Др Дарко Димовски,[*]
Ванредни професор,
Правни факултет Универзитета у Нишу

ПРЕГЛЕДНИ НАУЧНИ РАД
10.5937/zrpfn0-32144

UDK: 343.85
Рад примљен: 07.05.2021.
Рад прихваћен: 07.07.2021.

ПРЕВЕНЦИЈА КРИМИНАЛИТЕТА ПУТЕМ ДИГИТАЛИЗАЦИЈЕ[**]

***Апстракт*:** *Уобичајене мере превенције не дају очекиване резултате. Стога аутор полази од тога да треба размислити о могућностима коришћења достигнућа савременог света у превенцији криминалитета. Једна од тих могућности јесте дигитализација. Аутор сматра да постоје четири правца у којима је могуће посматрати утицај дигитализације на превенцију криминалитета: 1. дигитализација валута, 2. дигитализација идентитета и потписа, 3. употреба паметних уређаја и 4. употреба мобилних апликација. У наставку рада аутор образлаже сваки од наведених праваца уз навођење начина превенције криминалитета.*

***Кључне речи*:** *криминалитет, превенција, дигитализација.*

---

[*] darko@prafak.ni.ac.rs

[**] Рад је реализован у оквиру пројекта бр. 451-03-9/2021-14/200120, Министарства за просвету, науку и технолошки развој Републике Србије.
[**] Рад је саопштен на међународној научној конференцији „Право и дигитализација“, која је одржана 23-24. априла 2021. године на Правном факултету Универзитета у Нишу.

1. Увод

Мере кривичноправне репресије у Републици Србији не дају адекватне резултате, јер је стопа рецидивизма код пунолетних лица 65%, док је код малолетних лица 17%. Међутим, у погледу стопе рецидивизма малолетних лица треба бити нарочито опрезан, јер због кратког трајања малолетства, а дугог трајања кривичних поступака, ствара се привид да је стопа повратa код малолетника знатно мања, без обзира на ситуацију да примарни малолетни делинквент учини кривично дело после напуњених 18 година живота. Када би се оваква лица ипак сматрала малолетницима, стопа рецидивизма малолетних лица би износила између 80 и 85% (аутор, 2015: 141). На основу наведеног можемо закључити да мере репресије не дају адекватне резултате, те је неопходно фокусирати се на мере превенције.

Иако се мере превенције могу поделити на различите категорије, попут поделе на опште, посебне и индивидуалне или примарне, секундарне и терцијарне, посебна пажња биће посвећена општим, односно примарним мерама превенције. Тако се под општом превенцијом подразумева свеукупност друштвених активности социјалног, економског, здравственог, образовног, културног, идејног и другог карактера, којима се утиче на отклањање или ублажавање општих друштвених криминогених фактора вршења кривичних дела (Лазаревић, 1988: 8). Слично одређење као и општа превенција има примарна област. Наиме, примарна област је превентивни део криминалне политике који идентификује физичке и друштвене услове чијим постојањем долази до стварања услова за вршење кривичних дела, како би се успешно борила против њиховог вршења (Lab, 2010: 27).

Један од услова који доводи до отклањања или ублажавања општих друштвених криминогених фактора вршења кривичних дела јесте дигитализација. Наиме, према Gartner-овом речнику под дигитализацијом се подразумева употреба дигиталних технологија за промену пословног модела и пружање нових могућности за стварање прихода и вредности.[1] Са разлогом се поставља питање како се путем дигитализације може утицати на превенцију криминалитета. Сматрамо да се могу одредити четири правца у којима ће постојати утицај дигитализације на превенцију криминалитета: 1. дигитализација валута, 2. дигитализација идентитета и потписа, 3. употреба паметних уређаја и 4. употреба мобилних апликација.

1 Према:https://www.gartner.com/en/information-technology/glossary/digitalization, преузето 21. 12. 2020.

2. Дигитализација валута као основ превенције криминалитета

Дигитализација новца има потенцијал да промени традиционалну структуру финансијског система. Иако поједини стручњаци за монетарну политику, попут професора Петера Бофингера (Peter Bofinger), сматрају да се под дигитализацијом новца могу подвести замена готовине електронским новцем, замена традиционалних банкарских депозита и новчаница криптовалутама, замена банкарских депозита депозитима централне банке за све („универзалне резерве“) и замена банкарског кредитирања равноправним позајмљивањем на основу дигиталних платформи, ми ћемо се у раду осврнути само на прво значење дигитализације новца.[2]

Наиме, највећи помаци у погледу дигитализације новца направљени су у погледу замене готовине електронским новцем. Како бисмо могли да анализирамо утицај дигиталног новца на смањење стопе криминалитета, неопходно је одредити његов појам. Тако се под дигиталним новцем сматра облик новца који је доступан само у електронском или дигиталном облику, а не у физичком облику. Као синоними за дигитални новац могу се употребљавати термини попут дигитална валута, електронски новац, електронска валута или сајбер готовина.[3]

Уколико бисмо анализирали удео дигиталног новца у државама евро зоне можемо рећи да је удео готовине у новчаној маси од 1980. године до данас опао са 23% на 14%. Ипак, са друге стране истраживање Хенка Еселинка (Henk Esselink) и Лоле Хернандез (Lola Hernández), спроведено током 2016. године, показало је да удео готовине у земљама евро зоне и даље веома велики и износи 79% од свих трансакција, што чини 54% од укупне вредности свих трансакција. Употреба кредитних картица се налази на другом месту са уделом од 19%, што представља 39% од укупне вредности свих трансакција. Анализа начина плаћања у појединим државама евро зоне открива различит удео употребе кредитних картица, односно дигиталног новца. У јужним држава евро зоне је највећа употреба готовине – око 80% свих трансакција. Исти је случај и са Немачком. Са друге стране готовина се најмање користи у државама попут Холандије, Финске и Естоније – између 45% и 54%. На основу представљених резултата можемо закључити да, иако је било очекивано да се у земљама евро зоне више користи дигитални новац за плаћање, још увек је знатно већа распрострањеност готовине у укупном плаћању. Објашњење треба тражити у чињеници да се две трећине трансакција и даље врши у износу

2 Према:https://voxeu.org/article/digitalisation-money-and-future-monetary-policy, преузето 24. 12. 2020.

3 Према:https://www.investopedia.com/terms/d/digital-currency.asp, преузето 24. 12. 2020.

до 15 евра за свакодневне потребе код којих се користи готовина. Мања употреба дигиталног новца се делимично може објаснити тиме да просечан грађанин евро зоне у појединим државама је уверења да инфраструктура за употребу дигиталног новца још није развијена у потпуности. За потребе рада је битно напоменути постојање навике код грађана евро зоне да готовину и даље држе код својих кућа као вид неког осигурања (Esselink, Hernández, 2017: 4–5), што утиче на повећање ризика да буду жртве кривичних дела имовинског карактера са применом насиља у појединим случајевима.

Уколико бисмо дигитализацију новца применили као основ за превенцију криминалитета битно је напоменути да стручњаци из области политике сузбијања криминалитета наводе да је употреба готовине заслужна за извршење бројних кривичних дела попут фалсификовања новца, пљачке, разбојништва, утаје пореза, корупције и финансирања тероризма. На основу тога навели бисмо најпростији пример у виду разбојништва или разбојничке пљачке. Наиме, ова кривична дела се не врше како би извршилац кривичног дела набавио хлеб или неку другу намирницу из продавнице, већ како би узели новац из касе. У случају веће употребе дигиталног новца, извршиоци ових кривичних дела не би имали шта да украду или би корист била мала, а ризик велики. Примењујући теорију развијену од стране Герија Бекера (Gary Becker) можемо истаћи да се људска бића не придржавају увек закона којима је држава поставила ограничења у погледу понашања прописујући шта се сматра делинквентним понашањем. Упркос постојању могућности да буду санкционисани за своје понашање, појединци врше кривична дела, јер, како је то Бекер истакао у својој књизи Crime and Punishment: An Economic Approach из 1968. године, појединци се делинквентно понашају уколико очекивана корист премашује корист коју би могли добити коришћењем свог времена и других ресурса у легалним активностима (van Velthoven, van Wijck, 2016: 8).

Према проценама Канцеларије Уједињених нација за дрогу и криминал (The United Nations Office on Drugs and Crime – UNODC) глобално тржиште психоактивних супстанци вреди 322 милијарде америчких долара (United Nations Office on Drugs and Crime, 2005: 143), док тржиште фалсификовања производа, како је то у свом извештају истакла Организација за економску сарадњу и развој (Organisation for Economic Co-operation and Development – OECD), вреди 250 милијарди америчких долара (OECD, 2009: 1). Процена је да уколико би постојало ограничење у погледу употребе готовинског новца дошло би до умереног смањења ових облика криминалитета у износу од 10 до 20% (Mai, 2016: 9), јер је знатно лакше пратити проток дигиталног од готовинског новца. Исто размишљање се може применити и у погледу

превенције тероризма. Ипак, у овом случају треба бити опрезан, јер су се терористи прилагодили већој употреби дигиталног новца, а самим тим и већој контроли држава, тако што су терористи у могућности да прикупљају новчана средства са територија које контролишу (случај Исламске државе), али и, како је то показало истраживање на узорку од 40 напада од стране џихадиста у последњих двадесет година на нивоу Европе, да су се напади финансирали из сопствених средстава, при чему је цена коштања једног напада мања од 10.000 америчких долара, што чак и када се држи у дигиталном новцу не изазива никакву сумњу.[4]

Сједињене Америчке Државе су у последњих десетак година покренуле више иницијатива с циљем повећања употребе дигиталног новца како би се смањио криминалитет. Први корак ка том циљу направило је Министарство одбране САД када је 2008. године промовисало употребу дигиталног новца у оквиру пројекта под називом Cashless Battlefield ради повећања степена безбедности војника у Ираку и Авганистану. На тај начин Министарство одбране је знатно снизило ризик да пошиљке новца буду предмет напада од стране непријатељских група. Четири године касније Америчка агенција за међународни развој је покренула сличан пројекат Better than Cash. Један од циљева пројекта је повећање физичке сигурности особа које не уживају довољан степен заштите, те су жртве пљачки (Armeya, Lipowa, Webba, 2014: 46–47).

На основу свега наведеног можемо закључити да две иницијативе из САД показују да су поменути државни органи уверени да ће већа употреба дигиталног новца у сиромашним државама довести до повећања сигурности. Битно је напоменути да су, поред процена међународних организација, опсежна криминолошка истраживања о утицају веће употребе дигиталног новца на превенцију криминалитета скромна, али да предвиђана стручњака, попут Варвика (Warwick), указују да би што брже прелажење са готовинског новца на дигитални новац довело да смањења криминалитета од најмање 15% па чак до 40% (Vaughan, 2007: 6). Да бисмо могли да закључимо колико је могућа превенција криминалитета гледано кроз призму вредности, навешћемо податак да је годишња штета од крађа у америчком малопродајном сектору 40 милијарди долара (Law, 2020).[5] Превенција криминалитета услед већег коришћења дигиталног

4 Norwegian Institute of international affairs, The Financing of Jihadi Terrorist Cells in Europe: A New Report, Према: https://www.nupi.no/en/About-NUPI/Projects-centers/Consortium-for-Research-on-Terrorism-and-International-Crime/The-Financing-of-Jihadi-Terrorist-Cells-in-Europe-A-New-Report, преузето 25. 12. 2020.

5 Law, M., (2020). Will a Cashless Society Be the End of Financial Crime?, Према: https://www.northrow.com/blog/will-a-cashless-society-be-the-end-of-financial-crime/, преузето

новца од само 15% би износила 6 милијарди долара, а превенција од 40% би смањила штету од крађа за 16 милијарди долара. Уједно, могуће је навести податке о утицају дигиталног новца на превенцију криминалитета на поједине савезне државе. Тако је, на пример, у Мисуријy (Missouri) стопа криминалитета у периоду од 1990. до 2011. године пала за 9,8% услед знатно већег коришћења дигиталног новца.

Поједине европске државе су знатно више напредовале од других у погледу замене готовинског новца дигиталним новцем. У том погледу највише је одмакла Шведска. Интересантан је податак да је током 2015. године у Шведској само 3% размене новца извршено путем готовине. Очекује се да ће убрзо сва плаћања да се врше употребом дигиталног новца. Више од половине банака више не држи депозите у готовини. Поставља се питање какав је утицај употребе дигиталног новца на криминалитет. Наиме, број пљачки, укључујући и банке, се знатно смањио. Тако је током 2008. године извршено 110 пљачки, док је та бројка свега три године касније пала на 16. Објашњење треба тражити не у повећању степена безбедности, већ зато што се готовина слабо држи у касама и сефовима (Henley, 2016).[6] Са друге стране последњих година је у Шведској повећана стопа прања новца. Током 2008. године надлежне институције су открилe нешто више од 100 случајева прања новца, док је та бројка током 2015. године порасла на преко 800. Поставља се питање да ли је увођење дигиталног новца, за разлику од уобичајеног криминалитета, утицало на повећање прања новца. Бројке говоре да је утицало. Објашњење треба тражити у томе да истраживањем није обухваћена вредност укупног прања новца, што је значајнији податак од броја забележених случајева. Уједно, све већим преласком на употребу дигиталног новца банке су у потпуности усмериле своју пажњу на сумњиве трансакције (Mai, 2016: 11).

У погледу анализе стања у Републици Србији у вези употребе дигиталног новца може се видети да грађани Србије са уделом од 42,3% заостају у поређењу са 60% грађана Европске уније који дигитални новац користе за куповину. Може се очекивати да се у наредном периоду повећа проценат грађана Републике Србије који користе дигитални новац за обављање свакодневних активности (Бировљев, 2016: 50). Ипак, за разлику од претходно наведених држава, у Републици Србији није спроведено ниједно истраживање о утицају дигиталног новца на превенцију појединих облика криминалитета.

26. 12. 2020.

6 Henley, J., (2016). Sweden leads the race to become cashless society. Према:https://www.theguardian.com/business/2016/jun/04/sweden-cashless-society-cards-phone-apps-leading-europe, преузето 26. 12. 2020.

3. Дигитализација идентитета и потписа

Други правац превенције криминалитета путем дигитализације јесу дигитални идентитет и потпис. Под дигиталним идентитетом подразумева се информација о ентитету који рачунарски системи користе за представљање спољног агента. Тај агент може бити особа, организација, апликација или уређај. ISO (International Organization for Standardization) и IEC (Internation Electrotechnical Commission) дефинишу идентитет као скуп атрибута повезаних са ентитетом (Brij, 2019: 255). Дуго се сматрало да је дигитални идентитет еквивалент идентитету корисника у стварном животу који мора да обухвата одговор на питања ко је корисник (име и презиме, држављанство, датум рођења), шта корисник воли (омиљена одећа, храна и књига) и шта је наша репутација (да ли је корисник искрен, са проблемима). Другим речима, дигитални идентитет се може посматрати проширеном личном картом која садржи скоро исте информације. Последња схватања указују да не мора постојати веза између стварног и дигиталног идентитета. Наиме, могуће је да на платформама за куповину и продају постоји дигитални идентитет који није у вези са стварним идентитетом, али је за друге кориснике платформе битнија дигитална репутација датог корисника него познавање података у вези држављанства (Vacca, 2009: 270).

Уједно, неопходно је одредити дигитални потпис. То је математичка шема за проверу аутентичности дигиталних порука или докумената (Moman, 2013: 119). Другим речима, то је виртуелни отисак прста. Његова основна својства су јединственост, валидност и аутентичност. Њиме се пружају докази о пореклу, времену, статусу и идентитету дигиталног документа. Важећи дигитални потпис даје примаоцу врло јак разлог да верује да је поруку креирао познати пошиљалац (аутентификација) и да порука није измењена у транзиту (интегритет) (Paul, 2017).[7]

Како смо одредили дигитални идентитет и дигитални потпис поставља се питање њиховог утицаја на превенцију криминалитета. Већа истраживања о утицају дигиталног идентитета и дигиталног потписа на превенцију криминалитета нису спроведена, али се стручњаци из области превенције криминалитета слажу да ће како ова област дигитализације заживи доћи до смањивања финансијског криминалитета извршеног путем интернета. Према последњем истраживању из 2018. године спроведеном од стране организације Refinitiv, напад на финансијске институције је огроман.

7 Paul, E., (2017). What are Digital Signatures: How it works, Benefits, Objectives, Concept. Према:https://www.emptrust.com/blog/benefits-of-using-digital-signatures, преузето 30. 12. 2020.

Скоро половина финансијских организација је одговорила да је била жртва напада. Стога, једна од мера борбе против финансијског криминалитета јесте увођење дигиталног идентитета и дигиталног потписа, јер уз помоћ ових облика дигитализације могуће је пратити проток новца, те на тај начин одржавати трансакцију сигурном (Mirfin, 2019).[8]

С тим у вези изнећемо могуће утицаје дигиталног идентитета и дигиталног потписа на превенцију криминалитета. Наиме, искуства из земаља широм света су показала да је број хакерских напада на финансијске институције знатно мањи када када постоји централни дигитални идентитет. Са друге стране, без постојања дигиталног потписа за фалсификовање неког документа је довољно мало боље познавање рада фотошопа. У случају постојања дигиталног потписа немогуће је фалсификовати документ а да се не види. Другим речима, било какве промене у дигитално потписаном документу је немогуће извршити а да не дође до прекида у потпису. Уједно, неминовно ће доћи до смањивања степена корупције, јер када је неопходно дигитално потписати неки документ то је могуће урадити код куће без контаката са јавним службеницима (аутор, 2010: 388), што самим тим умањује могућност да јавни службеник тражи или да му буде понуђен новац како би урадио нешто незаконито (Jensen, 2019).[9] Како бисмо илустровали значај овог облика дигитализације на превенцију криминалитета, навешћемо случај превара путем електронске поште у Јужноафричкој Републици када је стотине хиљада људи преварено (Schoeman, 2019). [10]

Република Србија је 2017. године донела Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању којим је створена нормативна основа у погледу употребе дигиталног идентитета и потписа. Битно је напоменути да је овај правац дигитализације у Републици Србији још увек у повоју, те да не постоје истраживања о његовом утицају на превенцију криминалитета.

8 Mirfin, J., (2019). Financial crime and the digital ID revolution. Према: https://www.refinitiv.com/perspectives/financial-crime/financial-crime-digital-id-revolution/, преузето 30. 12. 2020.

9 Jensen, H. H., (2019). Three ways digitalization will help end crime. Према:https://www.weforum.org/agenda/2019/10/3-ways-digitalization-will-help-end-crime/, преузето 30.12.2020.

10 Schoeman, R., (2019). Case Study - Utilising Digital Signatures to prevent email fraud. Према: https://www.lawtrust.co.za/news/general/2019/09/13/case-study---utilising-digital-signatures-to-prevent-email-fraud, преузето 30. 12. 2020.

4. Употреба паметних уређаја

Један од пратећих елемената дигитализације јесте стварање тзв. паметних уређаја. Такви уређаји се могу одредити као електронски уређаји који користе интернет или интранет за повезивање и комуникацију са другим уређајима или мрежама за испуњавање задатка или решавање проблема (Ray, Faure, 2018: 16). Другим речима, паметни уређаји су електронски уређаји који су способни за самостално рачунање и повезивање са другим уређајима жичаним или бежичним путем ради размене података. На основу оваквог одређења паметних уређаја могу се одредити три основне карактеристике: свест о контексту, повезаност уређаја и аутономија (Silverio-Fernández, Renukappa, Suresh, 2018: 9).

Са разлогом се поставља питање како паметни уређаји могу утицати на превенцију криминалитета. Одговор лежи у чињеници да нико неће бити заинтересован за куповину украдених паметних уређаја јер су они повезани на интернет. Како бисмо илустровали ову тезу, навешћемо један пример. Наиме, у случају крађе мобилног телефона жртва и надлежни државни орган су увек у могућности да коришћењем опција попут find my phone лако установе где се телефон налази. Очекује се да у будућности бројне ствари које користимо у свакодневном животу постану паметне. То се односи чак и на сијалице. Већ су направљени кораци ка томе да сијалице постану паметне, те да путем интернета буду повезане са одређеном особом која би могла једним кликом на мобилном телефону да контролише када се сијалица пали и којом јачином светли. Уједно, власник има могућност ограничавања контроле сијалице од стране других лица.[11] На тај начин већ сада би потенцијални лопови били демотивисани да их украду, јер нико не би желео да их купи због немогућности да их контролише.

Процењује се да само паметних мобилних телефона има преко 8 милијарди (Brown, 2019),[12] док укупно паметних уређаја има 25 милијарди (Silverio-Fernández, Renukappa, Suresh, 2018: 1). Према проценама тржиште паметних самовозећих аутомобила вреди 24.1 милијарди америчких долара са могућношћу великог раста у блиској будућности. Иако је на тржиште паметних самовозећих аутомобила утицала пандемија вируса COVID 19, познаваоци прилика процењују да ће 2023. године раст тражишта бити 16.84%, при чему ће његова вредност да буде 37.22 милијарди америчких

11 Према:https://www.pcmag.com/picks/the-best-smart-light bulbs?test_uuid=001OQhoHLBxsrrrMgWU3gQF&test_variant=b, преузето 31. 12. 2020.

12 Brown, H., (2019). Did you know that there are more gadgets in the world than people? Према:https://www.gadget-cover.com/blog/did-you-know-that-there-are-more-gadgets-in-the-world-than-people, преузето 31. 12. 2020.

долара.[13] Поред тога што паметни уређаји могу утицати на превенцију имовинског и насилног криминалитета, треба напоменути да тзв. паметни самовозећи аутомобили могу значајно смањити број кривичних дела повезаних са безбедношћу у саобраћају. Наиме, један од циљева рада водећих аутомобилских компанија, попут компаније Tesla, јесте да се број саобраћајних незгода са смртним исходом сведе на нулу. Према постојећим подацима број саобраћајних незгода са смртним исходом износи 1,35 милиона случајева.[14] Смањивање броја оваквих саобраћајних незгода, са крајњим циљем њиховог искорењивања, допринеће не само знатно мањим финансијским трошковима, већ и мањем броју људи осуђених за њихово изазивање.

5. Употреба мобилних апликација

Криминалитет насиља иако знатно мање заступљен од имовинског криминалитета привлачи већу пажњу опште и стручне јавности. Последице његовог извршења су знатно теже, при чему је у појединим случајевима немогуће нанету штету надокнадити. Ради превенције криминалитета насиља предлажемо прављење Anti-Violence апликације за мобилне телефоне чија се суштина огледа у томе да истовремено врши превенцију даљег вршњења криминалитета насиља, али истовремено помаже јавном тужилаштву да докаже извршење овог кривичног дела. Другим речима, апликација би функционисала на начин да се дугим држањем прста преко иконе апликације на мобилном телефону аутоматски позива полиција, при чему би полиција могла преко ГПС да лоцира где се налази жртва кривичног дела. Битно је напоменути да би се локација жртве континуирано бележила уз помоћ ГПС.

Уједно, активирањем апликација аутоматски би се укључила задња и предња камера на телефону и почео би да се прави аудио и видео снимак. Уколико услед техничких карактеристика телефона није могуће укључити истовремено обе камере, у зависности од положаја телефона смењивао би се рад предње и задње камере. Истовремено би се тај снимак аплоудовао на неки од тзв. клауда (cloud). Аплоудовањем аудио и видео снимка на интернет меморији, која је под контролом органа унутрашњих послова, предупредиле би се све ситуације немогућности доказивања извршења

13 Research and Markets, Global Autonomous Cars Market (2020 to 2030) - COVID-19 Growth and Change, Према: https://www.globenewswire.com/news-release/2020/05/20/2036203/0/en/Global-Autonomous-Cars-Market-2020-to-2030-COVID-19-Growth-and-Change.html, преузето 31. 12. 2020.

14 Према:https://www.mes-insights.com/everything-about-self-driving-cars-and-their-technology-a-975762/, преузето 31. 12. 2020.

кривичног дела у смислу накнадног брисања снимка из меморије мобилног телефона од стране насилника или жртве услед разних разлога.

Инсталирањем апликације корисник даје дозволу за тражене пермисије за приступ локацији, микрофону, камери, као и за остале пермисије које су предуслов за рад апликације. Након давања тражених пермисија, корисник врши обавезну регистрацију налога, остављајући основне податке о себи (име, презиме, број телефона, адреса, e-mail) који се верификују. У случају да прикупљени садржај, услед недоступности интернет везе, није прослеђен надлежним органима, приступ истом са мобилног уређаја могућ је само од стране овлашћених лица, не и од стране жртве или вршиоца насиља. Исто тако, у случају прекида интернет везе за време када је Anti-Violence апликација у функцији, снимак би се аплоудовао чим интернет веза буде поново успостављена.

Посебан проблем може бити кориснички интерфејс којим својим називом и изгледом након покретања не сме да открива своју праву намену. На овај начин, смањује се ризик откривања праве функције апликације од стране вршиоца насиља и евентуалних додатних последица по жртву насиља. Стога кориснички интерфејс може изгледати тако да апликација при покретању приказује листу најновијих вести, тзв. newsfeed, при чему је претрага и преглед вести у потпуности функционалан. Други предлог у погледу изгледа корисничког интерфејса је да апликација нема класичан интерфејс.

Као проблем се може јавити бојазан да неко не злоупотреби апликацију тако да је активира зарад пријављивања кривичног дела, а да оно није извршено. У том случају би се примењивале одредбе Кривичног законика везане за члан 334 и кривично дело лажно пријављивање. На тај начин би се спречила евентуална злоупотреба апликације од стране несавесних грађана. Уједно, зарад потребне разумљивости да би злоупотреба апликације резултирала кривичним гоњењем за кривично дело лажно пријављивање, приликом инсталирања апликације би се налазило обавештење о томе. Корисник апликације би морао да прочита, те кликне одговарајуће поље како би доказао да је разумео које су последице евентуалне злоупотребе апликације. Anti-Violence апликација за пријаву насиља у породици биће доступна у продавницама апликација најпопуларнијих мобилних платформи Google Playstore (Android) и Apple App Store (iOS).

6. Закључак

На основу наведеног можемо рећи да ће тек у будућности дигитализација остварити свој пуни потенцијал у погледу превенције криминалитета. Иако ће највећи утицај имати на превенцију имовинског криминалитета, треба нагласити да се може очекивати и смањење криминалитета насиља коришћењем мобилних апликација на начин на који смо објаснили у раду. Уједно, већа распрострањеност тзв. паметних самовозећих аутомобила ће допринети знатно мањем броју саобраћајних несрећа за које кривично одговарају возачи. Са друге стране, чешћа употреба дигиталног идентитета и дигиталног потписа ће отежати вршење компјутерског криминалитета. Другим речима, дигитализација ће довести до превенције читавог низа кривичних дела. Исто тако, бенефити дигитализације ће се огледати и у знатној уштеди новчаних средстава која су неопходна за функционисање правосудног и пенитенцијарног система, али и уштеде у погледу осигурања услед мањег броја саобраћајних незгода. Такође, не може се очекивати да ће све набројане правце дигитализације свет прихватити без икаквог отпора. Довољно је навести да у државама које су највише одмакле у дигитализацији новца постоји жеља становништва да и даље користи папирни новац јер се тако осећа сигурније (LaMagna, 2016).[15]

Ипак, са друге стране, треба истаћи да се криминалитет и криминалци одликују могућношћу прилагођавања на промене у друштву. Стога ће криминалци прећи да врше своје криминалне активности из стварног у дигитални свет. Може се очекивати знатни раст кривичних дела извршених путем компјутера. Наиме, постојали су случајеви крађе дигиталног идентитета. Процењује се да годишње око 210.000 особа буде жртва крађе дигиталног идентитета.[16] Ради даље превенције компјутерског криминалитета биће неопходна знатно већа сарадња држава међу собом, јер је много теже идентификовати извршиоца компјутерског криминалитета (аутор, 2010: 206–208).

15 LaMagna, M., (2016). Here's what would happen if America totally abandoned cash. Према: https://www.marketwatch.com/story/how-the-us-and-china-could-benefit-from-going-cashless-2016-06-03, преузето 31. 12. 2020.

16 Према: https://www.ingroupe.com/en/observatory/data-and-integrity/fraud-what-exactly-is-digital-identity-theft, преузето 31. 12. 2020.

Литература и извори

Armeya, L., Lipowa, J., Webba, N., (2014). The Impact of Electronic Financial Payments on Crime, (no. 29). Information Economics and Policy

Birovljev, A., (2016). Elektronska i mobilna plaćanja u svetu i Srbiji, Beograd: Bigrafplus

Brij, G. B., (2019). Modern Principles, Practices, and Algorithms for Cloud Security, USA: IGI Global

Brown, H., (2019). Did you know that there are more gadgets in the world than people? Prema: https://www.gadget-cover.com/blog/did-you-know-that-there-are-more-gadgets-in-the-world-than-people, preuzeto 31. 12. 2020.

Димовски, Д., (2010). Компјутерски криминалитет, Зборник радова Правног факултета у Нишу, (бр. 55). Ниш: Центар за публикације

Димовски, Д., (2010). Политичка корупција, Приступ правосуђу – инструменти за имплементацију европских стандарда у правни систем Републике Србије: тематски зборник радова, Ниш: Центар за публикације Правног факултета

Димовски, Д., (2015). Превенција криминалитета кроз бављење спортом и физичком активношћу, Зборник радова Правног факултета у Нишу, Ниш: Центар за публикације

Esselink, H., Hernández, L., (2017). The use of cash by households in the euro area, (no. 201). Frankfurt am Main: European Central Bank

Henley, J., (2016). Sweden leads the race to become cashless society. Prema: https://www.theguardian.com/business/2016/jun/04/sweden-cashless-society-cards-phone-apps-leading-europe, preuzeto 26. 12. 2020.

Jensen, H. H., (2019). Three ways digitalization will help end crime. Prema: https://www.weforum.org/agenda/2019/10/3-ways-digitalization-will-help-end-crime/, preuzeto 30. 12. 2020.

Lab, S. (2010). Crime Prevention: Approaches, Practices and Evaluations, New York: Matthew Bender & Company

LaMagna, M., (2016). Here's what would happen if America totally abandoned cash. Prema: https://www.marketwatch.com/story/how-the-us-and-china-could-benefit-from-going-cashless-2016-06-03, preuzeto 31. 12. 2020.

Лазаревић, Љ. (1988). Југословенска криминална политика и њена научна заснованост, Југословенска ревија за криминологију и кривично право,

Београд: Савез удружења за кривично право и криминологију Југославије и Институт за криминолошка и социолошка истраживања

Law, M., (2020). Will a Cashless Society Be the End of Financial Crime?, Prema: https://www.northrow.com/blog/will-a-cashless-society-be-the-end-of-financial-crime/, preuzeto 26. 12. 2020.

Mai, H., (2016). Cash, freedom and crime Use and impact of cash in a world going digital, Deutsche Bank Research

Mirfin, J., (2019). Financial crime and the digital ID revolution. Prema: https://www.refinitiv.com/perspectives/financial-crime/financial-crime-digital-id-revolution/, preuzeto 30. 12. 2020.

Moman, S., (2013). International Conference on Electrical, Control and Automation, Lancaster: DEStech Publications

Norwegian Institute of international affairs, The Financing of Jihadi Terrorist Cells in Europe: A New Report, Prema: https://www.nupi.no/en/About-NUPI/Projects-centers/Consortium-for-Research-on-Terrorism-and-International-Crime/The-Financing-of-Jihadi-Terrorist-Cells-in-Europe-A-New-Report, preuzeto 25. 12. 2020.

OECD, (2009). Magnitude of Counterfeiting and Piracy of Tangible Products. An Update

Paul, E., (2017). What are Digital Signatures: How it works, Benefits, Objectives, Concept. Prema: https://www.emptrust.com/blog/benefits-of-using-digital-signatures, preuzeto 30. 12. 2020.

Ray, B., Faure, C., (2018). Mini-Robots as Smart Gadgets: Promoting Active Learning of Key K-12 Social Science Skills, In: Handbook of Research on Mobile Devices and Smart Gadgets in K-12 Education (ed. Khan, A., A., Umair, S.,), Pakistan

Research and Markets, Global Autonomous Cars Market (2020 to 2030) – COVID-19 Growth and Change, Prema: https://www.globenewswire.com/news-release/2020/05/20/2036203/0/en/Global-Autonomous-Cars-Market-2020-to-2030-COVID-19-Growth-and-Change.html, preuzeto 31. 12. 2020.

Schoeman, R., (2019). Case Study - Utilising Digital Signatures to prevent email fraud. Prema: https://www.lawtrust.co.za/news/general/2019/09/13/case-study---utilising-digital-signatures-to-prevent-email-fraud, preuzeto 30. 12. 2020.

Silverio-Fernández, M., (2018). Renukappa, S., Suresh, S., What is a smart device? – a conceptualisation within the paradigm of the internet of things, (no. 3). Visualization in Engineering,

United Nations Office on Drugs and Crime, World Drug Report, 2005, Volume 1: Analysis,

Vacca, J., (2009). Computer and Information Security Handbook, Amsterdam: Morgan Kaufmann,

van Velthoven, B., van Wijck, P., (2016). Becker's theory on crime and punishment, a useful guide for law enforcement policy in The Netherlands, (no. 37(1)). Den Haag: Recht der Werkelijkheid

Vaughan, P., (2007). Early lessons from the Deployment of M-PESA, Vodafone's own Mobile Transactions Service, (no. 6). The Policy Paper Series „The Transormational Potential of M- Transactions"

Закон о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању, Сл. гласник РС, бр. 94/2017.

Интернет извори:

Према: https://voxeu.org/article/digitalisation-money-and-future-monetary-policy, преузето 24. 12. 2020.

Према: https://www.gartner.com/en/information-technology/glossary/digitalization, преузето 21. 12. 2020.

Према: https://www.ingroupe.com/en/observatory/data-and-integrity/fraud-what-exactly-is-digital-identity-theft, преузето 31. 12. 2020.

Према: https://www.investopedia.com/terms/d/digital-currency.asp, преузето 24. 12. 2020.

Према: https://www.mes-insights.com/everything-about-self-driving-cars-and-their-technology-a-975762/, преузето 31. 12. 2020.

Према: https://www.pcmag.com/picks/the-best-smart-light bulbs?test_uuid=001OQhoHLBxsrrrMgWU3gQF&test_variant=b, преузето 31. 12. 2020.

Darko Dimovski, LL.D.,
Associate Professor,
Faculty of Law, University of Nis

CRIME PREVENTION THROUGH DIGITALIZATION

Summary

Common crime prevention measures have not yielded the expected results. It is important to examine the possibilities of using the latest achievements in crime prevention. One of the available options is digitalization. Starting from the definition of digitalization as the use of digital technologies to change the business model and provide new opportunities for generating income and value, the author emphasizes that digitalization can be used as a measure to prevent crime. In this regard, some solutions for preventing crime through digitalization are embodied in the use of digital currencies, digital identities and signatures, smart devices, and mobile applications. The author elaborates on each of these solutions, focusing on specific crime prevention measures and examples from different countries worldwide. It may help crime prevention experts perceive digitalization as a measure for reducing the volume of crime. If the benefits of digitalization are put into good use, we can expect that the volume of property-related crimes, violence-related crimes and traffic delinquency will drop in the forthcoming period. On the other hand, the implementation of these measures may give rise to the commission of Internet-related crimes, thus leading to the increase in computer crime.

Keywords**:** *crime, prevention, digitalization.*