Stručni članak

PRAVO I TEHNOLOGIJA, TEHNOLOGIJA U PRAVU

Vlado Jovanić, master, email: v.jovanic@mup.vladars.net, vlado.jovanic@gmail.com
Diplomirani pravnik, Profesor civilne odbrane, Doktorant na Pravnom fakultetu IU u Travniku, Glavni inspektor, Zamjenik načelnika Uprave za policijsku podršku
MUP Republika Srpska

Sažetak: Vrijeme u kojem živimo je vrijeme informaciono komunikacionih tehnologija (IKT) i praktično nema nijednog segmenta u društvu, ekonomiji i nauci u koji nije inplementirana informaciono komunikaciona tehnologija (IKT). Bez aktivne uloge informacionih tehnologija danas je upitno funkcionisanje i održivi razvoj i napredak društva. Kako je tehnologija postala ključna za razvoj ekonomije i nauke, neophodno je da se na isti način iskoristi i za unapređenje pravnog poredka. Korištenje IKT u pravu, kroz sprovođenje posebnih istražnih mjera i radnji od strane policije u istražnom i u krivičnoprocesnom smislu (digitalna forenzika) je postavilo osnovne temelje za potpuno novi nivo u pristupu primjene prava, prije svega u sprečavanju izvršenja krivičnih djela, zaštite ličnih i građanskih prava i većeg stepena primjene prava u svrhu veće zaštite i bezbjednosti društva. U radu ćemo govoriti o značaju IKT u pravu sa aspekta otkrivanja, dokumentovanja, dokazivanja i procesuiranja krivičnih djela i izvršioca, odnosno o značaju IKT i digitalne forenzike u krivičnim istragama.
Ključne riječi: *Informaciono komunikacione tehnologije (IKT), digitalna forenzika, pravo i pravni poredak, posebne istražne mjere i radnje, krivična istraga.*

LAW AND TECHNOLOGY, TECHNOLOGY IN LAW

Summary: The time we live in is the time of information and communication technologies (ICT) and there is practically no segment in society, economy and science in which information and communication technology (ICT) is not implemented. Without the active role of information technologies, the functioning and sustainable development and progress of society is questionable today. As technology has become crucial for the development of economics and science, it is necessary to use it in the same way to improve the legal order. The use of ICT in law, through the implementation of special investigative measures and actions by the police in investigative and criminal proceedings (digital forensics) has laid the basic foundations for a whole new level in the approach to law enforcement, primarily in preventing crime, protection of personal and civil rights and a greater degree of application of the law for the purpose of greater protection and security of society. In this paper, we will talk about the importance of ICT in law in terms of detecting, documenting, proving and prosecuting crimes and perpetrators, and the importance of ICT and Digital Forensics in criminal investigations.
Keywords: *Information and Communication Technologies (ICT), Digital Forensics, Law and Legal Order, Special Investigative Measures and Actions, Criminal Investigation.*

UVOD

Devedesete godine prošlog vijeka predstavljaju početak transformacije u sektoru djelatnosti globalnih informaciono komunikacionih sistema usvajanjem novih tehnologija zasnovanih na kompjuterski baziranim sistemima. Nove tehnologije postavile su nove standarde pred zakonodavce i nove izazove pred agencije za zaštitu i sprovođenje zakona. Ekspanzija novog

vida kriminaliteta zasnovanog na kompjuterskoj i informaciono komunikacionoj tehnologiji (IKT) (kompjuterski, odnosno sajber-cayber kriminalitet) predstavlja globalni problem. Danas praktično i nema oblasti društvenog života u kojem ne postoji interakcija čovjeka sa kompjuterskom, odnosno informaciono komunikacionom tehnologijom (IKT). Sa druge strane upravo ta interakcija, povezanost čovjeka sa modernom tehnologijom ili putem moderne tehnologije (IKT), predstavlja mogućnost i sredstvo za napada i ugrožavanje kako pojedinca tako i društva u cjelini. Izazov za bezbjednosne agencije i zakonodavce je kako efikasno zaštititi pojedinca i društvo od ugrožavanja, prije svega u preventivnom pogledu (predvidjeti, otkriti i spriječiti mogući napad i prije nago što se desi), odnosno u represivnom pogledu (otkriti izvršioca, prikupiti dokaze, dokazati djelo) adekvatno sankcionisati izvršioca. Dakle, nove tehnologije su omogućile izvršenje klasičnih krivičnih djela na novi način i novim sredstvima, odnosno tehnološki napredak omogćio je nastanak i razvoj novih krivičnih djela i kriminalizaciju određenog dijela populacije koja isključivo koristi nove tehnologije za rad i komunikaciju. Sve što je čovjek novo otkrio i iskoristio za svoj razvoj i napredak društva, dio populacije je isto to zloupotrebio u cilju destrukcije društveno-ekonomskog sistema i odnosa ili sticanja određene lične koristi na štetu drugih i/ili društva u cjelini. Trenutno najveću prijetnju svakom društvu, a posebno nerazvijenim društvima koja nemaju izgrađen efikasan bezbjednosni sistem zaštite, predstavlja novi vid kriminaliteta koji nazivamo kompjuterski ili sajber kriminalitet. Pod kompjuterskim ili sajber kriminalitetom podrazumijevaju se konkretna krivična djela koja se izvršavaju pomoću kompjutera kao sredstva izvršenja i/ili objekta napada, i kao takva su predviđena krivičnim ili nekim posebnim zakonima i sadrže sva specifična obilježja koja su vezana za sredstva i način njihovog izvršenja. (*Vasić, Šarić, Jovanić, 2012.*) Kao jedan od trenutno najzastupljenijih oblika kriminaliteta koji se ispoljava kroz nove forme prilagođene naučno tehnološkom razvoju društva u vidu transnacionalnog organizovanog kriminaliteta, kompjuterski (sajber) kriminalitet predstavlja najveću globalnu prijetnju. Prijetnja se ogleda u neograničenim mogućnostima koje pružaju IKT za brzo djelovanje, anonimnost, mogućnost prikrivanja ili potpunog uništenja tragova izvršenja krivičnog djela i za djelovanje sa velike daljine. Meta napada je kompjuter i/ili kompjuterski sistem i/ili mreža sa povezanim uređajima. Kompjuterski sistem označava svaki uređaj ili grupu međusobno povezanih ili uslovljenih uređaja, od kojih jedan ili više njih, u zavisnosti od programa, vrši automatsku obradu podataka, dok kompjuterski podaci označavaju svako izlaganje činjenica, podataka ili koncepata u obliku koji je pogodan za njihovu obradu u kompjuterskom sistemu, uključujući tu i odgovarajući program na osnovu kojeg kompjuterski sistem vrši svoju funkciju. (*Vasić, Šarić, Jovanić, 2012.*) Nova, kompjuterska, odnosno IKT elita, koristeći monopol nad tokovima informacija, u mogućnosti je da manipuliše društveno socijalnim mrežama, i utiču na određena dešavanja u kriminalnim, političkim i ekonomskim tokovima u određenom društvu. Današnjeg kompjuterskog eksperta (sa kriminalnim predispozicijama) moguće je profilisati kao uglavnom mladog, inteligentnog, visokomotivisanog, uzornog i povjerljivog radnika, spremnog da radi prekovremeno, da istražuje i da se bori s iznenadnim problemima u radnim situacijama kada je potreban dodatni napor kako bi se prevazišao nastali problem. (*Vasić, Šarić, Jovanić, 2012.*) Ovako potencijalno profilisano lice posjeduje veoma izgrađen logički sistem razmišljanja i savršeno poznavanje rada kompjutera, kompjuterskih mreža i sistema.

1. TEHNOLOGIJA U ISTRAZI

Naučno tehnološki razvoj omogućio je počinjenje postojećih krivičnih djela na novi način i novim sredstvima. Kriminalni dio društva nesporno prati tehnološki razvoj i koriguje svoja postupanja u skladu sa novim mogućnostima, prilagođava se i evoluira. Trenutno imaju prednost jer ne sprovode komplikovane procedure i rasprave za prelazak na novi način rada u

odnosu na pravni sistem ugroženog kolektiviteta, odnosno pravnu državu. Novi načini i sredstva izvršenja krivičnih djela zahtjevaju isti takav pristup za otkrivanje krivičnih djela, počinilaca i sprovođenje istrage. To praktično znači da nosioci istražne i pravosudne djelatnosti (policijske agencije, tužilaštva i sudovi) moraju pratiti nove tehnološke trendove u etiološkom i fenomenološkom pogledu, uspostavljati adekvatne i efikasne mehanizme i alate za sprečavanje i suprostavljanje novim pojavnim oblicima i vidovima krivičnih djela. Korištenje klasičnih metoda i sredstava za sprovođenje istraga i prikupljanje dokaza u krivičnim djelima koja su izvršena uz pomoć ili nad sredstvima informaciono komunikacionih tehnologija (IKT) je praktično nemoguće ili je vezano za određene poteškoće. Zakonodavac je iz ovih razloga razvio određene procedure i tehnike koje omogućavaju novi pristup u prikupljanju i dokumentovanju dokaza u istragama. Nove procedure su (od 2003. godine) ugrađene u važeće ZKP u Bosni i Hercegovini (kao posebna glava u važećim ZKP) pod nazivom „posebne istražne mjere i radnje“ a obuhvataju sedam radnji koje je moguće uz odobrenje suda (naredba nadležnog sudije za predhodni postupak) primjeniti u istragama.[101] Iako su ove procedure omogućile efikasniji rad policijskih agencija i tužilaštava, i dalje je ostao problem prikupljanja i dokumentovanja dokaza kod određenih krivičnih djela (kompjuterski ili sajber-cayber kriminalitet) koja su počinjena nad ili uz pomoć IKT (kao sredstvo izvršenja ili kao objekat napada). Iskorak u otkrivanju i sprečavanju ovih vrsta djela je učinjen od strane zemalja EU donošenjem Konvencije o sajber kriminalitetu 2003. godine u Budimpešti[102], aktivnostima grupe G8, INTERPOL-a i EUROPOL-a. Navedena Konvencija je dala osnovne smjernice državama potpisnicama za donošenje krivičnih i krivično procesnih zakona na nacionalnom nivou i definisanje univerzalnih principa za međunarodnu saradnju na polju suprostavljanja novim pojavnim oblicima kriminaliteta koji su vezani za IKT. Implementacija navedenih smjernica u domaća zakonodavstva nije u potpunosti dala mogućnost adekvatnog odgovora na nove prijetnje. Pored implementacije smjernica, neophodno je uvesti i nove metode u otrkivanju, dokumentovanju i dokazivanju novih oblika krivičnih djela kao i edukaciju relevantnih subjekata (policija, tužilaštva, sudovi). Pored navednih aktivnosti neophodno je sve to i pravno uobličiti i verifikovati kako bi se sve nove aktivnosti mogle koristiti u sudskom postupku kao relevantni dokazi. Klasične metode više nisu dovoljne i efikasne a nove još uvijek izazivaju podozrenje i strah za korištenje tako da se mnogi slučajevi vode duže od potrebnog vremena sa neizvjesnim rezultatom a ne rijetko dolazi i do obustavljanja istrage ili odbacivanja predmeta u kasnijoj fazi. Jedna od novih metoda koje se koriste u istragama a koja je vezana za IKT je oblast digitalne forenzike koja obuhvata sve segmente u istrazi (predistražne, istražne, procesne i radnje vještačenja i dokazivanja) a koristi u svom radu najsavremenije IKT. Praktično je nemoguće otkriti djelo počinjeno uz pomoć novih IKT ako se iste ne koriste i za otkrivanje djela, načina izvršenja djela i identifikaciju počinioca. Ovdje se radi o istrazi koja koristi takozvani „obrnuti put“ koji je ostao kao trag prilikom korištenja IKT za izvršenje krivičnog djela a koji vodi prema sredstvu izvršenja i izvršiocu. To znači da je svako logovanje, odnosno pristup putem IKT registrovan i da je ostao u sistemu i kao takav da je dostupan za analizu ukoliko se istraga vodi uz pomoć IKT i lica-eksperata (policijski službenik-digitalni forenzičar) koja su edukovana za ovu vrstu istrage (digitalna istraga i digitalna forenzika).

[101] ZKP RS član 234., ZKP BiH član 116., ZKP FBiH član 130., ZKP BD član 116.

[102] Konvencija o kibernetičkom kriminalu (Budimpešta 23.11.2001.), Odluka Bosne i Hercegovine o ratifikaciji Konvencije o kibernetičkom kriminalu: Na osnovu člana V.3.(d) Ustava Bosne i Hercegovine i saglasnosti Parlamentarne skupštine Bosne i Hercegovine (Odluka PS BiH br. 274/06 od 10. marta 2006.godine), Predsjedništvo Bosne i Hercegovine na 89. sjednici, održanoj 25. marta 2006. godine, donijelo je Odluku o ratifikaciji Konvencije o kibernetičkom kriminalitetu, Broj 01-011-398-12/06 25. mart 2006. godine, Sarajevo.

2. DIGITALNA FORENZIKA

Kao odgovor na visokotehnološki kriminal javila se potreba za razvojem nove naučne discipline koja će se njime baviti, kao i regulisanje pravnih osnova vezanih za uspješno procesuiranje krivičnih djela iz ove oblasti. (*Korać, 2012*) Da bismo shvatili novu oblast koja se naziva digitalna forenzika i njenu primjenu u materijalnom i procesnom pravu, potrebno je da se osvrnemo ukratko na njenu definiciju, nastanak i razvoj.
Digitalna forenzika je nauka koja ima za cilj oporavak[103], prikupljanje, čuvanje, pronalaženje, analizu i dokumentovanje digitalnih dokaza, odnosno podataka koji su uskladišteni, obrađivani ili prenošeni u digitalnom obliku na nekom pogodnom mediju.[104] Pojam digitalna forenzika u početku se koristio kao izraz isključivo vezan za kompjutersku forenziku ali je s vremenom dobijao sve širu dimenziju obuhvatajući i druge uređaje (hardware) koji su u interakciji sa kompjuterom a na kojima je moguće skladištenje i čuvanje digitalnih podataka u nekom digitalnom formatu. Sa razvojem i uvođenjem kompjuterskih tehnologija u sve segmente poslovanja i društveno ekonomskih odnosa (kasnih 1970-tih i ranih 1980-tih godina) razvila se 1990-tih godina disciplina koju početkom XXI vijeka uvode mnoge zemlje kroz nacionalne politike u zakonodavstva i nazivaju digitalna forenzika. Danas digitalna forenzika kao kompleksna nauka obuhvata sljedeće oblasti:

- Kompjuterska forenzika,
- Forenzička analiza podataka,
- Forenzika baza podataka,
- Forenzika mobilnih uređaja,
- Forenzika kompjuterskih mreža,
- Video forenzika,
- Audio forenzika.

Razvoj i kompleksnost digitalne forenzike uslovila je i specijalizaciju forenzičkih stručnjaka za pojedina područja. U vezi sa navedenim, forenzičari, odnosno informatičari redovno prate IKT trendove kako bi mogli da prilagođavaju svoje znanje potrebama i izazovima u istragama. Digitalni forenzičar, slijedeći strogo uspostavljena i definisana pravila, prikuplja digitalne dokaze sa medija i/ili medije za koje opravdano smatra da se na njima nalaze dokazi za kojima traga, osigurava ih od bilo kakvih promjena (utvrđuje heš (hash) vrijednosti svakog digitalnog dokaza-zapisa)[105] i sprovodi analizu prikupljenih dokaza i medija kako bi rekonstruirao aktivnosti koje su vršene nad njima i sačinio razumljiv i pravno utemeljen izvještaj (policijski službenik - vještak forenzičar svoj izvještaj na sudu prezentuje i brani) koji će poslužiti za vođenje sudskog postupka.[106] Utemeljenost izvršenih analiza prikupljenih digitalnih dokaza nadležni forenzičar dokazuje licenciranim softverom (alatima i mehanizmima) određenih kompanija koje prepoznaje i prihvata nacionalno zakonodavstvo konkretne države. Pored

[103] Oporavak ili restitucija podataka predstavlja proces kojim se uz pomoć određenog licenciranog softvera vraćaju podaci koji su namjerno obrisani ili oštećeni u cilju skrivanja izvršenog krivičnog djela i/ili identiteta izvršioca.
[104] https://hr.wikipedia.org/wiki/Digitalna_forenzika, 03/05/2022 u 13.10 h.,

[105] Heš (Hash) vrijednost predstavlja jedinstveni digitalni potpis koji se dodjeljuje digitalnom dokazu. Heš (Hash) funkcija je svaki algoritam koji podacima proizvoljne dužine dodeljuje podatke fiksne dužine. Vrijednost koju vraća hash funkcija zove se hash vrijednost ili hash kod. Heš (Hash) funkcije se prvenstveno koriste za generisanje fiksne dužine izlaznih podataka koji se ponašaju kao reference na originalne podatke. Ovo je korisno kada su originalni podaci suviše glomazni da bi se koristili u cijelosti, odnosno da se vrše potrebne analize na kopiranim sadržajima kako ne bi došlo do uništenja originalnih podataka.
https://sh.wikipedia.org/wiki/He%C5%A1_funkcija, 03/05/2022 u 14.57 h.
[106] https://wikihrhr.top/wiki/digital_forensics, 03/05/2022 u 13.16 h.

licenciranih analitičkih alata (software) svaki digitalni forenzičar (kao i bilo koji drugi forenzilčar iz bilo koje druge oblasti) mora da posjeduje odgovarajuću licencu-dozvolu za obavljanje poslova iz određene oblasti (položen ispit za forenzičara iz određene oblasti i upis u spisak ovlaštenih sudskih vještaka nadležnih sudova u nacionalnom zakonodavstvu). Kako je ova oblast nova, nadležne institucije u BiH još uvijek nisu (ili su u toku) uspostavile stručne komisije za polaganje ispita iz oblasti digitalne forenzike iako određeni policijski službenici obavljaju te poslove po inerciji i postojećim zakonodavnim okvirom koji podrazumijeva da sud prihvata izvještaje lica koja posjeduju određena znanja i iskustvo iz određene oblasti.[107] Ovo pitanje je pripritet zbog trenda rasta krivičnih djela počinjenih uz pomoć ili nad IKT. Od toga kako će se pravno uobličiti i rještiti problem u vezi sa istragama i nadležnim tijelima za sprovođenje istraga (policija, tužilaštvo, sudovi) zavisit će i ishod sudskih postupaka. To prije svega nameće obavezu zakonodavcu za implementaciju odgovarajućih tehnoloških rješenja i mogućnosti u nacionalno zakonodavstvo kroz adekvatne procedure i edukaciju svih relevantnih subjekata uključenih u istragu.

Pod digitalnom istragom podrazumijevamo postupak kojim se postavljaju, razvijaju i analiziraju određene verzije-hipoteze kojima se dolazi od mogućih odgovora na pitanja o nastalim digitalnim događajima a na osnovu korištenja digitalnih dokaza koji su pronađeni. Postupak je isti kao i kod klasičnih krivičnih djela (odbacivanje ili potvrđivanje verzije-hipoteze) ali je jedina razlika u dokazima koji su u digitalnom obliku, tako da kvalitet istrage zavisi od edukacije i znanja lica, policijskog službenika koji vodi istragu. Digitalni dokaz predstavlja svaki digitalni zapis (oblik) informacije na nosaču medija o događaju ili procesu koji je izvršen putem ili nad računarom, računarskom mrežom i/ili sistemom i uređajima uvezanim u sistem. Problem u određivanju pojma digitalni dokaz je tema mnogih rasprava i uglavnom se svodi na potrebu za mogućnost izjednačavanja pravne snage digitalnih i materijalnih dokaza, kao i dokaza u drugim oblicima i formama. U vezi sa digitalnim dokazima postoje i nedoumice u pogledu zapisa koje računari samostalno generišu bez vanjskog uticaja kao proizvod određenih procesa koji se odvijaju kao pomoćne aktivnosti (algoritmi) u kreiranju traženih podataka ili postupaka, nezavisno da li se radi o nasumičnim procesima koji nastaju kao određena greška (bug) u izvršenju programa (usljed promjena u električnom napajanju, EMP ili drugi uticaji) ili kao kreirani proces (samouništenje ili brisanje podataka) u situacijama koje su hipotetički ali ne i stvarno moguće (izostanak višestepene vanjske kontrole u radu sistema i njegovom resetovanju kao sigurnosnom mjerom pod uticajem više sile[108]). Kada su u pitanju podaci koji se kreiraju na osnovu ljudskog uticaja u vidu digitalnih zapisa koji se pohranjuju u računaru (memorijske jedinice, izmjenjive i trajne) ili se distribuiraju putem mreže u kompjuterski sistem i druge povezane uređaje, oni predstavljaju jedinstven digitalni potpis (digitalni trag, otisak) jednog ili više lica koji imaju snagu kao i otisak papilarnih linija ili DNK profil i predstavlja originalnu identifikacionu potvrdu.

Forenzička (digitalna) istraga kod krivičnih djela iz oblasti kompjuterskog (sajber-cayber) kriminaliteta predstavlja postupak koji obuhvata: otkrivanje (pretraga, istraga), izuzimanje-oduzimanje (sakupljanje, prikupljanje), forenzičko snimanje-kopiranje (izrada forenzičke kopije)[109], čuvanje (upravljanje), analizu digitalnih sadržaja i/ili digitalnih medija (testiranje i provjera verzija-hipoteza, dokazivanje) te izradu izvještaja o prikupljenim dokazima

[107] Zakon o krivičnom postupku Republike Srpske, Član 160., Službeni glasnik Republike Srpske, broj 53/2012, 91/2017, 66/2018 i 15/2021., isto je i u drugim procesnim zakonima koji su na snazi u Bosni i Hercegovini.
[108] Elementarne nepogode, rat - kad je neophodno zaštititi podatke od pada u neprijateljske ruke, odnosno pokretanje samouništenja ili nekog drugog procesa usljed izostanka opoziva.
[109] Zakon o krivičnom postupku Republike Srpske, Član 137a. Naredba za kreiranje forenzičke kopije , Službeni glasnik Republike Srpske, broj 53/2012, 91/2017, 66/2018 i 15/2021.

korišćenjem priznatih naučnih metoda i tehnologija (licencirani software i hardware) kako bi se verifikovali dobijeni rezultati u vidu relevantnih dokaza (svjedočenje-vještačenje, prezentacija) koji bi se koristili u postupku pred sudom. Dakle, cilj i ove itrage je utvrđivanje relevantnih činjenica i okolnosti u vezi sa izvršenjem djela (način izvršenja) i subjektivne veze sa izvršiocem (motiv).

Digitalna forenzika, kao nauka, ima široku primjenu i nije ograničena samo na policijsko-sudske i vojno-obavještajne aktivnosti, već ima aktivnu primjenu u bankarskom poslovanju, sektoru osiguravajućih društava kao i u kompanijama raznih profila koje koriste IKT za obradu podaka kojima raspolažu u svom poslovanju. Pored primjene novih metoda i naučnotehnoloških dostignuća u cilju sprovođenja određenih postupaka i analiza u digitalnoj istrazi i sudskom postupku, digitalna forenzika takođe sprovodi analize i testiranje ugroženosti nekog ciljanog sistema (naručena kontrolisana nasilna penetracija u zatvoreni i zaštićeni sistem) koji koriste IKT i predlaže na osnovu toga najbolja rješenja za zaštitu od svih vrsta ugrožavanja (unutrašnja i vanjska zaštita) u vidu softvera i hardvera (software i hardware).

3. NOVI POJMOVI U ISTRAZI, DIGITALNA ISTRAGA

Shodno predhodno navedenom i analogijom sa tradicionalnim istragama možemo reći da i kod ovih novih djela (s obzirom na sredstva i objekta izvršenja) razlikujemo:

- **Mjesto događaja** - (digitalno mjesto događaja) predstavlja uređaj koji generiše (kompjuter, pametni telefon, tablet ...) ili procesuira (server u mreži i/ili mreža, internet ili intranet) digitalne podatke i/ili medij nosač digitalnih podataka (baza podataka i/ili pohranjeni podaci) koji predstavlja sredstvo i/ili objekat napada. Priprema ili mjesto izvršenja krivičnog djela iniciranjem određenih digitalnih aktivnosti u sajber-cayber prostoru[110] koji su kao takvi inkriminisani pozitivnim nacionalnim pravnim propisima. S obzirom na okruženje u kontekstu mjesta izvršenja (mjesto događaja) možemo govoriti o osnovnom ili početnom mjestu izvršenja i narednom mjestu, gdje je nastupila prva ili sljedeća štetna aktivnost-posljedica (računar, mreža, server, sistem...).
- **Pravna kvalifikacija** - identifikacija protivpravne radnje od strane nadležne institucije u skladu sa pozitivnim pravnim propisima u nacionalnom okviru (iniciranje istrage - predkrivični postupak za potvrdu elemenata krivičnog djela i dostupnih dokaza u cilju pribavljanja neophodnih akata - naredba za pretres, oduzimanje predmeta, saslušanje lica, vještačenja ili druga pravna akta pribavljena od strane nadležnog tužilaštva i suda za sprovođenje istrage).
- **Dokaz, digitalni dokazi** - predstavlja svaki digitalni zapis (otisak u vidu log-fajla ili nekog drugog registracionog formata) koji je nastao (trajno ili privremeno i koji je kao takav registrovan u memoriji i/ili nakon toga obrisan) kao posljedica interakcije digitalnih aktivnosti iniciranih putem nekog digitalnog uređaja ili sistema ili u digitalnom uređaju, odnosno sistemu a na zahtjev čovjeka, odnosno potencijalnog izvršioca. Dokaz u ovom kontekstu je svaka informacija, zapis, podatak i/ili proces koji je nastao kao posljedica zahtjevane interakcije u/ili nad nekim digitalnim uređajem ili sistemom a kojim se može dokazati ta nezakonita interakcija (inkriminacija u postojećem materijalnom zakonodavstvu) i subjektivna veza sa nalogodavcem (procesno zakonodavstvo), odnosno izvršiocem inkrimisane aktivnosti.

[110] Sajber (Cyber) prostor predstavlja digitalni prostor (računarska memorija ROM i RAM, medij nosač digitalnih zapisa i informacija, interne i globalne mreže, baze podataka, serveri, snimači-storage, povezani uređaji-hardware, software) u kojem dolazi do interakcije digitalnih aktivnosti iniciranih putem određenih digitalnih uređaja a na zahtjev čovjeka.

- **Forenzička kopija,** nije definisana kao pojam u važećim procesnim zakonima u BiH i RS, iako se u procesnom smislu naređuje njena izrada (član 137a. ZKP RS)[111]. Ovakav pristup je opravdan sa aspekta zaštite integriteta originalnog digitalnog zapisa koji se nalazi na nekom nosaču medija, uređaju, serveru ili je pohranjen u neku bazu podataka i koji služi ili može poslužiti kao dokaz. Originalni uređaj u ovom kontekstu treba biti sačuvan jer je upravo on dokaz u postupku tako da nijedan podatak na njemu ne bi smio biti izmjenjen.
  Forenzička kopija predstavlja originalnu kopiju (identičnu originalu i na adekvatnom nosaču medija) digitalnih zapisa pohranjenih na nekom digitalnom uređaju ili nosaču medija (otisak u vidu log-fajla ili nekog drugog registracionog formata) koji su nastali (trajno ili privremeno i koji je kao takav registrovan u memoriji i/ili nakon toga obrisan) kao posljedica interakcije digitalnih aktivnosti iniciranih putem nekog digitalnog uređaja ili sistema ili u digitalnom uređaju, odnosno sistemu a na zahtjev čovjeka, odnosno potencijalnog izvršioca. Izrada forenzičke kopije kojoj se dodjeljuje heš (Hash) vrijednost[112] bitna je kako bi se mogle sprovesti sve forenzičke analize i radnje u istrazi a u cilju utvrđivanja istine i okolnosti pod kojima je došlo do određenog događaja (inkrimisanog djela) bez uticaja na originalne uređaje i nosače medija, odnosno digitalne zapise (izbjegavanje bilo kakvih izmjena ili uništenja sadržaja na originalnim digitalnim uređajima ili nosačima medija) koji se na njima nalaze a predstavljaju dokaze za postupak pred sudom. Izrada forenzičke kopije se primjenjuje i u slučajevima kada nije moguće iz objektivnih razloga fizički izuzeti digitalni uređaj ili nosač medija za transport u laboratoriju za digitalnu forenziku. Međutim, problem sa izradom forenzičke kopije koja se naređuje prema ZKP Republike Srpske i člana 137a se ogleda u nedostatku procedura koje se moraju koristiti za njenu izradu, a koju zakonodavac nije predvidio. Praktično to predstavlja opasnost jer često puta pristup određenim medijima i uređajima nije moguće bez predhodno sprovedenih procedura kojima se zaobilazi (bajpasira) zaštita koju je izvršilac instalirao upravo da bi spriječio prikupljanje dokaza i dokazivanje djela koje je počinio. Svaki neovlašteni pristup (ukoliko je uređaj ili nosač medija isključen, ili je uključen a nije u modu za korištenje bez autentifikacije i odgovarajućih kredencijala) automatski uključuje trajno uništenje uređaja ili nosača medija i pohranjenih zapisa. U navedenom kontekstu izrada forenzičke kopije nije moguća iako je naređena. U takvim situacijama neophodno je ukoliko je to moguće izuzeti originalan uređaj ili nosač medija ili korištenje blokatora[113] kako bi se izradila forenzička kopija.
- **Digitalna imovina,** definisana prema Zakonu o digitalnoj imovini Republike Srbije[114] predstavlja: „digitalna imovina, odnosno virtuelna imovina, označava digitalni zapis vrednosti koji se može digitalno kupovati, prodavati, razmenjivati ili prenositi i koji se može koristiti kao sredstvo razmene ili u svrhu ulaganja, pri čemu digitalna imovina ne uključuje digitalne zapise valuta koje su zakonsko sredstvo plaćanja i drugu finansijsku imovinu koja je uređena drugim zakonima, osim kada je drugačije uređeno ovim

[111] Naredba za izradu forenzičke kopije regulisana je samo u ZKP Republike Srpske, ostali procesni zakoni u Bosni i Hercegovini nemaju propisanu ovu radnju.
[112] Nakon provjere autentičnosti heš (Hash) vrijednosti forenzičke kopije, pristupa se skidanju i analizi kopiranih sadržaja (digitalna forenzika) kako bi se pohranjeni podaci u vidu digitalnih zapisa mogli logički povezati u cilju utvrđivanja činjenica i okolnosti o događaju (krivično djelo).
[113] Blokator predstavlja softver kojim se prepoznaje i blokira (zadržava) operativni sistem od unošenja bilo kakvih promjena u originalni (ili sumljivi medij na koji se prebacuje originalni sadžaj) medij kako bi se spriječilo oštećenje ili brisanje podataka koji mogu poslužiti kao dokazi.

[114] Zakon o digitalnoj imovini Republike Srbije, Službeni glasnik Republike Srbije broj 153/2020, Pojmovi član 2. stav 1).

zakonom“. Definicije imovine prema važećim krivičnim zakonima u BiH preferiraju pravnim dokumentima ili instrumentima (materijalnim supstratima) kojima se može dokazati pravo na imovinu iako ona može biti materijalna i nematerijalna i pokretna i nepokretna, s tim što pojam „digitalna imovina“ nije obuhvaćena u značenju pojmova i izraza u krivičnim zakonima. Prema tome, i materijalna i nematerijana imovina se mora materijalizovati u nekom adekvatnom dokaznom (fizičkom) obliku. Ako stavimo na stranu u ovom slučaju materijalnu imovinu koja ima svoj fizički, odnosno materijalni supstrat, postavlja se pitanje šta predstavlja nematerijalnu imovinu i kako je dokazati. Ovo je svakako tema za neku širu naučnu raspravu a u radu ćemo se fokusirati na pojam digitalna imovina.

Da bismo sagledali suštinsko značenje pojma imovine i njene ugroženosti novim djelima (novi načini izvršenja, sredstvo izvršenja i objekat napada) uz pomoć IKT, neophodno je da se upoznamo i sa novim pojmovima koji se vežu za imovinu a koji su tekovina naučno tehnološkog razvoja društvenih odnosa i društva u cjelini. Ovdje prije svega mislimo na razvoj IKT i pojmove digtitalno i virtuelno koji se sve češće pominju u svakodnevnim komunikacijama i medijima (internet). Ako sagledamo definiciju pojma virtuelno u jezičkom smislu, vidjet ćemo da pojam virtuelno predstavlja ono što proizilazi iz privida, ono što je nestvarno i što nema fizički oblik ili bilo koji drugi oblik. U filozofskom smislu pojam virtuelno predstavlja nešto što nije stvarno i postoji samo u umu pojedinca i može da posjeduje u određenim situacijama neke bitne kvalitete. Etimološki pojam vitruelno vodi porjeklo iz latinskog jezika od riječi *virtualis* u značenju moguć, ostvariv i riječi *virtus* u značenju hrabrost, sposobnost, vrlina. Riječ virtuelno se često spominje u kontekstu interneta i IKT i označava nešto što u fizičkom smislu ne postoji a što je vidljivo u kompjuterskom softveru koji to grafički simulira. Sagledavajući navedeno očito je da etimološko, odnosno lingvističko značenje pojma virtuelno i prihvaćenog (uobičajenog) značenja tog pojma u praksi i društveno socijalnoj komunikaciji nisu isto. Ako je nešto predstavljeno kompjuterskim softverom, bez obzira što to (oblik) ne postoji ili je nemoguće i nepostojeće u stvarnom životu (proces ili događaj) i komunikaciji, dobilo je svoj fizički, odnosno materijalni supstrat u vidu zapisa matematičkog algoritma, matematičkih, lingvističkih ili nekih drugih znakova i simbola a koji su putem GUI (Graphical User Interface) grafički uobličeni u digitalni oblik. Dakle, virtuelno je metrijalizovano i nije više virtuelno, dobilo je svoj digitalni oblik koji se može i materijalizovati u vidu ispisa na papir. Digitalna imovina bi bio prihvatljiv izraz za imovinu čiji je materijalni supstrat (vrijednost) predstavljena matematičkim algoritmima u vidu softvera (određeni program) putem određenih impulsa, signala ili grafike u digitalni oblik kako bi se lakše, jednostavnije ili brže izvršila razmjena ili pružila neka druga usluga putem nekog IKT uređaja. Sagledavajući navedeno, imamo materijalnu vrijednost koju predstavljamo digitalno (koja ostaje ista) i koja se putem sistema IKT uvezanih kompjutera u mrežu distributira drugim pravnim ili fizičkim licima na udaljene lokacije gdje se mogu konvertovati, odnosno transformisati u materijalni oblik i vrijednost. Ovakva imovina i dalje ima svoju vrijednost u materijalnom supstratu upravo iz razloga saglasnosti volja (obligacioni odnos) između lica koja vrše razmjenu. Transakcija se zasniva na međusobnom povjerenju i ima visok stepen zaštite od mogućnosti trećih lica da saznaju za detalje transakcije. Svako logovanje se evidentira i o tome ostaje trajni zapis.

4. ZAKLJUČAK

I pored shvatanja i razumijevanja novih (IKT) pojmova u vezi sa dokazima i primjene novih naučnotehnoloških metoda (digitalna forenzika) u istragama, neophodno je da se u sve istražne radnje u novom kriminalnom okruženju i događajima koji ih prate, uvede pravilna primjena

pravnih propisa u smislu utvrđivanja i dokazivanja svih relevantnih činjenica koje se kao rezultat istrage mogu koristiti u sudskom postupku. Kako su dokazna sredstva (dokazi) izvor saznanja za sud o postojanju činjenica koje su odlučujuće u utvrđivanju istine (činjeničnog stanja) a koja se koriste u dokaznom postupku primjenom određenih procesnih radnji od strane suda i stranaka u postupku, a povodom prikupljenih dokaza i činjenica, onda je sasvim jasno da je neophodno i sve nove pojmove i izraze kao i naučnotehnološke metode i radnje koje se koriste, pravno uobličiti i propisati u procesnom smislu. Ovo je prije svega važno kako bi se prikupljeni dokazi (digitalni dokazi), dokazni postupak i vještačenja (digitalna forenzika) mogli pravno verifikovati i iskoristiti u sudskom postupku koji bi se okončao donošenjem adekvatne sudske odluke (odluka, presuda, rješenje, naredba...). Iako sve situacije nije moguće unaprijed predvidjeti i pravno regulisati, zakonodavac je određene institute postavio uopšteno kako bi omogućio usklađivanje sa novonastalim trendovima, prije svega zbog fragmentarnog karaktera krivičnog prava. (*Stojanović, 2020*) Prema važećim zakonim o krivičnom pstupku u Bosni i Hercegovini u poglavljima Značenje izraza pod Osnovni pojmovi, zakonodavac nije uopšte ili nije u potpunosti definisao pojmove: dokaz, dokazni postupak, digitalni dokaz (novu vrstu dokaza), digitalna istraga, digitalna forenzika, kao ni potpuno novi prostor (sajber-cyber, odnosno digitalni prostor) u kojem se odvijaju postojeći i neki novi pojavni oblici krivičnih djela (uz pomoć potpuno novih sredstava izvršenja i prema novom objektu napada). Dokazi koji nastaju prilikom izvršenja krivičnih djela u novonastalom prostoru se nalaze i ispoljavaju u potpuno novom, digitalnom formatu što može da predstavlja određni problem za njihovu upotrebu u sudskom postupku. Transformacija digitalnog dokaza u materijalni (papirni) oblik prihvatljiv za sudski postupak, takođe može predstavljati problem jer ni ovaj postupak nije naveden u značenju izraza i osnovnih pojmova u procesni zakon. Pored navedenih nedostataka, najveći problem je svakako nedostatak edukovanih kvalifikovanih operativnih radnika, tužilaca i sudija, odnosno operativnih, tužilačkih i pravosudnih specijalizovanih organizacionih struktura. Iz navedenog je očito da je digitalna forenzika kao nauka bitan faktor u istragama vezanim za IKT i da je neophodno da kao takva dobije mjesto u pravom sistemu u svakom nacionalnom zakonodavstvu. To znači da bi pravnici (policijski službenici, tužioci i sudije) trebali da posjeduju određena informatička znanja za sprovođenje istrage (digitalna istraga), odnosno, da bi mogli koristiti dostupne naučne metode i sredstva (digitalna forenzika) u skladu sa propisanim standardima kako bi prikupljeni dokazi (digitalni dokazi), činjenice i nalazi vještačenja (digitalna forenzika) bili korišteni i prihvaćeni u sudskom postupku.

Preporuke:

- U sve procesne zakone u Bosni i Hercegovini potrebno je implementirati nove pojmove i izraze koji su vezani za IKT (digitalni dokazi, digitalna istraga, digitalna imovina, sajber-cayber prostor, digitalna forenzika...) kao i nove metode za prikupljanje dokaza, njihovu analizu i vještačenje.
- Propisati procedure za sprovođenje novih istraga (digitalna istraga) s obzirom na nova krivična djela, trendove i okruženje.
- Uvesti nove vještake na postojeće liste vještaka (vještak za digitalnu forenziku), propisati nove procedure za izbor i imenovanje novih vještaka, kao i potrebne opšte i posebne uslove za obavljanje poslova.
- Izvršiti edukaciju u svim relevantnim isnstitucijama iz oblasti IKT i uspostaviti specijalizovane strukture u istražnom, tužilačkom i sudskom kapacitetu za efikasno suprostavljanje novim pojavnim oblicima krivičnih djela i saradnju u nacionalnom i međunarodnom okruženju.
- Standardizovati neophodne licencirane softvere (program) i hardvere (uređaje) i formate, odnosno oblike za predstavljanje dokaza, analiza i izvještaja za obavljanje određenih poslova i procedura u sprovođenju istrage i vještačenja koji će na sudu biti prihvaćeni kao dokazi.

- Omogućiti bržu i efikasniju izmjenu procesnih zakona s obzirom na trendove.

5. LITERATURA

[1] Korać, V.: *Digitalna forenzika kao arheologija podataka u visokotehnološkom kriminalu,* Centar za nove tehnologije Viminacium Arheološki institut Beograd, Beograd 2012., strana 77.
[2] Stojanović, Z.: *Krivično pravo opšti deo*, Univerzitet u Beogradu - Pravni fakultet Centar za izdavaštvo i informisanje, Beograd 2020, strana 6.
[3] Vasić G., Šarić B., Jovanić V.: *Kompjuterski kriminalitet*, Zbornik radova, Međunarodna naučnostručna konferencija, Suzbijanje kriminala i Evropske integracije, s osvtrom na visokotehnološki kriminal, Hans Zajdel fondacija u saradnji sa Vlada Republike Srpske Ministarstvo unutrašnjih poslova Uprava za policijsko obrazovanje Visoka škola unutrašnjih poslova Republika Srpska, Laktaši 2012., strana 181, 183 i 184.

Zakoni

[1] Zakon o krivičnom postupku Bosne i Hercegovine, „Službeni glasnik Bosne i Hercegovine“, br. 3/2003, 32/2003 - ispr, 36/2003, 26/2004, 63/2004, 13/2005, 48/2005, 46/2006, 29/2007, 53/2007, 58/2008, 12/2009, 16/2009, 53/2009 - dr. zakon, 93/2009, 72/2013 i 65/2018.
[2] Zakon o krivičnom postupku Brčko Distrikta Bosne i Hercegovine, „Službeni glasnik Brčko Distrikta BiH“ br. 34/2013-prečišćeni tekst, 27/2014, 3/2019 i 16/2020.
[3] Zakon o krivičnom postupku Federacije Bosne i Hercegovine, „Službene novine Federacije BiH“, br. 35/2003, 56/2003 - ispravka, 78/2004, 28/2005, 55/2006, 27/2007, 53/2007, 9/2009, 12/2010, 8/2013, 59/2014 i 74/2020).
[4] Zakon o digitalnoj imovini Republike Srbije, „Službeni glasnik Republike Srbije“ broj 153/2020.
[5] Zakon o krivičnom postupku Republike Srpske, “Službeni glasnik Republike Srpske“, broj 53/2012, 91/2017, 66/2018 i 15/2021.

Internet

[1] https://hr.wikipedia.org/wiki/Digitalna_forenzika, 03/05/2022 u 13.10 h.
[2] https://sh.wikipedia.org/wiki/He%C5%A1_funkcija, 03/05/2022 u 14.57 h.
[3] https://wikihrhr.top/wiki/digital_forensics, 03/05/2022 u 13.16 h.