat" važi za izuzetno unosan, logično je da oni koji se bave ovom kriminalnom djelatnošću stalno usavršavaju kako u organizaciji tako i u tehnici, kao i u metodama falsifikovanja.

Nalazimo se na povoljnom, tranzitnom položaju za širenje falsifikovanog novca organizovane mafije. Mjesta gdje se novčanice falsifikuju biraju se sa posebnom pažnjom i čuvaju u tajnosti, da bi se nakon proizvodnje određene količine falsifikovanog novca, sklonile mašine i drugi predmeti i tragovi, a gotov falsifikat smjestio u posebna skladišta, odakle se dalje distribuira. Organizovan pristup falsifikovanju novca, sa vremenskim i prostorno odvojenim fazama i ljudima koji u njima rade, najopasniji je i veoma teško se otkriva.

Osim kriminalnih organizacija, postoje i pojedinci koji se bave pravljenjem falsifikovanog novca i njegovim stavljanjem u opticaj, kao i pojedine grupe gdje je jedno lice glavni inicijator.

Najčešći falsifikatori, gledajući sa stanovišta međunarodne prakse institucija za sprovođenje zakona, su lica koja imaju iskustva u štamparskoj industriji ili su pak izuzetno informatički pismena sa iskustvom u sferi digitalne štampe.

Što se tiče Crne Gore, do danas nijesmo imali falsifikatore novca koji su profesionalno, vršeći ovo krivično djelo kao kriminalnu djelatnost, flasifikovali novčanice eura ili neke druge inostrane valute. U Crnoj Gori su najčešće procesuirani slučajevi falsifikovanja novca iz st. 2 KD Falsifikovanja novca (Ko pribavlja, drži, prenosi, unosi ili iznosi lažan novac u namjeri da ga stavi u opticaj kao pravi ili ko lažan novac stavlja u opticaj, kazniće se zatvorom od dvije do deset godina), a samo u par navrata iz st. 1 ovog krivičnog djela, kada su lica na kopir/štampač aparatima pravili falsifikovane novčanice jako lošeg kvaliteta, koje su lako otkrivane prvim stavljanjem u promet.

FALSIFIKOVANI METALNI NOVAC

Metalni novac je jednostavniji za falsifikovanje. Taj posao se obavlja livenjem, kovanjem ili galvanoplatikom.

Najpogodniji sistem falsifikovanja novca je livenje novca u specijalnim kalupima od gipsa, metala ili nekog drugog pogodnog materijala, ali novac izrađen ovako se razlikuje od originalnog novca, jer nema oštar reljef i ivice su loše izrađene.

Kako je falsifikat rađen od neplemenitog metala prepoznaje se i po razlici u zvuku, ako se na kamen baci prvo pravi, a zatim sumnjivi komad novca. Lažni liveni novac nema težinu kao pravi. Bakar i slični materijali od kojih je napravljen, ostavljaju karakterističan miris kada se trljaju među prstima. Boja novca je takođe različita. Lažnom novcu nedostaje i sjaj pravog.

Često kod falsifikata susrijećemo lažan novac sa jedne strane deblji, netačno položeno lice i naličje, falsifikator je uprostio crteže koji nisu toliko upadljivi, npr. izmijenio je broj zvjezdica i crtica, razmak između slova i brojeva nije identičan onom kod pravog novca, kalup rezan rukom mora da pokaže razlike u crtežu prema originalu, jer falsifikator reže lijevo ono što se nalazi desno, falsifikat se razlikuje i po boji. Kalaj blješti svijetlo-žuto, a olovo ima crnkast odnosno plavičast izgled. Falsifikatori se često trude da gotovom lažnom novcu daju izgled starog novca, zbog čega ga premažu crnim mastima i poslije toga istrljaju krpom.

Pravi metalni kovani novac je dobio svoju sliku pod snažnim pritiskom čeličnih žigova, pa je ona jasna, oštra i reljefna, bez greške. Lažan metalni novac ima nedovoljno oštru sliku i slabu izradu.

Pri ispitivanja pravilnosti metalnog novca trebamo obratiti pažnju na sledeće: zvuk novca (falsifikati daju tup zvuk), boja novca, slika novca, rub metalnog novca, težinu, mogućnost savijanja, reakcija na magnet (falsifikati reaguju na magnet).

U Crnoj Gori u 2023 godini otkriveno je 19.363 komada falsifikovanih kovanica, prema podacima iz Centralne banke, dok je samo u prvih sedam mjeseci 2024. godine, obrađeno 12,609 falsifikovanih kovanica. Najviše se krivotvore kovanice u apoenima od 2, 1 i 0.50 eura, dok se najčešće javlja apoen od 2 eura. Praksa pokazuje da se kovanice najviše ubacuju u promet na mjestima sa velikim prometom lica i novca, kao što su auto-putevi, naplate parkinga, samouslužne perionice, plaćanje na različitim aparatima, i slično.

FALSIFIKOVANJE PAPIRNOG NOVCA

Falsifikovanje papirnog novca t.j. novčanica je složeniji postupak i zavisi od načina na koji se vrši, s obzirom na to da pojavom lasera i kolor-kopi mašina mogu i lica bez posebnog stručnog znanja falsifikovati novac u većoj količini. Danas je falsifikovanje novca udruženo ne samo sa ljudskim znanjem i umećem već i sa neslućenim mogućnostima koje pruža savremena tehnika i tehnologija. U borbi protiv falsifikata uključene su u svetu brojne institucije: centralne banke, policija, Interpol, Europol, Olaf (Evropska komisija za borbu protiv prevara) i dr.

Osnovni načini falsifikovanja papirnog novca su: ručno, mašinski i fotokopirajem originalnih novčanica.

Novčanice se mogu ručno falsifikovati: precrtavanjem, preinačenjem, prepravljanjem, i skraćivanjem. Ovaj vid ima puno nedostataka i rijetki su slučajevi da ovakav falsifikat bude uspješan.

Najveći broj falsifikata izrađuje se u cjelini mašinskim putem, tj. fotokopiranjem originalne novčanice. Falsifikovanje papirnog novca je veoma teško, jer od falsifikatora zahtijeva poznavanje fotografske, cinkografske, litografske i štamparske tehnike. Međutim, čak i kada su zadovoljeni ti uslovi, ostaje jedna nepremostiva teškoća, a to je nabavka specijalnog papira, čiji bi kvalitet i sastav u potpunosti odgovarao potrebnom standardu. Naime, izrada hartije za štampanje novčanica je pod najstrožijom kontrolom države, a u tehnološkom postupku se primjenjuju različite mjere zaštite, kao što su vodeni žig, svileni končići, kružići planšete, sigurnosna metalna nit, posebna boja, fluorescentne materije, luminiscentni znakovi, materije koje reaguju na elektronske aparate.

Štampanje je kvalitetniji i češći metod a sam proces izrade falsifikata se organizuje na isti način kao i izrada originala, što znači da se za svaku vrstu štampe (visoka, ravna, duboka) i svaku boju, izrađuju posebni klišei na osnovu fotoreprodukcija originalne novčanice. Ovako izrađeni falsifikati se teško razlikuju od originala, štampa se ne može uočiti golim okom. Hendikep za falsifikatore je činjenica da su troškovi proizvodnje visoki, pa su prinuđeni da naprave i puste u promet veliki broj falsifikata. To povećava mogućnost da se otkrije falsifikat, tako što će neko lice uočiti neku grešku ili će se na istom mjestu pojaviti dvije novčanice sa istim serijskim oznakama.

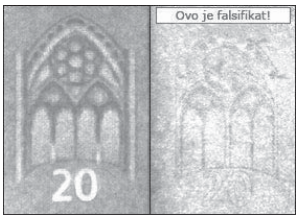
ELEMENTI ZAŠTITE KOJE SADRŽE PAPIRNE NOVČANICE EURA

Euri kao elemente zaštite sadrže:

1. **Intaglio štampa** nanosi se na novčanice pod velikim pritiskom i toplotom tako da pod rukom djelovi novčanice tretirani takvom štampom djeluju reljefno.

Slika br.1: Intaglio štampa na novčanici od 20 € (lijevo), i intaglio štampa na falsifikovanoj novčanici od 20 € (desno)

2. **Vodeni žig** proizvodi se procesom tanjenja papira, numerički dio vodenog žiga je svjetliji (tanji).

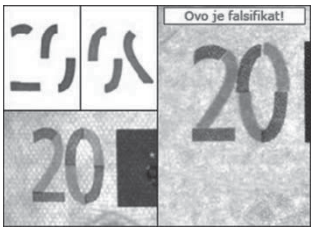


Slika br.2: Vodeni žig na novčanici od 20 € (lijevo), i vodeni žig na falsifikovanoj novčanici od 20 € (desno)

3. **Zaštitna nit** utkana u papir, uočava se tek kada se novčanica okrene prema svjetlu. Na njoj se nalazi mini i mikro štampa.

Slika br. 3: Zaštitna nit utkana u papirna novčanici od 20 €(lijevo), i zaštitna nit na falsifikovanoj novčanici od 20 € (desno)

4. **Poklapajući detalji** - providni registar, detalji motiva nanose se preciznom štampom sa obje strane novčanice tako da kada se novčanica pogleda ka svjetlu motiv postaje kompletan.



Slika br. 4: Providni registar na novčanici od 20 € (lijevo), i providni registar na falsifikovanoj novčanici od 20 € (desno)

5. **Hologramska traka** prilikom naginjanja reflektuje širok spektar boja i motiva: oznaku valute, nominalne vrijednosti, mini i mikro tekst u prvoj seriji euro novčanica u apoenima od 5,10 i 20 eura, dok se u drugoj seriji novčanica uočava više motiva; motiv kapije, nominalne vrijednosti, oznaka eura, apoena, te boginja Evrope.

Slika br. 5: Hologramska traka na novčanici od 20 € (lijevo), i Hologramska traka na falsifikovanoj novčanici od 20 € (desno)

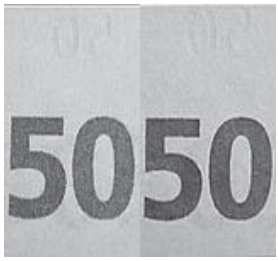
5. **Presijavajući sloj ili traka** nanesen ja sa poleđine novčanice i uočava se prilikom naginjanja. Veoma je otporan na habanje i na njemu se nalaze oznake valute i nominalne vrijednosti.

Slika br. 6: Presijavajući sloj na novčanici od 20 € (lijevo), i Presijavajući sloj na falsifikovanoj novčanici od 20 € (desno)

7. **Hologramski pečat** (kod apoena od 50, 100, 200 i 500 eura) na kome je prikazan centralni motiv, mikro tekst sa oznakama valute i nominalne vrijednosti, perforacija oznake € i demetalizirana zona.

Slika br. 7: Hologramski pečat na novčanici od 50 € (lijevo), i Hologramski pečat na falsifikovanoj novčanici od 50 € (desno)

8. **OVI mastilo mijenjajuće** boje pri naginjanju prelazi od sjajno tamno roze u maslinasto zelenu boju. Važi za apoene od 50, 100, 200 i 500 eura.



Slika br. 8: OVI mastilo mijenjajuće boje na novčanici od 50 € (lijevo), i OVI mastilo mijenjajuće boje na falsifikovanoj novčanici od 50 € (desno)

9. **"Smaragdni broj"** nalazi se u donjem lijevom uglu na licu novčanice koji je smaragdno zelene boje na teget podlozi, i to kod druge serije euro novčanica, navode iz Centralne banke Crne Gore (CB CG Zaštitni elementi novca, 07.11.2024. godine.)[1]

OTKRIVANJE I DOKAZIVANJE KRIVIČNOG DJELA FALSIFIKOVANJA NOVCA

Osnovni izvor saznanja da se planira ubacivanje i rasturanje falsifikovanog novca, u Crnoj Gori jeste operativna djelatnost policije, dok se o pojavi novca na tržištu policija informiše prijavom preduzeća, službi za platni promet, pošti, mjenjačnica, organizacija i drugih pravnih lica koja su uključena u platni promet a najčešće ba-

1 Centralna banka Crne Gore – zaštitni elementi novca, dostupno na https://www.cbcg.me/me/novac/zastita-euro-novcanica-i-kovanog-novca-od-falsifikovanja/zastitni-elementi-novca, od 01.11.2024. godine.

naka. Na osnovu sklopljenog Protokola o saradnji, Centralna banka sve podatke o falsifikovanom novcu šalje Upravi policije i Vrhovnom državnom tužilaštvu. Drugi najčešći izvor saznanja za ovo krivično djelo je prijava građana, koji dođu u posjed falsifikovanog novca.

Policijski službenik će donijeti pravilnu taktičku odluku da li će se osoba koja je sumnjiva kao proturač lažnog novca odmah lišiti slobode ili pratiti izvjesno vrijeme. Ako je ona zadržana od osoblja u banci, u pošti ili negdje drugo, ta se dilema ne postavlja.

Dokazivanje krivičnog djela falsifikovanja novca je kompleksno iz razloga što se osim dokazivanja da je sumnjiva novčanica falsifikat, dokazuje i umišljaj eventualnom počiniocu ovog krivičnog djela (u namjeri da ga stavi u opticaj), ovo otežava i komplikuje činjenica da je, po pravilu, sve do kraja kriminalističke obrade nepoznato mjesto izvršenja falsifikata novca (radionica u kojoj se izrađuju falsifikati). Za dokazivanje ovog krivičnog djela i procesuiranje počinioca, potrebna je i jaka međuinstitucionalna saradnja Uprave policije kako na nacionalnom nivou, tako i na međunarodnom nivou. Na nacionalnom nivou međuinstitucionalna saradnja se ogleda u odličnoj sporazumnoj saradnji Državnog tužilaštva, Centralne banke Crne Gore i Uprave policije.

Na međunarodnom nivou, saradnja Uprave policije tj. Crne Gore ogleda se kroz saradnju sa EUROPOL-om, Evropskom komisijom, Evropskom Centralnom bankom, INTERPOL-om i SELEC Centrom u Bukureštu (Međunarodna regionalna organizacija sa sjedištem u Bukureštu, čiji je cilj borba protiv prekograničnog kriminala).

Falsifikovani novac, pogotovo euro i USD u Crnu Goru dospijevaju iz inostranstva i uglavnom je Crna Gora samo tranzitna destinacija. Zbog svog geografskog položaja, demografske strukture i veličine, Crna Gora nije interesantna falsifikatorima kao tržište na kojem se može staviti u promet velika količina falsifikovanog novca. Konstantan monitoring CBCG i UP reaguje na svaku masovniju pojavu plasiranja falsifikovanog novca na nivou grada, opštine, i regionalnog dijela Crne Gore.

Mjere tajnog nadzora

U crnogorskoj praksi za razjašnjavanje i dokazivanje k.d. falsifikovanog novca veoma značajnu ulogu ima primjena mjera tajnog nadzora, koja se vrši u saradnji sa tužilaštvom i nadležnim sudom Crne Gore. Prema Zakoniku o krivičnom postupku mjere tajnog nadzora, na obrazloženi predlog policije ili po službenoj dužnosti, pisanom Naredbom određuje državni tužilac, shodno članu 158. mogu se primijeniti za krivično djelo falsifikovanja novca. Pretres stana, vozila i lica falsifikatora je obavezan prilikom hapšenja lica sa falsifikovanim novcem.

Vještačenje falsifikovanog novca

U crnogorskoj praksi vještačenje vrši Centralna banka Crne Gore, u Trezoru, Nacionalni centar za analizu novčanica, kao i Forenzički centar u Danilogradu.

Centralna banka Crne Gore vrši određivanje specifičnosti falsifikata i određivanje indikativa. Indikativ sadrži podatke o načinu i kvalitetu izrade, što na kraju može dovesti do otkrivanja štamparije u kojoj je falsifikovani novac nastao. Takvim vještačenjem policija dobija "ime i prezime novčanice" jer su to podaci u kojoj državi je novčanica odštampana, pa navodi policiju na dalje operativno taktičke radnje, i usmjerava istragu prema daljem praćenju kriminalne grupe.

NACIONALNI PRAVNI OKVIR I USKLAĐENOST SA MEĐUNARODNIM INSTRUMENTIMA I EVROPSKIM ZAKONODAVSTVOM

U cilju zaštite eura od falsifikovanja, na nivou Evropke unije razvijen je pravni okvir u cilju osiguranja te zaštite. Crna Gora, kao zemlja u kojoj je euro zvanično sredstvo plaćanja, u procesu evropskih integracija, posebnu pažnju posvećuje zaštite eura od falsifikovanja u okviru Pregovaračkog poglavlja 24. Naime, Akcioni plan za poglavlje 24 - Pravda, sloboda i bezbjednost sadrži podoblast Falsifikovanje eura.
Međunarodni Instrumenti

Na međunarodnom nivou, osnovni dokument za zaštitu valute od falsifikovanja jeste Međunarodna konvencija o sprečavanju falsifikovanja valute, potpisana u Ženevi 1929. godine, a stupila je na snagu 1931. godine. Crna Gora je Zakonom i potvrdila.[2] Potisivanjem ovog ugovora Lige naroda, države članice su preuzele obavezu kažnjavanja radnji falsifikovanja valute. Primarno „pravilo" koje propisuje ova konvencija jeste da države članice ne prave razliku u visini sankcije za krivična djela falsifikovanja domaće valute u odnosu na falsifikovanje strane valute. Konvencijom se utvrđuje da falsifikovanje novca predstavlja krivično djelo koje podliježe izručenju, da se falsifikovani novac mora oduzeti odnosno zaplijeniti itd. Takođe, članice su u obavezi da osnuju centralne organe koji imaju dužnost da obavještavaju sve ostale države o povlačenju primjeraka svoje valute iz opticaja i o svim ostalim promjena koje se tiču njihove valute.

Usklađenost Zakonodavstva Crne Gore sa Međunarodnim instrumentima i Evropskim Zakonodavstvom

Pravni okvir Crne Gore na polju krivično-pravne zaštite novca od falsifikovanja, u potpunosti je usklađen sa međunarodnim instrumentima i evropskim zakonodav-

2 Vlada Crne Gore - Zakon o potvrđivanju međunarodne konvencije o sprečavanju falsifikovanja novca, 14.05.2021. godine, dostupno na: https://www.gov.me/dokumenta/d8a78d94-4668-4eed-be57-b1c13699394e

stvom, čini Krivični zakonik Crne Gore, Zakon o odgovornosti pravnih lica za krivična djela i Zakonik o krivičnom postupku.

Prije svega, definicija termina novac data je u članu 142 stav 26 Krivičnog zakonika usklađena je sa onom koju daje Ženevska konvencija i Direktiva 2014/62/EU,[3] bez obzira na to što su ova dva standarda koriste termin "valuta".

ANALIZA POLICIJSKE AKCIJA "TREZOR"

Smatra se da je akcija „TREZOR" jedna od najuspješnijih realizovanih akcija u Crnoj Gori do sada, za krivično djelo falsifikovanja novca.

U periodu januar – avgust 2006. godine, Uprava policije Crne Gore je, na osnovu operativnih saznanja, započela sveobuhvatnu akciju presijecanja organizovanog međunarodnog krijumčarskog lanca velike količine falsifikovanih eura i američkih dolara. Operativna saznanja upućivala su na sumnju o postojanju međunarodne organizovane kriminalne grupe, koja se bavila rasturanjem falsifikovanih eura i američkih dolara. Falsifikovani novac je planiran da se ilegalno unese u Crnu Goru, a odatle da se distribuira prema Albaniji, Kosovu, i dalje prema državama Zapadne Evrope. Manji dio planiran je za rasturanje u Crnoj Gori. Na osnovu prikupljenih saznanja, Uprava policije je sačinila plan za sprovođenje Akcije "TREZOR".

Iz sprovedenih mjera i radnji, službenici Uprave policije su identifikovali ukupno deset lica, koji su predstavljali organizovanu kriminalnu grupu, zaduženu za krijumčarenje falsifikovanih novčanica iz Bugarske u Crnu Goru, sa namjerom rasturanja i daljeg krijumčarenja prema zemljama u okruženju.

Na osnovu prikupljenih dokaza, dana 12. avgusta 2006. godine, u sinhronizovanoj akciji službenika Uprave kriminalističke policije, Centra bezbjednosti Bar, Centra bezbjednosti Podgorica, Odjeljenja bezbjednosti Tivat, Odjeljenja bezbjednosti Plav, i Odjeljenja bezbjednosti Ulcinj, lišeno je slobode sedam lica, članova međunarodne organizovane kriminalne grupe. Struktura kriminalne grupe činila su lica iz Bugarske, Srbije i Crne Gore. Sprovedeno je i više pretresa stanova i drugih objekata koje koriste članovi kriminalne grupe. Osim zaplijenjenih falsifikovanih novčanica, u navedenom periodu u Crnoj Gori stavljen je u promet manji iznos falsifikovanih novčanica u apoenima od 500 €, 200 €, i 100 $.

Kao rezultat akcije "TREZOR" oduzeto je ukupno: 714.000 falsifikovanih eura, u apoenima od 500 € i 200 €. Zatim, 100.500 falsifikovanih američkih dolara, u apoenima

3 Directive 2014/62/EU of the European Parliament and of the Council of 15 May 2014 on the protection of the euro and other currencies against counterfeiting by criminal law, and replacing Council Framework Decision 2000/383/JHA, dostupno na https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0062

od 100 $. Protiv deset lica podnijeta je krivična prijava za: Zločinačko udruživanje (čl. 401 KZ RCG), Falsifikovanje novca (čl. 258 KZ RCG), izvršenim na organizovan način (čl. 507, st. 3 i 4 ZKP). Grafološkom ekspertizom oduzetih novčanica utvrđeno je da se radi o falsifikatu veoma dobrog kvaliteta.

ZAKLJUČAK

Ako falsifikatore novca posmatramo kao "prve primaoce novca", onda je jasno da oni svojim lažnim novcem kupuju proizvode i usluge po cijenama koje su se formirale u odnosu na "staru" količinu novca u opticaju, i da na taj način maksimizuju svoju korist. Falsifikovani novac bi poremetio cjenovni sistem, tj. tržišnim učesnicima bi poslao pogrešne signale u pogledu realne tražnje. Ako bi falsifikovani novac ostao neprimijećen, onda bi on trajno poremetio cjenovni sistem, a sve cijene, bilo da se radi o cijenama proizvoda, radne snage ili ostalih privrednih resursa, pre ili kasnije, prilagodile bi se toj novoj, uvećanoj novčanoj masi. Povećana novčana masa bi smanjila kupovnu moć novčane jedinice, što znači da bi negativne posledice osetio skoro svaki član društva. Falsifikovani novac bi pogrešno usmeravao raspoloživi kapital. Takav novac bi preduzetnike naveo na pogrešan zaključak da je povećana tražnja rezultat povećane realne kupovne moći stanovništva. Investitori bi neminovno zaključili da su se ostali članovi društva dobrovoljno odrekli sadašnje potrošnje zarad veće potrošnje u budućnosti i sa takvim pogrešnim uverenjem bi ušli u proces investiranja.

Možemo zaključiti da je falsifikovani novac je izuzetno štetan i zato svaka država donosi zakone kojima se propisuju kazne za počinioce tog krivičnog djela, dok borba protiv falsifikatora novca zahtijeva kontinuiranu saradnju između policije, tužilaštva, finansiskih institucija, tehnoloških kompanija, i građana. Veoma je važno i podizanje svijesti građanima o tome kako da prepoznaju lažan novac i kako da ga prijave, što se realizuje kroz različite obuke i kampanje. Sve veća upotreba bezgotovinskog plaćanja i promocija digitalnih valuta ukazuje na smanjenu potrebu za fizičkim novcem. Dok sa druge strane postoje izazovi usled upotrebe napredne tehnologije poput 3D štampača za proizvodnju falsifikata. Neophodno je neprestalno ulaganje u istraživanje i razvoj novih zaštitnih elemenata novca, kao i stalno obučavanje stručnih ljudi da prepoznaju sve nove oblike falsifikata, i sa tim opasnostima upoznaju građane i nadležne institucije, za dobro svih nas.

LITERATURA

1. Becker K.Harold, 1973. Police Systems of Europe, Tomas,
2. Bošković Mićo, 1998. Kriminalistička Metodika I, Beograd, Policijska Akademija,

3. Bošković Mićo, 2000. Kriminalistička metodika 2, Beograd Policijska Akademija,
4. Centralna banka Crne Gore – zaštitni elementi novca, dostupno na https://www.cbcg.me/me/novac/zastita-euro-novcanica-i-kovanog-novca-od-falsifikovanja/zastitni-elementi-novca, od 01.11.2024. godine
5. Čejović Bora, 2006. Krivično Pravo, Beograd
6. Directive 2014/62/EU of the European Parliament and of the Council of 15 May 2014 on the protection of the euro and other currencies against counterfeiting by criminal law, and replacing Council Framework Decision 2000/383/JHA, dostupno na https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=-CELEX:32014L0062
7. Đurđević Zoran, Radović Nenad, 2012. Kriminalistička operativa, Beograd, Kriminalističko Policijska Akademija
8. Krivični zakonik Crne Gore ("Službeni list RCG", broj 070/03, 013/04, 047/06, "Službeni list CG" 040/08, 025/10, 073/10, 032/11, 064/11, 040/13, 056/13, 014/15, 042/15, 058/15, 044/17, 049/18, 003/20, 026/21, 144/21, 145/21, 110/23.)
9. Krivokapić Dragan, Brđanin Zoran – Zakonik o krivičnom postupku, priručnik za policijske službenike
10. Krivokapić, V. Žarković, Z. 1995. Kriminalistička taktika, VŠUP, Beograd
11. Ministarstvo pravde, 2014. Analiza normativno pravnog okvira za zaštitu eura od falsifikovanja - Krivični aspekt
12. Odluka o postupanju sa sumnjivim primjercima euro novčanica i kovanog novca i drugim aktivnostima za zaštitu eura od falsifikovanja ("Službeni list Crne Gore", br. 35/11 od 21.07.2011, 61/18 od 14.09.2018)
13. Rakočević Velimir, Krivično pravo
14. Rakočević, Velimir, 2007. Kriminologija, Podgorica, BD Graf
15. Rakočević, Velimir, 2010. Osnovi kriminalistike, Podgorica, Pokret
16. Vlada Crne Gore,2013. Akcioni plan za poglavlje 24. Pravda, sloboda i bezbjednost, 27.07.2013. godine,
17. Vlada Crne Gore, 2021. Zakon o potvrđivanju međunarodne konvencije o sprečavanju falsifikovanja novca, 14.05.2021. godine, dostupno na: https://www.gov.me/dokumenta/d8a78d94-4668-4eed-be57-b1c13699394e
18. Vučković Branko, Vučković Vesna, 2009. Krivično Pravo Crne Gore, Cetinje
19. Zakon o Centralnoj Banci Crne Gore ("Službeni list Crne Gore", br. 040/10 od 22.07.2010, 046/10 od 06.08.2010, 006/13 od 31.01.2013, 070/17 od 27.10.2017, 125/23 od 31.12.2023),
20. Zakonik o krivičnom postupku („Sl. List CG", broj 57/09, 49/10, 47/14, 002/15, 035/15, 058/15, 028/18, 116/20, 145/21, 054/24.)
21. Žarković Milan, Banović Božidar, Stupar Ljubinka, Ivanović Vukašin, 1999. Kriminalistička taktika, Beograd, VŠUP

UPUTSTVO ZA AUTORE

Naučno-stručni časopis "*Crnogorska revija za bezbjednost*" objavljuje: izvorne naučne radove (sadrži opis izvornih rezultata istraživanja), pregledne radove (daje pregled postojeće značajne literature iz oblasti bezbjednosnih nauka), stručne radove (daje prikaz određenih zapažanja koja nisu novost u pojedinoj struci, ali mogu svojom sistematizacijom obogatiti znanje oblasti bezbjednosti), prikaze slučajeva (kada stručnjaci u toku svog rada naiđu na slučaj važan za stručnu i naučnu zajednicu i smatraju da bi on bio interesantan svojim kolegama) i prikaze knjiga (daje prikaz o aktuelnim naučnim i stručnim knjigama), koji su urađeni po sledećem upustvu:

Tekst rada obima do 15 stranica, na Crnogorskom jeziku, napisan prema sledećem uputstvu:
Format teksta: MS Word 2007 i stariji (*.docx; *.doc);
Font: Times New Roman;
Format stranice: A4 (210×297 mm);
Razmak između redova (Line spacing): jednostruki;
Margine: leva (left) 2.0 cm, desna (right) 1.5 cm, gornja (top) 2.0 cm, donja (bottom) 1.5 cm;
Naslov rada na Crnogorskom jeziku: 12 pt., bold, centralno ravnanje (*Alignment centered*), velika slova;
Naslov rada na engleskom jeziku: 12 pt., bold, centralno ravnanje (*Alignment centered*), velika slova;
Imena autora: 11 pt., centralno ravnanje (*Alignment centered*),
Institucije i e-mail adrese: 11 pt., italic, centralno ravnanje (*Alignment centered*);
Izvod na Crnogorskom jeziku i ključne reči: 11 pt., potpuno ravnanje (*Alignment justified*);
Izvod na engleskom jeziku i ključne reči: 11 pt. potpuno ravnanje (*Alignment justified*);
Tekst rada: 11 pt., potpuno ravnanje (*Alignment justified*) nazivi cjelina velikim slovima bez rednog broja;
Citiranje: Ispod teksta u fusnote upisivati samo propratne komentare. Propratni komentar pisati fontom *Time New Roman 8 pt*. Na kraju citata u tekstu otvoriti zagradu i u njoj upisati prezime autora, godinu izdanja i broj strane.

- Primer za citiranje bibliografske jedinice jednog autora: (*Krivokapić, 2008:74*).
- Primer za citiranje bibliografske jedinice dva autora (*Matijević & Mitrović, 2011: 77*).

- Primer za citiranje više bibliografskih jedinica: (*Krivokapić, 2005: 36; Simonović, 2004: 183*).
- Primer citiranja bibliografske jedinice bez autora: (*Deklaracija, 1948: 2*).
- Primer citiranja bibliografske jedinice jednog autora u slučaju da postoje druge bibliografske jedinice istog autora izdate iste godine: (*Ivanović, 2011b: 45*);

Literatura: 11 pt., sa rednim brojem ispred. Referentni izvori se navode prema abecednom redu. Abecednim redom navesti sve citirane bibliografske jedinice. Knjiga se navodi sledećim redom: prezime, ime, godina izdanja, naslov knjige kurzivom, mesto izdanja, naziv izdavača. Članak u knjizi se navodi sledećim redom: prezime (autora), ime (autora), godina izdanja, naslov članka, u:, prezime (urednika), ime (urednika), skraćena oznaka uredništva (u zagradi), naslov knjige kurzivom, mesto izdanja, naziv izdavača. Članak u časopisu se navodi sledećim redom: prezime, ime, godina izdanja, naslov članka, naslov časopisa kurzivom, godište, broj, izdavač i broj prve i poslednje strane na kojima je članak objavljen.

- Primer navođenja knjige: Jović, Miodrag. 2011. Krivično pravo-opšti deo. Novi Pazar: Univerzitet u Novom Pazaru.
- Primer navođenja teksta u knjizi: Pillar, Paul 2008. Counterterrorism, u: Williams, Paul (ur.). Security studies: an introduction. London and New York: Routledge.
- Primer navođenja članka u časopisu: Ivanović, Aleksandar 2009. Privredni kriminalitet i korupcija u Republici Srbiji. Kriminalističke teme: Časopis za kriminalistiku, kriminologiju i sigurnosne studije, god. IX, br. 3-4: 153-172.

Naslovi slika: 11 pt., *italic*, centrirano ispod slike
Naslovi tabela: 11 pt., *italic*, centrirano iznad tabele
Slike: prihvatljivi su formati TIF, GIF, JPG, BMP, WMF i CDR

Radovi se predaju elektronskom poštom na adresu:
marijana.radunovic@mup.gov.me
sa naznakom „Za časopis Crnogorska revija za bezbjednost"

INSTRUCTIONS FOR AUTHORS

The scientific and professional journal "Montenegro Review for Security" publishes: original scientific papers (contains a description of the original research results), review papers (provides an overview of the existing significant literature in the field of security sciences), professional papers (provides an overview of certain observations that are not new in a particular profession , but with their systematic approach they can enrich knowledge in the field of security), case presentations (when experts in the course of their work come across a case important for the professional and scientific community and think that it would be of interest to their colleagues) and book reviews (gives an overview of current scientific and professional books), which were done according to the following instructions:

The text of the work is up to 15 pages, in the Montenegrin language, languages in official use in Montenegro, English, written according to the following instructions:

Text format: MS Word 2007 and older (*.docx; *.doc);
Font: Times New Roman;
Page format: A4 (210×297 mm);
Line spacing: single;
Margins: left 2.0 cm, right 1.5 cm, top 2.0 cm, bottom 1.5 cm;
The title of the work in the Montenegrin language and languages in official use in Montenegro: 12 pt., bold, alignment centered, capital letters;
Title of the paper in English: 12 pt., bold, alignment centered, capital letters;
Names of authors: 11 pt., alignment centered,
Institutions and e-mail addresses: 11 pt., italic, alignment centered;
Extract (abstract) in the Montenegrin language and languages in official use in Montenegro, key words: 11 pt., alignment justified;
Extract (abstract) in English and keywords: 11 pt. full alignment (Alignment justified);
Paper text: 11 pt., full alignment (Alignment justified), unit names in capital letters without serial number;
Citation: Under the text in the footnotes, enter only accompanying comments. The accompanying comment should be written in Time New Roman 8 pt font. At the end of the quotation in the text, open the parenthesis and enter the last name in it author, year of publication and page number.

- Example for citing a bibliographic unit of one author: (Krivokapić, 2008:74);
- Example for citing a bibliographic unit of two authors (Matijević&Mitrović, 2011:

77);
- Example for citing several bibliographic units: (Krivokapić, 2005: 36; Simonović, 2004: 183);
- Example of citing a bibliographic unit without an author: (Declaration, 1948: 2).;
- Example of citing a bibliographic unit of one author in case there are other bibliographic units of the same author published in the same year: (Ivanović, 2011b: 45);

Literature: 11 pt., with serial number in front. Reference sources are listed in alphabetical order.
List all cited bibliographic units in alphabetical order.
The book is listed in the following order: surname, first name, year of publication, book title in italics, place of publication, publisher's name.
The article in the book is listed in the following order: last name (author), first name (author), year of publication, title of the article, in:, last name (editor), first name (editor), abbreviated editorial code (in parentheses), title of the book in italics, place editions, name of the publisher.

The article in the magazine is listed in the following order: surname, first name, year of publication, title of the article, title of the magazine in italics, year, number, publisher and number of the first and last pages on which the article is published.

- Example of citing a book: Stojanović, Zoran, 2022, Criminal Law-general section, Belgrade, University of Belgrade.
- Example of citing the text in the book: Pillar, Paul 2008, Counter terrorism, in: Williams, Paul (ed.), Security studies: an introduction, London and New York, Routledge.
- Example of citing an article in a journal: Ivanović, Aleksandar 2009, Economic crime and corruption in the Republic of Serbia, Criminal topics: Journal of criminalistics, criminology and security studies, vol. IX, no. 3-4, 153-172.

Image titles: 11 pt., italics, centered below the image
Table titles: 11 pt., italics, centered above the table
Images: TIF, GIF, JPG, BMP, WMF and CDR formats are acceptable

Papers are submitted by e-mail to the address:
marijana.radunovic@mup.gov.me
with the indication "For the magazine Montenegrin review for security".

ISSN 3027-3390