XXI МАЈСКО САВЕТОВАЊЕ

САВРЕМЕНО ПРАВО У ЕРИ ДИГИТАЛИЗАЦИЈЕ И ОДРЖИВОГ РАЗВОЈА

УРЕДНИК:
Драган Вујисић

УНИВЕРЗИТЕТ У КРАГУЈЕВЦУ
ПРАВНИ ФАКУЛТЕТ

Крагујевац
2025.

ПРАВНИ ФАКУЛТЕТ УНИВЕРЗИТЕТА У КРАГУЈЕВЦУ
Институт за правне и друштвене науке

FACULTY OF LAW UNIVERSITY OF KRAGUJEVAC
Institute for Legal and Social Sciences

МЕЂУНАРОДНА НАУЧНА КОНФЕРЕНЦИЈА
САВРЕМЕНО ПРАВО У ЕРИ ДИГИТАЛИЗАЦИЈЕ И ОДРЖИВОГ РАЗВОЈА

INTERNATIONAL SCIENTIFIC CONFERENCE
CONTEMPORARY LAW IN ERA OF DIGITALIZATION AND SUSTAINABLE DEVELOPMENT

Уредник
Проф. др Драган Вујисић

Крагујевац
2025.

САВРЕМЕНО ПРАВО У ЕРИ ДИГИТАЛИЗАЦИЈЕ И ОДРЖИВОГ РАЗВОЈА

CONTEMPORARY LAW IN ERA OF DIGITALIZATION AND SUSTAINABLE DEVELOPMENT

Зборник научних реферата по позиву са Међународног научног скупа одржаног од 26. до 27. септембра 2025. године, на Правном факултету у Крагујевцу у оквиру Програма истраживања Правног факултета Универзитета у Крагујевцу за 2025. годину, који се финансира из средстава Министарства науке, технолошког развоја и иновација Републике Србије

Међународна конференција „**САВРЕМЕНО ПРАВО У ЕРИ ДИГИТАЛИЗАЦИЈЕ И ОДРЖИВОГ РАЗВОЈА**" је двадесетпрво по реду Мајско саветовање које се традиционално организује сваке године на Правном факултету Универзитета у Крагујевцу ради дисеминације научноистраживачких резултата наставника и сарадника факултета, у оквиру Програма истраживања Правног факултета, које се финансира из средстава Министарства науке, технолошког развоја и иновација Републике Србије.

ИЗДАВАЧ: Правни факултет Универзитета у Крагујевцу
Институт за правне и друштвене науке
Јована Цвијића 1, 34000 Крагујевац
телефон: (034) 306 513, 306 504
телефакс: (034) 306 540
е-пошта: faculty@jura.kg.ac.rs
веб: http://.jura.kg.ac.rs

РЕЦЕНЗЕНТИ Проф. др Миодраг Мићовић, редовни професор
Правног факултета Универзитета у Крагујевцу
Проф. др Жељко Бартуловић, редовни професор
Правног факултета Свеучилишта у Ријеци, Хрватска
Проф. др Игор Камбовски, редовни професор
Правног факултета Универзитета „Гоце Делчев"у
Штипу, Северна Македонија
Проф. др Џевад Дрино, редовни професор
Правног факултета Универзитета у Зеници,
Федерација БиХ

ЗА ИЗДАВАЧА: Проф. др Јелена Вучковић, редовни професор
Правног факултета Универзитета у Крагујевцу

УРЕДНИК: Проф. др Драган Вујисић, редовни професор
Правног факултета Универзитета у Крагујевцу

ШТАМПА: Графичка радња "кварк", Краљево

ТИРАЖ: 100

ISBN 978-86-7623-149-2

Штампање Зборника подржало Министарство науке, технолошког развоја и иновација Републике Србије

С А Д Р Ж А Ј

Одељак I
ЈАВНО ПРАВО

Одељак II
КРИВИЧНО ПРАВО

Др Игор Камбовски, редовни професор
Правног факултета Универзитета „Гоце Делчев"
у Штипу, Северна Македонија
ORCID: 0009-0000-5884-2997

Мр Ѓорѓи Манчев, докторанд
Правног факултета Универзитета "Гоце Делчев"
у Штипу, Северна Македонија
ORCID: 0009-0005-5600-1795

Прегледни научни рад
УДК: 004.738.5:349.9(497.7)"2018-2022"
DOI: 10.46793/XXIMajsko.289K

ЗАШТИТА ЛИЧНИХ ПОДАТАКА У САЈБЕР ПРОСТОРУ СА ПОСЕБНИМ ОСВРТОМ НА САЈБЕР КРИМИНАЛ У РЕПУБЛИЦИ СЕВЕРНОЈ МАКЕДОНИЈИ У ПЕРИОДУ ОД 2018. ДО 2022. ГОДИНЕ

Резиме

Брзи развој информационих технологија и њихова све већа софистицираност све више отежавају и усложњавају борбу против криминалних активности из области компјутерског криминала. Најчешћи облици крађа и превара који подразумевају злоупотребу информационих и комуникационих технологија укључују: повреду личних података, преваре са кредитним картицама и хартијама од вредности, крађу идентитета, неовлашћено коришћење и узурпацију компјутерских услуга, као и компјутерску шпијунажу. Један од највећих изазова у савременом дигиталном окружењу свакако је заштита приватности и личних података, нарочито у контексту све веће примене вештачке интелигенције. Посебан акценат ставља се на поштовање начела заштите личних података током развоја вештачке интелигенције, на право појединца да буде изузет из процеса аутоматизованог доношења одлука, као и на заштиту права гарантованих Законом о заштити личних података. У оквиру овог рада извршена је анализа и истраживање степена сајбер криминала у Републици Северној Македонији у периоду од 2018 до 2022 године. Приказани су број и врсте кривичних дела из области компјутерског криминала, могући починиоци, као и процењена материјална штета настала као последица сајбер напада. Истраживање је спроведено на основу званичних података добијених од Министарства унутрашњих послова кроз њихове годишње извештаје о раду.

Кључне речи: *лични подаци, сајбер криминал, вештачка интелигенција, преваре*

1. Увод - Дигитална права и људска права.

Порекло људских права заснива се на теорији природног права. Људска права као природна права стиче свако људско биће рођењем. Она представљају неотуђива права и слободе која подједнако важе за све људе, без обзира на расу, пол, језик, религију, економски статус, образовање, политичко или друго мишљење, у било којим околностима. Без обзира на разлике између друштава и појединаца, људска права чине везивно ткиво које их повезује. Она представљају универзалне вредности, заједничке свим људима. У суштини концепта људских права налази се стремљење ка заштити људског достојанства. Тај концепт поставља човека у средиште пажње и заснован је на заједничком, општеприхваћеном систему вредности.

2. Заштита људских права и личних података

У дигиталном окружењу и људска права добијају нову, савремену димензију. Сваком кориснику дигиталних услуга требају бити омогућена и загарантована следећа права[1]:

• **Приступ интернету и недискриминација** – Ниједан корисник не сме бити искључен са интернета против своје воље, осим по одлуци суда (ово не подразумева искључење због неиспуњавања уговорних обавеза према провајдеру). Приступ интернету треба да буде неселективан и без дискриминације.

• **Слобода изражавања и приступ информацијама** – Сваки корисник има право да се слободно изражава на интернету, као и да приступа и дели информације и мишљења, укључујући и она која могу бити увредљива или узнемиравајућа, под условом да се поштује туђа част, углед и приватност. Ограничења могу бити прописана само ради легитимних циљева у складу са Европском конвенцијом о људским правима и домаћим законодавством – на пример, у случају подстицања на дискриминацију, мржњу или насиље, или уколико представљају претњу националној безбедности или јавном реду. Корисници могу одлучити да не откривају свој идентитет, али морају бити

[1] Камбовски, И., Стојановска, Е., *Истражување за ефектот на новите технологии, со особен фокус на вештачката интелигенција, врз човековите права на интернет и развивање етички стандарди за заштита на човековите права на интернет при автоматско донесување одлуки*-електронско издање, Фондација за интернет и општество Метаморфозис – Скопје, 2024, https://metamorphosis.org.mk/wp-content/uploads/2024/05/istrazhuvanje-za-efektot-na-novite-tehnologii-so-osoben-fokus-na-veshtachkata-inteligencija-vrz-chovekovite-prava-na-internet.pdf, посећено 12.04.2025.

информисани да власти могу, у строго дефинисаним околностима, прибавити податке који откривају идентитет.

• **Слобода окупљања, удруживања и учешћа** – Корисници имају право да користе било који вебсајт, апликацију или услугу за контакт, сарадњу и дружење са истомишљеницима, пријатељима, колегама. Остваривање права на миран протест у онлајн простору такође је дозвољено. Међутим, корисници треба да буду свесни правних последица уколико дође до блокаде, прекида услуга, оштећења имовине или угрожавања права других лица.

• **Приватност и заштита личних података** – Лични подаци треба да се обрађују само уз изричиту сагласност корисника или на основу закона. Корисници морају бити информисани о начину на који се њихови подаци прикупљају, чувају, обрађују или преносе трећим лицима – када, од кога и у коју сврху. Такође, имају право на приступ, исправку и брисање сопствених података. Забрањено је било какво масовно надгледање, снимање или прислушкивање, осим у изузетним ситуацијама прописаним законом, као што су кривичне истраге и угрожавање јавне безбедности, искључиво уз судско овлашћење.

• **Заштита деце и младих** – Деца имају право на посебну заштиту при коришћењу интернета. Због недовољне свести и разумевања дигиталног окружења, деца су посебно рањива. Повреде приватности могу укључити откривање осетљивих података, лажно приказивање детета, манипулације и изложеност штетним садржајима као што су сајбер насиље, говор мржње, експлицитни садржаји и слично. Играчке и апликације које користе вештачку интелигенцију често прикупљају велике количине података без знања детета или његових родитеља. Алгоритми могу довести до ширења дезинформација, манипулације, па чак и укључивања деце у ризичне активности попут сајбер криминала или самоповређивања. Уколико садржај који је објављен од стране детета или трећих лица угрожава његово достојанство, безбедност или приватност, он мора бити обрисан у најкраћем року на захтев детета или његовог старатеља. Деца морају бити заштићена од злоупотребе њихових података, нарочито у погледу сексуалне експлоатације.

Ови постулати о заштити података и дигиталним правима садржани су у **Водичу за људска права за кориснике интернета**[2], који је израдио Савет Европе 2014. године. Циљ Водича је да помогне корисницима да разумеју своја права у дигиталном простору и да укаже на кораке које могу предузети у случају њиховог угрожавања. Водич на једноставан начин објашњава права садржана у Европској конвенцији о људским правима и примену тих права у интернет окружењу. Намењен је корисницима, државним институцијама и приватном сектору, са циљем унапређења одговорног и правичног понашања у

[2] https://www.coe.int/en/web/freedom-expression/guide-to-human-rights-for-internet-users, посећено 07.04.2025.

дигиталном окружењу. Водич је документ који се развија и треба редовно ажурирати у складу са технолошким иновацијама.

Према **Закону о заштити личних података**[3], који представља *lex generalis* у овој области у Републици Северној Македонији, право на заштиту података је интегрисано у национални правни систем. Тим законом се поставља нови концепт који наглашава значај овог права као темељног заштитног механизма сваког појединца у савременом, технолошки напредном друштву. Концепт подразумева заштиту приватности и личног интегритета у свакој ситуацији у којој долази до обраде личних података.

3. Лични подаци и вештачка интелигенција

Када је у питању повезаност између вештачке интелигенције и заштите личних података, може се рећи да су то две области које све више међусобно пресрећу. Технологија развоја вештачке интелигенције је све напреднија, што поставља бројна питања која се односе на етичку употребу вештачке интелигенције у контексту заштите личних података потенцијалних корисника система који користе вештачку интелигенцију. Лични подаци постали су незаменљиви део развоја и употребе вештачке интелигенције, где служе и користе се као основа за обуку система вештачке интелигенције у препознавању образаца, побољшању тачности и омогућавању персонализације која се користи у различитим индустријама. Чак и након развоја, функционисање система вештачке интелигенције зависи од података са којима се "храни" вештачка интелигенција, без којих они не би могли да примењују, нити да дају жељене резултате и усаврше своје учење. Општа регулатива за заштиту података *(GDPR)*[4] поставља низ стандарда како би се обезбедило високо ниво заштите личних података у ЕУ, док многи национални закони морају да прате ове стандарде. Вештачка интелигенција је до недавно била регулисана кроз меке законске инструменте, такозвани *"soft law"*, као што су Етичка упутства за поуздану вештачку интелигенцију[5]. Међутим, јавила се потреба да се успостави правни оквир који осигурава да вештачка интелигенција функционише на сигуран и разумњив начин, без уграђене (или наслеђене) дискриминације и без њеног коришћења као алата за манипулацију. У последњих неколико година у оквиру ЕУ и Савета Европе усвојен је значајан број докумената, препорука, декларација и предлога који имају за циљ подизање свести о утицају вештачке интелигенције у свим сферама друштвеног

[3] Закон за заштита на личните податоци (Сл. весник на Република Северна Македонија, бр. 42/20 и бр.294/21).

[4] https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng, посећено 03.04.2025.

[5] https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, посећено 08.04.2025.

живота, кроз стварање одговарајућег правног оквира заснованог на обавезујућим и необавезујућим нормама и стандардима.

Правилни приступ у заштити људских права у контексту производа и услуга заснованих на технологијама вештачке интелигенције предвиђен је и регулисан Законом ЕУ о Вештачкој интелигенцији из 2024 године[6]. Законодавна решења укључена у ову регулативу ЕУ представљају основу за регулисање овог питања у националним оквирима земаља чланица ЕУ, као и у многим другим државама. Овај закон регулише системе које генеришу садржај, предикције, препоруке или одлуке које утичу на окружење, укључујући алате за интеракцију међу људима, паметне системе за надзор или апликације које се могу користити за генерисање тзв. *deepfake* садржаја (синтетички медији). Овакви системи вешташке интелигенције, према новим правилима, класификују се према висини ризика, од минималног до недопустивог (забрањеног), док су за јавне и приватне актере који их производе или користе прописане одговарајуће обавезе, али и казне, у случају непоштовања. Ипак, неке од најопаснијих примена вештачке интелигенције нису означене као недопустив ризик, односно нису забрањене, укључујући системе за масовни биометријски надзор и предиктивне полицијске системе. Увођењем двојних стандарда за полицију и службе безбедности, законодавци су оставили довољно простора и могућности за повреду људских права. Такође, са аспекта ефикасности будуће регулативе, од великог значаја је да сваки нови правни инструмент буде у складу са постојећим правним и етичким стандардима, али, с обзиром на динамику технолошког напретка и његову непредвидивост, важно је да будући закони буду конструисани и формулисани на начин који ће им омогућити максималну флексибилност у адаптацији на промене.

Све институције, организације, компаније које су укључене у процес развоја и употребе вештачке интелигенције морају да обезбеде транспарентност у употреби вештачке интелигенције, односно, да дају јасне и концизне информације корисницима о томе да ли и на који начин њихови лични подаци буду прикупљени и обрађени током коришћења система који користи вештачку интелигенцију. Додатно, корисницима треба бити јасно саопштено за коју специфичну сврху ће бити прикупљени, складиштени или на други начин обрађени њихови лични подаци, као и да им се понуди експлицитна могућност да дају или не дају своју сагласност.

Питање које је од изузетне важности када је реч о повезаности вештачке интелигенције и заштите личних података је и питање аутоматског доношења одлука. Према Општој регулативи за заштиту личних података *(General Data Protection Regulation – GDPR)*, свака особа има право да не буде предмет аутоматског доношења одлука, укључујући и профилисање[7]. Ово значи да у

[6] The AI Act, https://artificialintelligenceact.eu/, посећено 28.03.2025.

[7] „Профилисање“ значи сваки облик аутоматизоване обраде личних података који се састоји од коришћења личних података за процену одређених личних аспеката

процесу развоја система који користе вештачку интелигенцију мора бити извршена анализа потенцијалног утицаја који би употреба вештачке интелигенције имала на заштиту личних података и да се неће доносити одлуке о корисницима нити ће се вршити профилисање без узимања у обзир људских права.

Успостављање баланса између потребе за технолошким достигнућима, развојем вештачке интелигенције и потребе за поштовањем правила, смерница и закона за заштиту личних података је истовремено и кључна и комплексна активност. Заштита личних података не сме бити схваћена само као законска обавеза са којом се морају усагласити они који раде на развоју вештачке интелигенције, већ као једна од основних компоненти за разумну употребу вештачке интелигенције. Са друге стране, заштита личних података не сме бити разлог за успоравање иновационих процеса и развоја вештачке интелигенције. Заштита личних података треба да се гледа као нешто што ће обезбедити етичку, фер употребу вештачке интелигенције уз поштовање права корисника.

У циљу усаглашавања са европским регулативама, Република Северна Македонија је донела нови Закон за заштиту личних података у 2020 години, који је у потпуности усаглашен са Општом регулативом за заштиту личних података *(GDPR),* а додатно Агенција за заштиту личних података је донела и подзаконске акте за континуирану процену утицаја на заштиту личних података.

4. Компјутерске крађе личних података

Крађе заузимају високо место у области компјутерског криминала, а у односу на разрађену проблематику од посебног значаја је крађа идентитета и личних података. Овај тип крађе има посебно значење у друштву јер, поред свега осталог, смањује поверење у интегритет комерцијалних трансакција и угрожава индивидуалну приватност. Процене стручњака су да ће компјутерске крађе расти са електронском трговином, развојом мобилног банкарства и све већом употребом вештачке интелигенције. Опскрбљени са индивидуалним личним подацима, криминалци с украденим идентитетом и личним подацима могу отворити електронске рачуне у банкама, извршити куповину, а у земљама где су аутоматизоване сервисне услуге за грађане, могу добити документе попут извода из матичне књиге рођених, пасоша, кредита и слично, све то у име особе чији су подаци украдени. Са лажним идентитетом криминалци могу добити кредите од банака, купити аутомобил, стан, итд., чиме могу изазвати

који се односе на физичко лице, посебно за анализу или предвиђање аспеката који се односе на обављање професионалних дужности тог физичког лица, економску ситуацију, здравље, личне преференције, интересовања, поузданост, понашање, локацију или кретање.

финансијску штету жртви, а у неким случајевима и направити криминално досије. Жртва у већем броју случајева није свесна да је њен идентитет "коришћен" све док не стигну "рачуни за наплату". Значи, и финансијска и "хумана" цена крађе за индивидуалну жртву може бити веома висока, иако је једини разлог за многе жртве то што су њихови лични подаци били у неком фајлу који је украден или су наивно давали информације погрешним људима, интернет страницама или апликацијама[8].

Компјутерске преваре извршавају се с намером да се за себе или другог стекне противправна материјална корист, при чему код њих није доведена у заблуду нека особа, као што су случајеви са обичним преварама, већ заблуда се односи на компјутер у који се уносе нетачни подаци, или се пропушта унос тачних података, или се на било који други начин, компјутер користи за остваривање превара у кривично-правном смислу. Компјутерске преваре представљају најраспрострањенији облик компјутерског криминала.

Компјутерски преваранти злоупотребљавају карактеристике сајбер простора које доприносе расту електронске трговине: анонимност, дистанца између продаваца и купаца и тренутна трансакција. На тај начин, они користе и предност чињенице да превара путем интернета не захтева приступ неком систему за исплату, као што захтева свака друга врста преваре, као и чињеницу да је дигитално тржиште још увек недовољно уређено, што ствара одређену конфузију за потрошаче, што за компјутерске преваранте ствара скоро идеалне услове за компјутерске преваре.

5. Правни оквир и надлежност

У Републици Македонији санкционисање ових кривичних дела регулисано је чланом 251 Кривичног законика, (Оштећење и неовлашћени упад у компјутерски систем). Ово кривично дело је уведено у македонски КЗ 1996 године и од тада се примењује овај члан у пракси. Став 1 овог члана: "Онај ко неовлашћено избрише, измени, оштети, сакрије или на други начин учини непотребним компјутерски податак или програм или уређај за одржавање информационог система, или онемогући или отежа коришћење компјутерског система, података или програма или компјутерске комуникације, биће кажњен новчаном казном или затвором до три године."

6. Међународни правни извори

Иако су раније постојали покушаји да се дефинишу материјални стандарди који регулишу међународну правну сарадњу, Конвенција о рачунарском криминалу Савета Европе је својом свеобухватношћу, флексибилношћу и лакоћом имплементације у национална законодавства, иако првобитно

[8] Тупанчески, Н., *Економско казнено право*, 2015, стр. 34.

намењена државама Европе, постала препознатљив механизам за ефикасну комуникацију између држава широм света. Конвенција садржи материјалне и процесне норме као и норме за међународну сарадњу. Одредбе из области материјалног права односе се на неовлашћени приступ, неовлашћено пресретање, упад у податке, упад у систем, злоупотребу уређаја, фалсификовање везано за рачунар, рачунарске преваре, дела везана за дечју порнографију и повреду ауторских и сродних права

Савет Европе је усвојио Конвенцију о рачунарском криминалу у Будимпешти 23.11.2001 године[9]. Укупно 58 држава потписало је Конвенцију, од којих је 28 ратификовало. Конвенција је потписана од стране Македоније 23.11.2001 године, ратификована је 15.09.2004. године, а ступила је на снагу 01.01.2005 године.

Конвенција о рачунарском криминалу касније је допуњена Конвенцијом за заштиту личних права у аутоматизованим процесима обраде личних података са амандманима, Допунским протоколом о овлашћеном прелазу личних података преко граница, Допунским протоколом Конвенције о рачунарском криминалу за заштиту од расизма и ксенофобије, Конвенцијом за заштиту деце од сексуалне експлоатације и сексуалног злостављања и директивама ЕУ.

Правни оквир који регулише рачунарски криминал у Републици Северној Македонији обухвата: Кривични законик (КЗ), Закон о кривичном поступку (ЗКП), Закон о електронским комуникацијама, Закон о праћењу комуникација, Закон о електронској трговини, Закон о електронском управљању, Закон о парничном поступку, Закон о подацима у електронском облику и електронском потпису и Декларацију о безбеднијем интернету.

7. Стопа сајбер криминала у Републици Северној Македонији у периоду од 2018 до 2022 године

У **2018** години[10] откривено је 105 кривичних дела извршених од стране 73 починиоца, што у поређењу са претходном годином представља повећање откривања дела за 29,5%. Карактеристично је да је уз извршење ових дела на физичким и правним лицима нанета штета у вредности од 11,2 милиона денара, што у поређењу са претходном годином када је штета износила 611,8 милиона денара, представља значајан пад. Најзаступљенија кривична дела су "оштећење и неовлашћени приступ рачунарском систему" (53) и "рачунарска превара" (14), са материјалном штетом која чини 96% укупне штете. Дела су извршена коришћењем претходно украдених платних картица за подизање новца са банкомата, као и нелегалним трансакцијама са фалсификованим платним картицама приликом куповине на интернету и плаћања рачуна преко интернета *(E-commerce)*, као и са неовлашћеним приступом рачунарским системима и

[9] https://www.coe.int/en/web/cybercrime/the-budapest-convention, посећено 23.04.2025.
[10] https://mvr.gov.mk/Upload/Editor_Upload/Godisen%20izvestaj%202018.pdf

изменом садржаја веб страница правних лица. Осим тога, и даље је присутан тренд нелегалног преузимања и посредовања у пословној комуникацији путем електронске поште између македонских и страних компанија, при чему је обављано преусмеравање банкарских трансакција. У већини случајева ова активност била је усмерена на мала и средња предузећа. Такође, актуелни политички догађаји те године и злоупотреба комуникације путем друштвених мрежа резултирали су са 21 кривичним делом "угрожавање сигурности" путем информатичког система и пет кривичних дела "ширење расистичког и ксенофобичног материјала путем рачунарског система". Повећана је и употреба друштвених мрежа за објављивање слика посланика и владиних функционера уз претње по живот.

У **2019** години[11] бележимо пораст од 65,7%, односно регистровано је 174 кривичних дела, за које је кривично пријављено 124 починиоца. Карактеристично је да је са извршењем ових дела на физичким и правним лицима нанесена материјална штета од 42,6 милиона денара, што у поређењу са претходном годином када је штета износила 11,2 милиона денара, представља повећање од 280%. Повећање у откривању, пре свега, има везе са великом количином садржаја на интернет порталима и друштвеним медијима у којима се промовише или подстиче мржња, дискриминација или насиље против појединаца или група на основу етничке, верске и политичке припадности, као и повећан број случајева злоупотребе личних података. У 2019 години регистровано је 29 кривичних дела угрожавања сигурности, 27 кривичних дела ширења расистичког и ксенофобичног материјала путем рачунарског система, као и 19 дела злоупотребе личних података. Према извршеним анализама у области рачунарског криминала, идентификовани су неки специфични трендови: У сектору платних картица, у поређењу са претходном годином, бележимо повећање кривичних дела за 28%, односно откривено је 73 дела, од којих 65 се односи на "оштетење и неовлашћено упадање у рачунарски систем", док је осам случајева за "израду и употребу лажне платне картице". Најчешће, ова кривична дела су извршена путем претходно украдених дебитних и кредитних картица, које су касније злоупотребљене за подизање новца са банкомата. Са повећаном доступношћу друштвених мрежа и интернет садржаја младој популацији, повећан је и ризик од сексуалне злоупотребе деце, као и експанзија тржишта за дечју порнографију. Ове (2019) године, број кривичних дела за сексуалну експлоатацију деце путем интернета повећао се за 150%, односно регистровано је 10 кривичних дела, од којих је шест за "производњу и дистрибуцију дечје порнографије", а четири за "показивање порнографског материјала детету", са пет, односно два кривично пријављена починиоца. У области рачунарских

[11] https://mvr.gov.mk/Upload/Editor_Upload/%D0%9E%D0%9A%D0%A0%D0%90/%D0%93%D0%BE%D0%B4%D0%B8%D1%88%D0%B5%D0%BD%20%D0%B8%D0%B7%D0%B2%D0%B5%D1%88%D1%82%D0%B0%D1%98%202019.pdf

превара, регистровано је 12 кривичних дела, која се одликују већом комплексношћу извршења и значајно већом материјалном штетом, која износи 36,3 милиона денара или 85,2% од укупне материјалне штете за ову годину. Најчешћи случајеви интернет превара укључују лажне огласе за купопродају на интернет порталима и пресретање e-mail комуникације између приватних фирми с циљем преваре, усмеравања и плаћања на друге банкарске рачуне.

У **2020** години[12], кривична дела у области рачунарског криминала бележе пад од 8,6%, односно регистровано је 160 кривичних дела, а кривично су пријављена 88 починилаца. Причињена материјална штета износи 12,6 милиона денара, што представља значајно смањење у поређењу са 2019 годином, када је материјална штета процењена на 42,6 милиона денара. Најзаступљенија кривична дела су она која се односе на злоупотребу платних картица, са укупно 103 регистрована дела, од којих је 85 за "оштетење и неовлашћено упадање у рачунарски систем", а 18 за "израду и употребу лажне платне картице". Динамика ових кривичних дела бележи континуирано повећање од 2017 године, као резултат раста безготовинског плаћања и употребе платних картица. У вези са кривичним делима "израда и употреба лажне платне картице", расветљено је седам случајева, са осам кривично пријављених починилаца. Посебно је занимљив случај у којем су два румунска држављанина, у периоду од 2017 године, поставили илегалну опрему на банкомате Комерцијалне банке, којом су прибављали податке од корисника и касније их злоупотребљавали за израду лажних платних картица. Додатно, у једном случају, починилац је успео да прибави банкарске податке са платне картице правног лица из Скопља и извршио 11 успешних трансакција на странским продајним местима.

Министарство унутрашњих послова Републике Македоније континуирано предузима активности на откривању злоупотреба интернета и друштвених мрежа, посебно са циљем спречавања ширења лажних вести, говора мржње и позивања на насиље. У оквиру ових активности, посебно су наглашене мере за детектовање, праћење и расветљавање кривичних дела повезаних са ширењем расистичког и ксенофобичног материјала, при чему су откривена 28 дела "угрожавања сигурности" и 16 дела "ширења расистичког и ксенофобичног материјала путем рачунарског система", са 25, односно 16 кривично пријављених починилаца.

Широка распрострањеност и лак приступ интернету, као и масовна употреба друштвених медија, платформи и апликација за онлајн комуникацију међу младом популацијом још од најранијег узраста, драстично повећавају ризик од сексуалне злоупотребе деце и ширења тржишта дечје порнографије. У 2020 години број кривичних дела из области сексуалне експлоатације деце

[12] https://mvr.gov.mk/Upload/Editor_Upload/%D0%93%D0%BE%D0%B4%D0%B8%D1%88%D0%B5%D0%BD%20%D0%B8%D0%B7%D0%B2%D0%B5%D1%88%D1%82%D0%B0%D1%98%202020.pdf

путем интернета бележи пад од 27,3%, односно регистрована су осам кривичних дела, од којих су четири дела „приказивање порнографског материјала детету", при чему су два расветљена и кривично су пријављена два извршиоца, затим два кривична дела „обљуба или друго полово дејство са дететом које није напунило 14 година", за које су кривично пријављена два извршиоца, као и два дела „производња и дистрибуција дечје порнографије" која су извршена од непознатих извршилаца. Ова врста инкриминација често подразумева слање фотографија и видео снимака са компромитујућим и експлицитним порнографским садржајем жртвама, њихово накнадно ширење, претње, уцене, телефонске позиве, као и слање порука с циљем заведивања на интимни сусрет са жртвама.

У делу рачунарских превара, у 2020. години бележимо пад од 75% у броју кривичних дела. Регистрована су само 3 кривична дела, која су извршена путем преваре при електронској уплати за изнајмљивање стана, подизању новчаних средстава са кредитних картица правног лица и пресретању e-mail комуникације између приватних фирми с циљем њихове преваре, усмеравања и уплате на другу банкарску рачуна.

У **2021** години[13] кривична дела из области рачунарског криминала бележе пораст од 6,3%, односно регистрована су 170 кривична дела. Извршењем ових инкриминација настала је материјална штета од више од 19,6 милиона денара, што је повећање од 56% у поређењу са 2020 годином. Предузете мере и активности резултирале су кривичним прогоном 114 извршилаца (112 физичких и два правна лица), а постигнута је ефикасност у расветљавању дела од више од 58%, што је повећање од више од 6% у поређењу са претходном годином. Најзаступљенија су дела извршена злоупотребом платних картица, при чему је регистровано укупно 83 кривична дела, што је смањење од 19% у односу на претходну годину. Најчешће се јавља кривично дело „оштећење и неовлашћено упадање у рачунарски систем" - 71 дело, која се најчешће извршавају путем крађе или пронађених изгубљених електронских банкарских картица грађана, као и искоришћавањем немара власника картица у заштити личних и банкарских података, након чега су извршиоци подизали новац са банкомата, плаћали рачуне, плаћали у трговинама, обављали плаћања путем интернета, аплицирали за онлајн кредите и користили веб платформе за игре на срећу. (карактеристичан је случај у којем је лице из Тетова, са привременим боравком у Немачкој, неовлашћено упало и пријавило се на кориснички профил туристичке агенције на друштвеној мрежи *„Facebook"*, након чега је извршило трансакцију са службене картице агенције која је била повезана са корисничким профилом). Регистровано је и 12 кривичних дела „израда и употреба лажне платне картице", од којих су, након предузетих мера, расветљена седам дела, а кривично је пријављено 10 извршилаца.

[13] https://mvr.gov.mk/Upload/Editor_Upload/Godisen%20izvestaj/Godisen-izvestaj-na-MVR-za-2021-godina-15_04_2022.pdf

Карактеристичан је случај у којем је кривично пријављено пет извршилаца који су, преко једног од пријављених, у својству запосленог у Јавном предузећу за државне путеве, прибавили податке са платних картица лица који су обавили плаћање путарине са платним картицама у периоду од августа 2019 до јуна 2020 године, након чега су из истих бројева картица, издатих од стране две домаће банке, слали новац више пута путем интернет сервиса „Paysend" и других финансијских сервиса, након чега су средства подигнута. На овај начин пријављени су стекли противправну имовинску корист од више од милион денара.

С обзиром на све веће коришћење интернета и појачану активност на друштвеним мрежама, у 2021 години изазов је био откривање злоупотреба на интернету и друштвеним мрежама с циљем спречавања ширења лажних вести, говора мржње, претњи, позива на насиље и слично. Ово је резултирало откривањем 30 кривичних дела „ширење расистичког и ксенофобичног материјала путем компјутерског система", за које је кривично пријављено 30 починилаца, као и 29 кривичних дела „угрожавање сигурности", за које је кривично пријављено 21 лице. Ове године, у односу на претходну, примећено је двоструко повећање кривичних дела „компјутерска превара". Регистровано је шест кривичних дела, од којих су два расветљена, а кривично су пријављена пет лица. Модус извршења ових кривичних дела је специфичан, што их чини тешким за откривање. Такође, ове године забележено је десетоструко повећање материјалне штете у односу на претходну, која износи више од 15,5 милиона денара. Посебан случај се односи на четири држављанина Мађарске који су привремено боравили у Великој Британији од августа до децембра 2020 године и више пута неовлашћено упали у електронску комуникацију између правног субјекта из Републике Македоније и страног правног лица из Лондона. Уз измену и прикривање компјутерских података, доставили су лажне фактуре, доводећи у заблуду правне субјекте, због чега је извршено четири уплата на различите рачуне у банкама у Великој Британији. На тај начин, пријављена лица су остварила противправну имовинску корист у износу од 15 милиона денара на рачун правног субјекта из Републике Македоније. Такође, запослени у јединици локалне самоуправе извршио је неовлашћен упад, измену и уношење лажних података у финансијску картицу пореског обвезника, док су друга кривична дела извршена путем преваре на основу уплата за изнајмљивање станова, куповину криптовалута и уплате новца лицима из Турске на основу наводне добити од награде.

Што се тиче сексуалне експлоатације деце путем интернета, у 2021 години забележен је пораст од 37,5% у броју регистрованих кривичних дела, са укупно 11 пријављених дела. Широка распрострањеност и лак приступ интернету међу грађанима, као и масовно коришћење друштвених мрежа, платформи и апликација за онлајн комуникацију од стране младе популације, олакшавају извршење ових криминалних активности. Пет кривичних дела односи се на „показивање порнографског материјала детету", при чему су четири

расветљена и кривично су пријављена четири починиоца, затим, четири кривична дела везана су за „производњу и дистрибуцију дечје порнографије“, за која су кривично пријављена пет лица, а такође су регистрована два дела „намамљивање детета на обљубу или друго полно дејство на детету које није напунило 14 година“, од којих је једно расветљено и кривично је пријављен један починилац. Ове инкриминације извршене су путем намамљивања малолетних лица на сексуалне активности, вршења обљубе, снимања и сподељивања путем друштвених мрежа, приказивања порнографских фотографија и видеа, као и путем постављања линкова са садржајем сексуалне експлоатације деце.

У **2022** години[14], кривична дела у области компјутерског криминала бележе раст од 68,8%, односно регистрована су 287 кривичних дела. Извршењем овог вида инкриминација причињена је материјална штета која се процењује на више од 15,7 милиона денара (око 240.000 евра) и бележи смањење од 20% у поређењу са 2021 годином. Предузете мере и активности резултирале су расветљавањем 180 кривичних дела из текуће године, као и додатних четири дела из претходних година, а мере кривичног прогона предузете су против 220 починилаца, чиме је постигнута ефикасност у расветљавању дела од 63%, што је за 5% више у односу на прошлу годину. По врстама, најбројнија су дела која су извршена злоупотребом платежних картица, регистровано је укупно 173 кривична дела, која су ове године повећана за 2,1 пута. Најзаступљеније кривично дело је „оштетавање и неовлашћено упадање у компјутерски систем“ – 138 дела. Она се најчешће извршавају неовлашћеним одузимањем раније пронађених или украдених платежних картица, неовлашћеним прикупљањем података са трансакцијских рачуна и картица, након чега починиоци врше подизање новца са банкомата, плаћање рачуна, плаћање у трговинама и онлајн куповину на различитим продајним местима. Регистровано је и 35 кривичних дела „израда и употреба лажне платежне картице“, од којих је расветљено 18, као и три дела из претходних година, а кривично је пријављено 37 лица. Карактеристични су случајеви које су извршила два лица из Скопља, од којих је једно лице, као запослени у маркету, 11 пута фотографисало платежне картице купаца мобилним телефоном, након чега су заједно са другим лицем неовлашћено плаћали рачуне за електричну енергију и допуњавали рачуне, стекавши имовинску корист већу од 530.000 денара. Сличан начин извршења преовладава и у другим случајевима, где су починиоци на неовлашћен начин прикупили податке са платежних картица оштећених и извршили електронска плаћања на више продајних места. Министарство унутрашњих послова је континуирано предузимало акције за мониторинг, откривање и санкционисање

[14] https://mvr.gov.mk/Upload/Editor_Upload/Godisen%20izvestaj/%D0%93%D0%BE%D0%B4%D0%B8%D1%88%D0%B5%D0%BD%20%D0%B8%D0%B7%D0%B2%D0%B5%D1%88%D1%82%D0%B0%D1%98_2022_%D0%9C%D0%92%D0%A0.pdf,

злоупотреба интернета и друштвених мрежа у смислу спречавања промовисања или подстицања мржње, дискриминације или насиља, као и угрожавања сигурности у погледу послатих порука или објављених садржаја на интернету. Ове активности резултирале су повећањем броја откривених кривичних дела за 32,2% у поређењу са 2021. годином. Регистрована су 51 кривична дела „ширење расистичког и ксенофобичног материјала путем компјутерског система“, против 51 починиоца, као и 27 кривичних дела „угрожавање безбедности“ са 20 кривично пријављених осумњичених.

У области компјутерских превара у 2022 години бележимо стабилизујући тренд у броју регистрованих кривичних дела, који остаје на истом нивоу као 2021. године. Годишња материјална штета је смањена на 1,1 милион денара. Регистрована су 6 кривична дела, од којих су три расветљена и три лица су кривично пријављена. Један од карактеристичних случајева обухвата бугарског држављанина који је, путем електронских порука са страног позивног броја, довео у заблуду оштећеног, обећавајући му наследство и, у више наврата, успео да изнуди новчана средства у износу од 570.000 денара. Такође, регистрован је случај у којем је шалтерски радник у АД „Македонска пошта“ приликом наплате рачуна од странаца, избацивао евиденцију из система и преписивао податке са рачуна других корисника, задржавајући новчана средства за себе. Једно кривично дело извршено је и од стране запосленог у правном субјекту који је брисао компјутерске податке, што је нанело штету од око 494.000 денара.

У области сексуалне експлоатације деце путем интернета, у 2022 години бележимо пораст од 27,3% у односу на 2021. годину, са укупно 14 регистрованих кривичних дела. Од ових, 8 дела су расветљена, а према 8 осумњичених је покренут кривични поступак. Шест од ових кривичних дела односи се на „приказивање порнографског материјала деци“, од којих су 5 расветљена и 5 осумњичених пријављено, а пет кривичних дела везаних за „производњу и дистрибуцију детске порнографије“, од којих су 2 расветљена и два починиоца пријављена. Регистрована су и три кривична дела „намамљивање деце на полове радње“, од којих је једно расветљено и један починилац је пријављен. Ова кривична дела извршена су путем комуникације са малолетницама на друштвеним мрежама, уз слање фотографија и видео снимака експлицитног сексуалног садржаја, креирање лажних профила на друштвеним мрежама са порнографским садржајем, слање порука о интимним сусретима, као и снимање видеа са сексуалним односима.

8. Закључак

Лични подаци су постали најскупља, али и најјефтинија роба у сајбер простору. Лични подаци постали су незаменљиви део развоја и употребе вештачке интелигенције, где служе и користе се као основа за обуку система вештачке интелигенције у препознавању образаца, побољшању тачности и

омогућавању персонализације која се користи у различитим индустријама. Приватност, заштита података и безбедност система, мрежа и података су међусобно зависни. Да би се заштитили корисници од оваквих сајбер претњи, неопходна је едукација како у образовном процесу у школама, тако и путем различитих кампања за онлајн безбедност и заштиту личних података, додатни савети и препоруке надлежних институција, као и друге мере обазривости и безбедности.

Компјутерски криминал представља дело које извршава стручан корисник рачунара, понекад назван „хакер“, који незаконито приступа или краде приватне информације компанија или појединаца. Према анализираним подацима, може се уочити да је у периоду од 2018 до 2022 године компјутерски криминал у континуираном порасту, са акцентом на 2022 годину, када је дошло до двоструког повећања. Најзаступљенији облик криминала је злоупотреба кредитних картица у циљу стицања материјалних средстава од корисника. Ово је последица појачане онлајн трговине и плаћања са кредитним и дебитним картицама на интернет страницама. Недовољна едукација и информираност корисника у онлајн простору доводи до нежељених ситуација као што су уношење личних података са картица на небезбедне и сумњиве интернет странице, отварање *Phishing email* линкова, СМС порука и слично.

Igor Kambovski, Ph.D., Full-time Professor
Faculty of Law, Goce Delcev University of Štip

Gjorgji Manchev, LLM, Ph.D student
Faculty of Law, Goce Delcev University of Štip

PROTECTION OF PERSONAL DATA IN CYBER SPACE WITH SPECIAL REFERENCE TO CYBER CRIME IN THE REPUBLIC OF NORTH MACEDONIA IN THE PERIOD FROM 2018 TO 2022

Summary

Rapid development of information technologies and their increasing sophistication make the fight against criminal activities in the field of computer crime increasingly difficult and complicated. The most common forms of theft and fraud involving the misuse of information and communication technologies include: violation of personal data, fraud with credit cards and securities, identity theft, unauthorized use and usurpation of computer services, as well as computer

espionage. One of the biggest challenges in the modern digital environment is the protection of privacy and personal data, especially in the context of increasingly applied artificial intelligence. Special emphasis is placed on respecting the principles of personal data protection during the development of artificial intelligence, on the right of an individual to be exempted from the automated decision-making process, as well as on the protection of rights guaranteed by the Personal Data Protection Act. In the framework of this work, an analysis and investigation of the level of cybercrime in the Republic of North Macedonia in the period from 2018 to 2022 was carried out. The number and type of crimes in the area of computer crime, possible crimes, as well as estimated material damage caused as a result of a cyber attack are shown. The research was conducted on the basis of official data obtained from the Ministries of Internal Affairs through their annual work reports.

Key words: *personal data, cybercrime, artificial intelligence, fraud.*

Литература

Тупанчески, Н., *Економско казнено право*, Скопје, 2015.

Камбовски, И., Стојановска, Е., *Истражување за ефектот на новите технологии, со особен фокус на вештачката интелигенција, врз човековите права на интернет и развивање етички стандарди за заштита на човековите права на интернет при автоматско донесување одлуки*-електронско издање, Фондација за интернет и општество Метаморфозис – Скопје, 2024, https://metamorphosis.org.mk/wp-content/uploads/2024/05/istrazhuvanje-za-efektot-na-novite-tehnologii-so-osoben-fokus-na-veshtachkata-inteligencija-vrz-chovekovite-prava-na-internet.pdf

Закон за кривична постапка (Сл. весник на Република Македонија, бр. 150/2010; бр. 100/12 и бр.198/18).

Закон за заштита на личните податоци (Сл. весник на Република Северна Македонија, бр. 42/20)

Зрлевски, М., Андонова, С., Милошевски, В., *Прирачник за компјутерски криминал*, Скопје, 2014. https://www.osce.org/files/f/documents/1/3/121224.pdf

The AI Act, https://artificialintelligenceact.eu/

https://www.coe.int/en/web/freedom-expression/guide-to-human-rights-for-internet-users

https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng,

https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

https://ipmall.law.unh.edu/sites/default/files/hosted_resources/CyberCrime/roboslo.pdf

https://www.britannica.com/topic/cybercrime

https://www.fbi.gov/investigate/cyber

https://mvr.gov.mk/Upload/Editor_Upload/Godisen%20izvestaj%202018.pdf

https://mvr.gov.mk/Upload/Editor_Upload/%D0%9E%D0%9A%D0%A0%D0%90/%D0%93%D0%BE%D0%B4%D0%B8%D1%88%D0%B5%D0%BD%20%D0%B8%D0%B7%D0%B2%D0%B5%D1%88%D1%82%D0%B0%D1%98%202019.pdf
https://mvr.gov.mk/Upload/Editor_Upload/%D0%93%D0%BE%D0%B4%D0%B8%D1%88%D0%B5%D0%BD%20%D0%B8%D0%B7%D0%B2%D0%B5%D1%88%D1%82%D0%B0%D1%98%202020.pdf
https://mvr.gov.mk/Upload/Editor_Upload/Godisen%20izvestaj/Godisen-izvestaj-na-MVR-za-2021-godina-15_04_2022.pdf
https://mvr.gov.mk/Upload/Editor_Upload/Godisen%20izvestaj/%D0%93%D0%BE%D0%B4%D0%B8%D1%88%D0%B5%D0%BD%20%D0%B8%D0%B7%D0%B2%D0%B5%D1%88%D1%82%D0%B0%D1%98_2022_%D0%9C%D0%92%D0%A0.pdf