eudaimonia

Revija za pravnu, političku i socijalnu teoriju i filozofiju

Vol. 8 No. 1 • 2024.

Izdavač

IVR Srbija

Srpsko udruženje za pravnu i socijalnu filozofiju

KRAĐA IDENTITETA KAO KRIVIČNO DELO: *DE LEGE LATA* I *DE LEGE FERENDA*

Nataša Ranković

Strane: 123–132

UDK 343.525:004.738.5
DOI 10.51204/IVRS_24106A

Nataša Ranković*

KRAĐA IDENTITETA KAO KRIVIČNO DELO: *DE LEGE LATA* I *DE LEGE FERENDA*

U radu su definisani osnovni pojavni oblici kompjuterskog kriminala sa akcentom na krađu identiteta kao posebnom obliku koji bi de lege ferenda okarakterisali i adekvatno propisali kao krivično delo u Krivičnom zakponiku Republike Srbije. Cilj ovog rada je da se pokaže mesto krađe identiteta u spektru raznih kriminalnih radnji koje se svrstavaju u visokotehnološki kriminal. Rad je podeljen na tri celine. Prva predstavlja uvodno izlaganje u kome je opisan način na koji utiče veoma brz razvoj informacionih i komunikacionih tehnologija na razvijanje novih metoda za njihovu zloupotrebu, nakon čega su opisane definicije krađe identiteta i njene karakteristike. Drugi deo rada je posvećen načinima, obeležjima i modalitetima krađe identiteta, dok je u trećem delu značaj dat načinima zaštite i prevencije krađe identiteta te argumentovan predlog za njeno definisanje u Krivičnom zakoniku Republike Srbije. Na kraju rada dat je kratak sažetak u vidu zaključka.

Ključne reči: *visokotehnološki kriminal, kompjuterski kriminal, krađa identiteta, krivični zakonik, krivično delo*

1. UVOD

Napretkom i brzinom razvoja informacionih i komunikacionih tehnologija recipročno raste broj njihove zloupotrebe u vidu narušavanja poverljivosti informacija, ometanja njihove funkcionalnosti, uzurpiranja i krađe intelektualnih dobara i raznih vrsta krađa i prevara. Visokotehnološki kriminal je relativno nov oblik kriminalnog ponašanja, veoma složen i adaptivan u odnosu na brzinu razvoja tehnologije, lako se širi i razvija nove oblike. Prilikom određivanja termina visokotehnološkog kriminala može se naići na veliki broj različitih definicija, međutim svima je zajednički element vršenje kriminalne radnje kori-

* Autorka je studentkinja osnovnih akademskih studija na Pravnom fakultetu Univerziteta u Beogradu, *natasarankovic24@gmail.com*.

šćenjem tehnika visoke tehnologije, pri čemu je naneta šteta žrtvama kriminalne radnje.

Mrežno okruženje i internet pružaju širok dijapazon mogućnosti za krađu i poslovnih i drugih tajni, softvera i autorskih dela, ali predstavljaju i veoma pogodno područje za krađu ličnih tajni i njihovu zloupotrebu krađom novca i drugim napadima na ličnost. Krađa identiteta kao oblik visokotehnološkog kriminala prolazila je kroz razne faze definisanja, međutim svi bitni elementi obuhvaćeni su sledećim određivanjem: „Krađa identiteta je forma kriminala u kojem neko koristi tuđi identitet da bi izvršio kriminalnu radnju" (Đukić 2017, 100). Krađa identiteta je zapravo poseban oblik visokotehnološkog kriminala koji objedinjuje nelegalno pribavljanje poverljivih ličih podataka za jedno ili više lica i upotrebu tih podataka za izvršenje novih krivičnih dela, pri čemu se nelegalno pribavljanje podataka o ličnosti obavlja bez znanja osobe koja predstavlja žrtvu uz prisvajanje njenog imena i drugih ličnih podataka. Kako smo videli, jedan od uočljivijih fenomena savremenog sveta je sve češće korišćenje podataka nekog drugog lica sa ciljem da se pribavi nekakva korist ili da se nanese šteta. Iz tog razloga se pribegava različitim propisima kojima se definišu jasna pravila o postupanju sa podacima o ličnosti, uređuje se kako se s njima postupa, kako se čuvaju i po potrebi uništavaju. U svetlu toga nezaobilazno je pitanje – kako stvari stoje kod nas?

2. POJAM KRAĐE IDENTITETA

Krivična dela koja spadaju u visokotehnološki kriminal uslovno se mogu podeliti na dve vrste – krivična dela koja se tiču isključivo visokotehnološkog kriminala i krivična dela koja imaju elemente visokotehnološkog kriminala, ali nisu isključivo u nadležnosti Posebnog tužilaštva i Odeljenja za suzbijanje visokotehnološkog kriminala. Prvu grupu krivičnih dela čine krivična dela koja su uređena u glavi dvadeset sedam Krivičnog zakonika[1] (čl. 298–304a). U drugu grupu spada mnogo više krivičnih dela nego u prvu. To su krivična dela protiv intelektualne svojine (član 198, 199, 202), ali i pojedinačna krivična dela, kao što su ugrožavanje sigurnosti, najčešće putem društvenih mreža (čl. 138), neovlašćeno objavljivanje i prikazivanje tuđeg spisa, portreta

[1] Krivični zakonik Srbije – KZ, *Sl. glasnik RS* 85/2005, 88/2005 – ispr., 107/2005 – ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019.

i snimka (čl. 145), neovlašćeno prikupljanje ličnih podataka (čl. 146), prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju (čl. 185), iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnog dela protiv polne slobode prema maloletnom licu (čl. 185b), falsifikovanje i zloupotreba platnih kartica (čl. 243) i druga krivična dela za čije se izvršenje koriste računari.

Izraz „socijalni inženjering" se često u istoriji spominjao kao zamena za izraz „krađa identiteta". Socijalni inženjering, u značenju u kojem je ranije korišćen, podrazumevao je širok dijapazon načina manipulisanja ljudima ubeđivanjem i lažnim predstavljanjem radi pribavljanja željenih informacija, pri čemu se nisu morala koristiti tehnička sredstva. Dakle, socijalni inženjering je u sadržajnom smislu širi pojam od krađe identiteta. Pod opštim pojmom krađe identiteta mogu se podrazumevati različiti modeli i pojavni oblici krađe podataka o ličnosti i veliki broj metoda i postupaka njihove upotrebe prilikom izvršenja novih kriminalnih radnji (Đukić 2017, 101).

Pojavom interneta, računari su počeli da se koriste za krađu informacija, novca i mnogih drugih stvari, međutim, neretko se dešava da lopovi kradu celokupan identitet strpljivo, prikupljajući informacije i podatke nekog lica. Sve većim i bržim razvojem novih tehnologija značajno se olakšavaju prikupljanje ličnih informacija, njihovo deljenje, ali i njihova zloupotreba. Zanimljivo je to što polaznu tačku za izvršenje kriminalnih dela čine različite vrste drugih oblika kriminalnih aktivnosti koje se dovode u vezu sa sajber kriminalom i koje u osnovi, zapravo, imaju krađu identiteta (Vidojković 2015, 47).

Dragan Prlja i Mario Reljanović su se bavili određivanjem pojma krađe identiteta. U svom radu govore o krađi lika i identiteta i drugim vidovima (ne)zakonitog ponašanja, a krađu identiteta određuju kao: „preuzimanje 'uloge' nekog lica na Internetu, redovno u cilju sticanja neke materijalne ili druge koristi" (Prlja, Reljanović 169). Prlja i Reljanović karakterizuju krađu identiteta kao: najdrastičniji atak na privatnost ličnosti jer se učinilac, nakon što je prevarom ili na drugi način došao do vitalnih podataka za preuzimanje nečijeg identiteta (internet i druge šifre, brojevi platnih kartica i sl.), predstavlja u njegovo ime, zaključuje poslove ili ostvaruje društvene kontakte, ispravno primećujući i da može vršiti krivična dela na taj način, prikriven iza tuđeg identiteta (Prlja, Ivanović, Reljanović 2011, 110). U svom radu su pružili i sopstvenu definiciju po kojoj: krađa identiteta pretpostavlja prethodno

izvršenje nekog drugog krivičnog dela kao što su prevare, upadi u tuđi računar ili računarski sistem itd.

Krađa identiteta je krivično delo u čijem se izvršenju neko lice lažno predstavlja kao drugo lice (sa identifikacionim podacima tog drugog lica) sa namerom da pribavi protivpravnu imovinsku korist ili druge lične koristi. Žrtva ili pasivni subjekt tog dela može biti fizičko ali i pravno lice, kao što i izvršilac može biti pojedinac ili više lica, koja predstavljaju delove organizovane grupe (Prlja, Ivanović, Reljanović 2011, 108). Ne možemo reći da je redak slučaj da se krađa identiteta koristi kao sekundarno krivično delo kako bi se izvršilo primarno, gde se pojavljuje kao sredstvo kojim se vrši glavno delo, kako bi izvršilac sakrio svoj trag. Klasični primeri takvog načina izvršenja, danas svima poznati, jesu prevare sa kreditnim karticama i podnošenje lažnih dokumenata za dobijanje kredita na ime lica čiji je identitet ukraden.

Kao što možemo videti, u najvećem broju slučajeva krajnji cilj krađe identiteta je izvršenje novog krivičnog dela čija posledica može biti materijalne ili nematerijalne prirode. Iz tog razloga je u mnogim anglosaksonskim državama predviđena kao krivično delo, dok evrokontinentalne države stoje na stanovištu da je identitet na adekvatan način dovoljno zaštićen postojećim krivičnim delima poput prevare, lažnog predstavljanja, falsifikovanja isprave, neovlašćenog prikupljanja ličnih podataka i sl. (Bajović 2018, 262).

3. OBELEŽJA I MODALITETI KRAĐE IDENTITETA

Izraz „fišing" se u savremenoj literaturi definiše kao najčešći vid krađe identiteta koji podrazumeva skup aktivnosti kojima neovlašćena lica korišćenjem lažnih elektronski poruka ili lažnih internet stranica korisnike interneta navode da otkriju poverljive podatke (JMBG, korisničko ime, lozinku, PIN kartice i sl.).

Prevaranti metodom fišinga ili širenjem računarskih virusa preuzimaju lozinke i otimaju mejl adrese korisnika, a čitanjem mejlova dolaze do značajnih saznanja o toj osobi. Ako, recimo, saznaju da je neko otputovao u inostranstvo, ne libe se da sa njegove internet adrese, nakon što preuzmu kontrolu nad njom, poznanicima žrtve pošalju poruke. Lažno se predstave kao da su vlasnici tog naloga, tvrde da su pokradeni i da treba da im se na određeni račun uplati novac da bi doputovali kući (Ivanović 2021, 284).

Korisnici interneta imaju sve veću svest i znanje o fišingu te su oprezniji, ali su izvršioci takvih krivičnih dela u koraku sa razvojem tehnologije, pa su razvili nove tehnike. Slanje poruka kojima se korisnici ubeđuju da posete neku internet stranicu na adresi iz lažne poruke zamenili su virusima kako bi se od žrtava prevare preuzimali osetljivi podaci.

Zahvaljujući sve bržem razvoju tehnologije, razvijaju se i razne vrste fišinga: farming, spam, ciljani fišing, fišing pretraživačkih servisa, koji se, kao noviji oblik fišing prevare, sastoji u kreiranju veb-stranica (sajtova) u vezi s lažnim proizvodima i uz pomoć kojeg izvršilac dolazi do poverljivih informacija tako što žrtvu navede da naruči te lažne proizvode ili da se loguje na takve sajtove.[2]

S obzirom na karakteristike te vrste napada, može se reći da je fišing izrazito sofisticirana pojava, koja je u velikom usponu. Kao izvršioci se ne javljaju amateri već su najčešće u pitanju profesionalci, organizovani u grupe sa vrlo preciznim ulogama i delatnostima. Takođe, veoma je moguća veza tog oblika kriminala sa organizovanim kriminalom (Ivanović 2021, 294).

Krađe identiteta na osnovu pribavljenih informacija o ličnosti mogu se ostvariti na više načina: zloupotrebom postojećih računa (kreditnih kartica, tekućih bankovnih računa); zloupotrebom postojećih računa (na kojima nisu izdate kreditne i platne kartice) i zloupotrebom postojećih uz korišćenje debitnih i kreditnih kartica, a moguće je vršiti i klasična krivična dela, kao što su falsifikovanje kartice ili zloupotreba postojećih podataka (Ivanović 2021, 332).

Munjevitim napretkom tehnologije, internet servisi postaju pogodan ambijent za krađu i zloupotrebu identiteta. Krađa identiteta započinje prisvajanjem ličnih podataka o nekom licu, bez pristanka i znanja tog lica, obmanom, krađom i prevarom, a nastavlja se upotrebom prikupljenih podataka za izvršenje krivičnih dela koja se u najvećem broju slučajeva odnose na sticanje protivpravne imovinske koristi licima koja zloupotrebljavaju ukradeni identitet (Milošević, Urošević 2009, 53–64).

Ne može se reći da je redak slučaj da se krađa identiteta, korišćena kao sekundarno krivično delo kako bi se izvršilo primarno, pojavljuje i kao sredstvo kojim se vrši glavno delo, kako bi izvršilac sakrio svoj trag ili ga zametnuo (Marković 2021, 7). Klasični, svakome po-

[2] Više o tome u: Ivanović 2021, 288–300.

znati primeri su prevare sa kreditnim karticama ili podnošenje lažnih dokumenata za dobijanje kredita na ime lica čiji je identitet ukraden.

Krađe podataka se naširoko koriste u fišing napadima sa ciljem komercijalne i industrijske špijunaže, na osnovu pretpostavke da se na privatnim računarima zaposlenih nalaze veće količine poverljivih informacija i podataka o njihovih firmi. Tim putem se može doći i do dokumentacije kao što su poslovna prepiska ili dokumenti o zaštićenim dizajnima, čijim se objavljivanjem nanosi ekonomska šteta ili urušava reputacija žrtve (Ivanović 2021, 297). Dakle, u najvećem broju slučajeva krajnji cilj krađe identiteta je izvršenje novog krivičnog dela, čija posledica može biti materijalne ili nematerijalne prirode, zbog čega je u mnogim anglosaksonskim državama predviđena kao krivično delo, dok se evrokontinentalne države drže mišljenja da je identitet na adekvatan način i dovoljno zaštićen postojećim krivičnim delima (prevara, falsifikovanje, zloupotreba, lažno predstavljanje).

Krađa identiteta ima i međunarodnu dimenziju. Obično izvršioci i žrtve nisu u istim državama, što povlači pitanja jurisdikcija, primenu načela *nullum crimen nulla poena sine lege* i probleme nadležnosti institucija za saradnju (Ivanović 2021, 339).

4. ZAŠTITA I PREVENCIJA OD KRAĐE IDENTITETA

Zvonimir Ivanović zauzima pozitivan stav kada je reč o postojanju potrebe da se na adekvatan i sveobuhvatan način definiše krivično delo krađe identiteta. Međutim, kako se pojam krađe identiteta koristi veoma neprecizno, čemu doprinosi nepostojanje opšteprihvaćene definicije, inkriminacija krađe identiteta je otežana već na samom početku. Pojam krađe identiteta se prvenstveno koristi u značenju krađe, to jest radnje pribavljanja i upotrebe identifikacionih obeležja drugog lica, a s druge strane taj termin označava i krivična dela izvršena upotrebom tuđeg identiteta putem tuđih identifikacionih obeležja.

Velika Britanija krađu identiteta nije smatrala krivičnim delom sve do 2007. godine kada je prevara inkriminisana u zakonu *UK Fraud Act 2006*[3], obuhvatajući i prevaru izvršenu onlajn. Prema tom zakonu, prevara se može izvršiti na tri načina: 1. lažnim predstavljanjem, pri-

[3] Fraud Act 2006, Chapter 35. *https://www.legislation.gov.uk/ukpga/2006/35*, poslednji pristup 26. septembra 2023.

kazivanjem činjenica, 2. namernim neiznošenjem i prikrivanjem činjenica i 3. zloupotrebom položaja i odnosa podređenosti ili zavisnosti.

Možda najbolje inkriminisana krađa identiteta, kako tvrdi Ivanović (2021, 340), u SAD se definiše pod naslovom prevara i aktivnosti povezane sa identifikacionim dokumentima, autentifikacionim sredstvima i informacijama, te se pod krađom identiteta podrazumeva: „svesno transferisanje, posedovanje ili korišćenje, bez zakonskog ovlašćenja, sredstva za identifikaciju drugog lica u nameri izvršenja, pomaganja ili navođenja na izvršenje, ili u vezi sa delom, koje predstavlja delo kažnjivo delo po federalnom ili zakonu države članice SAD, kao i lokalnim propisima".[4] Tim delom se pokriva širok dijapazon radnji povezanih sa identifikacionim sredstvima, pa tako i krađom identiteta.

Kanada je krajem 2007. godine uvela krađu identiteta kao poseban oblik krivičnog dela, a kao razlog za preciznije definisanje navedena je okolnost da postojeći krivični zakon ne obuhvata sve elemente tog krivičnog dela. Naime, zloupotreba tuđeg identiteta je pokrivena zakonom kao falsifikovanje ili lažno predstavljanje, ali pripremne radnje za krađu identiteta, kao što su prikupljanje, posedovanje i promet podataka za identifikaciju, nisu obuhvaćene postojećim krivičnim delima. Svrha inkriminacije tih krivičnih dela je popunjavanje praznina u krivičnom zakonu (Ivanović 2021, 335).

Što se tiče standarda, Srbija je 2006. godine potpisala Konvenciju 108 Saveta Evrope, kojom se reguliše oblast zaštite podataka, čime je na sebe preuzela određeni standard u toj oblasti, ali ga, međutim, u praksi slabo primenjuje (Đalović 2018, 28). U navođenju zakona kojima se indirektno reguliše oblast računarske prevare, neophodno je naglasiti da krađa identiteta nije *de lege lata* inkriminisana kao krivično delo u krivičnom zakonodavstvu. Neki od zakona kojima se reguliše ta oblast su: Zakon o elektronskim komunikacijama, Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Zakon o zaštiti podataka o ličnosti i Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu.

Ivanović naglašava da je u određivanju prostora za inkriminaciju krađe identiteta neophodno prepoznati nekoliko segmenata samog akta koji bi se mogao definisati kao prevarno pribavljanje i korišće-

[4] United States Code (U.S.C.) Title 18, Section 1028 (a) (7): „a single identification document or false identification document that contains 1 or more means of identification shall be construed to be 1 means of identification".

nje identifikacionih obeležja drugog lica. Akcenat stavlja na to da se delo može izvršiti fizičkim putem, bez primene tehničkih i tehnoloških sredstava, ali i uz pomoć, u svakodnevnim životima sve zastupljenijih, interneta i tehničkih i tehnoloških metoda.

Takođe, izdvaja i tri faze napada: 1. izvršilac ubeđuje žrtvu, metodama socijalnog inženjeringa, da otkrije poverljive informacije i podatke na određenom sajtu u nameri da ih koristi u kriminalne svrhe; 2. izvršilac pribavlja podatke o kreditnim karticama ili debitnim karticama žrtve, koje potom koristi za naručivanje ili pribavljanje robe i usluga; 3. izvršilac pribavlja podatke o korisničkom imenu i lozinki na internet nalogu i imejl adresu i koristi ih da šalje mejlove sa negativnim sadržajem (Ivanović 2021, 338). Može se zaključiti da Ivanović, na osnovu izloženih zakonskih inkriminacija, smatra da, u smislu pokrivenosti i u odnosu na svakodnevno ažuriranje i menjanje pojavnih oblika, tradicionalnim oblicima krivičnih dela ne može da bude potpuno obuhvaćeno svako delo te vrste.

5. ZAKLJUČAK

Sve brži i sve turbulentniji napredak tehnologija znatno olakšava njihovo korišćenje, ali i zloupotrebu, pa se tako sve češće javljaju slučajevi kriminala putem interneta. Internet je, kako vidimo, pogodno tle za razne vrste kriminala, od povrede prava na privatnost zloupotrebom društvenih mreža, pa sve do krađe identiteta. Krađa identiteta je u domaćem krivičnom zakonodavstvu indirektno uređena drugim propisima (primera radi: neovlašćen pristup zaštićenom računaru, zloupotreba podataka o ličnosti i dr.), međutim, radi preciznijeg i bližeg određivanja i jednostavnijeg određivanja sankcija, krađa identiteta bi mogla da se podvede pod krivična dela visokotehnološkog kriminala, krivična dela protiv bezbednosti računarskih podataka, pomenuta krivična dela neovlašćen pristup zaštićenom računaru i zloupotreba podataka o ličnosti itd. Opet, tu se javlja problem pod koje krivično delo podvesti krađu identiteta tako da bude na adekvatan način definisana i sankcionisana, a da pri tome obuhvati sve oblike u kojima se javlja. Značajno je obratiti pažnju na to kako je krađa identiteta definisana u SAD jer je tim krivičnim delom obuhvaćen širok dijapazon radnji povezanih aa identifikacionim sredstvima, što smanjuje

mogućnost pojave praznina u njihovom krivičnom zakonodavstvu. To je dobar primer inkriminacije i jasnijeg određivanja i definisanja krađe identiteta koji bi mogao da bude koristan za eventualno preciziranje i definisanje krađe identiteta u domaćem krivičnom zakonodavstvu. Situacija u domaćem zakonodavstvu je najsličnija onoj u kanadskom, pa možemo povući paralelu u kontekstu analogije u odnosu na njega i u nekoj skorijoj budućnosti, vodeći se primerom inkriminacije krađe identiteta u kanadskom ili krivičnom zakonodavstvu SAD, u domaće uvesti krivično delo krađe identiteta.

LITERATURA

1. Antonović, Ratomir. 2023. *Sajber kriminalitet kao kriminalitet današnjice*. Beograd: Centar za stratešku analizu.
2. Bajović, Vanja. 2018. *Krađa identiteta i krivičnopravna zaštita ličnih podataka u sajber okruženju*. Beograd: Pravni fakultet Univerziteta u Beoradu.
3. Vidojković, Miloš. 2015. *Kompjuterski kriminalitet*. Master rad. Niš: Pravni fakultet Univerziteta u Nišu.
4. Đalović, Ratko. 2018. *Krađa identiteta*. Diplomski rad. Beograd: Fakultet bezbednosti Univerziteta u Beogradu.
5. Đukić, Anđelija. 2017. *Krađa identiteta – oblici, karakteristike i rasprostranjenost*. Beograd: Fakultet bezbednosti Univerziteta u Beogradu.
6. Ivanović, Zvonimir. 2021. *Kriminalistički aspekti visokotehnološkog kriminala*. Beograd: Kriminalističko-policijski univerzitet u Beogradu.
7. Marković, Stefan. 2021. *Mogućnost suprotstavljanja visokotehnološkom kriminalu u Republici Srbiji*. Master rad. Beograd: Fakultet bezbednosti Univerziteta u Beogradu.
8. Milošević, Milan. 1/2007. Aktuelni problemi suzbijanja kompjuterskog kriminala. *NBP (Nauka, bezbednost, policija)* 12: 57–74.
9. Milošević, Milan, Vladimir Urošević. 2009. Krađa identiteta zloupotrebom informacionih tehnologija. 53–64. *Bezbednost u postmodernom ambijentu*, zbornik radova, knjiga VI.
10. Mirković, Dragan. 2017. *Kriminološki aspekti komputerskog kriminaliteta*. Niš: Pravni fakultet Univerziteta u Nišu.
11. Prlja, Dragan, Mario Reljanović. 3/2009. Visokotehnološki kriminal – uporedna iskustva. *Strani pravni život* 53: 161–184.
12. Prlja, Dragan, Zvonimir Ivanović, Mario Reljanović. 2011. *Krivična dela visokotehnolokog kriminala*. Beograd: Institut za uporedno pravo.

Nataša Ranković*

IDENTITY THEFT AS A CRIMINAL OFFENSE: *DE LEGE LATA* AND *DE LEGE FERENDA*

Summary: The paper defines the basic forms of computer crime with an emphasis on identity theft as a special form that would de lege ferenda be characterized and adequately prescribed as a criminal offense in the Criminal Code of the Republic of Serbia. The aim of the work is to show the place of identity theft in the spectrum of various criminal acts that are classified as high-tech crime. The paper is divided into three parts, where the first is an introductory presentation describing the way in which the very rapid development of information and communication technologies affects the development of new methods for their abuse, after which the definitions of identity theft and its characteristics are described. The second part of the paper is dedicated to the ways, characteristics and modalities of identity theft, while the third part gave importance to the ways of protection and prevention of identity theft, within which a reasoned proposal was given for defining it in the Criminal Code of the Republic of Serbia. At the end of the paper, a short summary is given in the form of a conclusion.

Key words: *High-tech crime, Computer crime, Identity theft, Criminal Code, Crime*

* Author is an undergraduate student at the University of Belgrade – Faculty of Law, *natasarankovic24@gmail.com*. This paper was written under the mentorship of Ivan Đokić, Phd, assistant professor at the University of Belgrade – Faculty of Law, *djokic@ius.bg.ac.rs*