UDK 343.51/.52
343.72:004.7(497.5:4EU)
004.7:343.72(497.5:4EU)
Primljeno 31. ožujka 2020.
Pregledni znanstveni rad

Dr. sc. Maja Buhovac *

MODERNI OBLICI PRIJEVARA I KRIVOTVORENJA BEZGOTOVINSKIH INSTRUMENATA PLAĆANJA PREMA DIREKTIVI 2019/713/EU

Dinamičnim društvenim promjenama i razvojem suvremenih načina plaćanja roba i usluga nastali su različiti instrumenti bezgotovinskog plaćanja, osobito oni u nefizičkom obliku. Transakcije platnim karticama najraširenije su oblik plaćanja u Europskoj uniji, pa su često i meta kriminalnim skupinama, koje putem prijevara i krivotvorenja protupravno prisvajaju impozantne novčane iznose. Osigurati kaznenopravnu zaštitu imovine u obliku nematerijalnog pravnog dobra glede prijevarnih oblika postupanja s bezgotovinskim sredstvima plaćanja izazov je i za zakonopisca i za sudsku praksu. S druge strane to je i nužnost s obzirom na gubitke koji nastaju njihovim činjenjem. Autorica se u ovom radu bavi analizom recentne Direktive 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. Direktiva je stupila na snagu 30. svibnja 2019. godine, a njezina bi implementacija u hrvatsko kazneno zakonodavstvo trebala uslijediti do 31. svibnja 2021. godine. Stoga se u radu iznose temeljne postavke na kojima počiva Direktiva, uz analizu novih oblika kaznenih djela s bezgotovinskim instrumentima plaćanja, te njezina implementacija u hrvatsko kazneno zakonodavstvo.

Ključne riječi: prijevare, elektronički novac, krivotvorenje, implementacija, računalna prijevara, kibernetički kriminalitet

I. UVOD

Novac predstavlja specifičnu vrstu robe, odnosno platežno sredstvo koje služi razmjeni dobara. Prije njegova nastanka funkciju novca imala je stoka, školjke, krzno, žito. S razvojem trgovine i društvenih zajednica pojavljuju se novčane vrste nastale na temelju definiranja vrijednosnih odnosa među me-

* Dr. sc. Maja Buhovac, docentica, vanjska suradnica, Pravni fakultet Sveučilišta u Mostaru, maja.buhovac@pf.sum.ba

talima. Tako se pri izradi prvog novca koristilo zlato, srebro, bakar, bronca i mjed. On se ručno izrađivao sve do nastanka prvih strojeva za kovanje novca.[1] Stoljećima je gotovi novac bio glavno sredstvo plaćanja. Međutim danas se sve više koristi bezgotovinski način plaćanja roba i usluga kao posljedica razvoja tehnologije i digitalnog bankarstva. Prema definiciji Hrvatske narodne banke bezgotovinsko je plaćanje svako plaćanje pri kojem se ne koristimo gotovim novcem, a najčešće sredstvo takve vrste plaćanja jesu platne kartice. Transakcije platnim karticama najrašireniji su oblik plaćanja i u EU-u.[2] Međutim takve su transakcije često meta kriminalnim skupinama, koje putem prijevara s platnim karticama godišnje protupravno prisvoje više od 1,5 milijardi eura. U tu vrstu prijevarnih postupanja s platnim karticama spada *skimming* ili kopiranje podataka s magnetne vrpce bankovne kartice. Taj se oblik prijevare izvodi tako da počinitelji instaliraju uređaje (*skimmere*), najčešće na bankomate, a svrha im je da kopiraju podatke s magnetne vrpce vlasnika platne kartice.[3] Nadalje, sve je više zastupljena zlouporaba POS-uređaja (engl. *Point of Sales terminals*), koja poprima različite oblike, od manipulacija tim uređajima do nabave krivotvorenih. Osim s financijskim gubitkom žrtve se često suočavaju i s krađom identiteta. Naime kriminalci preuzimaju identitet žrtava kako bi dobili pristup njihovu novcu (*phishing*).[4] Tako počinitelji pristupaju važnim osobnim podacima, kao što su korisničko ime i lozinka, a prijevara se čini tako što se velikom broju primatelja šalje poruka e-poštom, gdje se kao pošiljatelj pojavljuje naizgled pouzdana tvrtka. Poruka primatelja može usmjeriti na lažnu *web*-stranicu, na kojoj se od njega traži da unese osobne podatke.[5] Jedna od sofisticiranijih metoda *phishinga* jest *pharming*, tehnika kojom se zlorabi internetska domena kako bi se žrtve preusmjerile na lažnu *web*-stranicu (npr. umjesto *google.com* počinitelji se služe domenom *google.org*, pri čemu žrtve ne sumnjaju u istinitost *web*-stranice).[6] Europska javnost sve je više zabrinuta

[1] Više o povijesti prvog novca vidjeti na http://old.hnb.hr/novcan/povijest/h-nastavak-1.htm (pristup 4. ožujka 2020.)

[2] Ukupni broj bezgotovinskih plaćanja u eurozoni porastao je za 7,9 % na 90,7 milijardi u 2018. u odnosu na prethodnu godinu. Plaćanje putem kartica činilo je 46 % ukupnog broja bezgotovinskih plaćanja u eurozoni. Podaci dostupni na: European Central Bank, Payments statistics: 2018, 26 July 2019, https://www.ecb.europa.eu/press/pr/stats/paysec/html/ecb.pis2018~c758d7e773.en.html (pristup 4. ožujka 2020.)

[3] O *skimmingu* vidjeti više: Clough, J., Principles of Cybercrime, Second Edition, Cambridge University Press, 2015, str. 225-227.

[4] O *phishingu* vidjeti više: *Ibid*, str. 220-221; Sokanović, L., Orlović, A., Oblici prijevara u kaznenom zakonu, Hrvatski ljetopis za kazneno pravo i praksu, vol. 24, broj 2/2017, Zagreb, str. 608.

[5] Prijedlog Direktive Europskog parlamenta i Vijeća o borbi protiv prijevara i krivotvorenja bezgotovinskih sredstava plaćanja i zamjeni Okvirne odluke Vijeća 2001/413/PUP COM(2017) 489 final, str. 19, (bilj. 40).

[6] O *pharmingu* vidjeti više: Clough, J., *op. cit.,* str. 223-224.

zbog prijevara s kreditnim karticama i internetskim bankarstvom te krađom identiteta. Zbog šire uporabe sigurnijih kreditnih kartica s čipom (EMV – međunarodni sigurnosni standard koji su prvotno razvili Europay, MasterCard i Visa) počinitelji sve češće prelaze na prijevare u vezi s plaćanjima pri kojima nije potrebno predočiti karticu.[7]

Zbog razvoja navedenih pojava EU radi na stalnom jačanju pravnog okvira kojim će se poboljšati mjere za sprječavanje tih vrsta prijevara. Posljednja je takva 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 (dalje u tekstu: Direktiva).[8] Stoga je cilj ovog rada analizirati postojeći normativni okvir na razini EU-a glede tog oblika kibernetičkog kriminaliteta te novih oblika kaznenih djela, kao i njihovu implementaciju u hrvatski pravni sustav.

II. PRETHODNI INSTRUMENTI

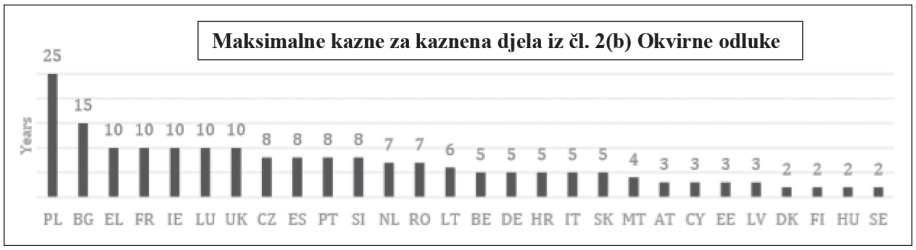
Prvi korak u zaštiti novca od prijevara i krivotvorenja bila je Okvirna odluka Vijeća 2001/413/PUP o borbi protiv prijevara i krivotvorenja bezgotovinskih sredstava plaćanja od 28. svibnja 2001. godine (dalje u tekstu: Okvirna odluka).[9] Okvirna je odluka stupila na snagu pet dana poslije, 2. lipnja 2001. godine. Njezin cilj bio je inkriminirati ona ponašanja koja dovode do prijevara i krivotvorenja svih oblika bezgotovinskih instrumenata plaćanja te osigurati mehanizme prekogranične suradnje i razmjene informacija te tako ojačati i pravosudne sustave samih država članica u borbi protiv prijevara s platnim karticama. Tako je Okvirna odluka predviđala da države članice inkriminiraju krađe ili neko drugo protupravno prisvajanje instrumenata plaćanja, krivotvorenje, zlouporabu, primanje, nabavu, prijevoz, prodaju ili prijenos na drugu osobu ukradenog instrumenta plaćanja, zatim protupravna ponašanja vezana za računala (poput „hakiranja" računalnih sustava u svrhu protupravnog prijenosa novca) te kaznena djela povezana s posebno prilagođenim uređajima (koja uključuju krivotvorenje instrumenata, predmeta, računalnih programa i

[7] Dostupno na: https://what-europe-does-for-me.eu/data/pdf/social/P03_hr.pdf (pristup 5. ožujka 2020.).

[8] 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 123/19 dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32019L0713&from=EN (pristup 5. ožujka 2020.).

[9] Okvirna odluka Vijeća od 28. svibnja 2001. o borbi protiv prijevara i krivotvorenja bezgotovinskih sredstava plaćanja (2001/413/PUP), SL 149/1, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32001F0413 (pristup 7. ožujka 2020.).

sl.).[10] Međutim Okvirna odluka nije propisivala ni vrstu ni visinu kaznenopravnih sankcija za pojedina kaznena djela, nego je pozivala države članice da „osiguraju mjere kojima će ova ponašanja biti kažnjiva učinkovitim, razmjernim i odvraćajućim kaznama, uključujući ... kazne vezane uz lišavanje slobode ....". To je rezultiralo različitim zakonodavnim rješenjima u državama članicama, a razlike u kaznama predstavljene su u Radnom dokumentu Komisije.[11]



Izvor: Radni dokument, str. 208.

Prema članku 1. Okvirne odluke 'instrument plaćanja' znači fizički instrument koji nije novac i koji omogućuje vlasniku ili korisniku prijenos novca ili novčane vrijednosti te navodi popis platnih instrumenata: „kreditne kartice, euroček kartice, druge kartice koje izdaju financijske institucije, putnički čekovi, euro-čekovi, drugi čekovi i mjenice ....". Dok se Okvirna odluka ograničava samo na bezgotovinski instrument plaćanja u fizičkom obliku, neki drugi pravni akti EU-a proširuju pojam instrumenta plaćanja. Tako Direktiva (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu[12] definira „platni instrument" kao personalizirani uređaj i/ili skup postupaka dogovorenih između korisnika platnih usluga i pružatelja platnih usluga koji se koriste za iniciranje naloga za plaćanje. Direktiva 2009/110/EZ Europskog parlamenta i Vijeća od 16. rujna 2009. o osnivanju, obavljanju djelatnosti i bonitetnom nadzoru poslovanja institucija za elektronički novac[13] definira „elektronički novac" kao pohranjenu novčanu

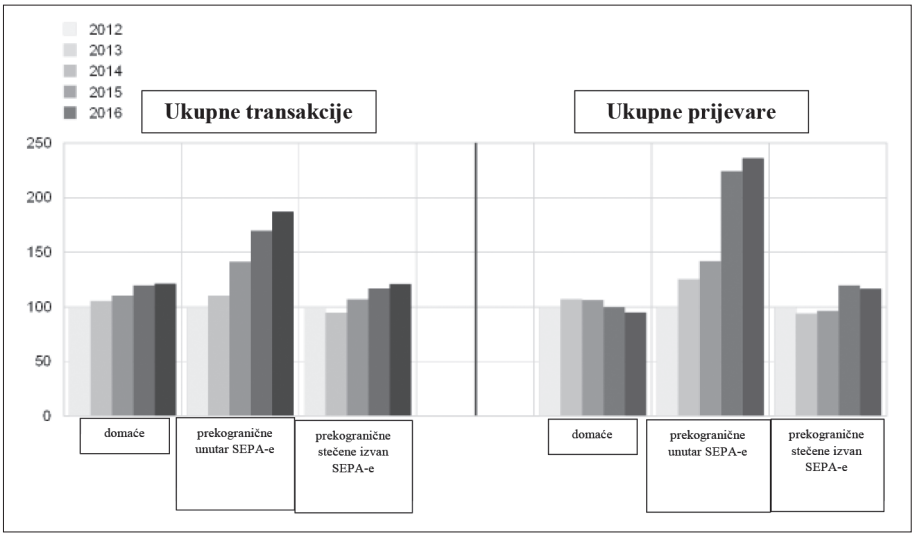
[10] Čl. 2., 3., 4. Okvirne odluke.

[11] Commission Staff Working Document, Impact Assessment, Accompanying the document Proposal for a Directive of the European Parliament and the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, 13. 9. 2017. Bruxelles, final 298 (dalje u tesktu: Radni dokument), dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:52017SC0298&qid=1508925039726&from=EN (pristup 7. ožujka 2020.).

[12] Čl. 4. st. 14. Direktive (EU) 2015/2366 Europskog parlamenta i Vijeća od 25. studenoga 2015. o platnim uslugama na unutarnjem tržištu, o izmjeni direktiva 2002/65/EZ, 2009/110/EZ i 2013/36/EU te Uredbe (EU) br. 1093/2010 i o stavljanju izvan snage Direktive 2007/64/EZ.

[13] Čl. 2. st. 2. Direktive 2009/110/EZ Europskog parlamenta i Vijeća od 16. rujna 2009. o osnivanju, obavljanju djelatnosti i bonitetnom nadzoru poslovanja institucija za elektronički

vrijednost u svrhu izvršenja platnih transakcija. Iz navedenih definicija vidljivo je da instrument plaćanja nisu samo platne kartice iz Okvirne odluke nego i na drugi način pohranjene novčane vrijednosti kojima se omogućava prijenos novca. Posebno važne odredbe Okvirne odluke odnose se na suradnju između država članica i razmjenu informacija s obzirom na prekograničnu dimenziju prijevara i krivotvorenja bezgotovinskih sredstava plaćanja. U Petom izvješću Europske središnje banke[14] u tablici ispod prikazane su prijevare bezgotovinskim instrumentima plaćanja u domaćim sustavima te prekogranične prijevare.



Izvor: Peto izvješće Europske središnje banke

Iz tablice je vidljivo da su kroz razdoblje od 2012. do 2016. godine domaće transakcije bile veće od ukupnih prijevara u domaćim sustavima, dok su prekogranične transakcije bile manje od ukupnog broja prekograničnih prijevara. To upućuje i na činjenicu da su kriminalne skupine u navedenom razdoblju iskorištavale postojeći normativni okvir, odnosno nedostatke koje Okvirna odluka sadrži, a koje se osobito tiču nemogućnosti vođenja prekograničnih istraga za ta kaznena djela.[15] Okvirnom se odlukom inkriminiraju kaznena djela

novac te o izmjeni direktiva 2005/60/EZ i 2006/48/EZ i stavljanju izvan snage Direktive 2000/46/EZ.

[14] Vidjeti više u: European Central Bank, Fifth Report on Card Fraud, September 2018, dostupno na: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html (pristup 8. ožujka 2020.).

[15] Na to upućuje i Prijedlog Direktive, koji uspoređuje odredbe Okvirne odluke i predložene mjere u Direktivi. Prijedlog Direktive od 13. 9. 2017. godine COM(2017) 489 final, str. 17.

koja se tiču prijevara i krivotvorenja platnih instrumenata u fizičkom obliku, ali temeljni problem zbog kojeg se određena kaznena djela ne mogu učinkovito procesuirati jest to što se kaznena djela počinjena određenim instrumentima plaćanja (posebno nefizičkim) u državama članicama različito inkriminiraju ili se uopće ne inkriminiraju. Okvirnu odluku u svoje nacionalno zakonodavstvo implementiralo je 20 država članica EU-a. Premda je Republika Hrvatska u tada važećem Kaznenom zakonu (dalje u tekstu: KZ/97)[16] sadržavala neka kaznena djela koja odgovaraju onima propisanim u Okvirnoj odluci,[17] ipak je u smjeru implementacije Okvirne odluke izvršila određene izmjene Kaznenog zakona.[18]

2.1. Što se promijenilo od donošenja Okvirne odluke do danas

Od donošenja Okvirne odluke do danas prošlo je 19 godina. U tom razdoblju došlo je do značajnih promjena u načinu na koji građani EU-a plaćaju robu i usluge. Plaćanja se sve više vrše bezgotovinskim sredstvima, poput kreditnih ili debitnih kartica. Štoviše, tehnološki razvoj donio nam je nove vrste bezgotovinskog plaćanja; sada kupujemo putem interneta, obavljamo internetski prijenos novca, koristimo mobilne novčanike, virtualne valute, e-novac itd. U međuvremenu su se i kriminalne skupine prilagodile novonastalim trendovima i tehnološkom razvoju. Istraživanja pokazuju da prijevare s bezgotovinskim platnim instrumentima donose prihode od organiziranog kriminaliteta[19] i time omogućavaju druge kriminalne aktivnosti, kao što su terorizam, trgovina drogom i trgovina ljudima. Prihod od prijevara s bezgotovinskim plaćanjem najviše se koristi za putovanja, odnosno kupnju ilegalnih avionskih karata ukradenim kreditnim karticama,[20] ili se pak ulaže u daljnja

[16] Kazneni zakon (NN 110/97).

[17] Krađa (čl. 216. KZ/97), oštećenje i uporaba tuđih podataka (čl. 223. KZ/97), krivotvorenje novca (čl. 274. KZ/97), krivotvorenje isprave (čl. 311. KZ/97), izrada, nabavljanje, posjedovanje, prodaja ili davanje na uporabu sredstava za krivotvorenje isprava (čl. 314. KZ/97).

[18] Zakonom o izmjenama i dopunama Kaznenog zakona (NN 105/04) u kaznenopravni sustav uvedeno je kazneno djelo računalne prijevare (čl. 224. a) KZ/97) te kazneno djelo računalnog krivotvorenja (čl. 223. a) KZ/97).

[19] Prema Petom izvješću Europske središnje banke, u kojem je sadržana analiza prijevara s bezgotovinskim instrumentima plaćanja u razdoblju od 2012. do 2016. godine u jedinstvenom europskom platnom području, utvrđeno je da su one dosegnule 1,8 milijardi eura u 2016. godini, a da je u toj godini ukupna vrijednost transakcija s platnim karticama iznosila 4,38 bilijuna eura.

[20] U 12. izdanju akcije *Global Airline Action Days* 60 zemalja, 56 zrakoplovnih kompanija i 12 mrežnih putničkih agencija na više od 200 aerodroma širom svijeta sudjelovalo je u međunarodnoj i multidisciplinarnoj operaciji u borbi protiv lažnih internetskih kupnji avionskih karata s kompromitiranim podacima o kreditnoj kartici. Tijekom te međunarodne operacije

tehnička dostignuća te se koristi za financiranje drugih kriminalnih aktivnosti ili pokretanje legalnih poslova. Kao počinitelji tih kaznenih djela pojavljuju se, osim dobro organiziranih skupina transnacionalnog organiziranog kriminaliteta, i žrtve trgovine ljudima te osobe koje se pojavljuju kao novčane mule.[21] Važan je aspekt prijevara s karticama i njihova prekogranična priroda [22] – u prekograničnim transakcijama znatno su veće stope prijevara nego u domaćim transakcijama.[23] Zbog toga se policija i pravosudna tijela suočavaju s novim izazovima u istrazi, kaznenom progonu i presuđivanju predmeta prijevara i krivotvorenja bezgotovinskih instrumenata plaćanja.[24]

usmjerene na prijevare zračnih prijevoznika prijavljeno je 165 sumnjivih transakcija. Otvorene su istrage i uhićeno je 79 osoba osumnjičenih za putovanje avionskim kartama kupljenim korištenjem ukradenih, kompromitiranih ili lažnih podataka o kreditnoj kartici. Vidjeti više: Europol 79, Arrested in worldwide crackdown on airline fraud, 27 November 2019, dostupno na: https://www.europol.europa.eu/newsroom/news/79-arrested-in-worldwide-crackdown-airline-fraud (pristup 22. ožujka 2020.).

[21] Izraz "acting as a money mule" odnosi se na osobe koje prenose novac u različite dijelove svijeta. Novčane mule primaju prihod na svoj račun; od njih se zatim traži da ih povuku na drugi račun, često u inozemstvo, zadržavajući dio novca za sebe. Vidjeti više na: https://www.europol.europa.eu/newsroom/news/228-arrests-and-over-3800-money-mules-identified-in-global-action-against-money-laundering (pristup 19. ožujka 2020.).

[22] Izvješće Europola iz 2013. otkriva da su takve istrage složene i skupe jer zahtijevaju suradnju policijskih i pravosudnih tijela iz više država te da je većina prijevara počinjena izvan EU-a, ali je utjecala na EU. Kao najboljih šest lokacija navedene su: SAD, Dominikanska Republika, Kolumbija, Ruska Federacija, Brazil i Meksiko Vidjeti više: Europol Situation Report – Payment Card Fraud in the European Union, January 2013 (dalje u tekstu: Izvješće iz 2013.), dostupno na: https://www.europol.europa.eu/publications-documents/situation-report-payment-card-fraud-in-european-union (pristup 20. ožujka 2020.).

[23] Vidjeti prikaz domaćih i prekograničnih prijevara u tablici *supra*, str. 5.

[24] Tijekom 2017. i 2018. godine poduzeto je nekoliko akcija u kojima su raskrinkani lanci transnacionalnih kriminalnih skupina koje se bave različitim vrstama prijevara s platnim karticama. Tako su u studenom 2017. godine tijekom akcije „Neptun" uhićena četiri ključna člana međunarodne kriminalne mreže odgovorna za kompromitiranje podataka o platnim karticama te ilegalne transakcije. Zajednička operacija koju su predvodile talijanske vlasti u suradnji s bugarskom i češkom policijom, a koju je podržao i Europol, kulminirala je uhićenjem vođa transnacionalne kriminalne skupine koji su aktivno nadzirali sve faze kriminalnih aktivnosti, uključujući postavljanje tehničke opreme na bankomatima u središtima europskih gradova, proizvodnju krivotvorenih kreditnih kartica i naknadno unovčavanje novca s bankomata u neeuropskim zemljama. Tijekom koordinirane akcije deseci bankomata identificirani su kao mjesta neovlaštenog postavljanja uređaja za *skimming*, poput mikrokamera i čitača magnetskih vrpca. Zaplijenjeno je više od 1000 krivotvorenih kreditnih kartica, a prikupljeni su dokazi lažnih međunarodnih transakcija u vrijednosti većoj od 50 000 eura. Drugi oblik prijevara na koje Europol u ovom izvješću upozorava jesu prijevare s naplatom cestarina. U svibnju 2018. godine španjolska nacionalna policija i civilna organizacija *Guardia* uhitile su 24 osobe tijekom međunarodne operacije u kojoj su sudjelovale Španjolska i Francuska uz potporu Europola. Organizirana kriminalna skupina bila je specijalizirana za zlouporabu korištenja pogonskog goriva i kreditnih i debitnih kartica kako bi izbjegla plaćanje cestarina te je vršila

U proteklom razdoblju od gotovo dva desetljeća na razini EU-a usvojeno je nekoliko izvješća europskih institucija koje su vršile procjenu primjene Okvirne odluke. Prva takva dva izvješća Komisije iz 2004.[25] i 2006.[26] vršila su procjenu implementacije Okvirne odluke u nacionalna zakonodavstva država članica. Pri tome je utvrđeno da je nekoliko država članica pokrenulo novo zakonodavstvo posebno osmišljeno u skladu s odredbama Okvirne odluke, dok su ostale države članice obavijestile Komisiju da je njihovo postojeće zakonodavstvo već u skladu s odredbama Okvirne odluke te stoga ne zahtijevaju zakonodavne izmjene. Na primjer u nekoliko slučajeva države članice[27] u provedbi odredaba iz Okvirne odluke u svom nacionalnom zakonodavstvu pozvale su se na općenitija već postojeća kaznena djela (npr. krađa, prijevara i sl.).[28]

prodaju tih kartica vozačima kamiona i tvrtkama za prijevoz. Policijski službenici izvršili su 21 pretragu kuća u Španjolskoj i zaplijenili 15 000 krivotvorenih praznih kartica i nekoliko čitača kartica i uređaja, uz 19 770 eura u gotovini te 4 luksuzna automobila. Raskrinkano je 11 laboratorija za izradu kartica, a smatra se da je procijenjeni gubitak veći od 500 000 eura. Pri tome počinitelji imaju različite *modus operandi* za korištenje POS-uređaja. Jedna od poznatih metoda jest manipuliranje POS-uređajem radi snimanja podataka klijenata, dok je alternativna metoda stvaranje lažnih tvrtki od strane kriminalnih skupina za registraciju POS-uređaja. Počinitelji tada koriste POS-uređaje za dobivanje podataka o karticama koje mogu sami upotrijebiti ili dalje prodavati u digitalnom podzemlju. Organizirana kriminalna skupina koristila je novu tehnologiju kako bi omogućila izmjenu elektroničkih platnih terminala za snimanje bankovnih podataka klijenata. Europol upozorava da bi se ta strategija kriminalnih skupina mogla proširiti, osobito s obzirom na to što podaci potrebni za lažnu registraciju takva terminala nisu povjerljivi, zbog čega je nabava i registracija takva uređaja pogodna za prijevaru. Tako je u provedenim istragama došlo do otkrivanja strukturirane mreže koja je distribuirala modificirane elektroničke platne terminale, a ukradeni podaci zatim su korišteni za kodiranje kartica za uporabu na Karibima. Procijenjeni je gubitak više od 338 000 eura i više od milijun eura u neuspjelim pokušajima. U listopadu 2017. uhićene su četiri osobe koje su posjedovale modificirane elektroničke platne terminale, opremu koja se koristila za umnožavanje bankovnih kartica i hrpu bankovnih kartica spremnih za kodiranje. Europol Report, Internet Organised Crime Threat Assessment (IOCTA) 2018, September 2018, str. 41-42, dostupno na: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 (pristup 20. ožujka 2020.).

[25] Report from the Commission based on Article 14 of the Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, COM(2004) 346, 30 April 2004. See also Annex II to the aforementioned report, SEC(2004) 532 (dalje u tekstu: Izvješće 2004.), dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52004DC0346&qid=1477313787667 (pristup 9. ožujka 2020.).

[26] 40 Report from the Commission: Second report based on Article 13 of the Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, COM(2006) 65, 20 February 2006. See also Annex II to the report SEC(2006) 188 (dalje u tekstu: Izvješće 2006.), dostupno na: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1477314730679&uri=CELEX:52006DC0065 (pristup 9. ožujka 2020.).

[27] Belgija, Danska, Luksemburg, Nizozemska, Poljska, Švedska. Izvješće 2006., str. 3.

[28] Italija je jedina država članica EU-a koja je u svoje nacionalno zakonodavstvo implementirala inkriminaciju prijevara protiv platnih naloga, oblika platnog instrumenta koji nije

U svom pregovaračkom stajalištu[29] za ulazak u EU Hrvatska je istaknula kako je u skladu s Okvirnom odlukom donijela nekoliko mjera za njezinu implementaciju u hrvatski pravni sustav.[30] Što se tiče kaznenopravnih sankcija, izvješća otkrivaju da su mjere koje su države članice izabrale u skladu s člankom 6. Okvirne odluke dovele do „daleko od jednoličnih" rješenja.[31]

U razdoblju od donošenja Okvirne odluke do danas utvrđeno je da prijevare s bezgotovinskim instrumentima plaćanja ne slabe, na što upozorava i Europol u svojim izvješćima. Štoviše, uz postojeće oblike prijevara kriminalne skupine bave se i različitim oblicima zlouporabe bankomata, primjerice *jackpottingom*, koji uključuje povezivanje neovlaštenog uređaja na bankomat i slanje naredbi za izdavanje kako bi počinitelj mogao podići gotovinu bez korištenja kreditne ili debitne kartice. Drugi je oblik tog kaznenog djela napad na crne kutije u bankomatima, koji zahtijeva od napadača da fizički ošteti bankomat bušenjem ili kovanjem rupe kako bi povezao svoj uređaj. Pored toga u recentnom razdoblju nastala su i kaznena djela vezana za telekomunikacije, a tiču se zlouporabe telekomunikacijskih mreža putem SIM-kartica, pri čemu počinitelj koristi tehniku višestrukih poziva po visokoj cijeni prilikom kojih određeni udio prihoda protupravno prisvaja. Drugi oblik tog kaznenog djela postoji kada počinitelj uputi poziv žrtvi jednim zvonjenjem te prekine poziv, a protupravna se radnja događa u onom trenutku kad žrtva uzvrati taj poziv. Još je jedno kazneno djelo vezano za telekomunikacije prijevara s pretplatama. U tom slučaju počinitelj, koristeći krivotvorene ili ukradene žrtvine isprave, sklapa pretplatnički ugovor s teleoperaterom za račun i na ime žrtve, a najčešći je prihod takva postupanja uređaj s ponude, koji poslije dalje prodaje. U posljednjem izvješću iz 2019. godine Europol upozorava na napade na poslovne e-adrese, pri kojima počinitelji koriste strategije socijalnog inženjeringa lažno se predstavljajući kao član osoblja tvrtke ili direktor koji može odobriti prije-

naveden na popisu u Okvirnoj odluci. Francuska, Njemačka, Italija, Švedska i Ujedinjeno Kraljevstvo posebno razlikuju krivotvorenje s jedne strane i izmjenu s druge strane u svom nacionalnom pravu. Španjolsko kazneno zakonodavstvo ne predviđa kaznu za lažno mijenjanje platnih instrumenata, već samo krivotvorenje. Izvješće 2004., str. 10.

[29] Vlada Republike Hrvatske, Pregovaračko stajalište poglavlje 24. – pravda, sloboda i sigurnost, 2008, str. 26.

[30] Vidjeti *supra,* str. 5.

[31] Kiendl Krišto, I., Council Framework Decision 2001/413 on combating fraud and counterfeiting of non-cash means of payment, European Parliamentary Research Service, 2017, str. 8. Vidjeti različite kazne po državama članicama u: Izvješće 2004., str. 13, Izvješće 2006., str. 4-5. To potvrđuje i vanjska studija pripremljena za Komisiju, gdje je utvrđeno da se primjerice minimalna kazna za krivotvorenje kreće od šest mjeseci (Njemačka) do četiri godine (Španjolska). O tome vidjeti: Reuters, T., Study on criminal sanction legislation and practice in representative Member States, Aranzadi for the European Commission, November 2013.

nos sredstava i prevariti zaposlenike unutar tvrtke. Meta takvih napada najčešće su tvrtke koje posluju *online* ili imaju strane dobavljače.[32]

Dakle promjene koje su nastupile na globalnoj razini glede načina plaćanja roba i usluga dovele su do razvoja novih oblika kriminaliteta u vezi s bezgotovinskim instrumentima plaćanja, zbog čega je bilo nužno posegnuti za uvođenjem sveobuhvatnijeg pravnog instrumenta u svrhu njihova suzbijanja. Osim toga borba protiv prijevara i krivotvorenja u vezi s bezgotovinskim instrumentima plaćanja uključena je u mjere za borbu protiv kibernetičkog kriminaliteta[33] kao jedan od tri glavna prioriteta za europsku sigurnost.[34] Osim što su prepoznate kao sigurnosna prijetnja, prijevara i krivotvorenje bezgotovinskih instrumenata plaćanja identificiraju se kao prepreka razvoju jedinstvenog digitalnog tržišta. Tako Strategija digitalnog jedinstvenog tržišta za Europu[35] napominje da prijevare s bezgotovinskim instrumentima plaćanja dovode do nepovjerenja potrošača u sigurnost mrežnih aktivnosti[36] i posljedično do ekonomskih gubitaka.

2.2. Radni dokument Europske komisije od 13. rujna 2017.

Bezgotovinska plaćanja, koja čine sve veći udio plaćanja, podliježu različitim oblicima prijevara. Želeći riješiti taj problem, u okviru Europske agende o

[32] IOCTA 2018, str. 44; Europol Report, Internet Organised Crime Threat Assessment (IOCTA) 2019, October 2019, str. 40, dostupno na: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (pristup 23. ožujka 2020.).

[33] Kibernetički kriminalitet obuhvaća prijevare na području internetskog bankarstva i prijevare na internetu s kreditnim karticama, a procjenjuje se kako je s godišnjom stopom rasta od oko 40 % i sa zaradom od oko 100 milijardi dolara riječ o najbrže rastućem sektoru globalnog organiziranog kriminaliteta. Vuković, H., Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj, National security and the future, vol. 13, br. 3, 2012, str. 20.

[34] Communication from the Commission: The European Agenda on Security, COM(2015) 185, 28 April 2015, dostupno na: https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf (pristup 10. ožujka 2020.).

[35] Communication from the Commission: A Digital Single Market Strategy for Europe, COM(2015) 192, 6 May 2015, dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:52015DC0192&from=EN (pristup 14. ožujka 2020.).

[36] U četvrtom izvješću Eurobarometra o kibernetičkoj sigurnosti navode se rezultati ankete u kojoj je sudjelovalo više od 28 000 ispitanika u 28 država članica EU-a. Tako je 42 % ispitanika iskazalo zabrinutost zbog sigurnosti internetskih transakcija, dok je u 2017. godini 11 % ispitanika iskazalo da je bilo žrtva prijevare s bankovnim karticama ili internetskim bankarstvom, što je povećanje u odnosu na 2014. (8 %) i 2013. (7 %). Više na: Special Eurobarometer 464a: Europeans' attitudes towards cyber security, dostupno na: https://data.europa.eu/euodp/en/data/dataset/S2171_87_4_464A_ENG (pristup 4. ožujka 2020.).

sigurnosti iz travnja 2015. Komisija je najavila namjeru preispitati i eventualno proširiti zakonodavstvo o borbi protiv prijevara i krivotvorenja bezgotovinskih instrumenata plaćanja. U pismu namjere predsjednika Komisije pod prioritetom br. 7 navodi se preispitivanje Okvirne odluke, odnosno prijevara s bezgotovinskim instrumentima plaćanja, među prioritetima koje treba riješiti.[37] Razlog je to što Komisija vjeruje da Okvirna odluka više ne odražava današnju stvarnost, poput korištenja virtualnih valuta i mobilnog plaćanja. Iako su se dosad preventivni napori na razini EU-a usmjerili na prijevare s karticama, razvoj novih tehnologija doveo je do novih oblika kriminaliteta, poput *skimminga* ili *pharminga*. Procjene Okvirne odluke sugeriraju da definicija instrumenta plaćanja koja je usredotočena na fizičke kreditne kartice i čekove možda nije dovoljna za pravilno rješavanje tog problema. Tako se Rezolucijom Europskog parlamenta od 23. listopada 2013.[38] o organiziranom kriminalitetu, korupciji i pranju novca zahtijeva jačanje pravosudne i policijske suradnje na europskoj i međunarodnoj razini s ciljem poboljšanja sustava za prikupljanje dokaza i omogućavanja podataka i informacija relevantnih za istragu kaznenih djela te na zajedničkoj definiciji i usklađivanju propisa koji se odnose na definiranje elektroničkog i mobilnog novca s obzirom na njihovu potencijalnu uporabu za pranje novca i financiranje terorizma.[39] Novija Rezolucija Europskog parlamenta od 3. listopada 2017. naglašava važnost usklađivanja na razini EU-a definicija kaznenih djela povezanih s napadima na informacijske sustave i potrebu da države članice postave sustave za snimanje, proizvodnju i pružanje statističkih podataka o povezanim kaznenim djelima kako bi se osigurala učinkovitija borba protiv te vrste kriminaliteta.[40]

Ocjenu postojećeg zakonodavstva Europska je komisija donijela u Radnom dokumentu 13. rujna 2017. zajedno s procjenom učinka i prijedlogom nove

[37] Letter of Intent from Commission President Juncker and First Vice-President Timmermans to the then EP President Schulz and Luxembourg Prime Minister Bettel, 9 September 2015, str. 5.

[38] European Parliament resolution of 23 October 2013 on organised crime, corruption and money laundering: recommendations on action and initiatives to be taken (final report) (2013/2107(INI)), dostupno na: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013-0444+0+DOC+PDF+V0//EN (pristup 23. ožujka 2020.).

[39] O pravnom okviru za suzbijanje pranja novca i financiranja terorizma vidjeti: Primorac, D., Miletić, N., Pilić, M., Safety and legal framework on preventing of use of the financial system for money laundering according to solutions of Directive (Eu) 2015/849, 31st International Scientific Conference on Economic and Social Development – "Legal Challenges of Modern World" – Split, 7-8 June 2018, str. 67-78.

[40] European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)), dostupno na: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0366_EN.pdf?redirect (pristup 23. ožujka 2020.).

direktive koja će zamijeniti Okvirnu odluku.[41] Radnim dokumentom primarno se utvrđuje da definicija instrumenta plaćanja nije u potpunosti relevantna s obzirom na razvoj platnih tehnologija nastalih od 2001. godine. Novi oblici platnih instrumenata, npr. mobilno plaćanje, virtualne valute, digitalni novčanici, nisu uključeni u trenutne definicije koje definiraju platni instrument kao "tjelesni", tj. fizički, dok su ostali platni instrumenti uključeni u definicije Okvirne odluke zastarjeli, npr. euro-čekovi. Također, otkriveni su nedostaci u načinu definiranja kaznenih djela. Naime utvrđeno je da Okvirna odluka ne inkriminira pripremne radnje kad one ne rezultiraju prijenosom novca ili novčanom vrijednošću. S obzirom na to da prijevara s bezgotovinskim instrumentom plaćanja uključuje dva stadija: 1) pripremni akti: prikupljanje, trgovina, stavljanje na raspolaganje, posjedovanje podataka o uplatama i 2) stvarno korištenje podataka o uplatama, Radni dokument upozorava da su pripremni akti koji prethode prijevari, a koji nisu izravno povezani s njom, isključeni iz članka 3. Okvirne odluke o kaznenim djelima koja se odnose na računala.[42]

Što se tiče učinkovitosti, Radnim dokumentom utvrđeno je da je Okvirna odluka samo djelomično ispunila svoja tri specifična cilja: 1) osigurati da prijevara i krivotvorenje bezgotovinskih instrumenata plaćanja budu prepoznati kao kaznena djela, 2) osigurati da se za ta kaznena djela primjenjuju učinkovite, proporcionalne i odvraćajuće sankcije i 3) poboljšati prekograničnu suradnju. Na prvom mjestu primjećuju se teškoće u procjeni uloge Okvirne odluke u uspostavi relevantnog nacionalnog zakonodavstva u državama članicama s obzirom na to da su odredbe Okvirne odluke u međuvremenu (od 2001. godine) dopunjene zakonodavstvom iz drugih područja, npr. financijskim, navodeći države članice da na odgovarajući način izmijene svoje zakonodavstvo. Osim toga i tehnološki razvoj koji se odnosi na bezgotovinsko plaćanje također je prouzročio izmjene zakonodavstava mnogih država članica. Radnim dokumentom utvrđeno je da Okvirna odluka nije donijela zadovoljavajući stupanj ujednačavanja sankcija u državama članicama.[43] S obzirom na razlike u kaznama u državama članicama počinitelji su u mogućnosti iskoristiti sustav tako što će svoje kriminalne aktivnosti usmjeriti na one države koje imaju blaže sankcije. Osim toga razlike u sankcijama mogu imati negativan utjecaj na pravosudnu suradnju ili primjenu odgovarajućeg zakonodavstva o europskom uhidbenom nalogu.[44]

[41] O tome vidjeti i kod: Vikolainen, V., Combating fraud and counterfeiting of non-cash means of payment, European Parliamentary Research Service, 2017., dostupno na: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2017)611031 (pristup 24. ožujka 2020.).

[42] Radni dokument, str. 213.

[43] *Ibid*, str. 232.

[44] Europski uhidbeni nalog može se izdati radi kaznenog progona tražene osobe za djelo za koje je propisana kazna zatvora u najdužem trajanju od jedne godine zatvora ili više; radi kaznenog progona tražene osobe za djelo za koje je propisana kazna zatvora ili mjera koja

Što se tiče unaprjeđenja prekogranične suradnje kao trećeg cilja, Radni dokument primjećuje važnost Okvirne odluke s obzirom na prekograničnu prirodu prijevara s platnim karticama budući da manje od 10 % transakcija čine prekogranične transakcije, a one čine više od polovice ukupnih prijevara.[45] Međutim Radnim se dokumentom utvrđuje da prekogranična priroda prijevara s karticama dovodi do komplikacija u istragama i procesuiranju, kao i do teškoća za žrtve prijevara u pristupu svojim pravima.

Tako Radni dokument bilježi nekoliko važnih dodatnih pitanja koja nisu u cijelosti ili uopće uključena u područje primjene Okvirne odluke, ali su ipak relevantna u širem kontekstu. Ona se odnose na raspodjelu nadležnosti, žrtve prijevara i nedostatak javno-privatne suradnje.[46] Posebno se bilježi problem vezan uz dodjelu nadležnosti: „Glavni rizik je da se kaznena djela ne mogu istražiti, jer nijedna zemlja ne preuzima nadležnost ili nedostatak pravosudne suradnje onemogućava postupak prekogranične istrage u praksi.“[47] Što se tiče žrtava prijevare, uočava se da Okvirna odluka ne sadrži odredbe o žrtvama i da kriminalne mreže često iskorištavaju nedostatak svijesti žrtava o činjenju prijevara. Također, Radni dokument utvrđuje da nedostatak odredbi o javno-privatnoj suradnji, tj. između tijela kaznenog progona i financijskih institucija, predstavlja prepreku učinkovitim istragama i procesuiranju. Zaključak Radnog dokumenta ogleda se u činjenici da je posljedica različitih oblika prijevara i teškoća u njihovu procesuiranju uglavnom regulatorni propust jer je Okvirna odluka djelomično zastarjela uglavnom zbog tehnološkog razvoja.[48]

III. DIREKTIVA

Kroz navedena izvješća i evaluacije vidljivo je kako je pred tijelima EU-a velik izazov pri donošenju sveobuhvatnog instrumenta kojim će se inkriminirati svi oblici prijevara s platnim karticama. U tom smjeru Komisija je 13. rujna 2017. godine na temelju članka 83. stavka 1. Ugovora o funkcioniranju EU-a (dalje u tekstu: UFEU) usvojila prijedlog Direktive. U usporedbi s Okvirnom

uključuje oduzimanje slobode u najdužem trajanju od tri godine ili više, bez provjere dvostruke kažnjivosti; kad je donesena pravomoćna presuda na kaznu zatvora u trajanju od najmanje četiri mjeseca. Vidjeti: Primorac, D., Europski uhidbeni nalog – teorija i praksa, Alfa, Zagreb, 2018, str. 44.

[45] Radni dokument, *op. cit.*, str. 219-220.

[46] U ovoj evaluaciji nalaze se i drugi instrumenti EU-a usvojeni nakon Okvirne odluke koji su relevantni u rješavanju prijevara o gotovinskom plaćanju s obzirom na to da se zakonodavni kontekst značajno promijenio od donošenja Okvirne odluke 2001. Za popis relevantnih propisa vidjeti: *ibid*, str. 5-10.

[47] *Ibid*, str. 223.

[48] Kiendl Krišto, I., *op. cit.*, str. 5-6.

odlukom prijedlog obuhvaća širu definiciju platnih instrumenata, uključujući bilo koji elektronički novac i virtualne valute. Tako Direktiva inkriminira ne samo zlouporabu nezakonito prisvojenih, krivotvorenih platnih instrumenata već, između ostalog, i njihovo krivotvorenje, posjedovanje, nabavu za upotrebu, uvoz, izvoz, prodaju, prijevoz, distribuciju, ili ako se na drugi način čine dostupnima za zlouporabu. Nadalje, predložena Direktiva definira kaznena djela protiv informacijskih sustava, poput namjernih transfera novca, novčane vrijednosti ili virtualnih valuta radi protupravne dobiti ili ometanja funkcioniranja informacijskog sustava i bespravnog uvođenja, izmjene, brisanja, prijenosa ili prikrivanja računalnih podataka.

U procesu usvajanja prijedloga i donošenja Direktive o njoj su svoja mišljenja davali odbori unutar Europskog parlamenta,[49] koji su upozorili na nedostatke iz Okvirne odluke, poput dodjele nadležnosti, uspostave mehanizama za informiranje javnosti, kao i na zahtjeve za prijavljivanje prijevara s bezgotovinskim instrumentima plaćanja. Europski gospodarski i socijalni odbor predlagao je da se izmijeni naslov Direktive zamjenjujući izraz „bezgotovinski instrument plaćanja" izrazom „elektronički i digitalni instrument plaćanja". Konačni tekst Direktive usvojen je na plenarnom zasjedanju 13. ožujka 2019. godine, a Vijeće je usvojilo Direktivu 9. travnja 2019. godine. Potpisao ju je predsjednik Europskog parlamenta i predsjednik Vijeća 17. travnja 2019. godine, a stupila je na snagu dvadeseti dan nakon dana objave u Službenom listu EU-a.[50]

Kad je riječ o novostima koje donosi Direktiva, najprije treba kazati kako se navođenjem predmeta i definicijama koje nudi Direktiva nadopunjuju i Okvirna odluka i Direktiva Europskog parlamenta i Vijeća o napadima na informacijske sustave (dalje u tekstu: Direktiva 2013/40/EU)[51] jer uključuje i klasične oblike prijevara i krivotvorenja instrumenata plaćanja u fizičkom obliku i digitalne, odnosno prijevare s bezgotovinskim instrumentima plaćanja, koji nisu u fizičkom obliku. Dakle Direktivom su ažurirana kaznena djela iz Okvirne odluke s obzirom na to da su neki instrumenti plaćanja zastarjeli, npr. euro-čekovi. Također, za razliku od Okvirne odluke Direktiva navodi minimalne i maksimalne kazne za pojedina kaznena djela fizičkih osoba. Ono što se prigovaralo Okvirnoj odluci jest i nemogućnost vođenja prekograničnih istraga jer njome one nisu bile regulirane. Direktiva je to riješila te u čl. 13. omogućuje

[49] Vidjeti u: Kaufmann, S. Y., Extension of rules on combating fraud and counterfeiting of non-cash means of payments, 2016, dostupno na: https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-combating-fraud-and-counterfeiting-of-non-cash-means-of-payments (pristup 25. ožujka 2020.).

[50] Stupila na snagu 30. svibnja 2019. godine.

[51] Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i zamjeni Okvirne odluke Vijeća 2005/222/PUP SL 218.

državama članicama da poduzmu mjere za osiguranje istražnih mjera koje će biti proporcionalne počinjenom kaznenom djelu te slanje informacija istražnim tijelima o kaznenim djelima iz Direktive. U vezi s razmjenom informacija Direktiva je ažurirala regulativu Okvirne odluke tako što propisuje da države članice osiguravaju dostupnost operativne nacionalne kontaktne točke 24 sata dnevno sedam dana u tjednu te postupovne odredbe o rješavanju hitnih zahtjeva za pomoć.

Od ostalih noviteta treba spomenuti mjere prijavljivanja kaznenih djela, gdje se potiču financijske institucije i druge pravne osobe da prijave svaku sumnju na počinjenje tih kaznenih djela te uspostavu *online*-prijava prijevara. S obzirom na prirodu kaznenih djela posebnu kategoriju čine osobe koje su pretrpjele štetu tim kaznenim djelima. Direktiva potiče države članice da osiguraju žrtvama kaznenih djela (fizičkim i pravnim osobama) konkretne informacije o zaštiti od negativnih posljedica djela te popis posebnih institucija zaduženih za potporu žrtvama. Novosti u odnosu na Okvirnu odluku jesu i odredbe o prevenciji te praćenju i statističkim podacima.[52] Prevencija bi se vršila informiranjem i podizanjem svijesti građana o tim kaznenim djelima te istraživačkim i obrazovnim programima kojima se nastoji smanjiti ukupan broj prijevara. Također, države članice prikupljaju statističke podatke o fazama prijavljivanja, istrazi i postupcima za kaznena djela iz Direktive te ih dostavljaju Komisiji svake godine, a Komisija ih objavljuje i predaje nadležnim specijaliziranim agencijama i drugim tijelima EU-a. Direktiva propisuje i da će Komisija do 31. svibnja 2023. godine Europskom parlamentu i Vijeću podnijeti izvješće kojim se procjenjuje u kojoj su mjeri države članice uskladile svoje zakonodavstvo s tom Direktivom, a do 31. svibnja 2026. godine Komisija će provesti evaluaciju učinka Direktive te izvijestiti o učinkovitosti uvođenja *online*-sustava za prijave tih kaznenih djela, kao i za pomoć i potporu žrtvama.[53]

3.1. Kaznena djela iz Direktive

Analizom inkriminacija iz Direktive uočava se da su one podijeljene u tri skupine. Prvu skupinu čine kaznena djela prijevara i krivotvorenja platnih kartica u fizičkom obliku, drugu čine prijevare i krivotvorenja platnih instrumenata koji nisu u fizičkom obliku, poput virtualnih valuta, e-novčanika i sl., a treću čine kaznena djela u vezi s informacijskim sustavima. Pri tome Direktiva razlikuje bezgotovinski instrument plaćanja u fizičkom i nefizičkom obliku. Prvo kazneno djelo iz prve skupine inkriminacija odnosi se na uporabu bezgotovinskih instrumenata plaćanja s ciljem prijevare, a koja se sastoji u uporabi

[52] Prijedlog Direktive, str. 17.
[53] Čl. 21. Direktive.

ukradenog ili na drugi način nezakonito prisvojenog ili stečenog bezgotovinskog instrumenta plaćanja s ciljem prijevare i uporabi krivotvorenog ili falsificiranog bezgotovinskog instrumenta plaćanja s ciljem prijevare. To kazneno djelo može se počiniti samo s namjerom te za njega Direktiva propisuje maksimalnu kaznu zatvora u trajanju od najmanje dvije godine. Drugo je kazneno djelo iz prve skupine ono koje je bilo propisano i Okvirnom odlukom, a odnosi se na namjerno počinjenje „a) krađe ili drugog nezakonitog prisvajanja bezgotovinskog instrumenta plaćanja koji je u fizičkom obliku, b) krivotvorenja ili falsificiranja bezgotovinskog instrumenta plaćanja koji je u fizičkom obliku s ciljem prijevare, c) posjedovanja ukradenog ili na drugi način nezakonito prisvojenog ili krivotvorenog bezgotovinskog instrumenta plaćanja koji je u fizičkom obliku radi uporabe s ciljem prijevare, kao i d) nabave za sebe ili druge, uključujući primanje, prisvajanje, kupnju, prijenos, uvoz, izvoz, prodaju, prijevoz ili distribuciju ukradenog, krivotvorenog ili falsificiranog bezgotovinskog instrumenta plaćanja koji je u fizičkom obliku radi uporabe s ciljem prijevare“. To kazneno djelo odnosi se na protupravno raspolaganje tuđim platnim karticama. Direktiva propisuje za kaznena djela iz točke a) i b) maksimalnu kaznu zatvora u trajanju od najmanje dvije godine, a za djela iz točke c) i d) maksimalnu kaznu zatvora u trajanju od najmanje jedne godine.

Novost koju Direktiva donosi jesu upravo kaznena djela iz druge skupine inkriminacija (čl. 5. Direktive) koja se odnose na prijevare s bezgotovinskim instrumentima plaćanja u nefizičkom obliku. Pri tome je Direktiva proširila definiciju pojma bezgotovinskog instrumenta plaćanja, koji predstavlja „zaštićeni uređaj, predmet ili zapis ili njihovu kombinaciju, osim zakonskih sredstava plaćanja, koji jest ili nije u fizičkom obliku, a nositelju ili korisniku omogućuje, samostalno ili u vezi s postupkom, odnosno nizom postupaka, prijenos novca ili novčane vrijednosti, među ostalim s pomoću digitalnih sredstava razmjene“.[54] Sam koncept bezgotovinskog instrumenta plaćanja u smislu postojanja tih kaznenih djela treba shvatiti tako da se njime doista može ostvariti transfer novca, novčane vrijednosti ili aktivirati platni nalog. To znači da se ne može smatrati nezakonitim stjecanje bezgotovinskog instrumenta plaćanja ako netko nezakonito prisvoji mobilnu aplikaciju za plaćanje, a pritom nema potrebnu zaporku za pristup.[55] Dakle u pogledu počinjenja tih kaznenih djela bezgotovinskim instrumentom plaćanja treba se ostvariti funkcija plaćanja. Također, za postojanje tih kaznenih djela nije od značaja o kojoj se količini novca radi. Ta kaznena djela postojat će i kad je protupravno pribavljena mala količina novca.[56] Što se

[54] Čl. 2. toč. a) Direktive.
[55] Toč. 8. Preambule Direktive.
[56] Toč. 30. Preambule Direktive.

tiče zlouporabe[57] bezgotovinskog instrumenta plaćanja, ona se sastoji u radnji počinitelja koji posjeduje bezgotovinski instrument plaćanja koji nije u fizičkom obliku da svjesno bespravno upotrijebi taj instrument za vlastitu korist ili korist druge osobe.[58] Oblici počinjenja kaznenog djela u vezi s bezgotovinskim instrumentom plaćanja u nefizičkom obliku jesu: „*a) nezakonito stjecanje bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku, barem kad je to stjecanje uključivalo počinjenje jednog od kaznenih djela iz čl. 3. do 6. Direktive 2013/40/EU,[59] ili zlouporabu bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku, b) krivotvorenje ili falsificiranje bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku s ciljem prijevare, c) držanje nezakonito stečenog, krivotvorenog ili falsificiranog bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku radi uporabe s ciljem prijevare, barem ako je u trenutku držanja instrumenta poznato njegovo nezakonito podrijetlo, d) nabava za sebe ili druge, uključujući prodajom, prijenosom i distribucijom ili stavljanje na raspolaganje nezakonito stečenog, krivotvorenog ili falsificiranog bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku radi uporabe s ciljem prijevare*.“ Za oblike tog kaznenog djela pod točkom a) i b) Direktiva propisuje maksimalnu kaznu zatvora u trajanju od najmanje dvije godine, a za oblike djela pod točkom c) i d) maksimalnu kaznu zatvora u trajanju od najmanje jedne godine.

U posljednju skupinu inkriminacija prema čl. 6. Direktive spadaju kaznena djela u vezi s prijevarama s informacijskim sustavima, i to namjerna provedba ili uzrokovanje prijenosa novca, novčane vrijednosti ili virtualnih valuta i time uzrokovanje nezakonitog gubitka imovine za drugu osobu u svrhu stjecanja nezakonite koristi za počinitelja ili nekog drugog ako je počinjeno: a) bespravnim sprječavanjem ili ometanjem funkcioniranja informacijskog sustava; b) bespravnim uvođenjem, izmjenom, brisanjem, prijenosom ili prikrivanjem računalnih podataka. Za kaznena djela u vezi s informacijskim sustavima Direktiva propisuje maksimalnu kaznu zatvora u trajanju od najmanje tri godine. Pored propisanih kaznenopravnih sankcija Direktiva zahtijeva da države članice propišu strože kazne (maksimalnu kaznu zatvora u trajanju od najmanje pet godina) ako je kazneno djelo počinjeno u okviru zločinačke organizacije, kao što je definirano u Okvirnoj odluci Vijeća o borbi protiv organiziranog kriminaliteta.[60]

[57] Razlikuje se od kaznenog djela zlouporaba čeka ili platne kartice iz čl. 239. KZ-a po tome što se kod ovog kaznenog djela radi o zlouporabi vlastite platne kartice, dok se kod kaznenog djela iz Direktive radi o zlouporabi tuđeg bezgotovinskog instrumenta plaćanja.

[58] Toč. 15. Preambule Direktive.

[59] Nezakonit pristup informacijskim sustavima (čl. 3.), nezakonito ometanje sustava (čl. 4.), nezakonito ometanje podataka (čl. 5.), nezakonito presretanje (čl. 6.).

[60] Čl. 9. st. 6. Direktive, čl. 3. Okvirne odluke Vijeća 2008/841/PUP od 24. listopada 2008. o borbi protiv organiziranog kriminaliteta SL 300/42.

Što se tiče oblika krivnje, vidljivo je da je ta kaznena djela moguće počiniti samo s namjerom jer nehajno počinjenje nekog od navedenih kaznenih djela ne bi bilo kažnjivo. U odnosu na oblik namjere, a s obzirom na prirodu tih kaznenih djela, mogli bismo reći da u većini slučajeva dolazi u obzir izravna namjera kao najteži oblik krivnje.[61] S druge strane kod tih kaznenih djela postavlja se pitanje kažnjivog pokušaja. Kad će se smatrati da je počinitelj ostao u kažnjivom pokušaju glede počinjenja kaznenog djela u vezi s prijevarom ili krivotvorenjem bezgotovinskog instrumenta plaćanja u nefizičkom obliku? Primjerice može se dogoditi da počinitelj bespravno prisvoji i pristupi tuđoj aplikaciji za plaćanje ili aktiviranje platnog naloga, ali ne uspije izvršiti transakciju zbog nedostatnih sredstava na računu žrtve. Hoće li on u tom slučaju odgovarati za pokušaj kaznenog djela zlouporabe bezgotovinskog instrumenta plaćanja u nefizičkom obliku s obzirom na to da mu je cilj prijevara ili će se zadržati na kažnjavanju za neko drugo kazneno djelo, primjerice neovlaštenog pristupa? U praksi je teško dokazati cilj, osobito ako je taj cilj ostao neuspješan. Međutim pokušaj je uvijek društveno opasno djelo i postoji uvijek i kad je izvršenje bilo pogrešno. Okolnost da je išao pogrešnim putem, ali ipak putem počinjenja kaznenog djela, znači opasnost za pravno dobro. Dakle počinitelj je htio povredu, zbog toga i odgovara za put do povrede, bio on pogrešan ili ispravan.[62] I Direktiva stoga poziva da se kao kazneno djelo regulira pokušaj kod skoro svih kaznenih djela, osobito barem pokušaj nabave nezakonito stečenog, krivotvorenog ili falsificiranog bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku za sebe ili druge s ciljem prijevare.[63]

Direktiva, kao i Okvirna odluka, propisuje odgovornost pravnih osoba za navedena kaznena djela te poziva države članice da poduzmu mjere za uspostavu kaznene odgovornosti pravnih osoba ako su ta kaznena djela počinjena u njihovu korist od strane odgovornih osoba u pravnoj osobi ili osoba koje imaju određeni položaj u pravnoj osobi, a koje su djelo počinile uslijed propusta nadzora ili kontrole od strane odgovorne osobe. Primjerice kaznena odgovornost odgovorne osobe postojala bi kad bi ona neovlašteno pristupala bankovnim računima putem internetskih aplikacija i protupravno vršila transakcije na svoj ili na račun neke druge osobe, dok bi za kaznenu odgovornost pravne osobe odgovorna osoba činila neku od radnji počinjenja djela u korist pravne osobe te joj na taj način osigurala protupravnu imovinsku korist. Također, Di-

[61] I to izravna namjera prvog stupnja – kada počinitelj ide za tim da ostvari obilježja kaznenog djela, kad mu je baš stalo do toga da počini kazneno djelo. Novoselec, P., Bojanić, I. G., Opći dio kaznenog prava, četvrto, izmijenjeno izdanje, Pravni fakultet Sveučilišta u Zagrebu, 2013, str. 241.

[62] Bačić, F., Kazneno pravo – opći dio, peto prerađeno i prošireno izdanje, Informator, Zagreb, 1998, str. 285.

[63] Čl. 8. st. 2. Direktive.

rektiva proširuje sankcije za pravne osobe u odnosu na Okvirnu odluku. Pored mjera koje su propisane Okvirnom odlukom (ukidanje prava na javne naknade ili pomoć, privremena ili trajna zabrana obavljanja poslovnih djelatnosti, stavljanje pod sudski nadzor i sudski nalog za likvidaciju) Direktiva sadrži još i privremeno isključenje iz pristupa javnom financiranju i privremeno ili trajno zatvaranje objekata koji su služili za počinjenje kaznenog djela.[64]

3.2. Implementacija Direktive u hrvatski kaznenopravni sustav

Analizom postojećeg kaznenog zakonodavstva u vezi s prijevarama s bezgotovinskim instrumentima plaćanja vidljivo je da zakonodavac ne propisuje posebno kaznena djela vezana za prijevare i krivotvorenje platnih kartica ili platnih instrumenata u nefizičkom obliku, ali sadrži neka kaznena djela koja se mogu podvesti pod kaznena djela u vezi s prijevarama i krivotvorenjem bezgotovinskih instrumenta plaćanja iz Direktive. Ta kaznena djela podijeljena su u različite glave unutar Kaznenog zakona (dalje u tesktu: KZ).[65] S obzirom na objekt kaznenopravne zaštite i cilj ta bi kaznena djela spadala u glavu imovinskih kaznenih djela. Imovina kao objekt zaštite u pogledu tih kaznenih djela dolazi u nematerijalnom obliku. Glede cilja u našem kaznenopravnom sustavu postoji nekoliko oblika prijevara (prijevara u gospodarskom poslovanju, računalna prijevara, subvencijska prijevara, izborna prijevara),[66] kao i krivotvorenja (krivotvorenje novca, računalno krivotvorenje, krivotvorenje isprava itd.) Za potrebe ovog rada posebno je karakteristična računalna prijevara, koja je regulirana u glavi kaznenih djela protiv računalnih sustava, programa i podataka. Pod računalnu prijevaru neki autori podvode i većinu pojavnih oblika prijevara s platnim karticama u nefizičkom obliku, što je i djelomično opravdano s obzirom na to da je za njihovo činjenje potreban pristup računalnim, mobilnim ili drugim sustavima.[67] Ali ono što razlikuje računalnu prijevaru od prijevare s bezgotovinskim instrumentom plaćanja u nefizičkom obliku jest funkcija plaćanja. Da bi postojalo kazneno djelo prijevare s bezgotovinskim instrumentom plaćanja, treba doći do funkcije plaćanja ili barem do njegova pokušaja, a kod računalne prijevare isti se cilj (stjecanje protupravne imovinske koristi) ostvaruje drugim radnjama počinjenja: unosom, izmjenom, brisanjem, oštećivanjem itd.

[64] Čl. 11. Direktive.

[65] Kazneni zakon (NN br. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19).

[66] O oblicima prijevara vidjeti: Sokanović, L., Orlović, A., *op. cit.*, 583-615.

[67] Tako *ibid,* str. 608-611. Vuletić, I., Nedić, T., Računalna prijevara u hrvatskom kaznenom pravu, Zbornik Pravnog fakulteta Sveučilišta u Rijeci (1991), v. 35, br. 2, 2014, str. 679-692.

Analizirajući odredbe Direktive glede kaznenih djela, možemo uočiti da kaznena djela u vezi s krađom platnih kartica (čl. 4. toč. a) Direktive) odgovaraju općem kaznenom djelu krađe iz čl. 228. KZ-a, dok primjerice krađu novca s bankomata naša sudska praksa smatra teškom krađom.[68] Nadalje, kazneno djelo krivotvorenja platne kartice (čl. 4. toč. b) Direktive) odgovara kaznenom djelu krivotvorenja isprave[69] iz čl. 278. KZ-a, koje se ogleda u izradi lažne ili preinačenju prave isprave s ciljem da se takva isprava upotrijebi kao prava. S obzirom na to da kod tog kaznenog djela nedostaje cilj koji postoji kod kaznenog djela iz čl. 4. toč. b) Direktive, a to je prijevara, naša sudska praksa stavlja u stjecaj kazneno djelo krivotvorenja isprave s kaznenim djelom prijevare (čl. 236. KZ-a). Kad je riječ o kaznenom djelu iz čl. 4. toč. c) i d) Direktive, možemo utvrditi da ono odgovara kaznenom djelu izrade, nabavljanja, posjedovanja, prodaje ili davanja na uporabu sredstava za krivotvorenje (čl. 283. KZ-a).[70] Time možemo zaključiti da je KZ već usklađen s čl. 4. Direktive.

Na sličan se način mogu svrstati kaznena djela iz čl. 5. Direktive, s tim što se tu radi o bezgotovinskim instrumentima plaćanja koji nisu u fizičkom obliku, poput virtualnog novca, internetskog bankarstva i sl. Samim time da bi došlo do počinjenja tog kaznenog djela u vidu nezakonitog stjecanja, krivotvorenja, falsificiranja, držanja nezakonito stečenog bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku ili nabavu istoga za sebe ili drugoga, počinitelj najprije mora neovlašteno pristupiti[71] takvu nefizičkom bezgotovinskom platnom instrumentu, čime čini kazneno djelo neovlaštenog pristupa iz čl. 266. KZ-a. Kako je već navedeno, to će djelo postojati samo ako je bezgotovinskim instrumentom plaćanja ostvarena funkcija plaćanja, odnosno izvršen transfer novca. Na taj bi način za dokazivanje tog kaznenog djela u vezi s uporabom bezgotovinskog instrumenta plaćanja u nefizičkom obliku s ciljem prijevare u domaćem pravnom sustavu nužno dolazilo do stjecaja kaznenih djela neovlaštenog pristupa, računalne prijevare i drugih, ovisno o radnji počinjenja. Pri

[68] *"…jer se radi o zatvorenom prostoru u kojem se nalazi novac i da bi se do njega došlo na protupravan način potrebno je savladati veću prepreku, što je ovdje bio i slučaj jer su osuđenici krivotvorili platne kartice i s neovlašteno preslikanim magnetskim zapisom na tim karticama podizali novac na bankomatima."* Presuda Vrhovnog suda RH br. III Kr 92/08-3 od 10. veljače 2009. Tako i Županijski sud u Splitu, Kž-205/08 od 20. svibnja 2008. Vidjeti u: Novoselec, P., Sudska praksa, Hrvatski ljetopis za kazneno pravo i praksu, vol. 15, broj 2/2008, Zagreb, str. 1167.

[69] Isprava je svaki predmet koji sadrži zapis, znak ili sliku koji je podoban ili određen da služi kao dokaz neke činjenice koja ima vrijednost za pravne odnose. Čl. 87. st. 15. KZ-a.

[70] Vidjeti Rješenje Vrhovnog suda RH br. II Kž 145/09-3 od 11. ožujka 2009.

[71] Škrtić navodi da bi to trebao biti svaki pristup koji nije odobrio vlasnik ili druga osoba koja je ovlaštena dati odobrenje ili svaki pristup koji je zabranjen zakonom. Škrtić, D., Kaznena djela računalnog kriminaliteta u novom kaznenom zakonu Republike Hrvatske, dostupno na: https://www.fvv.um.si/DV2012/zbornik/informacijska_varnost/skrtic.pdf (pristup 26. ožujka 2020.).

tome zakonodavac mora jasno definirati pojam bezgotovinskog instrumenta plaćanja koji se razlikuje od računalnog podatka.[72] S druge strane u usporedbi s pojmom isprave bezgotovinski instrument plaćanja jest isprava, kao što je platna kartica u fizičkom obliku također isprava, ali isprava je predmet u fizičkom obliku.[73]

Konačno, kaznenim djelima u vezi s informacijskim sustavima iz čl. 6. Direktive odgovara kazneno djelo računalne prijevare[74] (čl. 271. KZ-a), koje se sastoji u unosu, izmjeni, brisanju, oštećenju, činjenju neuporabljivim ili nedostupnim računalnih podataka ili ometanju rada računalnog sustava s ciljem protupravnog prisvajanja imovinske koristi za sebe ili drugoga.[75] Tim kaznenim djelima odgovara i kazneno djelo ometanja rada računalnog sustava (čl. 267. KZ-a), koje čini onaj tko onemogući ili oteža rad ili korištenje računalnog sustava računalnih podataka ili programa ili računalnu komunikaciju. U inkriminacije u vezi s računalnim sustavima spadaju i neka druga kaznena djela iz glave kaznenih djela protiv računalnih sustava, programa i podataka, poput kaznenog djela neovlaštenog pristupa (čl. 266. KZ-a), oštećenje računalnih podataka (čl. 268. KZ-a), neovlašteno presretanje računalnih podataka (čl. 269. KZ-a), računalno krivotvorenje (čl. 270. KZ-a), zlouporaba naprava (čl. 272. KZ-a) te teška kaznena djela protiv računalnih sustava, programa i podataka (čl. 273. KZ-a).[76] Cilj kaznenopravne zaštite jest sprječavanje stvaranja i širenja tzv. crnih tržišta naprava i instrumenata kojima se omogućava počinjenje kaznenih djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava.[77]

Dakle mogli bismo reći da je KZ u velikoj mjeri usklađen s Direktivom te da se modaliteti počinjenja kaznenih djela iz Direktive mogu podvesti pod već postojeće inkriminacije unutar KZ-a. Posebno treba uzeti u obzir da se kao počinitelji tih kaznenih djela pojavljuju posebno specijalizirane skupine organiziranog kriminaliteta, koje koriste moderne tehnologije pri činjenju tih kaznenih

[72] Računalni je podatak svako iskazivanje činjenica, informacija ili zamisli u obliku prikladnom za obradu u računalnom sustavu. Čl. 87. st. 19. KZ-a.

[73] Isprava je svaki predmet koji sadrži zapis, znak ili sliku koji je podoban ili određen da služi kao dokaz neke činjenice koja ima vrijednost za pravne odnose. Čl. 87. st. 15. KZ-a.

[74] Kazneno djelo računalne prijevare uvedeno je u kaznenopravni sustav 2004. godine. O računalnoj prijevari vidjeti i kod: Derenčinović, D., Aktualna pitanja kaznenog zakonodavstva, Inženjerski biro, Zagreb, 2004, str. 35.

[75] Vidjeti Presudu Županijskog suda u Zagrebu br. 1 Kž-90/2019-3 od 12. veljače 2019.

[76] O drugim pojavnim oblicima računalnog kriminaliteta vidjeti: Dragičević, D., Novi izazovi kibernetičkog kriminala, Hrvatska pravna revija, broj 7-8, godina V, 2005, str. 15-16; Franjić, S., Inkriminiranje nekih kaznenih djela iz područja računalnog kriminaliteta u Republici Hrvatskoj, Kriminalističke teme, Časopis za kriminalistiku, kriminologiju i sigurnosne studije, godište XII, broj 3-4, 2012, str. 243-254.

[77] Garačić, A., Značenje pojedinih izraza u Kaznenom zakonu i njihovo tumačenje u sudskoj praksi, Aktualna pitanja kaznenog zakonodavstva, Inženjerski biro, Zagreb, 2006, str. 35.

djela te gubitke koji nastaju kao njihova posljedica. Osim toga pored kaznenopravnih sankcija koje predviđa Direktiva, a koje se sastoje od zatvorskih kazni, treba imati na umu i sigurnosnu mjeru u nacionalnom zakonodavstvu u vidu zabrane pristupa internetu, koja se može izreći počinitelju koji je počinio kazneno djelo putem interneta, a za kojeg postoji opasnost da će zlouporabom interneta ponovno počiniti kazneno djelo.[78]

Glede odgovornosti pravnih osoba za ta kaznena djela u Zakonu o odgovornosti pravnih osoba za kaznena djela (dalje u tekstu: ZOPOKD)[79] uočava se da je već sad taj zakon usklađen s Direktivom. U pogledu kaznene odgovornosti pravne osobe za navedena kaznena djela Direktiva propisuje odgovornost pravne osobe za prijevare s bezgotovinskim instrumentima plaćanja i pod pojmom odgovorne osobe obuhvaća bilo koju osobu koja je u korist pravne osobe počinila kazneno djelo iz Direktive, a koja je djelovala samostalno ili kao dio tijela pravne osobe i koja ima vodeći položaj u okviru pravne osobe na temelju ovlasti za zastupanje pravne osobe; ovlasti za donošenje odluka u ime pravne osobe te ovlasti za provedbu kontrole unutar pravne osobe. Pod odgovornom se smatraju i osobe u pravnoj osobi koje imaju podređeni položaj, a koje su neko od tih djela počinile uslijed propusta nadzora ili kontrole od strane odgovorne osobe. Premda je o pitanju pojma odgovorne osobe u našem pravnom sustavu od uvođenja ZOPOKD-a 2003. godine bilo dosta prijepora u teoriji i praksi, možemo utvrditi da je pojam odgovorne osobe, a time i utvrđivanje kaznene odgovornosti pravne osobe, u skladu s Direktivom. Prema ZOPOKD-u kaznena odgovornost pravne osobe izvodi se iz odgovornosti odgovorne osobe kao fizičke osobe koja vodi poslove pravne osobe ili joj je povjereno obavljanje poslova iz područja djelovanja pravne osobe. U taj krug spadaju i osobe koje su kazneno djelo počinile uslijed propusta dužnog nadzora odgovorne osobe.[80]

Sankcije koje Direktiva propisuje za pravne osobe prema postojećem ZOPOKD-u kreću se u granicama sigurnosnih mjera i kazne ukidanja pravne osobe. Tako se pod sankciju iz Direktive koja se sastoji u ukidanju prava na javne naknade i pomoć može podvesti sigurnosna mjera zabrane poslovanja s korisnicima državnog i lokalnih proračuna (čl. 18. ZOPOKD-a) ili pak kazna ukidanja pravne osobe (čl. 12. ZOPOKD-a) kao najteža kazna. Nadalje, pod sankciju iz Direktive koja se sastoji u privremenom isključenju iz pristupa jav-

[78] Vidjeti kod: Cvitanović, L., Glavić, I., Uz problematiku sigurnosne mjere zabrane pristupa internetu, Hrvatski ljetopis za kazneno pravo i praksu, vol. 19, broj 2/2012, Zagreb, str. 914-915.

[79] Zakon o odgovornosti pravnih osoba za kaznena djela (NN br. 151/03, 110/07, 45/11, 143/12).

[80] Tako: Derenčinović, D., Zakon o odgovornosti pravnih osoba za kaznena djela s uvodnim napomenama, komentarskim bilješkama, pojmovnim kazalom i prilozima, Nocci, Zagreb, 2003, str. 31.

nom financiranju, uključujući postupke javnog nadmetanja, bespovratna sredstva i koncesije, može se podvesti sigurnosna mjera zabrane stjecanja dozvola, ovlasti, koncesija ili subvencija (čl. 17. ZOPOKD-a); pod sankciju iz Direktive koja se sastoji u privremenoj ili trajnoj zabrani obavljanja poslovnih djelatnosti može se podvesti sigurnosna mjera zabrane obavljanja određenih djelatnosti ili poslova (čl. 16. ZOPOKD-a); pod sankciju iz Direktive koja se sastoji u privremenom ili trajnom zatvaranju objekata koji su služili za počinjenje kaznenog djela može se podvesti kazna ukidanja pravne osobe (čl. 12. ZOPOKD-a). Ostale sankcije koje Direktiva predviđa jesu stavljanje pod sudski nadzor te sudski nalog za likvidaciju. Pri tome treba kazati da nije ni potrebno doslovno preuzimanje predloženih sankcija za implementaciju Direktive u naš pravni sustav, osobito zato što u velikoj mjeri za predložene sankcije već postoje kaznenopravne sankcije u ZOPOKD-u.

Kad je riječ o procesnim odredbama iz Direktive, one se sastoje u uspostavi djelotvornih istraga protiv tih kaznenih djela s obzirom na velik udio prekograničnih prijevara. Pri tome Direktiva poziva države članice da poduzmu potrebne mjere kako bi osigurale istražne alate za otkrivanje i procesuiranje tih kaznenih djela. S obzirom na prirodu tih kaznenih djela tijela kaznenog progona raspolagat će u najvećoj mjeri elektroničkim dokazima, pri čemu su digitalni podaci sveprisutni i važan izvor informacija, ali treba voditi računa da je i njima jednako lako manipulirati, pa je prilikom njihove uporabe uvijek potrebno postupati s dodatnim oprezom.[81] Premda Direktiva poziva na uspostavu teritorijalne nadležnosti država članica, prekogranična suradnja dolazi do izražaja kada počinitelj na teritoriju jedne države članice izvrši protupravnu radnju (primjerice neovlašteno pristupi aplikaciji i izvrši transfer novca), a posljedica nastupi u drugoj državi članici (primjerice za žrtvu koja živi i radi na području druge države članice). U tim slučajevima kao dokazi u kaznenom postupku mogu se koristiti različiti elektronički podaci: povijest pretraživanja, IP-adresa, e-pošta itd.[82] U svrhu pravosudne suradnje države članice trebaju imenovati kontaktne točke i obavijestiti Komisiju, Europol i Eurojust o imenovanim tijelima. Ta tijela imala bi operativni karakter u smislu uspostave postupka za rješavanje hitnih slučajeva, prikupljanja statističkih podataka o prijavama, istragama, optužnicama i presudama za ta kaznena djela. U Hrvatskoj već imamo neke inicijative usmjerene na borbu protiv svih oblika kibernetičkog kriminaliteta, u koji svakako spadaju prijevare s bezgotovinskim instrumentima plaćanja. Takva je inicijativa Ministarstva unutarnjih poslova (dalje u tekstu: MUP) za provođenje projekta koji se sastoji od opremanja ustrojstvenih jedini-

[81] Burić, Z., Prikaz konferencije: Uporaba novih tehnologija u kaznenom postupku, elektronički dokazi: valjanost i dopustivost elektroničkih dokaza u kaznenom postupku, Hrvatski ljetopis za kazneno pravo i praksu, vol. 18, broj 1/2011, Zagreb, str. 300.

[82] *Loc. cit.*

ca MUP-a potrebnim softverskim i hardverskim komponentama te edukacije policijskih službenika u radu s digitalnim dokazima i forenzičkim metodama i procedurama.[83] Važnost borbe protiv prijevara s platnim karticama potvrđuje i sam Europol, koji naglašava da je taj oblik kibernetičkog kriminaliteta jedan od prioriteta EMPACT-a[84] u okviru ciklusa politika EU-a od 2018. do 2021. Europol je sudjelovao u većini istraga koje su poduzete u vezi s tim kaznenim djelima, organizirao je tečajeve za forenziku prijevara s platnim karticama, koji uključuju ispitivanje uređaja za *skimming*, napade na bankomate i posebno napade zlonamjernog softvera. Europolova zajednička radna skupina za borbu protiv kibernetičkog kriminaliteta (J-CAT) podržala je nekoliko značajnih operacija usmjerenih na borbu protiv kibernetičkog kriminaliteta uz podršku Europskog centra za kibernetički kriminalitet Europola (EC3).[85]

Dakle može se zaključiti da je Hrvatska u velikoj mjeri već usklađena s Direktivom. Odredbe koje bi se trebale implementirati odnose se na definiranje pojma bezgotovinskog instrumenta plaćanja te uspostavu operativnih tijela za prekograničnu suradnju i provođenje djelotvornih istraga za ta kaznena djela, kao i osiguranje potpore i pomoći žrtvama. Kao i svaki pravno obvezujući akt koji se donosi na razini EU-a tako i ova Direktiva ima svoj put prenošenja u nacionalno zakonodavstvo. Rok za implementaciju Direktive jest 31. svibnja 2021. godine te o prenošenju Direktive u nacionalno zakonodavstvo države članice odmah obavještavaju Komisiju.[86] Kad bi države članice postupile suprotno i ne bi ispunile obveze iz Direktive, Komisija bi mogla pokrenuti postupak zbog povrede propisa pred Sudom EU-a.[87]

IV. UMJESTO ZAKLJUČKA

Bezgotovinski način plaćanja temeljni je oblik plaćanja roba i usluga na području EU-a. To potvrđuju i brojke, pa je u tijeku 2016. godine ukupna vrijednost transakcija s platnim karticama na području EU-a iznosila 4,38 bilijuna eura. Međutim takve su transakcije, nažalost, praćene negativnim posljedicama koje se ogledaju u različitim oblicima prijevara s platnim karticama. Prijevare s takvim oblicima instrumenata plaćanja predstavljaju 73 % ukupne vrijednosti prijevara s karticama u 2016. godini, a taj je trend u stalnom pora-

[83] Više na: https://www.svijetsigurnosti.com/mup-jaca-borbu-protiv-cyber-kriminala-raspisan-je-natjecaj-za-racunalnu-opremu-i-edukaciju-policajaca/ (pristup 26. ožujka 2020.).

[84] Engl. *European Multidisciplinary Platform Against Criminal Threats*.

[85] Vidjeti o akcijama u kojima je sudjelovao Europol *supra*, bilj. 24, str. 6-7.

[86] Čl. 20. Direktive; Direktiva se ne primjenjuje u odnosu na Ujedinjeno Kraljevstvo, Irsku i Dansku.

[87] Čl. 226. UFEU-a.

stu od 2008. godine. Te pojave predstavljaju jedan oblik kibernetičkog kriminaliteta koje su nastale kao posljedica tehnološkog razvoja i sve sofisticiranijih metoda kojima se služe kriminalne skupine pri njihovu činjenju.

Ovaj rad pisan je u vrijeme pandemije koronavirusa u Hrvatskoj i svijetu, kada financijske institucije i druge nacionalne i međunarodne organizacije pozivaju građane da u svrhu izbjegavanja socijalnih kontakata s ciljem sprječavanja širenja zaraze vrše svoja plaćanja putem internetskog bankarstva.[88] Međutim kriminalne su se skupine već brzo prilagodile i iskorištavaju tu situaciju za različite oblike kaznenih djela prijevara s bezgotovinskim instrumentima plaćanja, osobito onih u nefizičkom obliku. Tako Europol upozorava da je broj kibernetičkih napada već značajan i očekuje se daljnji porast. Kibernetički će kriminalci nastaviti s inovacijama u uvođenju različitih zlonamjernih softvera tematiziranih oko pandemije koronavirusa, a uz to mogu proširiti svoje aktivnosti i na druge vrste internetskih napada. Na meti takvih postupanja već su se našle tvrtke koje su htjele kupiti zaštitne maske i drugu zaštitnu opremu. Istraga jedne države članice usredotočena je na prijenos 6,6 milijuna eura od jedne tvrtke do druge u Singapur za kupovinu alkoholnih gelova i maski, pri kojoj transakciji roba nikada nije primljena. U drugom slučaju koji je prijavila druga država članica tvrtka je pokušala kupiti 3 milijuna maski i izgubila 300 000 eura. Slične prijevare za opskrbu traženih proizvoda izvijestile su i druge države članice.[89] Dakle moderni oblici kaznenih djela prijevara i krivotvorenja bezgotovinskih instrumenata plaćanja događaju se svakodnevno i pogađaju sve sfere društva. Stoga je vrlo važno da države članice EU-a do navedenog roka iz Direktive implementiraju u svoja nacionalna zakonodavstva nove inkriminacije kojima će se osigurati kaznenopravna zaštita takvih transakcija. U odnosu na Hrvatsku možemo zaključiti da je postojeći kaznenopravni okvir već u skladu s Direktivom glede kaznenih djela koja propisuje Direktiva na način da u nedostatku doslovnih inkriminacija iz Direktive naša sudska praksa rješava stavljanjem u stjecaj postojećih inkriminacija (krađa, krivotvorenje isprave, prijevara i dr.), čime se ostvaruju radnje pojedinih kaznenih djela iz Direktive. U odnosu na Hrvatsku implementacija bi se odnosila na definiranje pojma bezgotovinskog instrumenta plaćanja u nefizičkom obliku te uspostavu operativnih tijela za prekograničnu suradnju i provođenje djelotvornih istraga za ta kaznena djela, kao i osiguranje potpore i pomoći žrtvama.

[88] Vidjeti i COVID-19 – Cybersecurity Awareness, dostupno na: https://www.association-secure-transactions.eu/covid-19-cybersecurity-awarenesss/ (pristup 27. ožujka 2020.).

[89] Europol, Pandemic profiteering how criminals exploit the COVID-19 crisis, March 2020, dostupno na: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis (pristup 29. ožujka 2020.).

LITERATURA

1. Bačić, F., Kazneno pravo opći dio, peto prerađeno i prošireno izdanje, Informator, Zagreb, 1998.
2. Burić, Z., Prikaz konferencije: Uporaba novih tehnologija u kaznenom postupku, elektronički dokazi: valjanost i dopustivost elektroničkih dokaza u kaznenom postupku, Hrvatski ljetopis za kazneno pravo i praksu, vol. 18, broj 1/2011, Zagreb.
3. Clough, J., Principles of Cybercrime, Second Edition, Cambridge University Press, 2015.
4. Commission Communication: Commission Work Programme 2016: No time for business as usual, COM(2015) 610, 27 October 2015.
5. Cvitanović, L., Glavić, I., Uz problematiku sigurnosne mjere zabrane pristupa internetu, Hrvatski ljetopis za kazneno pravo i praksu, vol. 19, broj 2/2012, Zagreb.
6. Derenčinović, D., Zakon o odgovornosti pravnih osoba za kaznena djela s uvodnim napomenama, komentarskim bilješkama, pojmovnim kazalom i prilozima, Nocci, Zagreb, 2003.
7. Derenčinović, D., Aktualna pitanja kaznenog zakonodavstva, Inženjerski biro, Zagreb, 2004.
8. Dragičević, D., Novi izazovi kibernetičkog kriminala, Hrvatska pravna revija, broj 7-8, godina V, 2005.
9. Franjić, S., Inkriminiranje nekih kaznenih djela iz područja računalnog kriminaliteta u Republici Hrvatskoj, Kriminalističke teme, Časopis za kriminalistiku, kriminologiju i sigurnosne studije, godište XII, broj 3-4, 2012.
10. Garačić, A., Značenje pojedinih izraza u Kaznenom zakonu i njihovo tumačenje u sudskoj praksi, Aktualna pitanja kaznenog zakonodavstva, Inženjerski biro, Zagreb, 2006.
11. Kaufmann, S. Y., Extension of rules on combating fraud and counterfeiting of non-cash means of payments, 2016, dostupno na: https://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-combating-fraud-and-counterfeiting-of-non-cash-means-of-payments.
12. Kiendl Krišto, I., Council Framework Decision 2001/413 on combating fraud and counterfeiting of non-cash means of payment, European Parliamentary Research Service, 2017.
13. Novoselec, P., Sudska praksa, Hrvatski ljetopis za kazneno pravo i praksu, vol. 15, broj 2/2008, Zagreb.
14. Novoselec, P., Bojanić, I., Opći dio kaznenog prava, četvrto, izmijenjeno izdanje, Pravni fakultet Sveučilišta u Zagrebu, 2013.
15. Primorac, D., Europski uhidbeni nalog – teorija i praksa, Alfa, Zagreb, 2018.
16. Primorac, D., Miletić, N., Pilić, M., Safety and legal framework on preventing of use of the financial system for money laundering according to solutions of Directive (EU) 2015/849, 31st International Scientific Conference on Economic and Social Development – "Legal Challenges of Modern World" – Split, 7-8 June 2018.
17. Reuters, T., Study on criminal sanction legislation and practice in representative Member States, Aranzadi for the European Commission, November 2013.
18. Sokanović, L., Orlović, A., Oblici prijevara u kaznenom zakonu, Hrvatski ljetopis za kazneno pravo i praksu, vol. 24, broj 2/2017, Zagreb.
19. Vikolainen, V., Combating fraud and counterfeiting of non-cash means of payment, European Parliamentary Research Service, 2017, dostupno na: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2017)611031.
20. Vuletić, I., Nedić, T., Računalna prijevara u hrvatskom kaznenom pravu, Zbornik Pravnog fakulteta Sveučilišta u Rijeci (1991), v. 35, br. 2, 2014.

21. Škrtić, D., Kaznena djela računalnog kriminaliteta u novom kaznenom zakonu Republike Hrvatske, dostupno na: https://www.fvv.um.si/DV2012/zbornik/informacijska_varnost/skrtic.pdf.
22. Vuković, H., Kibernetska sigurnost i sustav borbe protiv kibernetskih prijetnji u Republici Hrvatskoj, National security and the future, vol. 13, br. 3, 2012.

Summary

MODERN FORMS OF FRAUD AND COUNTERFEITING OF NON-CASH PAYMENT INSTRUMENTS UNDER DIRECTIVE 2019/713/EU

With the dynamic social changes that are taking place and the development of modern methods of payment for goods and services, various instruments of non-cash payment have emerged, especially those in a non-physical form. Payment card transactions are the most widespread form of payment in the European Union, so they are often the target of criminal groups that illegally misappropriate substantial amounts of money through fraud and counterfeiting. Ensuring the criminal protection of property in the form of an intangible legal good with regard to fraudulent forms of handling non-cash means of payment is a challenge for both the legislator and the case law. On the other hand, this is also a necessity given the losses that occur. In this paper, the author analyses the recent Directive of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA. The Directive entered into force on 30 May 2019, and its implementation in Croatian criminal law should follow by 31 May 2021. Therefore, the paper presents the basic assumptions on which the Directive is based, along with an analysis of new forms of criminal offences related to non-cash payment instruments and their implementation in Croatian criminal legislation.

Keywords: fraud, electronic money, counterfeiting, implementation, computer fraud, cybercrime