

INSTITUT ZA UPOREDNO PRAVO
INSTITUTE OF COMPARATIVE LAW
INSTITUT ZA KRIMINOLOŠKA I SOCIOLOŠKA ISTRAŽIVANJA
INSTITUTE OF CRIMINOLOGICAL AND SOCIOLOGICAL RESEARCH
PRAVOSUDNA AKADEMIJA
JUDICIAL ACADEMY

VII MEĐUNARODNI NAUČNI SKUP
VII International Scientific Thematic Conference

DIGITALIZACIJA U KAZNENOM PRAVU I PRAVOSUĐU

Digitalization in Penal Law and Judiciary

Urednici/Editors:

Jelena Kostić
Marina Matić Bošković

Tematski zbornik radova međunarodnog značaja
Thematic Conference Proceedings of International Significance



BEOGRAD, novembar 2022.
BELGRADE, november 2022

VII MEĐUNARODNI NAUČNI SKUP
DIGITALIZACIJA U KAZNENOM PRAVU I PRAVOSUĐU

VII International Scientific Thematic Conference
Digitalization in Penal Law and Judiciary

Izdavač/Publisher:

Institut za uporedno pravo
(Institute of Comparative Law)
Institut za kriminološka i sociološka istraživanja
(Institute of Criminological and Sociological Research)

Za izdavača / For the Publisher:

Prof. dr Vladimir Čolović
Dr Ivana Stevanović

Recenzenti/Reviewers:

Prof. dr Ioana Vasii (Romania)

Dr Jovan Ćirić (Serbia)

Prof. dr Dražen Cerović (Montenegro)

Naučni odbor / Scientific Committee:

Prof. dr Ana Lucia Valvo (Italia)	Prof. dr Sun Wanhui (China)
Doc. dr Ana Đanić Čeko (Croatia)	Prof. dr Piotr Mikuli (Poland)
Prof. dr Anita Rodina (Latvia)	Prof. dr Gordana Gasmi (Serbia)
Prof. dr Ondrej Blažo (Slovakia)	Dr Ana Čović (Serbia)
Prof. dr Sándor Madai (Hungary)	Dr Miloš Stanić (Serbia)
Prof. dr Jurij Pudovočkih (Russia)	Doc. dr Hana Kovacikova (Slovakia)

Organizacioni odbor / Organizing Committee:

Prof. dr Vladimir Čolović, Institut za uporedno pravo (Institute of Comparative Law, Belgrade, Serbia);
dr Ivana Stevanović, Institut za kriminološka i sociološka istraživanja (Institute of Criminological and Sociological Research, Belgrade, Serbia); Nenad Vujić, Pravosudna akademija (Judicial Academy, Belgrade, Serbia); dr Jelena Kostić, Institut za uporedno pravo (Institute of Comparative Law, Belgrade, Serbia); Aleksandar Stevanović MA, Institut za kriminološka i sociološka istraživanja (Institute of Criminological and Sociological Research, Belgrade, Serbia); dr Marina Matić Bošković, Institut za kriminološka i sociološka istraživanja (Institute of Criminological and Sociological Research, Belgrade, Serbia); Aleksandra Višekruna, MA, Institut za uporedno pravo (Institute of Comparative Law, Belgrade, Serbia)

Radni jezici konferencije / Official Languages:

engleski i srpski / English and Serbian

Priprema za štampu / Prepress:

Branimir Trošić

Štampa / Printed by:

„Tri O d.o.o.“, Arandelovac

Tiraž/Copies:

200

ISBN 978-86-80186-92-4 (IUP)

ISBN 978-86-80756-52-3 (IKSI)

DOI: https://doi.org/10.56461/ZR_22.DUKPP

Zbornik je nastao kao rezultat naučnoistraživačkog rada Instituta za uporedno pravo koji finansira Ministarstvo prosvete, nauke i tehnološkog razvoja RS prema Ugovoru o realizaciji i finansiranju naučnoistraživačkog rada NIO u 2022. godini (evidencioni broj 451-03-68/2022-14/200049).

This Collection of Papers was created as a result of the scientific research work of the Institute of Comparative Law, funded by the Ministry of Education, Science and Technological Development of the Republic of Serbia under the Contract on the Realization and Financing of Scientific Research work of SRO in 2022 (record number 451-03-68/2022-14/200049).

FALSIFIKOVANJE I ZLOUPOTREBA BEZGOTOVINSKIH INSTRUMENATA PLAĆANJA I EVROPSKI STANDARDI

Zoran Pavlović*

Opšta društvena digitalizacija i dinamične promene življenja, uz sve veću upotrebu i rasprostranjenost „pametnih“ telefona, sa mnogim različitim sadržajima koje nude, dovode do pojave novih relacija između banaka, kupaca i prodavaca, koje se odnose na savremena poslovanja sa platnim karticama. Plaćanja se obavljaju, nezavisno od toga da li se radi o tradicionalnom ili on line poslovanju, a savremeno bankarstvo je u stalnoj potrazi za što optimalnijim načinom plaćanja uz korišćenje novih tehnoloških i komunikacionih rešenja. Transakcije platnim karticama su česta meta za izvršenje krivičnih dela, što nije izazov samo za zakonodavca da postavi pravni okvir zaštite, već i za organe otkrivanja i judikaturu. Evropski standardi koji se formulišu nastoje da odgovore na te izazove, što zahteva i implementaciju u domaće zakonodavstvo. Direktiva Evropskog parlamenta i Saveta 2019/713/EU o borbi protiv prevara i falsifikovanja u vezi s bezgotovinskim sredstvima plaćanja upravo pruža osnov za zaštitu bezgotovinskih instrumenata plaćanja, u skladu sa zahtevima koji se postavljaju u vezi sa plaćanjima danas i kaznenopravnom reakcijom u domaćem zakonodavstvu.

KLJUČNE REČI: platne kartice, rizik plaćanja, informatički kriminalitet.

* Doktor pravnih nauka, redovni profesor Pravnog fakulteta Univerziteta Privredna akademija u Novom Sadu, Professor et dr h. c. Univerziteta u Pečuju, Mađarska. E-mail: zoran.pav@hotmail.com

UVOD

Savremene modele platnih usluga danas nemoguće je zamisliti bez platnih kartica, bilo kontaktnih ili bezkontaktnih, koje su danas skoro u potpunosti potisnule upotrebu gotovog novca i/ili čekova. Iako je prvi elektronski transfer novca telegrafom *via Western Union* zabeležen još 1860. godine, još dugo nakon toga je upotreba platnih kartica pripadala sferi naučne fantastike i tehnoloških predviđanja. Na Ruzveltovoj predsedničkoj fotografiji u Beloj kući iz 1933. vidi se i naslov knjige E. Belamija iz 1888. godine „Pogled unazad“ (Immerwahr, 2021). To je priča o čoveku koji je zaspao 1887. i probudio se 2000. u elektrificiranom gradu, uz muzičke emisije, u društvu gde se više ne koristi gotov novac već - kreditne kartice! U Sjedinjenim Državama 19. veka Belamijev utopijski roman Pogled unazad bio je posle Čiča Tomine kolibe najprodavanija knjiga u prvim godinama izdanja.¹

Ipak, nešto manje od veka trebalo je da prođe od 1888. da bi se bezgotovinski način plaćanja roba i usluga kao rezultat tehnološkog i digitalnog razvoja utvrdio kao oblik plaćanja. Futurističku ideju oživeo je Franc McNamara stvaranjem Diners kluba kao instrument plaćanja za poslovne ljude, sa Corporate Card kojom bi mogli brzo da prikažu svoj finansijski kredibilitet (Pavlović, 2006: 164).

Platne usluge izvršene platnim karticama danas su u EU najrašireniji oblik platnih usluga. I upravo zbog toga su kao takve vrlo često izazov i meta mnogim pojedincima i organizovanim kriminalnim grupama, koji kroz falsifikovanje i zloupotrebe ovih sredstava plaćanja ostvaraju veliku protivpravnu imovinsku korist. Komad plastike na kome se nalazi sredstvo za identifikaciju u obliku potpisa ili slike postao je tako izuzetno često sredstvo falsifikovanja. Od *skimminga* ili kopiranja podataka sa magnetne trake bankarske kartice, koji se kopiraju najčešće na bankarskim automatima, preko zloupotrebe POS (*point of sales terminals*) aparata putem manipulacija i falsifikovanja istih, do krađe identiteta. Naime, *phishing* se sa sve širom primenom globalnog virtuelnog autoputa - Interneta sa preuzimanjem ličnih podataka i slanjem prevarnih e-mailova pretvorio u profitabilan posao za mnoge izvršioce IKT krivičnih dela. Putem *pharminga*, odnosno zloupotrebom internet domena (umesto google.com postavlja se na primer google.org kao lažna stranica) žrtva se preusmerava na lažnu *web* stranicu, gde se onda vrši preuzimanje novca kroz lažnu transakciju (Clough: 2015).

U bankarskom sektoru Srbije se pojavljuju ovakve zloupotrebe, pa je Narodna banka Srbije identifikovala lažnu internet stranicu pod nazivom DinaKartica - Srbija, na kojoj se traži ostavljanje podataka i preduzela mere radi sprečavanja prevarne aktivnosti i otkrivanje počinitelaca krivičnog dela. Narodna banka Srbije je saopštila da se stranica lažne kartice nalazi na adresi: www.dinakartica.com i da koristi ime i logo sistema DinaCard. Na lažnoj stranici od korisnika Dina kartica, u sklopu promotivne akcije,

¹ <https://www.nytimes.com/1988/01/17/books/looking-back-at-looking-backward-we-have-seen-the-future-and-it-didn-t-work.html>, [21.10.2022.].

<https://archive.nytimes.com/www.nytimes.com/books/00/12/24/bookend/bookend.html>, [21.10.2022.].

zahteva se da ostave podatke s platne kartice.² Ovo je bila dvostruka zloupotreba oglašene stranice, imajući u vidu da se radi o prikupljanju podataka o platnoj kartici ali i ličnih podataka, ugrožavajući i ljudsko pravo na privatnost.

Prevare sa internet bankarstvom, kreditnim (platnim) karticama i krađom identiteta su se dodatno počele usavršavati zbog sve šire upotrebe sigurnijih kreditnih kartica sa čipom. Dakle, radi se o krivičnim delima zloupotrebe i falsifikovanja platnih kartica kod plaćanja gde u stvari nije potrebno ni prikazati karticu u njenom fizičkom obliku.³

Sve ovo uslovalo je u okvirima Evropske unije stalno jačanje pravnog okvira unapređenja mera za sprečavanje ovih vrsta zloupotreba. Prvi korak u zaštiti platnih usluga bila je Okvirna odluka Saveta 2001/413/PUP o borbi protiv prevara i falsifikovanja bezgotovinskih sredstava plaćanja.⁴ Kao takva Direktiva je bila na određeni način sa svojim rešenjima implementirana i u nacionalno zakonodavstvo Srbije jer je i ranijim krivičnim zakonom RS imala neka krivična dela koja su odgovarala onima propisanim u Okvirnoj odluci (Pavlović, 2006). Od tada do danas došlo je do mnogih promena u stvarnom životu i načinima plaćanja robe i usluga. Kupovina preko interneta, mobilni novčanici, kriptovalute, elektronski novac i druga visokotehnološka dostignuća doprinela su prekograničnom širenju zabranjenih radnji sa bezgotovinskim sredstvima plaćanja, što višestruko povećava izazove u otkrivanju, dokazivanju, gonjenju, nadležnostima ali i presuđivanju kod zloupotreba i falsifikovanja bezgotovinskih instrumenata i oblika plaćanja.

Funkcionalna zajednica digitalnog društva nije moguća bez sveobuhvatnijeg pravnog instrumenta koji bi služio prvo prevenciji, a onda i represiji u odnosu na krivična dela prevare, zloupotrebe i falsifikovanja bezgotovinskih instrumenata plaćanja. Sam naslov rada ima za cilj da odredi predmet analize, ali ne i da se ograniči na jedno krivično delo i krivičnopravnu zaštitu bezgotovinskih oblika plaćanja, već da analizom relevantnih evropskih standarda, ponudi temu za razgovor o unapređenju pravne zaštite.

Ali, krenimo redom.

1. JEDAN PRIMER I NEKOLIKO PITANJA

Tokom avgusta 2018.godine su pred američkim pravosuđem optužena trojica ukrajinskih državljana, kao članovi hakerske grupe FIN7 (Carbanak ili Cobalt). U optužnici je navedeno da je grupa FIN7 ukrala više od 15 miliona brojeva platnih kartica sa više od 6000 POS (point-of-sale) terminala, na više od 3600 lokacija. Optuženi su zarađivali od prodaje podataka o platnim karticama na Dark Webu. Optužbe su se odnosile na krivična dela izvršena protiv američkih kompanija, ali je grupa jednako hakovala i kompanije u Velikoj Britaniji, Australiji i Francuskoj.

² <https://www.euronews.rs/biznis/biznis-vesti/42178/narodna-banka-srbije-upozorila-gradane-na-prevaru-sa-laznim-dina-karticama-ne-ostavljajte-licne-podatke/vest>, [2.10.2022.].

³ <https://what-europe-does-for-me.eu/>, [2.10.2022.].

⁴ <https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32001F0413>.

Svi napadi bi započinjali tako što su hakeri slali *spear* fišing emailove svojim ciljevima. Emailovi su navodno slali legitimni poslovni partneri ili saradnici a oni su sadržali priloge sa malicioznim softverom. Grupa je bila veoma kreativna, a posebno kada su bili u pitanju *spear* fišing emailovi. Na primer, grupa je često ciljala službe za podršku korisnicima kako bi upala u veće korporacije. Često su pozivali i tvrdili da imaju problema sa određenom uslugom ili proizvodom, a kasnije bi emailom slali maliciozni dokument predstavniku podrške za korisnike, tvrdeći da dokument sadrži detalje o problemu.

Kada bi hakeri dobili pristup sistemima, a posebno sistemima banaka, izabrali bi jedan od tri načina na koji su krali novac. Prvi je podrazumevao koordinaciju sa grupama pomagača (*money mule*), izbacivanje novca iz bankomata u unapred određenom satu i danu. Pomagači bi pokupili novac, i pošto bi uzeli svoj deo, ostatak novca je završavao u rukama članova grupe FIN7. Drugi način je podrazumevao da grupa prebacuje novac sa legitimnih računa na svoje račune ili račune pomagača, koji bi onda ispraznili račune na bankomatima ili koristili račune za kupovinu skupih proizvoda i pranje novca. Treće, izvršioci krivičnih dela bi koristili pristup internoj mreži banke kako bi veštački uvećali saldo na računima koje bi pre toga otvorili pomagači, bez prenosa sredstava sa drugih računa. Mule bi kasnije ispraznile ove veštački napunjene račune. Nešto od “zarađenog” novca, grupa je prala preko kriptovaluta ali su koristili i pripejd kartice povezane sa novčanicima kriptovaluta, kojima su kupovali robu kao što su luksuzni automobili, umetnički predmeti ili kuće.⁵

Ovako opisana aktivnost transnacionalne organizovane kriminalne grupe, koja je radila u izvornom sastavu od 2013. do 2018. godine (a prema izveštajima EUROPOLa te aktivnosti traju i dalje, sa drugim izvršiocima), pokazuju da se razvija novi oblik kriminaliteta u vezi sa bezgotovinskim instrumentima plaćanja, što uključuje i mere za borbu protiv IT kriminaliteta, bez čega nema ni nacionalne ni evropske bezbednosti. Osim kao bezbednosna sajber pretnja na kritičnu infrastrukturu, ova krivična dela predstavljaju branu razvoju digitalnog tržišta. To vodi jačanju nepoverenja korisnika u bezbednost bezgotovinskih instrumenata plaćanja, što posledično vodi padu prometa i gubicima.⁶

Samo pravovremenom reakcijom na ovakve zabranjene radnje, dobrim zakonodavnim okvirom i prekograničnom saradnjom moći će se ovakve posledice smanjivati ili svesti na minimum. Rešenja iz Okvirne odluke nisu dala odgovor na pitanja vezana za nadležnost, mehanizam za informisanje javnosti i zahteve za prijavljivanje prevara sa bezgotovinskim instrumentima plaćanja. Sve ovo, motivisalo je Evropski parlament i Savet za donošenje nove Direktive 2019.godine.

⁵ <https://www.informacija.rs/Sajber-hronika/SAD-optuzile-clanove-grupe-Carbanak-za-kradju-15-miliona-kreditnih-kartica.html>, [22.10.2022.].

⁶ <https://www.europol.europa.eu/media-press/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain>, [22.10.2022.].

2. DIREKTIVA 2019/713/EU

2.1. Opšte karakteristike

Direktiva dopunjava Okvirnu odluku i Direktivu EP i Saveta (2013/40/EU), jer ranija rešenja precizira, uključujući pored klasičnih oblika falsifikovanja i prevara u vezi sa instrumentima plaćanja sada i digitalne falsifikate i prevare, sredstava koja nisu u fizičkom obliku. Neki krivična dela su zastarela, kao što su ona u vezi sa euro-čecovima. Predviđa se prekogranična saradnja, kazne za fizička lica koja izvrše krivična dela određena su sa minimumom i maksimumom, predviđa se *on line* razmena informacija između država, ali i *on line* prijava prevara ove vrste. Posebna zaštita predviđena je za žrtve ovih krivičnih dela u odnosu na negativne posledice i drugo. Direktiva predviđa da će Komisija do 31. maja 2023. EP i Savetu podneti izveštaj o nacionalnim usklađenostima zakonodavstava sa Direktivom, a za još 3 godine i izveštaj o uspostavljanju *on line* sistema za prijave krivičnih dela i za pomoć i podršku žrtvama.

2.2. Krivična dela iz Direktive

Krivična dela su u Direktivi podeljena u tri grupe. U prvoj su krivična dela prevara i falsifikovanja platnih kartica u fizičkom obliku, drugu čine krivična dela istih koji nisu u fizičkom obliku, kao što su virtuelne valute, e-novčanici i sl., a treću čine krivična dela koja su u vezi sa informatičkim sistemima. Sama Direktiva vrši razlikovanje bezgotovinskih instrumenata plaćanja u fizičkom i nefizičkom obliku.

Prvo krivično delo iz prve grupe inkriminacija odnosi se na prevarnu upotrebu bezgotovinskih instrumenata plaćanja, a koja se sastoji u upotrebi ukradenog ili na drugi način nezakonito prisvojenog ili stečenog bezgotovinskog instrumenta plaćanja s ciljem prevare i upotrebi lažnog ili falsifikovanog bezgotovinskog instrumenta plaćanja u cilju prevare. To krivično delo može se izvršiti samo sa umišljajem, i za njega Direktiva propisuje maksimalnu kaznu zatvora u trajanju od najmanje dve godine. Drugo krivično delo odnosi se na izvršenje „a) krađe ili drugog nezakonitog prisvajanja bezgotovinskog instrumenta plaćanja koji je u fizičkom obliku, b) pravljenja lažnog ili falsifikovanog bezgotovinskog instrumenta plaćanja koji je u fizičkom obliku u cilju prevare, c) posedovanja ukradenog ili na drugi način nezakonito prisvojenog ili napravljenog bezgotovinskog instrumenta plaćanja koji je u fizičkom obliku radi upotrebe u cilju prevare, kao i d) pribavljanje za sebe ili druge, uključujući primanje, prisvajanje, kupovinu, prenos, uvoz, izvoz, prodaju, prevoz ili distribuciju ukradenog, lažnog ili falsifikovanog bezgotovinskog instrumenta plaćanja koji je u fizičkom obliku radi upotrebe u cilju prevare“. To krivično delo odnosi se na protivpravno raspolaganje tuđim platnim karticama. Direktiva za krivična dela iz tačke a) i b) maksimalnu kaznu zatvora u trajanju od najmanje dve godine, a za radnje iz tačke c) i d) maksimalnu kaznu zatvora u trajanju od najmanje jedne godine.

Krivična dela iz druge grupe inkriminacija (čl. 5. Direktive) odnose se na prevare s bezgotovinskim instrumentima plaćanja u nefizičkom obliku. Pri tome je Direktiva odredila definiciju bezgotovinskog instrumenta plaćanja, kao „zaštićeni uređaj, predmet ili zapis ili njihovu kombinaciju, osim zakonskih sredstava plaćanja, koji može ali i ne mora biti u fizičkom obliku, a koji korisniku omogućava, samostalno ili u vezi s postupkom, odnosno nizom postupaka, transfer novca ili ekvivalentne vrednosti, uključujući i digitalna sredstva razmene“.

Sam pojam bezgotovinskog instrumenta plaćanja u kontekstu ovih krivičnih dela podrazumeva mogućnost stvarnog transfera novca, novčane vrednosti ili aktivirati platni nalog. To znači da se ne može smatrati nezakonitim samo nezakonito prisvajanje mobilne aplikacije za plaćanje, ako se nema adekvatna šifra za pristup.

U odnosu na izvršenja ovih krivičnih dela bezgotovinskim instrumentom plaćanja treba da se ostvari funkcija plaćanja. Također, za postojanje tih krivičnih dela nije relevantno o kojoj se količini novca radi.

Oblici izvršenja krivičnog dela u vezi sa bezgotovinskim instrumentom plaćanja u nefizičkom obliku jesu: „a) nezakonito sticanje bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku, ili zloupotrebu bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku, b) pravljenje ili falsifikovanje bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku u svrhu prevare, c) držanje nezakonito stečenog, napravljenog ili falsifikovanog bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku radi upotrebe u svrhu prevare, bar ako je u trenutku držanja instrumenta poznato njegovo nezakonito poreklo, d) nabavljanje za sebe ili druge, uključujući prodaju, prenos i distribuciju ili stavljanje na raspolaganje nezakonito stečenog, napravljenog ili falsifikovanog bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku radi upotrebe u cilju prevare.“ Za oblike tog krivičnog dela pod a) i b) Direktiva normira maksimalnu kaznu zatvora u trajanju od najmanje dvije godine, a za oblike izvršenja pod c) i d) maksimalnu kaznu zatvora u trajanju od najmanje jedne godine.

U treću grupu inkriminacija prema čl. 6. Direktive ulaze krivična dela u vezi s prevarama sa ifnormatičkim sistemima, i to umišljajni prenos ili prouzrokovanje prenosa novca, novčane vrednosti ili kriptovaluta i time uzrokovanje nezakonitog gubitka imovine za drugoga u cilju sticanja nezakonite koristi za izvršioca ili nekog drugog ako je izvršeno: a) neovlašćenim sprečavanjem ili ometanjem funkcionisanja informatičkog sistema; b) neovlašćenim uvođenjem, izmenom, brisanjem, prenosom ili prikrivanjem računarski podataka. Za ova krivična dela Direktiva propisuje maksimalnu kaznu zatvora u trajanju od najmanje tri godine. Pored propisanih krivičnopravnih sankcija Direktiva zahteva da države članice propišu strože kazne (maksimalnu kaznu zatvora u trajanju od najmanje pet godina) ako je krivično delo izvršeno u okviru organizovane kriminalne grupe, a prema definiciji Okvirne odluke Saveta o borbi protiv organizovanog kriminaliteta.

Što se tiče oblika krivice, jasno je da se ova krivična dela mogu izvršiti isključivo sa umišljajem, i to direktnim umišljajem. Ali, pitanje za kažnjavanje za pokušaj je ovde stvar za diskusiju (Jovašević, 2021: 57). Kada će se smatrati da je izvršilac ostao u kažnjivom pokušaju kod krivičnih dela u vezi sa prevaram ili pravljenjem bezgotovinskog instrumenta

plaćanja u nefizičkom obliku? Šta raditi ako izvršilac neovlašćeno pristupi aplikaciji drugog lica za plaćanje ili aktiviranje platnog naloga, ali ne izvrši transakciju jer na računu žrtve nije bilo sredstava. Hoće li on u tom slučaju odgovarati za pokušaj krivičnog dela zloupotrebe bezgotovinskog instrumenta plaćanja u nefizičkom obliku ili će se zadržati na kažnjavanju za neko drugo krivično delo, npr. Neovlašćeni pristup?

U praksi je teško dokazati cilj – umišljajno postupanje, naročito u slučaju ako se krivično delo nije realizovalo. Ali, pokušaj je društveno opasno delo i uvek bi u ovakvim slučajevima trebalo imati u vidu da postoji opasnost ugrožavanja za pravno dobro. Izvršilac je želeo da dođe do protivpravne imovinske koristi, pa treba i da odgovara za put do povrede, bio on pogrešan ili ispravan.

Direktiva preporučuje da se pokušaj inkriminiše kao takav i bude kažnjiv kod skoro svih krivičnih dela a naročito pokušaj prbavljanja nezakonito stečenog, napravljenog ili falsifikovanog bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku za sebe ili druge s ciljem prevare. Direktiva predviđa i odgovornost pravnih lica za navedena krivična dela, i daje preporuku državama da preduzmu mere za uspostavljanje krivične odgovornosti u skladu sa opštim pravilima o tome.

3. BEZGOTOVINSKI OBLICI PLAĆANJA I MOGUĆE ZLOUPOTREBE LJUDSKIH PRAVA

Neposredno nakon donošenja Direktive 2019/713/EU došlo je do globalne epidemije izazvane virusom SARS-Cov-2 COVID19, koji je svoje posledice ostavio i na bezgotovinska (nefizička) plaćanja u EU. Koristeći se korona merama od početka 2020. povećan je broj učesnika u bezgotovinskim oblicima plaćanja, uz moto da plaćanje karticama ili smartphoneom nije samo brže, nego je i higijenski prihvatljivije. Ovakva preporuka bila je data ne samo u državama EU, već se mogla videti i kao preporuka Narodne banke Srbije.⁷ U kontekstu rešenja iz same Direktive, želimo da ukažemo ne samo na povećanje bezgotovinskih oblika plaćanja i zloupotreba, već i na moguće kršenje ljudskih prava u kontekstu ovih krivičnih dela, o čemu je reč i u samim rešenjima iz Direktive.

Tako je prema podacima Centralne banke Nemačke do povećanog obima plaćanja platnim karticama došlo od 2018. godine, a naročito od početka pandemije. U 2021. godini maloprodajni objekti su 56% prometa ostvarili preko bezgotovinskog plaćanja, čime je Nemačka negdje u sredini lestvice. U Luksemburgu, Francuskoj ili Estoniji ljudi češće plaćaju karticom. Na samom vrhu lestvice su skandinavske zemlje. Tamo mnogi hoteli, trgovački centri i drugi uopšte ne žele prihvatiti plaćanje novčanicama. U Švedskoj 82% ljudi u međuvremenu plaća bezgotovinski. U celoj EU se elektronsko plaćanje „reklamira” kao siguran i brz način plaćanja, odnosno kao „higijenska mjera”.⁸

⁷ https://www.rtv.rs/sr_lat/ekonomija/aktuelno/nbs-savetuje-gradjanima-da-koriste-bezgotovinsko-placanje_1103241.html, [22.10.2022.].

⁸ <https://www.dw.com/hr/korona-ubrzala-smrt-gotovinskog-pla%C4%87anja/a-56144847>, DW 21-7-2021, [22.10.2022.].

Pandemija je pokazala građanima ali i donosiocima odluka koliko je bezgotovinsko plaćanje praktično, pa je Evropska Komisija digitalizaciju i bezgotovinski način plaćanja proglasila vrhovnim prioritetima – odmah nakon zaštite klime.

Ono što Direktiva 2019/713/EU ukazuje u vezi krivičnopravne reakcije na zloupotrebe bezgotovinskih plaćanja može da ima i još jednu dimenziju, koja se tiče oblasti ljudskih prava, i to u sferi zaštite podataka o ličnosti ili prava na slobodu kretanja. Ovo se naročito odnosi na plaćanja uz pomoć smartphona, odnosno u onim situacijama kada se tokom procesa plaćanja mora na tastaturi upisati i PIN. To je slučaj pre svega kod takozvane NFC-komunikacije. Ta tehnika se koristi uglavnom kod beskontaktnog plaćanja manjih iznosa. Mnoge benzinske stanice ili diskonti su opremljeni takvim uređajima za plaćanje karticama bez kontakta, odnosno NFC-čitačima. A da bi se i mobilni aparati povezali sa uređajem potrebno je instalirati jednu aplikaciju. Koliko je taj način plaćanja u međuvremenu značajan, može se dobro videti u Holandiji. Tamo je NFC-plaćanje popularno, a od 2019 tako se obavlja najveći broj transakcija, više i od gotovinskog plaćanja, odnosno klasičnog plaćanja putem kartice.

To nije potpuno neproblematično, ali ni posebno obrađeno Direktivom, jer mobilni uređaji nisu u potpunosti zaštićeni od napada hakera. Ljudi koji tako kupuju stvari, ujedno i otkrivaju gde su – kupovali. A te podatke o lokaciji kupovine neke aplikacije evaluiraju i pohranjuju, iz bezbednosnih razloga. Kuda sve to vodi? I bez unošenja ličnih podataka na ovaj način se vrši prikupljanje podataka o kretanju lica koje je izvršilo plaćanje, kao i gde se nalazi. Koliko se ovim vrši ugrožavanja prava iz Evropske konvencije o ljudskim pravima?! U SAD-u Google već sada ima pristup velikom broju podataka kreditnih kartica i s njima može ciljano upravljati reklamama za trgovce na licu mesta, može ih analizirati, vršiti ponude vlasnicima računa i skuplje prodavati određene proizvode ili usluge. Ali, ovo bi već bila tema nekog drugog rada, sa drugačijim krivičnopravnim rešenjima koja nas kao izazov tek očekuju.

4. REŠENJA U KRIVIČNOM PRAVU SRBIJE U VEZI SA FALSIFIKOVANJEM I ZLOUPOTREBOM BEZGOTOVINSKIH OBLIKA PLAĆANJA

Analizom pozitivnog krivičnog zakonodavstva u vezi sa falsifikovanjem i zloupotrebom bezgotovinskih instrumenata plaćanja jasno je da je zakonodavac propisao posebno krivično delo protiv privrede vezano za zloupotrebe platnih kartica (član 243. KZ), ali i druga krivična dela koja se mogu podvesti pod krivična dela u vezi sa prevarama i falsifikovanjem bezgotovinskih instrumenta plaćanja iz Direktive. Ta krivična dela podeljena su u različite glave Krivičnog zakonika (dalje u tekstu: KZ). Imajući u vidu objekt krivičnopravne zaštite i cilj ta bi krivična dela mogla da budu u posebnoj glavi krivičnih dela. U ovom radu nećemo posebno izdvajati ni jedno krivično delo a u vezi odredbi Direktive, kako bi to možda bilo kod tradicionalnih naučnih radova napisano, imajući u vidu obim rada, ali i množinu krivičnih dela u našem krivičnom zakoniku, već ćemo dati isključivo opšti osvrt.

Imovina kao objekt zaštite u pogledu tih krivičnih dela dolazi u nematerijalnom obliku. Istovremeno, mogla bi isto tako i da budu u grupi krivičnih dela protiv privrede. U vezi umišljaja u našem krivičnopravnom sistemu postoji nekoliko oblika prevara (u privrednom poslovanju, računarska prevara, subvencijska, izborna...), kao i falsifikovanje (falsifikovanje novca, računarsko, falsifikovanje isprava itd.) Za potrebe ovog rada treba dakle posebno označiti i krivična dela protiv bezbednosti računarskih podataka. Ali ono što razlikuje računarsku prevaru od prevare sa bezgotovinskim instrumentom plaćanja u nefizičkom obliku jeste funkcija plaćanja. Da bi postojalo krivično delo prevare sa bezgotovinskim instrumentom plaćanja, treba doći do funkcije plaćanja ili bar do pokušaja, a kod računarske prevare isti se cilj (sticanje protivpravne imovinske koristi) ostvaruje drugim radnjama izvršenja: unosom, izmenom, brisanjem, oštećenjem itd.

Analizom Glave Direktive u vezi sa krivičnim delima, možemo konstatovati da je naš Krivični zakonik već usklađen sa članom 4- 6 Direktive i da se modaliteti izvršenja krivičnih dela iz Direktive mogu podvesti pod već postojeće inkriminacije u okviru Krivičnog zakonika (Stojanović, 2021).⁹ Ali, za razliku od Direktive koja vrlo precizno ovu problematiku obrađuje na jednom mestu, jasno je da se u našem krivičnom zakonodavstvu ona nalazi na različitim mestima i zaštitnim objektima. Posebno treba imati u vidu da se kao izvršioci ovih krivičnih dela pojavljuju i pojedinci, ali i posebno organizovane kriminalne grupe, koje koristeći moderne tehnologije pri izvršenju tih krivičnih dela i ne moraju da pojedinačno znaju jedni za druge, i da vrše radnje koje su kao takve inkriminisane. Pored zatvorskih kazni već predviđenih u našem zakonu, čini se da bi se moglo pronaći prostora i za uvođenje nove mere bezbednosti u vezi sa ovim krivičnim delima, kada je ono izvršeno putem internet, odnosno meru bezbednosti zabrane pristupa internetu ukoli postoji opasnost da bi se novom zloupotrebom intereneta moglo ponovo izvršiti krivično delo.

Dakle, u odnosu na odredbe krivičnog materijalnog prava, standardi utanovljeni Direktivom mogu da se grupišu u navedene tri grupe zaštitnog objekta (krivična dela protiv imovine, krivična dela protiv privrede i protiv računarskih podataka), ali povrede ovih prava u vezi sa bezgotovinskim sredstvima plaćanja i nekim od posledica mogu da se štite i drugim krivičnim delima. Tako bi bilo sa krivičnim delima protiv sloboda i prava čoveka i građanina, gde je krivično delo neovlašćeno prikupljanje ličnih podataka iz čl.146., jer to delo može da bude posledica zloupotrebe bezgotovinskih sredstava plaćanja, kao i kod krivičnih delima protiv pravnog saobraćaja, gde je krivično delo falizifikovanja isprave iz člana 355. i drugo.

Množina krivičnih dela kojima se štite bezgotovinski oblici plaćanja, zahtevaju u odnosu na rešenja u materijalnom krivičnom zakonodavstvu diskusiju o njihovom mogućem prekomponovanju u posebnu glavu u KZ, uz neophodno usklađivanje Zakona o platnim uslugama koji je donet 2018.godine, dakle pre Direktive, gde bi se određene blanketne odredbe trebale svakako nalaziti.

Uvažavajući ipak obim rada, ovde nećemo iznositi analize pojedinih krivičnih dela, već smo samo ukazali na neophodnost pravljenja sistema zaštite kod bezgotovinskih oblika plaćanja (uključujući i platne kartice), gde je KZ samo jedan od delova te zaštite.

⁹ Prečišćeni tekst KZ naveden kao deo Komentara sadrži u sebi stanje zakonodavstva sa 1.12.2019.,gde se nalaze krivična dela predviđena Direktivom.

Slično je i sa krivičnom odgovornošću pravnih lica, gde samo možemo da konstatujemo usklađenost Zakona sa odredbama Direktive. Ono što ovde želimo da naglasimo, jeste da što se tiče usklađenosti kaznenih odredbi i standarda iz Direktive za krivičnim pravom Srbije nije neophodno njihovo doslovno preuzimanje, jer u najvećoj meri sankcije za nabrojane zabranjene radnje iz Direktive već postoje sankcije u krivičnom zakoniku.

U odnosu na procesne odredbe Direktive koje se odnose na delotvorne (čitaj efikasne) istrage protiv sve tri grupe krivičnih dela iz nje, a naročito imajući u vidu da ova krivična dela nemaju samo nacionalni, već i prekogranični značaj i posledice, Direktiva opominje da se preduzmu potrebne mere radi što bržeg otkrivanja i procesuiranja ovih krivičnih dela. Činjenica je da je u najvećem reč o elektronskim dokazima, pri čemu su digitalni zapisi izuzetno važni u tom kontekstu, ali i da je sa njima izuzetno jednostavno manipulisti.

Iako sama Direktiva poziva nacionalna zakonodavstva na krivičnopravnu reakciju, upravo transnacionalni oblik izvršenja i posledica krivičnih dela protiv bezgotovinskih sredstava plaćanja ukazuje na prekograničnu situaciju i saradnju.

U navedenom primeru sa tri optužena jasno je da su izvršioci iz više različitih država izvršavali protivpravne radnje: neovlašćeni pristupi aplikacijama bili su u jednoj državi, transfer novca u drugoj, a posledice su nastupale nezavisno od toga na teritoriji potpuno treće države. U takvim situacijama koriste se različiti elektronski dokazi, od IP adrese, istorije pretraživanja, elektronske pošte i drugo.

Stoga bez pravosudne i policijske saradnje ne može biti ni preventivnog ni represivnog rada u cilju pružanja operativne i svake druge podrške. U Srbiji već postje posebne jedinice koje se bave u okviru tužilačke organizacije ili MUP-a borbom protiv visokotehnološkog kriminaliteta, gde bi ulazila i krivična dela gde se zloupotrebljavaju bezgotovinski instrumenti plaćanja.

Da bi imali zadovoljavajuće rezultate, a u okviru stvarne a ne samo deklaratorne implementacije odredbi analizirane Direktive, neopho je da nadležne organizacione jedinice MUP-a i tužilaštva budu opremljeni sa softverskim i hardverskim komponentama i da budu dovoljno edukovani u radu sa digitalnim dokazima i forenzičkim metodama i procedurama.

Važnost borbe protiv zloupotreba u ovoj oblasti navela nas je da izvršimo uvid i u programe edukacije nosilaca pravosudnih funkcija u cilju potpune implementacije odredbi Direktive, pa smo ostali uskraćeni za odgovor o vrsti i količini znanja koju sudije i tužioci imaju u ovoj oblasti, jer bi obuka trebala da bude permanentna i da obuhvati sve tužioce i sudije koji se bave ovom materijom. Reč je o kontinuiranoj edukaciji, a ne o projektnoj inicijativi, i na sajtu NBS nije pronađena ni jedna edukacija sa pravosuđem u vezi primene ove Direktive.

Ali, kako smo već više puta naveli, Republika Srbija jeste u najvećoj meri uskladi-la svoje zakonodavstvo sa odredbama Direktive. Odredbe koje bi trebalo poboljšati tiču se dakle eventualnog redefinisavanja mesta određenih krivičnih dela u sistematici KZ, uspostavljanja operativnih tela ne samo na nivou policije već i tužilaštava i sudova za sprovođenje delotvornih istraga za ova krivična dela, i poslednje ali ne i najmanje važno, da se obezbedi podrška i pomoć žrtvama ovih krivičnih dela. Jer, to nije samo u odnosu na žrtvu obligacioni odnos između oštećenog i banke, već je i stvar javnog interesa.

ZAKLJUČAK

Ubrzani procesi korišćenja „novih“ platnih usluga u poslednje vreme su ipak imali i svoj „bum“, koji se povezuje za globalnom epidemijom izazvanom virusom COVID-19, što je učvrstilo primat bezgotovinskog oblika plaćanja kao osnovnog u plaćanjima i roba i usluga u svim zemljama EU i van nje. Ali, takve transakcije su često praćene negativnim posledicama kroz različite oblike prevara sa platnim karticama. Zloupotrebe bezgotovinskih sredstava plaćanja su u uzlaznoj liniji od trenutka stalnog povećanja izdatih platnih kartica koje su u upotrebi, dakle od 2008. godine. Prevare ovog tipa predstavljaju oblik informatičkog kriminaliteta koji je rezultat tehnološkog razvoja i sve različitijih metoda kojima se služe kriminalne grupe pri njihovom izvršenju, bez obzira na državne granice i jurisdikcije. Kriminalne grupe su se brzo prilagodile i koriste situaciju za različite oblike krivičnih dela zloupotreba sa bezgotovinskim, nefizičkim instrumentima plaćanja.

Europol¹⁰ upozorava da će IT kriminalci pratiti stanje na tržištu i razvoju platnih usluga, kroz uvođenje različitih softvera u cilju internetskih napada. Savremeni oblici krivičnih dela zloupotreba i falsifikovanja bezgotovinskih instrumenata plaćanja događaju se svakodnevno i pogađaju sve sfere društva. Zato je važno da zemlje članice EU-a, ali i zemlje kandidati kao i zemlje koje pripadaju evropskoj pravnoj tradiciji zaista implementiraju u svoja domaća zakonodavstva nove inkriminacije kojima će se realizovati zaštita takvih transakcija.

U odnosu na Srbiju možemo zaključiti da je postojeći krivičnopravni okvir već u skladu sa Direktivom u vezi krivičnih dela koja inkriminiše Direktiva na način da u nedostatku bukvalnih rešenja i inkriminacija za svaku situaciju iz Direktive se koristimo postojećim inkriminacijama (krađa, falsifikovanje isprave, prevara i dr.), čime se ostvaruju radnje pojedinih krivičnih dela iz Direktive. Međutim, u odnosu na zaštitu podataka o ličnosti, neovlašćenom prikupljanju podataka i drugo, što može da bude posledica izvršenja krivičnih dela u vezi sa bezgotovinskim sredstvima plaćanja, u ovom trenutku još uvek nemamo dovoljnu društvenu reakciju nadležnih institucija.

Implementacija bi se najprvo odnosila na uspostavljanje operativnih tela za prekograničnu saradnju i vođenje delotvornih istraga za ta krivična dela, kao i obezbeđivanje podrške i pomoći žrtvama. Ni jednog trenutka ne smemo izgubiti iz vida prava oštećenog iliti žrtve, i da u konkretnom slučaju nikako ne može biti izgubljeno iz vida, zbog koga se zaista krivični postupak vodi! Usklađenost domaćeg zakonodavstva i odredbi Direktive ne znači samo postojanje inkriminacija u nacionalnom kaznenom zakonodavstvu u celini, već i čitav niz drugih mera i aktivnosti kako bi se one i primenjivale, uz eventualno uvođenje i nekih novih mera bezbednosti u krivičnom pravu. Pod drugim aktivnostima se pre svega misli na stalnu edukaciju profesionalaca, usvajanje novih znanja i praksi u radu relevantnih činilaca, kao i neophodnu specijalizaciju. Samo bi se na taj način došlo do zadatka definisanog kao stvaranje funkcionalne zajednice digitalnog društva uz adekvatan pravni mehanizam koji bi služio i prevenciji, represiji i zaštiti oštećenih u odnosu na krivična dela prevare, zloupotrebe i falsifikovanja bezgotovinskih instrumenata plaćanja, usklađenih sa evropskim standardima.

¹⁰ V.sajt European Multidisciplinary Platform v.Criminal Threats, <https://www.cepol.europa.eu/training-education/european-multidisciplinary-platform-against-criminal-threats>, [22.10.2022.].

LITERATURA

1. Clough, J. (2015) *Principles of Cybercrime* 2nd Ed. Cambridge University Press.
2. Immerwahr, D. (2021) *Opinions, Guest essay - New York Times*, 2 juli 2021.
3. Jovašević, D. (2021) *Krivično pravo*, opšti deo, 5. izmenjeno i dopunjeno izdanje, Beograd: Dosije.
4. Pavlović, Z. (2006) „Krivičnopravna zaštita platnih kartica“, XLIII Savetovanje Udruženja za krivično pravo i kriminologiju SCG, Zlatibor-Beograd, u: *Nova rešenja u krivičnom zakonodavstvu i dosadašnja iskustva u njihovoj primeni*, (Bejatović, S. (ur.)), Beograd: Udruženje za krivično pravo i kriminologiju SCG i Inter-mex, 164-171.
5. Stojanović, Z. (2021) *Komentar Krivičnog zakonika*, 9. izmenjeno i dopunjeno izdanje, Beograd: Službeni glasnik.

Internet izvori

1. <https://www.nytimes.com/1988/01/17/books/looking-back-at-looking-backward-we-have-seen-the-future-and-it-didn-t-work.html>, [21.10.2022.].
2. <https://archive.nytimes.com/www.nytimes.com/books/00/12/24/bookend/bookend.html>, [21.10.2022.].
3. <https://www.euronews.rs/biznis/biznis-vesti/42178/narodna-banka-srbije-upozorila-gradane-na-prevaru-sa-laznim-dina-karticama-ne-ostavljate-licne-podatke/vest>, [2.10.2022.].
4. <https://what-europe-does-for-me.eu/>, [2.10.2022.].
5. <https://www.informacija.rs/Sajber-hronika/SAD-optuzile-clanove-grupe-Carbanak-za-kradju-15-miliona-kreditnih-kartica.html>, [22.10.2022.].
6. <https://www.europol.europa.eu/media-press/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain>, [22.10.2022.].
7. https://www.rtv.rs/sr_lat/ekonomija/aktuelno/nbs-savetuje-gradjanima-da-koriste-bezgotovinsko-placanje_1103241.html, [22.10.2022.].
8. <https://www.dw.com/hr/korona-ubrzala-smrt-gotovinskog-pla%C4%87anja/a-56144847> DW 21-7- 2021, [22.10.2022.].
9. <https://www.cepol.europa.eu/training-education/european-multidisciplinary-platform-against-criminal-threats>, [22.10.2022.].

FALSIFICATION AND ABUSE OF NON-CASH PAYMENT INSTRUMENTS AND EUROPEAN STANDARDS

General social digitization and dynamic lifestyle changes, with the increasing use and spread of “smart” phones, with many different contents they offer, lead to the emergence of new relationships between banks, buyers and sellers, which relate to modern business with payment cards. Payments are made, regardless of whether it is a traditional or online business, and modern banking is constantly searching for the most optimal way of payment with the use of new technological and communication solutions. Payment card transactions are a frequent target for the commission of criminal acts, which is not only a challenge for the legislator to set up a legal framework for protection, but also for detection authorities and jurisprudence. The European standards that are being formulated try to respond to these challenges, which also requires implementation into domestic legislation. Directive 2019/713/EU of the European Parliament and the Council on the fight against fraud and counterfeiting in connection with cashless means of payment precisely provides the basis for the protection of cashless payment instruments, in accordance with the requirements set in connection with payments today and the criminal law reaction in domestic legislation.

KEYWORDS: *payment cards, payment risk, IT crime.*

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

343.533::004(082)
343:004.7(082)

МЕЂУНАРОДНИ научни скуп дигитализација у казненом праву и правосуђу (7 ; 2022 ; Београд)

Tematski zbornik radova međunarodnog značaja / VII međunarodni naučni skup digitalizacija u kaznenom pravu i pravosuđu, Beograd, novembar 2022. = Thematic Conference Proceedings of International Significance / VII International Scientific Thematic Conference Digitalization in Penal Law and Judiciary, Belgrade, november 2022 ; urednici, editors Jelena Kostić, Marina Matić Bošković. - Beograd : Institut za uporedno pravo : Institut za kriminološka i sociološka istraživanja = Institute of Comparative Law : Institute of Criminological and Sociological Research, 2022 (Arandelovac : Tri O). - X, 404 str. ; 24 cm

Tiraž 200. - Reč urednika = A Word from the Editors: str. VII-X. - Napomene i bibliografske reference uz tekst. - Bibliografija uz svaki rad. - [Rezimei ; abstracts].

ISBN 978-86-80186-92-4 (IUP)

ISBN 978-86-80756-52-3 (IKSI)

а) Рачунарска технологија -- Злоупотреба -- Зборници б) Кривично право -- Дигиталне технологије -- Зборници

COBISS.SR-ID 84081161