Kazneno djelo računalne prijevare kao oblik zlouporabe računalnih podataka i računalnog sustava

Škorić, Marissabell; Leder, Juraj Karlo

Source / Izvornik: **Zbornik radova Pravnog fakulteta u Splitu, 2024, 61, 239 - 261**

Journal article, Published version
Rad u časopisu, Objavljena verzija rada (izdavačev PDF)

https://doi.org/10.31141/zrpfs.2024.61.152.239

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:118:736897

Prof. dr. sc. Marissabell Škorić*
Juraj Karlo Leder, mag. iur.**

KAZNENO DJELO RAČUNALNE PRIJEVARE KAO OBLIK ZLOUPORABE RAČUNALNIH PODATAKA I RAČUNALNOG SUSTAVA

UDK: 343.72 : 004.7
DOI: 10.31141/zrpfs.2024.61.152.239
Pregledni znanstveni rad
Primljeno: 23. 2. 2024.

Nakon uvodnih napomena o informacijsko-telekomunikacijskoj tehnologiji koja je stvorila potpuno novi, specifičan, kibernetički prostor unutar kojeg pojedinci poduzimaju brojne i vrlo različite aktivnosti, u radu se analizira jedan od najčešćih oblika računalnog kriminala čiji je broj u stalnom porastu – kazneno djelo računalne prijevare iz čl. 271. Kaznenog zakona. Kako bi učinkovito odgovorio novim izazovima, zakonodavac je modalitete počinjenja ovog kaznenog djela postavio veoma široko, što je otvorilo pitanje njegova odnosa s drugim kaznenim djelima. Stoga se u radu, osim aktualne zakonske regulative, razmatra i pitanje stjecaja kaznenog djela računalne prijevare i drugih kaznenih djela. Posebno se ukazuje na vrlo raširenu uporabu zlonamjernih programa koji se koriste kao sredstva za prikupljanje računalnih podataka, *što nameće potrebu za konstantnom edukacijom o sigurn*im načinima korištenja suvremenom tehnologijom. Uočen problem konstantnog rasta prijava kaznenog djela računalne prijevare i iznimno visokog udjela nepoznatih počinitelja među njima, traži sustavno i cjelovito unapređenje mjera za njihovo otkivanje te naglašava potrebu za interdisciplinarnim znanjem kao nužnim uvjetom za uspješnu borbu protiv ovog oblika kriminaliteta.

Ključne riječi: *računalni kriminal, računalna prijevara, zlonamjerni programi, stjecaj, interdisciplinarnost*

1. UVOD

Promatrajući razvoj društva kroz povijest možemo zamijetiti konstantan trend povećanja složenosti raznih aspekata ljudskog života. Iz prvobitnih zajednica nastale su države, iz običaja kodifikacije, a iz jednostavnih alata, industrijske revolucije i tehnološka dostignuća o kakvima naši preci nisu mogli ni sanjati. Tehnologija predstavlja ukupnost cjelokupnog ljudskog znanja i omogućava pojedincima

* Dr. sc. Marissabell Škorić, redovita profesorica, Sveučilište u Rijeci, Pravni fakultet, Hahlić 6, 51000 Rijeka; marissabell.skoric@pravri.uniri.hr; ORCID0000-0003-0627-3651.
** Juraj Karlo Leder, mag. iur.

da prilagođavaju pojave oko sebe na način da one budu korisne čovječanstvu.[1] Istodobno, mijenjaju se, usklađuju i prilagođavaju pravni sustavi koji svojim normama definiraju primjereno i prihvatljivo ponašanje članova zajednica, nastojeći regulirati odnose među ljudima, a time i red i stabilnost u samoj zajednici. Kada se razmatra korelacija između ova dva aspekta društvene stvarnosti, tehnologije i pravnih sustava, mora se uzeti u obzir kompleksna dinamika njihova odnosa. Od ne tako davnog mehaničkog prethodnika modernih računala Charlesa Babbagea, iz 19. stoljeća, do prototipnih tehnologija današnjice poput kvantnih računala i umjetne inteligencije, može se uočiti kako se, po pitanju računalnih sustava, radi o polju tehnologije koje je napredovalo strelovito i koje je izazvalo svojevrsnu revoluciju u ljudskome društvu.

Razvojem računala i globalne internetske mreže stvoren je potpuno novi, tzv. kibernetički (virtualni) prostor unutar kojeg fizičke (i pravne) osobe poduzimaju različite i brojne aktivnosti. Ovi sustavi izrazito pomažu razvoju ljudskog društva te su u današnje vrijeme od presudne važnosti za njegovo funkcioniranje. Međutim, te iste mogućnosti računalnih sustava mogu biti, i često jesu, korištene kao alati za počinjenje kaznenih djela. Pojavom računalnih sustava i njihovom sve širom primjenom javljaju se novi načini počinjenja već postojećih kaznenih djela, ali i potpuno nova kaznena djela koja se mogu počiniti isključivo uporabom novonastale tehnologije, a počinitelji ih čine bez fizičkog kontakta sa žrtvom putem specifičnih računalnih programa.[2] Novonastali kibernetički prostor omogućuje počiniteljima da pristupe nekom računalnom sustavu s bilo kojeg kraja svijeta, kao i da uvelike otežaju otkrivanje svog pravog identiteta, što računalna kaznena djela čini dodatno atraktivnima za potencijalne počinitelje. Stoga se, kako pozitivne, tako moraju sagledati i negativne strane naše nove, izrazito virtualne stvarnosti.

U ovom radu analizirat će se kazneno djelo računalne prijevare koje se u praksi javlja kao jedan od najčešćih oblika računalnog kriminala i čiji je broj u konstantnom porastu. U domaće kazneno zakonodavstvo ono je implementirano

[1] Brian, A. W., *The Nature of Technology: What It Is and How It Evolves*, 1. izdanje, Free Press, New York 2009., str. 51.

[2] Veić i Martinović razlikuju računalna kaznena djela u užem i u širem smislu. Pod pojmom računalnih kaznenih djela u užem smislu podrazumijevaju računalna kaznena djela sadržana u glavi XXV. Kaznenog zakona (Narodne novine, 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23, dalje u tekstu: KZ/11), dok računalna kaznena djela u širem smislu (računalni kriminal) obuhvaćaju sva ostala kaznena djela za čije je počinjenje uporabljeno računalo / informatička tehnologija (primjerice, iskorištavanje djece za pornografiju ili prijetnja). Veić, P.; Martinović I., *Izazovi policijskog postupanja u otkrivanju i dokazivanju računalnog kriminala*, Zbornik radova 5. međunarodne znanstveno-stručne konferencije Istraživački dani Visoke policijske škole u Zagrebu, 2016., str. 404, 406.

relativno kasno, tek 2004. godine[3] kako bi se popunile zakonske praznine nastale razvojem tehnologija zbog kojih se pojedine računalne zlouporabe više nisu mogle podvesti pod postojeće imovinske delikte.[4] Od tada do danas kazneno djelo računalne prijevare pretrpjelo je značajne izmjene, što ne čudi budući da njegova pravna regulacija mora pratiti razvoj jedne od najmodernijih i najbrže razvijajućih grana tehnologije, informacijsko-komunikacijske tehnologije.[5]

2. KAZNENO DJELO RAČUNALNE PRIJEVARE

Stupanjem na snagu novog Kaznenog zakona 1. siječnja 2013. kazneno djelo računalne prijevare (kao i druga djela računalnog kriminaliteta) pretrpjelo je značajne izmjene. U prvom redu treba istaknuti da je izdvojeno iz glave o kaznenim djelima protiv imovine u novu glavu XXV., naziva „Kaznena djela protiv računalnih sustava, programa i podataka". Pored toga, može se zamijetiti znatno odstupanje u načinu njegovog normiranja u KZ/11, u usporedbi s prijašnjim KZ/97.[6] Razlog ovim promjenama bilo je daljnje usklađivanje s Konvencijom i drugim europskim

[3] Za usporedbu, u njemačko kazneno zakonodavstvo kazneno djelo računalne prijevare (*Computerbetrug*) uneseno je još 1986. godine kako bi se njime obuhvatili slučajevi u kojima počinitelj, koristeći se nedopuštenim sredstvima, utječe na rezultat procesa obrade podataka od značaja za imovinu s ciljem stjecanja nezakonite imovinske koristi za sebe ili drugoga. Pokazalo se, naime, kako postojeće kazneno djelo prijevare nije bilo dovoljno da se njime obuhvate sve zlouporabe sustava za obradu podataka čiji je značaj sve više rastao i to ne samo unutar platnog prometa u bankarskom sustavu, nego općenito. Postojećim kaznenim djelom prijevare nisu se mogla obuhvatiti ponašanja u kojima imovinska šteta nije bila prouzročena pogrešnim raspolaganjem (fizičke) osobe, odnosno njezinom zabludom, već je do nje došlo zbog zlouporabe sustava za obradu podataka. Perron, W., u: Schönke, A., Schröder, H., *Strafgesetzbuch*, Beck, München 2019., § 263a, rubni broj 1.

[4] Ključni utjecaj na domaću kaznenu politiku u području zaštite od računalnog kriminala imala je Konvencija o kibernetičkom kriminalu koju je donijelo Vijeće Europe 2001. i koja je stupila na snagu 1. srpnja 2004. godine. Vijeće Europe je, prepoznajući pretjeranu uskost kaznenopravnog normiranja u tom području, usvojilo Konvenciju koja se zatim pokazala kao najznačajniji međunarodni instrument za borbu protiv računalnog kriminaliteta. Ubrzo nakon njezina stupanja na snagu, stupile su na snagu i izmjene i dopune Kaznenog zakona čije su odredbe usklađene s Konvencijom. Između ostaloga, dodan je novi članak 224.a Računalna prijevara i prvi put u Kazneni zakon unesene definicije računalnog sustava, računalnog podatka i računalnog programa (čl. 89. st. 4. t. 31., 32. i 33.). Konvencija o kibernetičkom kriminalu, Narodne novine – Međunarodni ugovori, 9/02 (u daljnjem tekstu: Konvencija), Zakon o izmjenama i dopunama Kaznenog zakona, Narodne novine, 105/04.

[5] Informacijska tehnologija (IT) obuhvaća svu tehnologiju koja se koristi za prikupljanje, obradu, zaštitu i pohranu informacija. Odnosi se na hardver (računalno sklopovlje), softver (računalne programe) i računalne mreže, dok se pod pojmom informacijska i komunikacijska tehnologija (ICT) podrazumijevaju transfer i upotreba svih vrsta informacija. Ona je danas sveprisutna i prožima gotovo sve vidove poslovnog i privatnog života pojedinca. O temeljnim pojmovima IT i ICT više v. Čelebić, G.; Rendulić, D. I., *Osnovni pojmovi informacijske i komunikacijske tehnologije*, Zagreb 2011., dostupno na https://itdesk.info/prirucnik_osnovni_pojmovi_ informacijske_tehnologije.pdf.

[6] Dva privilegirana oblika kaznenog djela iz čl. 224.a st. 2. i 3. KZ/97 sada su regulirana u novim, zasebnim kaznenim djelima. Ekvivalente ranijem st. 2. pronalazi se u novim člancima 267. Ometanje rada računalnog sustava, 268. Oštećenje računalnih podataka te 269. Neovlašteno presretanje računalnih podataka, a ekvivalent ranijeg st. 3. u čl. 272. Zloporaba naprava.

zakonodavstvom, kao i specifičnosti kaznenih djela protiv računalnih sustava koje su, prema mišljenju zakonodavca, zahtijevale njihovo izdvajanje u zasebnu glavu.[7]

Nakon usvajanja KZ/11 i hrvatskog pristupanja Europskoj uniji 2013., stupila su na snagu još dva važna akta iz pravne stečevine EU-a s ciljem daljnje harmonizacije zakonodavstva država članica po pitanju kriminalizacije računalnih kaznenih djela. To su Direktiva 2013/40/EU o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća iz 2005. i Direktiva 2019/713 o borbi protiv prijevara i krivotvorenja u vezi s bezgotovinskim sredstvima plaćanja i zamjeni Okvirne odluke Vijeća iz 2001.[8] U Direktivi 2013., u alineji 15. preambule, ističe se kako ona nije u suprotnosti s odredbama Konvencije, već se njome nadograđuje postojeći okvir koji je Konvencija postavila. Ista misao vodilja može se pronaći i u preambuli Direktive 2019. kojom se nastoji nadopuniti i učvrstiti temelje postavljene Direktivom 2013. Potonja se direktiva u svojim odredbama izričito dotiče i problematike računalne prijevare, što je dovelo do izmjena i dopuna članka 271. KZ/11 u koji su dodani novi modaliteti počinjenja djela.[9]

Dublje razumijevanje kaznenog djela računalne prijevare čija aktualna definicija glasi *tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, prenese, izmijeni, izbriše, prikrije, ošteti, učini neuporabljivim ili nedostupnim računalne podatke ili ometa ili sprečava rad računalnog sustava i na taj način prouzroči štetu drugome, kaznit će se kaznom zatvora od šest mjeseci do pet godina,* zahtijeva prethodno proučavanje i razumijevanje temeljnih elemenata koji ga čine.[10] To su, u prvom redu, pojmovi računalni podatak i računalni sustav, kao i pojam računalni program, iako se potonji izričito ne spominje u njegovu opisu.

2.1. Računalni podatak, računalni program i računalni sustav – temeljni pojmovi kaznenog djela računalne prijevare

U KZ/11 računalni sustav definiran je kao *svaka naprava ili skupina međusobno spojenih ili povezanih naprava, od kojih jedna ili više njih na osnovi programa automatski obrađuju podatke, kao i računalni podaci koji su u njega spremljeni, obrađeni, učitani ili preneseni za svrhe njegovog rada, korištenja,*

---

[7] Obrazloženje Konačnog prijedloga kaznenog zakona iz listopada 2011., dostupno je na: https://edoc.sabor.hr/ Views/AktView.aspx?type=HTML&id=23270 (3. 7. 2023.). V. str. 121., 123. i 243.

[8] Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP, SL 218, 14. 8. 2013., str. 8-14 (u daljnjem tekstu: Direktiva 2013) i Direktiva 2019/713 Europskog parlamenta i Vijeća od 17. travnja 2019. o borbi protiv prijevara i krivotvorenja u vezi s bezgotovinskim sredstvima plaćanja i zamjeni Okvirne odluke Vijeća 2001/413/PUP, SL 123, 10. 5. 2019., str. 18-29 (u daljnjem tekstu: Direktiva 2019).

[9] Novelom iz 2021. godine opis kaznenog djela računalne prijevare dopunjen je na način da su dodani novi modaliteti ostvarenja djela, i to: prenošenje i prikrivanje računalnih podataka te sprečavanje rada računalnog sustava. Pored toga, u Kazneni zakon dodaje se definicija „bezgotovinskog instrumenta plaćanja". Zakon o izmjenama i dopunama Kaznenog zakona, Narodne novine, 84/21.

[10] Čl. 271. st. 1. KZ/11. Dodatno je u istom članku propisan kvalificirani oblik ovog kaznenog djela u slučaju kada je pribavljena znatna imovinska korist ili prouzročena znatna šteta (st. 2.) te da će se podaci nastali počinjenjem ovog kaznenog djela uništiti (st. 3.).

zaštite i održavanja.[11] Iz ove je definicije vidljivo da zakonodavac nije ograničio mogućnost počinjenja kaznenog djela računalne prijevare na određene naprave, već je kaznenopravnu zaštitu usmjerio na sve naprave čiji se računalni sustav ometa ili se sprečava njegov rad. Riječ je o široko postavljenoj definiciji pod koju se može podvesti velik broj naprava jer zadovoljavaju uvjet automatske obrade podataka. Na taj način zakonodavac očito nastoji držati korak s različitim oblicima računalne tehnologije koji se pojavljuju gotovo svakodnevno.[12] Naime, niz je naprava, a njihov se broj svakodnevno povećava, koje u sebi sadrže računalo koje na temelju programa automatski obrađuju podatke. Uz lako prepoznatljive primjere tehnologije za čiju su funkcionalnost zaslužni računalni sustavi koji operiraju na fizičkoj elektrotehničkoj opremi koja ih čini (primjerice, osobna računala, putna računala, tableti, pametni telefoni), ovom su definicijom obuhvaćene i puno manje naoko očite tehnologije, poput jednostavnih panela s tipkama za elektronsko otključavanje brave na vratima putem šifre, kućnih alarma ili elektronskih ruleta.[13] Niz modernih električnih automobila i druga slična prijevozna sredstva također mogu biti svrstani pod tu definiciju. Može se, nadalje, razmatrati i računalni sustav bankomata. Bankomat je, kao i svako osobno računalo, naprava koja na osnovi programa automatski obrađuje podatke i upravo je on česti objekt na kojem se poduzima radnja počinjenja kaznenog djela računalne prijevare. No, osim hardvera, opipljivog i vidljivog fizičkog dijela naprava koji ima sposobnost automatske obrade podataka, definicijom računalnog sustava obuhvaćen je i softver, odnosno računalni podaci koji se za razliku od hardvera ne mogu fizički dodirnuti jer se sastoje od kodiranih instrukcija pohranjenih na nekom mediju. Sukladnoj aktualnoj definiciji, računalni sustav čine oni računalni podaci koji su u njega spremljeni, obrađeni, učitani ili preneseni za svrhe njegova rada, korištenja, zaštite i održavanja.

Manipulacija računalnim sustavima može se ostvariti hardverski tj. vršenjem utjecaja na fizičke komponente koje čine računalo i softverski, odnosno utjecajem u kibernetičkom prostoru koji računalo stvara. Hardverska manipulacija pretpostavlja instalaciju vanjskih, fizičkih uređaja koji modificiraju očekivani način rada računala ili zlouporabu samih komponenti računala, dok se softverskom manipulacijom utječe na računalni sustav na njegovoj binarnoj razini nula i jedinica te se manipulira programima, odnosno računalnim podacima u virtualnom prostoru.[14] Potonje su u praksi veoma česte budući da ne čine nužnom fizičku prisutnost počinitelja uz računalo čijim podacima se želi manipulirati. Karakteristika je najmodernijih softverskih napada na računalne sustave i to da se mogu realizirati bez ikakve ili uz minimalnu interakciju žrtve. Kod softverskih manipulacija počinitelj može biti, a često i jest, u drugoj državi ili čak na drugom kontinentu, dakle na iznimno velikoj

[11] Čl. 87. st. 18. KZ/11.

[12] Automatski znači *bez izravne ljudske intervencije*. V. Explanatory Report to the Convention on Cybercrime, European Treaty Series – No. 185, Budapest, 23. 11. 2001., st. 23.

[13] V. presudu Županijskog suda u Osijeku, Kž-231/18 od 27. rujna 2018.

[14] Middleton, B., *Cyber Crime Investigator's Field Guide*, Boca Raton, London, New York, 3. izdanje, CRC Press, 2022., str. XII.

udaljenosti od žrtve, a zbog digitalne prirode dokaza dodatno je otežano otkrivanje, pa time i kažnjavanje počinitelja ovih kaznenih djela.[15]

Odgovarajuća definicija o tome što je to računalni podatak sadržana je u čl. 87. st. 19. i glasi: *Računalni podatak je svako iskazivanje činjenica, informacija ili zamisli u obliku prikladnom za obradu u računalnom sustavu.* Dakle, pojmom računalni podatak obuhvaćeni su oni podaci koji su u takvom obliku da se mogu izravno obrađivati u računalnom sustavu. Za razliku od stvari, podaci imaju netjelesni oblik i zato se ne mogu podvesti pod definiciju pokretne stvari.[16] Računalni je podatak osnovna konstruktivna jedinica moderne tehnologije. Pojednostavljeno rečeno, računalni su podaci na najnižoj razini funkcije nule i jedinice kojima elektrotehnička oprema dobiva signale za elektronsku obradu podataka. Slaganjem niza signala nula i jedinica (milijuna, milijardi, trilijuna itd.), mogu se automatski rješavati kompleksni zadaci i dobiti izračun koji omogućuje, primjerice, prikaz kretanja zrakoplova na kontrolnoj konzoli kontrolora letenja. No, može se ići i više od nula i jedinica – svako upisivanje šifri, brojeva za PIN, datuma, imena, adresa i bilo kojeg drugog podatka u računalni sustav, prislanjanje prsta na čitač otisaka prstiju ili izgovaranje riječi u mikrofon, može također predstavljati stvaranje novih računalnih podataka, budući da se ti podaci iskazuju u obliku prikladnom za obradu u računalnom sustavu. Osim nula i jedinica prenesenih putem fizičkih medija (primjerice, optičkih kabela), podaci mogu biti preneseni i u obliku valova (primjerice radiovalova) koji se šire zrakom bez potrebe za fizičkom, mehaničkom opremom po putu.[17] Računalni podaci mogu biti pohranjeni unutar računalnog sustava (primjerice na hard disku), na fizičkom mediju za pohranu računalnih podataka koji je odvojiv od računalnog sustava (primjerice, na CD-u, DVD-u, USB-u), a mogu se nalaziti i na računalnoj mreži, u oblaku (engl. *cloud*).

Iako se u opisu kaznenog djela računalne prijevare izričito ne spominje, uz pojmove računalni sustav i računalni podatak nužno je vezati i pojam računalnog programa koji zakonodavac definira kao *skup računalnih podataka koji su u stanju prouzročiti da računalni sustav izvrši određenu funkciju* (čl. 87. st. 20.). Računalnim programom čovjek nastoji usmjeriti procesnu moć računala k rješavanju kompleksnih

[15] Zato kod računalnih kaznenih djela posebno dolazi do izražaja potreba za međunarodnom pomoći i suradnjom. Veliki pomaci u međunarodnoj suradnji i sigurnosti učinjeni su djelovanjem institucija poput Interpola i Europola, kao i osnivanjem nacionalnih institucija, poput domaćeg Nacionalnog CERT-a (odjel CARNET-a) i Zavoda za sigurnost informacijskih sustava (ZSIS). Potrka, N., *Računalna prijevara – analiza djelotvornosti otkrivačke djelatnosti*, Policija i sigurnost, vol. 28, 3/2019., str. 272.

[16] U Kaznenom zakonu pod pojmom pokretne stvari obuhvaćeni su energija i telefonski impulsi koji također nemaju vidljiv fizički oblik (čl. 87. st. 16. KZ/11). No, zakonodavac navedenu definiciju nije proširio i u odnosu na računalne podatke pa se neovlašteno pribavljanje tuđih računalnih podataka ne može pravno označiti kao kazneno djelo krađe.

[17] Takav pristup koristi se u tehnologijama poput mobilnog interneta, koji se odašilja valovima putem tornjeva. Gelenbe, E.; Kahane, J., *Fundamental Concepts in Computer Science: Advances in Computer Science and Engineering: Texts*, London, 1. izdanje, Imperial College Press, 2009., str. 2.

zadataka, a u svrhu automatizacije, pojednostavljenja života i pojačavanja efikasnosti društva.[18]

Iz ovako definiranih pojmova računalnog sustava, računalnog podatka i računalnog programa može se primijetiti odnos između tri spomenuta pojma – računalni sustav krovni je pojam čiji sastavni dio čine računalni programi, a njih, pak, čine računalni podaci. Imajući u vidu sveobuhvatnost i apstraktnost ovih definicija, može se lako zaključiti kako osobi koja nema osnovna znanja iz područja računalnih znanosti može biti otežano razumijevanje različitih modaliteta počinjenja kaznenog djela računalne prijevare. Stoga je nedvojbeno potreban interdisciplinaran pristup u postupcima prepoznavanja, otkrivanja i dokazivanja ovog, kao i drugih kaznenih djela iz glave XXV. KZ/11.[19]

2.2. Radnje počinjenja kaznenog djela računalne prijevare i modaliteti pribavljanja računalnih podataka

U čl. 271. st. 1. predviđen je niz različitih radnji počinjenja kaznenog djela računalne prijevare, i to: unos, prijenos, izmjena, brisanje, prikrivanje, oštećenje, činjenje neuporabljivim, činjenje nedostupnim računalnih podataka te ometanje i sprečavanje rada računalnog sustava. Ono što je ključno da bi se radilo o kaznenom djelu računalne prijevare jest to da se manipulacijom računalnim podacima, odnosno računalnim sustavom nanosi šteta drugome, a u cilju pribavljanja protupravne imovinske koristi.[20] Do računalnih podataka počinitelji dolaze na brojne i raznovrsne načine. Tipičan i čest primjer kaznenog djela računalne prijevare u sudskoj praksi jest unos računalnih podataka do kojih je počinitelj došao krađom kartice i PIN-a. No, u današnje vrijeme iznimno je raširena uporaba malwarea, zlonamjernih programa koji se koriste kao sredstva za prikupljanje računalnih podataka nakon čega se njihovom daljnjom zlouporabom (unosom, prijenosom, sprečavanjem rada računalnog sustava ili drugim radnjama navedenima u čl. 271. st. 1.) može ostvariti biće kaznenog djela računalne prijevare.

2.2.1. Unos računalnih podataka neovlaštenim korištenjem tuđe kartice i PIN-a

U praksi se kazneno djelo računalne prijevare često čini na način da počinitelj s tuđom karticom i PIN-om neovlašteno podiže novac s bankomata ili tako da

[18] To može biti program poput *LibreOffice*, skupa programa za sastavljanje dokumenata, tablica, prezentacija na osobnim računalima, a može biti i, primjerice, program nadzorne kamere na naplatnim kućicama autoceste koji čita registraciju automobila dok prilaze kameri i uspoređuje ih s bazom podataka ili ih sprema za daljnje provjere.

[19] Tako i Sokanović, L.; Orlović, A., *Oblici prijevara u Kaznenom zakonu*, Hrvatski ljetopis za kaznene znanosti i praksu, vol. 24, 2/2017., str. 583-585.

[20] Računalna prijevara jest materijalno kazneno djelo za čije je dovršenje nužno da na strani treće osobe nastupi šteta. Novoselec, P., *Posebni dio kaznenog prava*, Pravni fakultet Sveučilišta u Zagrebu, Zagreb 2007., str. 237.

neovlaštenim provlačenjem tuđe kartice kroz POS-uređaj bezgotovinski plaća robu ili usluge, djelujući tako na elektroničku obradu podataka u cilju pribavljanja protupravne imovinske koristi.

Nakon uvođenja kaznenog djela računalne prijevare u domaće kazneno zakonodavstvo 2004. godine, bilo je određenih nesnalaženja i nedosljednosti u sudskoj praksi koja je podizanje novca pomoću tuđe kartice i PIN-a u pojedinim slučajevima kvalificirala kao kazneno djelo teške krađe provaljivanjem, a u drugim kao kazneno djelo računalne prijevare. Tako je, primjerice, podizanje gotovog novca s bankomata pomoću ukradene bankovne kartice i odgovarajućeg PIN-a sud označio kao kazneno djelo teške krađe, smatrajući da neovlašteno ulaženje tuđom karticom u bankomat predstavlja provaljivanje u zatvoreni prostor i time obilježje teške krađe.[21] Jednako tako, i Vrhovni je sud zaključio da krađa novca s bankomata sadrži obilježja teške krađe jer je riječ o zatvorenom prostoru u kojem se nalazi novac do kojeg su počinitelji došli na način da su krivotvorili platne kartice pomoću kojih su onda podizali novac.[22] I u kasnijoj sudskoj praksi mogu se pronaći slučajevi u kojima je otuđenje kreditne kartice i korištenje PIN-a na bankomatu pravno označeno kao kazneno djelo teške krađe.[23] S navedenom praksom slaže se Moslavac koji smatra da ovakve slučajeve treba kvalificirati kao tešku krađu zbog točno određenog načina počinjenja temeljnog kaznenog djela krađe, provaljivanjem, kao jednim od modaliteta protupravnog oduzimanja tuđih pokretnih stvari iz zatvorenih prostora, u ovom slučaju bankomata. Kao još jedan argument u prilog ovom zaključku ističe namjeru počinitelja koja ide isključivo u smjeru prisvajanja novca, a ne obuhvaća ometanje rada računalnih sustava ili manipulaciju računalnim podacima. Stoga ovaj autor zaključuje da otuđenje novca na bankomatu uporabom originalnog PIN-a i ukradene kartice nije kazneno djelo računalne prijevare.[24] S druge strane, Županijski sud u Splitu ukinuo je prvostupanjsku presudu smatrajući pogrešnim zaključak suda da se radi o kaznenom djelu teške krađe u slučaju okrivljenice koja je otuđila kreditnu karticu i potom unošenjem PIN-a na bankomatima u tri navrata podigla odgovarajući novčani iznos. Sud je zaključio kako podizanje novca s bankomata otuđenom karticom za koju je okrivljenica pribavila PIN ne predstavlja provaljivanje u zatvoreni prostor – bankomat.[25]

Pitanje kako kvalificirati podizanje novca s bankomata ukradenom karticom zaokupilo je i pažnju teoretičara kaznenog prava. Tako Vuletić smatra da se u tom slučaju radi o kaznenom djelu računalne prijevare, a ne teške krađe, ističući da se izvršenjem računalne prijevare ne ulazi u zatvoreni, nego u kibernetički prostor koji je stvoren računalnom tehnologijom i ne može se podvesti pod definiciju iz

[21] Županijski sud u Splitu, Kž-205/08 od 20. svibnja 2008.

[22] Vrhovi sud RH, III Kr-92/08-7 od 10. veljače 2009. Citirano prema, Moslavac, B., *Enigma (sudske) pravne kvalifikacije kažnjivog djela podizanja novca na bankomatu ukradenom karticom*, IUS-INFO, str. 4., dostupno na https://www.iusinfo.hr/strucni-clanci/CLN20V01D2018B1125.

[23] Primjerice, Općinski sud u Virovitici, 6 K-3/17-34 od 9. svibnja 2017.

[24] Moslavac, *op. cit.* u bilj. 22, str. 3-4, 7.

[25] Županijski sud u Splitu, Kž-497/17 od 7. rujna 2017.

teške krađe jer počinitelj u njega ne ulazi fizički nego s pomoću računala.[26] Prema ovom autoru, ne može se uspostaviti ekvivalencija između pojmova „zatvorenog prostora" i „kibernetičkog prostora" jer se u kibernetički prostor ne može ulaziti fizički, u tradicionalnom smislu te riječi.[27] Novoselec, pak, ističe kako se bankomat može označiti kao zatvoreni prostor a neovlašteno ulaženje u njega karticom kao provaljivanje, no s obzirom na to da je riječ o specifičnom ulaženju u zatvoreni prostor korištenjem računalnih podataka s ciljem pribavljanja protupravne imovinske koristi, radi se o kaznenom djelu računalne prijevare. Prema Novoselcu, računalna je prijevara u odnosu na kazneno djelo teške krađe *lex specialis* i treba joj dati prednost.[28] Navedena tumačenja, prema kojima podizanje novca iz bankomata neovlaštenom uporabom tuđe kartice uz korištenje tajnog identifikacijskog PIN-broja valja označiti kao kazneno djelo računalne prijevare, prevladavaju i u aktualnoj sudskoj praksi te im se valja prikloniti.[29]

U sudskoj praksi postojale su određene dvojbe i po pitanju je li neovlaštena uporaba ili korištenje tuđe kartice bez uporabe PIN-a jedan od mogućih načina počinjenja računalne prijevare iz čl. 271. KZ/11. Tako je Vrhovni sud u jednoj odluci negativno odgovorio na ovo pitanje, dok je Županijski sud u Bjelovaru za kazneno djelo računalne prijevare osudio počinitelja koji je provukao American Express karticu kroz POS-uređaj.[30] I Općinski sud u Zagrebu zbog kaznenog djela računalne prijevare osudio je dvojicu suokrivljenika koji su do podataka s kartice došli na način da ih je prvookrivljeni prepisao s kartice, nakon što mu je žrtva istu predočila u trgovačkom centru gdje je radio kao prodavač. Nakon toga su suokrivljenici opetovano unosili podatke s kartice u internetske aplikacije oštetivši na taj način žrtvu za iznos od 5.392,85 kuna.[31] U pravnoj teoriji nije sporno da se kazneno djelo računalne prijevare može počiniti i samom uporabom tuđe kartice, njezinim provlačenjem kroz POS-uređaj ili korištenjem podataka s kartice za plaćanje putem interneta.[32] U tim slučajevima postoji računalna prijevara neovisno o tome traži li se pri plaćanju PIN, potpis ili se, pak, transakcija provodi bez ikakve autorizacije, što je čest slučaj pri plaćanju manjih iznosa.[33] Zajedničko navedenim primjerima jest neovlašteno korištenje kartice kojim se „zavarava" računalni sustav

---

[26] Provaljivanjem se općenito smatra svako ulaženje u neki zatvoreni prostor protivno volji vlasnika. Cvitanović, L. *et. al.*, *Kazneno pravo, posebni dio,* Pravni fakultet Sveučilišta u Zagrebu, Zagreb 2018., str. 310.

[27] Vuletić, I., *Primjenjivost tradicionalnih kaznenopravnih koncepata na računalni kriminal,* Zbornik Pravnog fakulteta u Zagrebu, vol. 64, 5-6/2014, str. 899.

[28] Novoselec, P., *Sudska praksa*, Hrvatski ljetopis za kazneno pravo i praksu, vol. 15, 2/2008., str. 1166.

[29] V. primjerice Općinski sud u Sisku, K-276/2023-2 od 24. listopada 2023., Županijski sud u Zagrebu, 6 Kžmp-61/2022-11 od 14. veljače 2023., Županijski sud u Zagrebu, 1 Kž-90/2019-3 od 12. veljače 2019.

[30] Usp. Vrhovni sud RH, Kzz-18/16 od 11. travnja 2016. i Županijski sud u Bjelovaru, Kž-53/19 od 7. ožujka 2019.

[31] Općinski kazneni sud u Zagrebu, K-163/20-2 od 7. svibnja 2020.

[32] Usp. Škrtić, D., *Kaznenopravna zaštita informatičkih sadržaja*, doktorska disertacija, Sveučilište u Zagrebu, Pravni fakultet, Zagreb 2011., str. 320, Sokanović, Orlović, *op. cit.* u bilj. 19, str. 608.

[33] Veić, Martinović, *op. cit.* u bilj. 2, str. 414.

banke odnosno, primjenjujući terminologiju zakonskog opisa, unose se računalni podaci (u navedenim primjerima to su PIN ili podaci s tuđe magnetne trake kartice) čime se uzrokuje šteta drugome s ciljem da počinitelj sebi (ili drugome) pribavi protupravnu imovinsku korist.[34]

2.2.2. Malware – moćan alat za pribavljanje i zlouporabu računalnih podataka

Malware (zlonamjerni program ili software) krovni je pojam koji se koristi za računalne programe dizajnirane kako bi se infiltrirali u računalni sustav s namjerom da mu se našteti.[35] Postoje razni oblici malwarea, s različitim namjenama i razinama kontrole nad „zaraženim" računalnim sustavom te opsegom štete koju su sposobni izazvati. Svakim od oblika malwarea, koji će biti pojašnjen u nastavku, moguće je unositi, prenositi, mijenjati, izbrisati, prikriti, oštetiti, učiniti neuporabljivim ili nedostupnim računalne podatke i ometati ili sprečavati rad računalnog sustava. Ako počinitelj poduzme neku od navedenih radnji. bit će riječ o kaznenom djelu računalne prijevare pod uvjetom da su poduzete s ciljem stjecanja protupravne imovinske koristi te je prouzročena šteta drugome.

a) Spyware

Spyware je tip malwarea koji na prikriveni način prikuplja osjetljive i povjerljive računalne podatke s računala žrtve s ciljem njihove daljnje zlouporabe.[36] *Trojanski konj* ili *trojanac* česti je pojavni oblik u praksi kojim se računalo napada tako što se ovaj zlonamjerni računalni program lažno prikazuje kao legitimni software, no umjesto da izvršava očekivanu funkciju, izvršava maliciozni programski kod. Također je moguće da se maliciozni kod trojanca izvršava uz legitimni kod, čime se stvara bolji privid da se uistinu i radi o legitimnom programu, čak ako je žrtva imala određene početne sumnje.[37] S druge strane, *keyloggeri* nisu toliko učestali u praksi, no riječ je o izrazito opasnom obliku spywarea koji omogućuje počinitelju da vidi svaku tipku koju žrtva na tipkovnici zaraženog računala pritisne, kao i svaki pokret miša i drugu radnju koju poduzme hardwareom računala. Pomoću keyloggera

[34] U ovom je primjeru računalni sustav taj koji je *doveden u zabludu* da mu je pristupila ovlaštena osoba. Za razliku od kaznenog djela računalne prijevare, kod kaznenog djela prijevare (čl. 236. KZ/11) počinitelj dovodi u zabludu ili održava u zabludi fizičku osobu. Kazneno djelo prijevare nužno podrazumijeva određenu interakciju sa žrtvom koja se dovodi u zabludu pri čemu počinitelj kao sredstvo obmanjivanja koristi računalni sustav. O tehnikama socijalnog inženjeringa čija je temeljna karakteristika manipuliranje osobama u cilju otkrivanja povjerljivih informacija više v. Bullée, J. W.; Junger, M., *Social Engineering*, u: Holt, T., Bossler, A. (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Palgrave Macmillan, Cham, 2020., str. 849-875. O razgraničenju kaznenog djela prijevare i računalne prijevare te o razlikovanju izravne i neizravne računalne prijevare više v. Vuletić, I.; Nedić, T., *Računalna prijevara u hrvatskom kaznenom pravu*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 35, 2/2014., str. 680-689.

[35] Middleton, *op. cit.* u bilj. 14, str. 12.

[36] *Ibid.*, str. 14.

[37] Van Oorschot, P. C., *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin*, 2. izdanje, Springer, 2021., str. 194-195.

počinitelj može aktivirati snimanje mikrofonom i *web*-kamerom što mu omogućuje vizualni prijenos slike ili videa stanja računala. Na taj način počinitelj može vidjeti isti videoprikaz računalnih operacija koji vidi i žrtva na svojem monitoru.[38] Kada se uzmu u obzir razne svakodnevne situacije u kojima žrtva koristi računalo, primjerice korištenje internetskog bankarstva, pristup društvenim mrežama ili, pak, osjetljivim poslovnim zapisima, jasno je da se radi o iznimno opasnom obliku spywarea. Keyloggeri u pravilu „napadaju" računalo u softverskom obliku malwarea (npr. putem elektroničke pošte), no mogu se također pojaviti i u hardverskom obliku, kao uređaji spojeni na računalo žrtve ili kao modifikacije učinjene takvom računalu na razini hardverskih komponenti računala. Pojedini hardverski keyloggeri dizajnirani su na način da ih je lako, u vrlo kratkom vremenu, instalirati na računalo korisnika pa je moguća situacija da ih neprimjetno instaliraju osobe koje imaju omogućen pristup prostorijama gdje se računalo žrtve nalazi.[39]

U sudskoj praksi mogu se naći primjeri gdje su se počinitelji koristili malicioznim računalnim programom kako bi došli do ključnih podataka koje su onda upotrijebili za stjecanje protupravne imovinske koristi. Tako je presudom Općinskog kaznenog suda u Zagrebu okrivljenik osuđen zbog kaznenog djela računalne prijevare koju je izvršio na način da je pomoću malicioznog računalnog programa neovlašteno pristupio e-mail pretincu oštećenog trgovačkog društva te tako pribavio podatke vezane uz poslovni odnos tog trgovačkog društva s drugim trgovačkim društvom. Nakon toga je s adrese kojom se koristilo prvo trgovačko društvo poslao e-mail poruku dužnom trgovačkom društvu i tražio uplatu 76.474,40 američkih dolara, a kao primatelja je lažno naveo prvo trgovačko društvo. Novac je bio uplaćen na račun koji je otvorio osuđenik te je s njega podigao 3.107,77 američkih dolara, dok je u podizanju ostatka uplaćenih sredstava bio onemogućen temeljem rješenja županijskog suda kojim se zabranjuje daljnje raspolaganje preostalim novčanim sredstvima na predmetnom računu.[40] U drugom je slučaju Općinski kazneni sud u Zagrebu osudio okrivljenicu jer je u nakani da stekne protupravnu imovinsku korist na točno neutvrđeni način instalirala maliciozni računalni program „M.s.t." na računala 15 potencijalnih žrtava pomoću kojeg je neovlašteno prikupila njihove računalne podatke za pristup internetskom bankarstvu. Nakon toga je u tri slučaja uspješno dovršila financijske transakcije, dok je u 12 slučajeva kazneno djelo računalne prijevare ostalo u pokušaju jer nije došlo do prijenosa novca zbog preventivnih mjera banaka. Iako vještak za informatiku, telekomunikacije i biometriju nije mogao sa sigurnošću tvrditi na koji je način malware instaliran na računala klijenata banke, sud je smatrao nesporno utvrđenim da je okrivljenica

[38] Middleton, *op. cit.* u bilj. 14, str. 14.

[39] To mogu biti, primjerice, bliske osobe koje žive u istom kućanstvu gdje i žrtva ili djelatnik u prostorijama tvrtke. Van Oorschot, *op. cit.* u bilj. 37, str. 18.

[40] S ciljem da očekivani novčani prinos prikaže legalno stečenim, prilikom otvaranja računa okrivljenik je priložio krivotvoreni ugovor između trećeg trgovačkog društva, u kojem je naveden kao potpisnik, i dužnog trgovačkog društva pa je, osim za kazneno djelo računalne prijevare, osuđen i za krivotvorenja isprave (čl. 278.) te pranje novca (čl. 265.). Općinski kazneni sud u Zagrebu, K-2235/16-46 od 4. studenog 2019.

posjedovala ovaj računalni program i da ga je upravo ona na neutvrđeni način instalirala na računala klijenta banke.[41]

b) Ransomware

Ransomware (ucjenjivački zlonamjerni program) ubraja se među najmodernije i najteže oblike zlouporabe računalnih podataka i sustava jer koristi napredne tehnologije poput enkripcije i kriptovaluta te uzrokuje ogromne štete.[42] Njegovo iznimno važno obilježje kojim se ističe u usporedbi s ostalim oblicima malwarea jest to da, čak i ako se uspješno eliminira s računala, a već je proveo proces enkripcije računalnih podataka, računalni podaci i dalje ostaju enkriptirani.[43] U jednom od naprednijih oblika, to je moćan oblik malwarea koji koristeći enkripciju sprečava pristup računalnim podacima na zaraženom računalu, što računalo čini praktički neuporabljivim jer ono takve podatke (i sve naknadne koje se unose, koji se također enkriptiraju) ne može prikazivati korisniku.[44]

Instalacijom ransomwarea na računalo počinitelj je ostvario obilježja više kaznenih djela iz glave XXV. KZ/11.[45] S obzirom na to da je cilj počinitelja pribaviti imovinsku korist, a da svojim radnjama uzrokuje štetu drugome (fizičkoj ili pravnoj osobi), u obzir dolazi i kazneno djelo računalne prijevare.[46] No, iako počinitelj svojim radnjama nanosi štetu drugoj osobi, njima se ne može istodobno omogućiti

---

[41] Sud je utvrdio da je okrivljena u pet banaka otvorila na svoje ime ukupno osam računa (tekućih i deviznih), u vremenskom razdoblju od svega četiri dana (od 12. do 15. svibnja 2014.), a na koje je neovlašteno prebačen iznos od 64.720,00 kuna i pokušano prebacivanje novčanih sredstava klijenata banke u iznosu od 274.755,00 kuna. Općinski kazneni sud u Zagrebu, K-2215/16-43 od 6. listopada 2020. Okrivljenica je u ovom predmetu bila optužena osim za produljeno kazneno djelo računalne prijevare, i za kazneno djela zlouporabe naprava te pranje novca, za komentar v. *infra*, poglavlje 2.3.

[42] Primjer koji može poslužiti kao dobar pokazatelj potencijalno razorne moći ransomwarea je napad na računalne sustave kojima se održava infrastruktura Colonial Pipelinea, najvećeg sustava naftnih cjevovoda u SAD-u. Počinitelji su 2021. instalirali ransomware na računalne sustave Colonial Pipelinea koristeći se podatcima za pristup *Virtual Private Networku* (program koji, između ostalog, omogućava zaposlenicima pristup službenim računalnim sustavima na daljinu), a za koje se smatra da su pribavljeni putem *dark neta*. Maliciozni kod je enkriptirao računalne podatke Colonial Pipelinea i počeo prikazivati poruku u kojoj se traži plaćanje iznosa od 75 bitcoina (oko 5 milijuna američkih dolara u to vrijeme) u zamjenu za dostavljanje dekripcijskih ključeva. Colonial Pipeline je odlučio uplatiti cijeli zatraženi iznos budući da su desetci tisuća američkih državljana bili o njemu ovisni, uključujući bolnice, hitne službe, zračne luke, špeditere i javni prijevoz. Nakon izvršene uplate dostavljen im je alat za dekripciju i cjevovod je ubrzo vraćen u operativno stanje. Lubin, A., *The Law and Politics of Ransomware, Vanderbilt Journal of Transnational Law*, vol. 55, 5/2022, str. 1190, 1209. O ransomware-u i opasnostima sve češćih kibernetičkih napada na zdravstveni sustav v. Vuletić, I., *Data-driven healthcare and cybercrime: threat we are not aware of?*, Asia Pacific Journal of Health Law & Ethics, vol. 11, 2/2018, str. 16-32 i Mrčela, M.; Vuletić, I., *Healthcare, privacy, big data and cybercrime: which one is the weakest link?,* Annals of Health Law, vol. 27, 2/2018., str. 257- 280.

[43] Van Oorschot, *op. cit.* u bilj. 37, str. 202.

[44] DeBacher, J., *Ransomware*, Georgetown Law Technology Review, vol. 6, 1/2022, str. 300-310.

[45] U obzir dolazi kazneno djelo neovlaštenog pristupa (čl. 266. KZ/11), oštećenja računalnih podataka (čl. 268. KZ/11), ometanja rada računalnog sustava (čl. 267. KZ/11) i teška kaznena djela protiv računalnih sustava, programa i podataka (čl. 273. KZ/11).

[46] Tako Moslavac, B., *Plaćanje otkupnine u slučaju ransomware-a i posljedice za žrtvu*, IUS-INFO, str. 1-3, dostupno na https://www.iusinfo.hr/strucni-clanci/placanje-otkupnine-u-slucaju-ransomware-a-i-posljedice-za-zrtvu.

pribavljanje protupravne imovinske koristi. Da bi počinitelj stekao imovinsku korist, samo ometanje rada računalnog sustava nije dovoljno, već je nužno da poduzme daljnji korak koji se sastoji u tome da za ponovni pristup računalnim podacima zahtijeva plaćanje otkupnine. Na taj način ransomware postaje sredstvo tzv. virtualne iznude. Izjava počinitelja da će izvršiti dekripciju podataka samo pod uvjetom da mu oštećenik plati odgovarajući iznos, može se kvalificirati kao ozbiljna prijetnja zlom i sadrži u sebi sve elemente kaznenog djela iznude. S obzirom na to, prilikom kvalifikacije ponašanja vezanih uz uporabu ransonwarea ostvarena su i obilježja kaznenog djela iznude (čl. 243. KZ/11).[47]

Kako se ransomwareom ostvaruju obilježja više kaznenih djela, postavlja se pitanje njihova međusobnog odnosa. Kaznena djela iz čl. 266., 267. i 268. KZ/11 kaznena su djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava, dok je pravno dobro koje se štiti kaznenim djelima računalne prijevare i iznude, imovina. Smisao propisivanja kaznenog djela računalne prijevare bio je obuhvatiti situacije u kojima počinitelj manipulacijama unutar računalnog sustava, bez kontakta sa žrtvom, pribavlja protupravnu imovinsku korist, a ne mogu se podvesti pod tradicionalne imovinske delikte u kojima počinitelj stječe (ili može steći) protupravnu imovinsku korist. U slučaju ransomwarea nedvojbeno je da samom manipulacijom računalnim podacima i/ili sustavom počinitelj ne može ostvariti protupravnu imovinsku korist, već mu je za to nužna druga radnja – prijetnja ozbiljnim zlom. Stoga se čini ispravnim njegovu radnju podvesti pod kazneno djelo iznude, a ne računalne prijevare.[48] No, nedvojbeno je da se time ne iscrpljuje cijelo nepravo i da treba uzeti u obzir kako je počinitelj svojim radnjama također ostvario obilježja protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava. Kako ransomware u pravilu dovodi do sprečavanja rada računalnog sustava,[49] tek osudom počinitelja za stjecaj kaznenog djela ometanja rada računalnog sustava i iznude iscrpilo bi se cijelo nepravo njegovih radnji.[50] [51]

---

[47] Kazneno djelo iznude poseban je oblik kaznenog djela prisile kojim se štite sloboda odlučivanja i sloboda djelovanja. Njime se djeluje na volju osobe (silom ili ozbiljnom prijetnjom) od koje se iznuđuje ponašanje protiv njezine volje, koje bi izostalo kada ona na to ne bi bila prisiljena. Novoselec, *op. cit.* u bilj. 20, str. 243.

[48] Svrha je propisivanja kaznenog djela računalne prijevare da se inkriminiraju manipulacije tijekom obrade podataka poduzete s ciljem nezakonitog prijenosa vlasništava. Explanatory Report, *op. cit.* u bilj. 12, st. 86.

[49] Kaznenim djelom ometanja rada računalnog sustava pruža se kaznenopravna zaštita i sustavima koji obuhvaćaju jedno, pojedinačno računalo (čl. 87. st. 18. izričito navodi da je računalni sustav *svaka naprava*), a ne samo računalnim sustavima koji obuhvaćaju veći broj pojedinačnih računala.

[50] U njemačkoj sudskoj praksi slučajevi ransomwarea u kojem su žrtve bile tvrtke kvalificirani su kao stjecaj iznude i računalne sabotaže/ometanje računalnog sustava (§ 253 Erpressungi i § 303b Computersabotage), v. BGH, 08.04.2021 – 1 StR 78/21. Komentar presude v. Safferling, C., *Beihilfe zu Erpressung und Computersabotage – Konkurrenzen*, Neue Juristische Wochenschriftstr, 2021., str. 2301-2303.

[51] U čl. 273. KZ/11 propisana je pojačana kaznenopravna zaštita u odnosu na pojedina državna tijela, javne ustanove i trgovačka društva od posebnog javnog interesa te s obzirom na opseg ometanja i prouzročene štete, pa u obzir dolazi i stjecaj iznude s kaznenim djelom *teška kaznena djela protiv računalnih sustava, programa i podataka*. Ovo je rješenje svakako dobro budući da ransomware može prouzročiti ne samo ogromnu financijsku štetu, nego i izazvati potpuni kolaps poslovanja ili funkcioniranja organizacija ili institucija koje su od iznimne važnosti za društvo.

U posljednje se vrijeme u pretežitom broju slučajeva ponovni pristup računalnim podacima uvjetuje plaćanjem visokih novčanih iznosa u kriptovalutama. Kriptovalute pošiljatelju mogu osigurati potpunu anonimnost, onemogućiti utvrđivanje iznosa transakcija, stanja računa te povijest transakcija, zbog čega je puno teže ući u trag počinitelju kaznenog djela, u usporedbi s tradicionalnim načinima plaćanja, poput bankovnog transfera.[52] Također, zbog decentralizirane prirode tehnologije *blockchain* koja je temelj za razmjenu kriptovaluta, transakcije je nemoguće poništiti jednom kada su one na *blockchainu* potvrđene.

Ransomware je prepoznat kao globalni sigurnosni problem te je u listopadu 2021. godine više od trideset zemalja, uključujući SAD i Europsku uniju, usvojilo Zajedničku izjavu ministara i predstavnika Inicijative za borbu protiv ransomwarea u kojoj su istaknuli kako je ransomware eskalirajuća globalna sigurnosna prijetnja s ozbiljnim ekonomskim i sigurnosnim posljedicama.[53] Zbog velike opasnosti koju ransomware predstavlja ne samo za pojedince, nego za sigurnost države i njezinih institucija u cjelini, pojedini autori predlažu njegovo izdvajanje kao zasebnog kaznenog djela te propisivanje kazni koje će biti usklađene s njegovom potencijalno razornom moći.[54]

2.3. Stjecaj računalne prijevare i drugih kaznenih djela

Modaliteti radnje počinjenja kaznenog djela računalne prijevare, kao i drugih kaznenih djela propisanih u glavi XXV. KZ/11, veoma su široko postavljeni, međusobno se u određenoj mjeri preklapaju, a ono što ih je povezalo u istu glavu Kaznenog zakona nije zajedničko zaštićeno pravno dobro već to što se sva čine na istom objektu radnje – računalnom sustavu, programu ili podatku.[55] Upravo takav kriterij njihove kategorizacije može otežati utvrđivanje smisla konkretnog kaznenog djela[56] te dodatno naglasiti pitanje razgraničenja pravog i prividnog stjecaja kod ovih kaznenih djela.[57]

Ono što je specifično za kaznena djela propisana u glavi XXV. KZ/11 jest to da ona u velikoj mjeri mogu predstavljati pripremne radnje za počinjenje kaznenog djela računalne prijevare. Primjerice, radnje kojima se ostvaruju bića kaznenih djela neovlaštenog pristupa ili neovlaštenog presretanja računalnih podataka, većinom su

[52] Van Oorschot, *op.cit.* u bilj. 37, str. 202-205.

[53] V. *Joint Statement of the Ministers and Representatives of the Counter Ransomware Initiative*, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/.

[54] Robles-Carrillo, M.; García-Teodoro, P., *Ransomware: An Interdisciplinary Technical and Legal Approach*, Hindawi, Security and Communication Networks, 2022., dostupno na https://www.hindawi.com/journals/scn/ 2022 /2806605/., str. 14-15.

[55] Kaznenim djelima propisanima u glavi XXV. KZ/11 štite se različita pravna dobra kao što su privatnost, sigurnost i imovina.

[56] Veić, Martinović, *op. cit.* u bilj. 2, str. 406.

[57] Za razliku, njemački je zakonodavac ova kaznena djela rasporedio unutar postojećih glava Kaznenog zakona, vodeći se pri tome pravnim dobrom koje se štiti propisivanjem pojedinog kaznenog djela.

samo pripremne radnje za počinjenje računalne prijevare.[58] Ako počinitelj dovrši neko od tih djela i ne poduzme daljnje korake, odgovarat će samo za to dovršeno kazneno djelo. Tako je Županijski sud u Bjelovaru prihvatio žalbu okrivljenika te preinačio prvostupanjsku presudu u dijelu u kojem su okrivljenici bili osuđeni za stjecaj kaznenog djela neovlaštenog pristupa (čl. 266.) i pokušaja računalne prijevare (čl. 271.). Drugostupanjski je sud zaključio da opisane radnje počinjenja djela (optuženike je nadzorna kamera snimila uz bankomat oštećenika u inkriminirano vrijeme) predstavljaju pripremne radnje koje su kažnjive kao samostalno kazneno djelo iz čl. 266. st. 1. KZ/11. Budući da počinitelji nisu zašli u zonu pokušaja kaznenog djela računalne prijevare,[59] drugostupanjski sud oslobodio ih je optužbe za to kazneno djelo.[60] Da su, pak, počinitelji otišli korak dalje i nakon dovršetka kaznenog djela neovlaštenog pristupa u cilju stjecanja imovinske korist poduzeli druge radnje koje prostorno i vremenski neposredno prethode ostvarenju bića kaznenog djela računalne prijevare, otvorilo bi se pitanje postoji li u tom slučaju pravi ili prividni stjecaj.[61] I pod pretpostavkom da su počinitelji ušli u stadij pokušaja kaznenog djela računalne prijevare, ne bi bio prihvatljiv zaključak da je riječ o pravom stjecaju. Naime, kako kazneno djelo računalne prijevare u tom slučaju iscrpljuje cijelo nepravo bila bi riječ o prividnom stjecaju i to odnosu konsumpcije pa nema potrebe počinitelja kažnjavati i za kazneno djelo neovlaštenog pristupa čija obilježja njegova radnja također sadrži.[62] Ako bi počinitelji uspjeli u svom naumu i prouzročili štetu žrtvi, bila bi riječ o dovršenom kaznenom djelu računalne prijevare, a u slučaju da zbog, primjerice, upisivanja netočnog broja PIN-a, ne uspiju podići novac s bankomata, bila bi riječ o pokušaju tog kaznenog djela.[63]

U odnosu na kaznena djela računalnog krivotvorenja i računalne prijevare, Županijski sud u Zagrebu potvrdio je prvostupanjsku presudu kojom je počinitelj osuđen za stjecaj tih kaznenih djela.[64] U tom se slučaju može povući paralela

---

[58] Usp. Kokot, I., *Kaznenopravna zaštita računalnih sustava, programa i podataka,* Zagrebačka pravna revija, vol. 3, 3/2014., str. 309.

[59] Budući da se za temeljni oblik kaznenog djela računalne prijevare može izreći kazna zatvora u trajanju od šest mjeseci do pet godina, a za kvalificirani oblik od jedne do osam godina, radi se o kaznenom djelu za koje je pokušaj kažnjiv.

[60] Presuda Općinskog suda u Rijeci, K-581/2017-22 od 6. ožujka 2019. i Županijskog suda u Bjelovaru, Kž-219/2019-4 od 7. studenog 2019.

[61] O prividnom stjecaju detaljnije v. Grozdanić, V.; Škorić, M.; Martinović, I., *Kazneno pravo: opći dio*, Rijeka, 1. izdanje, Pravni fakultet Sveučilišta u Rijeci, 2013., str. 198-202.

[62] Ipak, odnos između ova dva kaznena djela ne mora uvijek nužno voditi k takvom zaključku. Svakim neovlaštenim pristupom, žrtvi se narušava privatnost. Izvjesne su situacije u kojima počinitelj koristi tek dio tako stečenih podataka za stjecanje imovinske koristi pa osudom samo za računalnu prijevaru ne mora nužno biti obuhvaćeno sve nepravo. Dodatno treba istaknuti da su pravna dobra koja se štite kaznenim djelima neovlaštenog pristupa i računalne prijevare različita, a u sudskoj praksi nerijetko se zauzima stajalište da pravi stjecaj postoji uvijek kada dva ili više kaznenih djela povređuju različita pravna dobra. Iako se potonje stajalište opravdano izlaže kritici, prilikom ocjene radi li se o prividnom ili stvarnom stjecaju kaznenih djela mora se voditi računa o pravnim dobrima koja ona štite, kao i o tome hoće li se osudom za jedno kazneno djelo obuhvatiti sve nepravo. Usp. Novoselec, Martinović, *op. cit.*, str. 345.

[63] Tako je optuženik, koji je u jedanaest navrata na dva bankomata Privredne banke s dvije različite kartice upisivanjem brojeva PIN-a pokušao podići novac, osuđen za produljeno kazneno djelo računalne prijevare u pokušaju. Županijski sud u Varaždinu, Kž-79/20 od 16. travnja 2020.

[64] Županijski sud u Zagrebu, Kž-525/18 od 12. lipnja 2018.

s „klasičnim“ kaznenim djelima krivotvorenja isprave i prijevare kod kojih krivotvorenje isprave predstavlja sredstvo za ostvarenje drugog kaznenog djela, prijevare. U sudskoj praksi zauzeto je stajalište da okolnost što ta kaznena djela jedno prema drugom stoje u odnosu sredstva prema cilju, ne isključuje postojanje stjecaja.[65]

U svakom slučaju, kada je riječ o (prividnom) stjecaju kaznenih djela iz glave XXV. Kaznenog zakona, treba pažljivo ocijeniti da li u konkretnom slučaju ostvarena kaznena djela, svako za sebe, predstavljaju posebnu kriminalnu količinu te da li se njima povređuju različita pravna dobra. Ako je odgovor na oba pitanja pozitivan, valjalo bi zaključiti da između takvih kaznenih djela postoji pravi, a ne prividni stjecaj.

U čl. 272. KZ/11 (zlouporaba naprava), zakonodavac je dodatno inkriminirao izradu, nabavu, uvoz, prodaju, posjedovanje, distribuciju ili omogućavanje drugome dostupnost uređaja (primjerice, uređaja za neovlašteno presretanje komunikacije), ili računalnih programa (primjerice, onih za izradu malicioznih programa) ili računalnih podataka (primjerice, računalnih lozinki ili drugih podataka kojima se može pristupiti računalnom sustavu) poduzetih u cilju da ih se uporabi za počinjenje kaznenih djela iz glave XXV. KZ/11. Kazneno djelo zlouporabe naprava inkriminira iznimno širok krug radnji koje po svom sadržaju predstavljaju pripremnu radnju kao samostalno kazneno djelo za ostvarenje nekog od taksativno nabrojenih kaznenih djela iz glave XXV. KZ/11[66] za koje će počinitelj odgovarati samo ako djelo koje je pripremano nije kasnije i pokušano, odnosno dovršeno.[67]

Pojava novih oblika kriminaliteta uvijek iznova otvara pitanje njihova odnosa s već postojećim kaznenim djelima pa ne iznenađuje da se u praksi javilo pitanje stjecaja kaznenog djela računalne prijevare i drugih kaznenih djela propisanima izvan glave XXV. KZ/11.[68] I u tim slučajevima treba utvrditi iscrpljuje li se u kaznenom djelu računalne prijevare cjelokupno nepravo radnje pa nema potrebe kažnjavati i za drugo kazneno djelo (prethodno, prateće ili naknadno) čija obilježja ta radnja također sadrži ili je, pak, riječ o stjecaju kaznenih djela. Ovo je pitanje bilo posebno aktualno za odnos kaznenog djela (teške) krađe i računalne prijevare. Naime, u praksi je čest slučaj da počinitelj prethodno ukrade bankovnu karticu koju zatim koristi za plaćanje ili podizanje novca iz bankomata.[69] Novoselec ističe da je stjecaj kaznenog djela (teške) krađe i računalne prijevare moguć budući da su ovim djelima oštećena dva različita subjekta – krađom je oštećen vlasnik kartice, a računalnom prijevarom banka kod koje se vodi račun s kojeg je podignut novac. No, i pod

[65] Cvitanović, D. *et. al.*, *op. cit.* u bilj. 26, str. 404.

[66] Turković, K. *et. al.*, *Komentar Kaznenog zakona*, Narodne novine, Zagreb 2013., str. 346.

[67] Ako je pripremano kazneno djelo kasnije pokušano ili dovršeno, pripremne radnje iz čl. 272. smatrat će se nekažnjivim prethodnim djelom. S obzirom na to, stjecaj kaznenih djela računalne prijevare i zlouporabe naprava nije moguć pa nije bila ispravna odluka suda (K-2215/16-43 od 6. listopada 2020.) koji je okrivljenicu, osim za kazneno djelo računalne prijevare, osudio i za kazneno djelo zlouporabe naprava. V. *supra* bilj. 41.

[68] O odnosu kaznenog djela računalne prijevare i iznude v. *supra* poglavlje 2.2.2. b).

[69] V. *supra* poglavlje 2.2.1.

pretpostavkom da se smatra kako je s oba kaznena djela oštećena samo jedna osoba (vlasnik kartice),[70] također će biti riječ o realnom stjecaju. Krađa bi bila nekažnjivo prethodno djelo samo ako bi se njome u cijelosti obuhvatilo nepravo sadržano u računalnoj prijevari, što ovdje nije slučaj budući da krađa kartice predstavlja za oštećenika i štetu koja nije obuhvaćena računalnom prijevarom.[71] Iako je nakon uvođenja kaznenog djela računalne prijevare u domaće kazneno zakonodavstvo bilo određenih prijepora oko ovog pitanja,[72] aktualna sudska praksa u skladu je s navedenim tumačenjem.[73]

Kada počinitelj provlači ukradenu kraticu kroz POS-uređaj te se pri plaćanju traži potpis, kao dodatno pitanje javlja se pitanje stjecaja računalne prijevare i krivotvorenja isprave. S obzirom na to da će u tom slučaju kazneno djelo računalne prijevare biti dovršeno tek potpisivanjem slipova na kojima je navedeno da se odobrava terećenje računa za navedeni iznos, u teoriji i sudskoj praksi zauzeto je stajalište da između kaznenog djela računalne prijevare i krivotvorenja isprave postoji prividni, a ne realni stjecaj. Upravo okolnost da je u ovom slučaju za dovršenje kaznenog djela računalne prijevare nužno krivotvorenje potpisa, upućuje na zaključak da se kazneno djelo krivotvorenja isprave javlja kao tipično prateće djelo koje se čini zajedno s kaznenim djelom računalne prijevare kao glavnim, tako da je njegovo nepravo već obuhvaćeno nepravom glavnog djela.[74]

3. STATISTIČKI PODACI O BROJU PUNOLJETNIH PRIJAVLJENIH, OPTUŽENIH I OSUĐENIH OSOBA ZA KAZNENO DJELO RAČUNALNE PRIJEVARE OD 2016. DO 2022.

U nastavku su prikazani statistički podaci Državnog zavoda za statistiku koji se odnose na broj prijavljenih, optuženih i osuđenih punoljetnih osobe za kazneno djelo računalne prijevare od 2016. do 2022. te posebno na udio nepoznatih počinitelja u ukupnom broju prijavljenih osoba.[75]

[70] Kao što je to uzeo Županijski sud u Splitu, Kž-205/08 od 20. svibnja 2008.

[71] Novoselec, *op. cit.* u bilj. 28, str. 1166-1177.

[72] Tako su prvostupanjskom presudom dvojica okrivljenika proglašena krivima za supočiniteljstvo u kaznenim djelima krađe i računalne prijevare, no drugostupanjski sud je po službenoj dužnosti preinačio ovu presudu te utvrdio da su optuženici počinili samo jedno kazneno djelo, i to teške krađe. *Loc. cit.*

[73] V. primjerice, presude Županijskog suda u Zagrebu, 1 Kž-90/2019-3 od 12. veljače 2019. i 15 Kž-711/2022-3 od 26. srpnja 2022.

[74] Tako i Županijski sud u Bjelovaru, Kž-53/19 od 7. ožujka 2019.

[75] Svi podaci Državnog zavoda za statistiku sadržani u ovom dijelu rada dostupni su na https://web.dzs.hr/ PXWeb/Menu.aspx?px_db=Pravosudje&px_language=hr.

Tablica 1.
Prijavljene, optužene i osuđene punoljetne osobe za kazneno djelo računalne prijevare od 2016. do 2022.

		PRIJAVE			OPTUŽBE	OSUDE
		Ukupno	**Od toga nepoznati**	**Nepoznati %**	**/**	**/**
2016.	st. 1.	436	319	73	88	81
	st. 2.	20	17	85	5	5
2017.	st. 1.	541	396	73	85	75
	st. 2.	28	15	53,6	2	2
2018.	st. 1.	496	320	64,5	109	103
	st. 2.	23	17	73	1	1
2019.	st. 1.	530	374	70,5	104	100
	st. 2.	22	15	68	4	2
2020.	st. 1.	629	488	77,5	94	91
	st. 2.	31	25	80,6	1	/
2021.	st. 1.	827	676	81,7	105	99
	st. 2.	30	22	73	6	5
2022.	st. 1.	1027	883	81	103	99
	st. 2.	71	60	84,5	3	1
Ukupno		**4711**	**3627**	**77 %**	**710**	**664**

U odnosu na ukupan broj prijava za sva kaznena djela od 2016. do 2022., na prijave zbog kaznenog djela računalne prijevare odnosi se tek manji broj, prosječno njih 1,3 % godišnje.[76] Iako ovaj udio nije velik, iz prikazanih podataka vidljivo je da broj prijava za kazneno djelo računalne prijevare iz godine u godinu raste (iznimka je samo 2018. kada je bilo nešto manje prijava u odnosu na prethodnu godinu).[77] Kada usporedimo podatke iz početne i završne godine u promatranom razdoblju, evidentan je značajan porast prijava za kazneno djelo računalne prijevare u završnoj godini, i to za više od dvostruko u odnosu na temeljni oblik računalne prijevare (st. 1.), dok je za kvalificirani oblik (st. 2.) broj prijava porastao više nego trostruko. Imajući u vidu da se gotovo sva komunikacija između ljudi temelji na uporabi tehnologije, da je broj transakcija i bankarskih usluga koje se provode online u konstantnom porastu i da načini počinjenja kaznenog djela računalne prijevare postaju sve raznovrsniji i sofisticiraniji, ovakvi podaci ne iznenađuju i za

[76] Prema podacima Državnog zavoda za statistiku od 2016. do 2022. u odnosu na sva kaznena djela bile su ukupno 367.304 prijave, dok je za kazneno djelo računalne prijevare bilo ukupno 4711 prijava.

[77] Suprotno od toga, ukupan broj prijava u odnosu na sva kaznena djela u kontinuiranom je padu. Tako su 2016. godine bile 60.194 prijave, a 2022. godine 46.045 prijava.

pretpostaviti je da će se trend povećanja broja prijava za kazneno djelo računalne prijevare nastaviti i u budućnosti.[78] [79]

Osim rasta broja prijava, važan podatak koji se može zamijetiti iz tablice 1. jest i konstantan te značajan porast broja nepoznatih počinitelja. Od 4711 prijave u promatranom razdoblju, na nepoznate počinitelje odnosilo se njih 3627 ili čak 77 %.[80] Ovaj podatak treba promatrati imajući u vidu specifičnost kaznenog djela računalne prijevare čije su sredstvo počinjenja suvremene tehnologije koje počinitelju omogućuju pristup žrtvama iz cijelog svijeta uz istodobno prikrivanje identiteta manipulacijom računalnim podacima. Sve to znatno otežava identifikaciju počinitelja te istragu i dokazivanje ovog kaznenog djela. Znatan udio nepoznatih počinitelja zasigurno je jedan od razloga postojanja velikog raskoraka između broja prijava i broja optužbi. Naime, prosječno svega 17 % prijava prelazi u stadij optuživanja. S druge strane, broj je osuda u odnosu na broj optužbi značajan: iznosi visokih 93 %, s time da je broj osuđenih za temeljni oblik kaznenog djela računalne prijevare (st. 1.) gotovo deset puta veći u odnosu na one osuđene za kvalificirani oblik (st. 2.).

4. ZAKLJUČAK

Karakteristika je kaznenog djela računalne prijevare to da ga počinitelji čine u specifičnom, kibernetičkom prostoru koristeći se različitim vrstama informatičke tehnologije. Kibernetički prostor, koji nije vidljiv, ni opipljiv, niti ima fizičku granicu, uvelike se razlikuje od fizičkog prostora u kojem se čini većina kaznenih djela. Istodobno, gotovo svakodnevno pojavljuju se nove tehnologije koje omogućavaju stvaranje novih oblika malwarea pa je raznovrsnost i promjenjivost modaliteta počinjenja kaznenog djela računalne prijevare te njihova prilagodljivost jedan od velikih izazova s kojima se države suočavaju u inkriminiranju ove vrste kriminaliteta.

Okolnost da je zakonodavac kaznena djela protiv računalnih sustava, programa i podataka svrstao u istu glavu KZ/11 zbog toga što se sva čine na istom objektu radnje (računalnom sustavu, programu ili podatku) i da ono što ih je povezalo u glavu XXV. KZ/11 nije bilo zajedničko zaštićeno pravno dobro, dodatno otežava utvrđivanje

[78] Trend porasta ovih kaznenih djela vidljiv je i u drugim državama. Cook, S. *et al.*, Fear of Economic Cybercrime Across Europe: A Multilevel Application of Routine Activity Theory, The British Journal of Criminology, vol. 63, 2/2023., str. 384.

[79] Prilikom zaključka o rasprostranjenosti ovog kaznenog djela dodatno se mora voditi računa o tzv. tamnoj brojci, odnosno o broju počinjenih djela koja nisu prijavljena nadležnim tijelima pa nisu ni evidentirana u službenim statistikama. Pojedini autori ukazuju na postojanje značajne razlike između broja stvarno počinjenih kaznenih djela računalne prijevare i onih koji su prikazani u statističkim podacima. Kemp, S.; Miró-Llinares, F.; Moneva, A., *The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain*, European Journal on Criminal Policy and Research, vol. 26, 4/2020, str. 293-312, Tcherni, M.; Davies, A.; Lopes G.; Lizotte, A., *The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?*, Justice Quarterly, vol. 33, 5/2016, str. 890-911.

[80] Za usporedbu, udio nepoznatih počinitelja u ukupnom kriminalu za navedeno razdoblje iznosio je 45 %.

njihova smisla i otvara pitanje stjecaja kaznenog djela računalne prijevare i ostalih kaznenih djela iz glave XXV., kao i njegov odnos s tradicionalnim kaznenim djelima, posebno onima protiv imovine. Poseban izazov predstavljaju uporaba i tumačenje informacijsko-komunikacijske tehnologije koji su nužni za razumijevanje kaznenih djela iz glave XXV. KZ/11 i ispravnu kvalifikaciju kriminalnog ponašanja. Zbog *sui generis* prirode računalnih sustava, ispravno tumačenje bića kaznenog djela računalne prijevare zahtijeva interdisciplinarno znanje koje, između ostalog, uključuje i razumijevanje osnovnih pojmova računalne znanosti. Samo takvim, sveobuhvatnim, interdisciplinarnim pristupom može se učinkovito pristupiti ovoj problematici.

Korištenje suvremene tehnologije omogućuje počiniteljima pristup žrtvama diljem svijeta, dok istodobno otežava njihovu identifikaciju, što potvrđuju i podaci Državnog zavoda za statistiku o značajnom broju prijava protiv nepoznatih počinitelja. To pokazuje da je nužno uložiti dodatne napore u osmišljavanju i provođenju kontinuirane interdisciplinarne suradnje različitih dionika na nacionalnoj i međunarodnoj razini te u razvoju i unapređenju adekvatnog sustava za pravovremeno otkrivanje počinitelja ovog kaznenog djela. Dodatno, posebno mjesto u suzbijanju računalnog kriminaliteta ima prevencija u kojoj naglasak treba staviti na informatičko opismenjivanje stanovnika. Čovjek svakog trenutka postaje sve ovisniji o tehnologiji na kojoj se temelji gotovo sva komunikacija, privatna i poslovna. Istodobno, zbog svog neznanja, nepažnje, nedovoljnog poznavanja funkcioniranja tehnologije i nedovoljne svijesti o važnosti zaštite podataka, pojedinci se izlažu nizu opasnosti kojima ugrožavaju svoju privatnost i sigurnost te postaju žrtve kaznenih djela. Boljim razumijevanjem virtualne stvarnosti prosječan stanovnik može postići višu razinu sigurnosti u svakodnevnom korištenju računalne tehnologije te je stoga edukacija o sigurnom načinu korištenja suvremenom tehnologijom, uz istodobno naglašavanje nužnosti zaštite povjerljivih podataka, *conditio sine qua non* za suzbijanje ovog vida kriminaliteta.

LITERATURA

Knjige i članci:

1. Brian, A. W., *The Nature of Technology: What It Is and How It Evolves*, New York, 1. izdanje, Free Press, 2009.
2. Bullée, J. W.; Junger, M., Social Engineering. u: Holt, T.; Bossler, A. (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Palgrave Macmillan, Cham, 2020.
3. Cook, S.; Giommoni, L.; Trajtenberg Pareja, N.; Levi, M.; Williams, M. L., *Fear of Economic Cybercrime Across Europe: A Multilevel Application of Routine Activity Theory*, The British Journal of Criminology, vol. 63, 2/2023., str. 384-406.
4. Cvitanović, L.; Derenčinović, D.; Turković, K.; Munivrana Vajda, M.; Dragičević Prtenjača, M.; Maršavelski, A.; Roksandić Vidlička, S., *Kazneno pravo, posebni dio,* Pravni fakultet Sveučilišta u Zagrebu, Zagreb 2018.

5. Čelebić, G.; Rendulić, D. I., *Osnovni pojmovi informacijske i komunikacijske tehnologije*, Zagreb, 2011., dostupno na https://itdesk.info/prirucnik_osnovni_pojmovi _informacijske_tehnologije.pdf .
6. DeBacher, J., *Ransomware, Georgetown Law Technology Review*, vol 6., 1/2022, str. 300-310.
7. Gelenbe, E.; Kahane, J., *Fundamental Concepts in Computer Science: Advances in Computer Science and Engineering: Texts*, London, 1. izdanje, Imperial College Press, 2009.
8. Grozdanić, V.; Škorić, M.; Martinović, I., *Kazneno pravo: opći dio*, Rijeka, 1. izdanje, Pravni fakultet Sveučilišta u Rijeci, 2013.
9. Kemp, S.; Miró-Llinares, F.; Moneva, A., *The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain,* European Journal on Criminal Policy and Research, vol. 26, 4/2020, str. 293-312.
10. Kokot, I., *Kaznenopravna zaštita računalnih sustava, programa i podataka,* Zagrebačka pravna revija, vol. 3, 3/2014., str. 303-330.
11. Lubin, A., *The Law and Politics of Ransomware,* Vanderbilt Journal of Transnational Law, vol. 55, 5/2022, str. 1177-1216.
12. Middleton, B., *Cyber Crime Investigator's Field Guide*, Boca Raton, London, New York, 3. izdanje, CRC Press, 2022.
13. Moslavac, B., *Enigma (sudske) pravne kvalifikacije kažnjivog djela podizanja novca na bankomatu ukradenom karticom*, IUS-INFO, dostupno na https://www.iusinfo.hr/strucni-clanci/CLN20V01D2018B1125.
14. Moslavac, B., *Plaćanje otkupnine u slučaju ransomware-a i posljedice za žrtvu*, IUS-INFO, dostupno na https://www.iusinfo.hr/strucni-clanci/placanje-otkupnine-u-slucaju -ransomware-a-i-posljedice-za-zrtvu.
15. Mrčela, M.; Vuletic, I., *Healthcare, privacy, big data and cybercrime: which one is the weakest link?,* Annals of Health Law, vol. 27, 2/2018., str. 257-280.
16. Novoselec, P., *Posebni dio kaznenog prava*, Pravni fakultet Sveučilišta u Zagrebu, Zagreb 2007.
17. Novoselec, P., *Sudska praksa*, Hrvatski ljetopis za kazneno pravo i praksu, vol. 15, 2/2008., str. 1166-1167.
18. Potrka, N., *Računalna prijevara – analiza djelotvornosti otkrivačke djelatnosti*, Policija i sigurnost, vol. 28, 3/2019., str. 270-283.
19. Robles-Carrillo, M.; García-Teodoro, P., *Ransomware: An Interdisciplinary Technical and Legal Approach*, Hindawi, Security and Communication Networks, 2022., dostupno na https://www.hindawi.com/journals/scn/2022/2806605/.
20. Safferling, C., *Beihilfe zu Erpressung und Computersabotage – Konkurrenzen*, Neue Juristische Wochenschriftstr,2021., str. 2301-2303.
21. Schönke, A.; Schröder, H., *Strafgesetzbuch*, Beck, München 2019.
22. Sokanović, L.; Orlović, A., *Oblici prijevara u Kaznenom zakonu*, Hrvatski ljetopis za kaznene znanosti i praksu, vol. 24, 2/2017., str. 583-615.

23. Škrtić, D., *Kaznenopravna zaštita informatičkih sadržaja*, doktorska disertacija, Sveučilište u Zagrebu, Pravni fakultet, Zagreb 2011.
24. Tcherni, M.; Davies, A.; Lopes G.; Lizotte, A., *The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?*, Justice Quarterly, vol. 33, 5/2016, str. 890-911.
25. Turković, K.; Novoselec, P.; Grozdanić, V.; Kurtović Mišić, A.; Derenčinović D.; Bojanić, I.; Munivrana Vajda, M.; Mrčela, M.; Nola, S.; Roksandić Vidlička S.; Tripalo, D.; Maršavelski A., *Komentar Kaznenog zakona*, Narodne novine, Zagreb 2013.
26. Van Oorschot, P. C., *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin*, 2. izdanje, Springer, 2021.
27. Veić, P.; Martinović, I., *Izazovi policijskog postupanja u otkrivanju i dokazivanju računalnog kriminala*, Zbornik radova 5. međunarodne znanstveno-stručne konferencije Istraživački dani Visoke policijske škole u Zagrebu Unaprjeđivanje sigurnosne uloge policije primjenom novih tehnologija i metoda, 2016., str. 404-423.
28. Vuletic, I., *Data-driven healthcare and cybercrime: threat we are not aware of?*, Asia Pacific Journal of Health Law & Ethics, vol. 11, 2/2018, str. 16-32.
29. Vuletić, I., *Primjenjivost tradicionalnih kaznenopravnih koncepata na računalni kriminal*, Zbornik Pravnog fakulteta u Zagrebu, vol. 64, 5-6/2014, str. 895-909.
30. Vuletić, I.; Nedić, T., *Računalna prijevara u hrvatskom kaznenom pravu*, Zbornik Pravnog fakulteta Sveučilišta u Rijeci, vol. 35, 2/2014., str. 679-692.

Pravni propisi:

1. Kazneni zakon, Narodne novine, br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, 114/22, 114/23.
2. Kazneni zakon, Narodne novine, br. 111/97, 27/98, 50/00, 129/00, 84/05, 51/01, 111/03, 190/03, 105/04, 71/06, 110/07, 152/08, 57/11, 77/11, 125/11, 143/12.
3. Konvencija o kibernetičkom kriminalu, Narodne novine – Međunarodni ugovori, br. 9/02.
4. Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP, SL 218, 14. 8. 2013.
5. Direktiva (EU) 2019/713 Europskog parlamenta i Vijeća od 17. travnja 2019. o borbi protiv prijevara i krivotvorenja u vezi s bezgotovinskim sredstvima plaćanja i zamjeni Okvirne odluke Vijeća 2001/413/PUP, SL 123, 10. 5. 2019.

Sudska praksa:

1. Općinski sud u Sisku, K-276/2023-2 od 24. listopada 2023.
2. Županijski sud u Zagrebu, 6 Kžmp-61/2022-11 od 14. veljače 2023.
3. Županijski sud u Zagrebu, 15 Kž-711/2022-3 od 26. srpnja 2022.
4. Općinski sud u Zagrebu u predmetu K-2215/16-43 od 6. listopada 2020.
5. Općinski kazneni sud u Zagrebu, K-163/20-2 od 7. svibnja 2020.

6. Županijski sud u Varaždinu, Kž-79/20 od 16. travnja 2020.
7. Županijski sud u Bjelovaru, Kž-219/2019-4 od 7. studenog 2019.
8. Općinski kazneni sud u Zagrebu, K-2235/16-46 od 4. studenog 2019.
9. Županijski sud u Bjelovaru, Kž-53/19 od 7. ožujka 2019.
10. Općinski sud u Rijeci, K-581/2017-22 od 6. ožujka 2019.
11. Županijski sud u Zagrebu, 1 Kž-90/2019-3 od 12. veljače 2019.
12. Županijski sud u Osijeku, Kž-231/18 od 27. rujna 2018.
13. Županijski sud u Zagrebu, Kž-525/18 od 12. lipnja 2018.
14. Županijski sud u Splitu, Kž-497/17 od 7. rujna 2017.
15. Općinski sud u Virovitici, 6 K-3/17-34 od 9. svibnja 2017.
16. Vrhovni sud RH, Kzz-18/16 od 11. travnja 2016.
17. Vrhovni sud RH, III Kr-92/08-7 od 10. veljače 2009.
18. Županijski sud u Splitu, Kž-205/08 od 20. svibnja 2008.

CRIMINAL OFFENCE OF COMPUTER FRAUD AS AN ABUSE OF COMPUTER DATA AND THE COMPUTER SYSTEM

Following the introductory remarks about information and telecommunication technology, which has created a fully new and specific cyberspace within which individuals undertake numerous and diverse activities, the paper analyzes one of the most common forms of computer crime, whose number is continuously increasing – the criminal offense of computer fraud under Article 271 of the Criminal Code. In order to effectively respond to the new challenges, the legislator has set the modalities of committing this criminal offense very broadly, which raises the question of its relationship with other criminal offenses. Therefore, in addition to the current legal regulation, the paper also considers the issue of the concurrence of the criminal offense of computer fraud with other criminal offenses. The paper particularly points to the highly widespread use of malicious software as a means of collecting computer data, which imposes the need for constant education on the safe ways of using modern technology. The observed problem of the constant increase in the number of reports of the criminal offense of computer fraud and the extremely high proportion of their unknown perpetrators calls for a systematic and comprehensive improvement of measures needed for their identification, and it emphasizes the need for interdisciplinary knowledge as a necessary condition for a successful fight against this form of crime.

Key words: *computer crime, computer fraud, malicious software, concurrence, interdisciplinarity*