

Александра З. Илић¹
Универзитет у Београду, Факултет безбедности
Београд (Србија)

Ивана П. Бодрожић²
Криминалистичко-полицијски универзитет
Београд (Србија)

Младен М. Милошевић³
Универзитет у Београду, Факултет безбедности
Београд (Србија)

343.983:004

Преједни научни рад

Примљен 22/02/2025

Прихваћен 07/03/2025

doi: [10.5937/socpreg59-56973](https://doi.org/10.5937/socpreg59-56973)

ДРУШТВЕНА РЕАКЦИЈА НА КРИМИНАЛИТЕТ У ДИГИТАЛНОЈ ЕРИ – ЗНАЧАЈ ДИГИТАЛНЕ КРИМИНОЛОГИЈЕ И КРИВИЧНОГ ЗАКОНОДАВСТВА

Сажетак: Савремени живот заснован на дигитализацији утиче у значајној мери на карактеристике криминалитета који се налази у фокусу дигиталне криминологије као специфичног приступа у проучавању криминалног феномена у дигиталној ери. Имајући у виду комплексност феномена у раду се истиче важност сагледавања поменуте проблематике у свим димензијама. Посебно се издваја перспектива жртве због важности превенције виктимизације у дигиталном простору, а која је уско повезана са питањем адекватне кривичноправне реакције. Аутори указују на значај континуираног праћења резултата истраживања о стању дигиталног криминалитета, посебно у контексту препознавања и инкриминисања нових облика криминалног понашања. У дигиталној ери се трансформише и друштвена реакција на криминалитет, у оба своја вида: неформалном и формалном. Анализирајући поједине аспекте оба облика друштвене реакције, аутори указују како на позитивне тако и на негативне стране те трансформације.

Кључне речи: друштвена реакција, дигитални криминалитет, дигитална криминологија, кривично законодавство, кривичноправна заштита

УВОДНА РАЗМАТРАЊА

Дигитализација је присутна у свакодневном животу људи у различитим сегментима функционисања, у приватном, али и у пословном окружењу. Налазимо се у дигиталној ери која обликује физиономију различитих друштвених појава.

¹ aleksandra.ilic@fb.bg.ac.rs; <https://orcid.org/0000-0001-7298-2347>

² ivana.bodrozic@kpu.edu.rs; <https://orcid.org/0000-0001-5010-7832>

³ mladen.milosevic@fb.bg.ac.rs; <https://orcid.org/0000-0001-8978-3475>

Доступност многобројних дигиталних алата и њихово стално унапређивање, али и присутност великог броја људи у дигиталном простору, представљају факторе који значајно утичу на карактеристике савременог криминалног феномена. Можемо се и даље крити иза оквира онога што представља традиционални приступ анализи криминалног феномена, али чињеница је да је дошло до дигиталног односно „big data” заокрета у криминологији. Дигитални медијуми, како они који се сматрају „тврдим” односно „материјалним”, тако и ови други, „меки” или „нематеријални”, имају значајнији учинак, односно улогу, у структури и доживљају друштвеног живота и односа међу људима (Smith, Bennett, Chan, 2017, стр. 263).

Потпуно разумевање свих новина у дигиталној сфери и њихов утицај на начин испољавања криминалног феномена подразумева свеобухватну анализу свих битних чинилаца који га обликују. Није довољно само да се позабавимо профилем или скупом карактеристика типичних учинилаца дигиталних кривичних дела, већ је неопходно уврстити перспективу жртве, али и размотрити друштвену реакцију на криминалитет у контексту дигиталне ере у којој се налазимо. Живимо у периоду веома развијених медија, информације се брзо преносе и у одређеним случајевима извршења појединих кривичних дела изазивају бурну реакцију јавности која захваљујући истим тим медијима има моћ да изврши утицај на поступање органа гоњења. То с једне стране отвара питање граница утицаја јавности на рад тих органа, али и осликава реалност у којем се налази савремени свет, односно начин на који он функционише.

Традиционални оквир бављења криминалним феноменом није више довољан, јавља се потреба за неким новијим приступима и објашњењима, што би имало не само теоријски већ и практични значај. Чини се да је више него икада потребна сарадња свих кривичних дисциплина, посебно криминологије и кривичног права, како би се на оптималан начин одговорило изазовима сузбијања онога што ћемо у овом раду називати дигиталним криминалитетом. Имајући у виду сложеност тог задатка, чини се да је најбоље све његове аспекте објединити у оквиру посебног приступа у криминологији који ћемо назвати дигиталном криминологијом.

ПОВЕЗАНОСТ КРИМИНОЛОГИЈЕ И КРИВИЧНОПРАВНЕ ЗАШТИТЕ У ДИГИТАЛНОЈ СФЕРИ

Потреба за развојем и бављењем посебним криминолошким приступом који би се заснивао на препознавању и свеобухватној анализи утицаја дигиталне технологије у различитим аспектима испољавања криминалног феномена, искристалисала је нови правац у криминолошкој мисли, који се последњих година превасходно назива дигитална криминологија (Smith, Moses, Chan, 2017; Stratton, Powel, Cameron, 2016). Неки други аутори више користе термине сајбер или кибер криминологија (Grabosky, 2016; Dupont, Whelan, 2021) па чак и израз компјутерска криминологија (Berk, 2013; Brantingham, 2011).

Криминологија као динамична научна дисциплина и кривична наука бави се мултидисциплинарним и интердисциплинарним изучавањем криминалног феномена као једне сложене појаве састављене од неколико међусобно повезаних елемената: злочин, учинилац, жртва, криминалитет и реакција друштва на криминално

понашање (Ignjatović, 2019, str. 15, 16). У оквиру свог бављења поменутом целином предмета, односно неких њених елемената, криминолошко проучавање може имати три димензије: феноменолошку, етиолошку и виктимолошку, које, редом наведене, подразумевају анализу појавних облика и карактеристика различитих облика криминалитета, затим истраживање њихове узрочности⁴ односно прецизније условљености и на крају перспективу жртве.

У свом развоју криминологија се суочавала са низом изазова попут покушаја да се као целина распарча на низ криминолошких дисциплина у зависности од тога шта је био основни критеријум те поделе, попут утицаја монокаузалистичког приступа у објашњењу узрочности криминалитета који је превасходно доминирао у раним фазама развоја криминолошке мисли у оквиру позитивистичке оријентације.⁵ Превазилажењем, као једино могућег и легитимног, позитивистичког оквира у контексту бављења објашњењем криминалног феномена и укључивањем новијих теоријских перспектива, теорија друштвене реакције и новијих криминолошких теорија, дошло се и до другачијег приступа у развоју криминолошких дисциплина које стављају акценат на актуелне тенденције у вршењу кривичних дела односно савремени оквир решавања проблема криминалитета где, између осталих чинилаца, све више доминира дигитализација у различитим облицима.

Иако се све дешавало успорено, постајало је с временом јасно да се традиционални приступи проучавања криминалног феномена морају прилагођавати промењеним условима живота који су донели промене и у контексту извршења већ постојећих, добро познатих кривичних дела, али су довели и до појаве неких нових, до тада потпуно непознатих форми криминалног деловања. „Основна социолошка теза која се испољава у оквиру усложњавања дигиталног доба је да паралелно са незаустављивим процесом развоја дигитализације у свим сегментима живота сведочимо о истој таквој убрзаној мутацији од аналогних до електронских и дигиталних облика девијантног понашања и криминалитета и то на глобалном плану” (Sandywell, 2010, str. 42).

Једно од основних питања, које се мора поставити у склопу разматрања предмета проучавања дигиталне криминологије, јесте како ћемо дефинисати дигитални злочин односно дигитално кривично дело. Анализа литературе о кривичним делима учињеним коришћењем савремене технологије показује да се не даје потпуна слика и дефиниција оних кривичних дела која се врше у области дигиталне технологије или

⁴ Иако је уобичајено да се у свим аспектима живота, али и научног бављења различитим феноменима, користи термин „узрочност”, односно да свака појава има свој узрок/е, то оставља утисак да на одређену појаву, без обзира на њене конкретне карактеристике, делују одређени фактори чији се утицај може тачно измерити. Тај ниво егзактности и прецизности ипак је резервисан за научне дисциплине у којима се може остварити такав закључак, попут природних и техничких наука, док се у наукама о човеку и друштву, каква је и сама криминологија, не могу и не смеју извлачити такви закључци. Можемо говорити само о вероватноћи деловања неког чиниоца, јачем или слабијем утицају у конкретном случају.

⁵ Бављење узрочношћу по узору на егзактне научне дисциплине попут различитих природних наука, довело је до тога да су поједини аутори, попут Ломброза, истицали тачно одређене факторе криминалног понашања као узрочнике вршења кривичних дела, што је у једном тренутку довело до одвајања ужих дисциплина у оквиру криминологије, које су се бавиле само тим изолованим чиниоцима и њиховим утицајем на вршење кривичних дела.

коришћењем дигиталне технологије, што потврђује и прилично разуђена терминологија која се може пронаћи: „електронски криминал“, „компјутерски криминал“, „злочин учињен коришћењем рачунарске технологије“, „злочин високе технологије“, „сајбер криминал“ итд. (Rakhamnova & Pinkevich, 2020, стр. 195). Поједини аутори користе и термин „интернет криминал“ (Furnell, 2010; Jewkes & Yar, 2010). Интернет, веб (Web) и сајбер простор се описују као „дивљи запад“ нових облика криминалитета организованих на планетарном нивоу (Sandywell, 2010, стр. 39). Место где се чине дигитални злочини је виртуелно окружење, паралелни универзум, и у том смислу за само извршење конкретних дела користе се компјутерски подаци, дигитални системи, или друштвени медији (Rakhamnova & Pinkevich, 2020, стр. 195).

Предацавање многобројних животних активности у виртуелни простор, односно њихово модификовање под утицајем незаустављивих процеса у оквиру дигиталног доба, променило је човека па самим тим и оне појединце који су изабрали пут вршења кривичних дела. Неки постојећи учиниоци су се прилагодили, односно прилагођавају се стално измењеним околностима. Исто тако, нове околности су произвеле неке нове учиниоце који су, можда захваљујући дигиталном оквиру одвијања живота генерално, одабрали да крену путем кршења закона. „Преступник гротескно деформише свој прави имиџ када се представља на мрежи, мења нормалне интеракције између људи и, последично, класичне обрасце криминала, на такав начин да постаје неопходно значајно модификовати постојеће криминолошке и догматске категорије када се анализирају иста кривична дела“ (Agustina, 2015, стр. 39).

С тим у вези, један од најважнијих изазова дигиталне криминологије је упознавање с карактеристикама учинилаца кривичних дела чије се криминалне активности превасходно заснивају на тој дигитализацији. Имајући у виду разноврсност и сложеност криминалне типологије, криминалних мотива као и профила учинилаца у дигиталном простору, поједини аутори праве разлику између економског, социјалног и политичког сајбер криминалитета (Agustina, 2015, стр. 49). Досадашња криминолошка сазнања, иако и даље значајна, морају да буду употпуњена савременим оквиром промишљања о овој проблематици.

Поједини аутори истичу да криминологија мора развити дигитални специјализам који истражује вишеслојну улогу коју имају дигиталне технологије као интерсекционални и трансформативни медији у области криминала и правде (Smith et al., 2017). Посебан замах у развоју идеје о новој грани криминологије наступио је захваљујући ширењу интернета као глобалне мреже за комуникацију и размену информација. Тако је Јашанкар (Jaishankar) истакао да је развој интернета, поред поменутих промена у сфери међуљудске комуникације, довео и до настанка новог облика криминалитета за чије изучавање је неопходно развити нову криминолошку грану. Та грана би кроз мултидисциплинарни приступ интегрисала сазнања различитих научних дисциплина које би могле бити позване да из свог угла дају допринос разумевању злочина који се одвијају у сајбер простору, али и њиховом утицају на физички простор (Jaishankar, 2007; наведено према Ignjatović, 2019, стр. 96). Подразумева се да је криминолошки приступ мултидисциплинаран али са развојем идеје о сајбер или дигиталној криминологији, на списку већ препознатих научних дисциплина које имају шта да пружи у контексту анализе условљености злочина, нашле би се и неке нове научне дисциплине, попут наука о интернету, односно Информатика и Рачунарство.

Смит (Smith), Бенет (Bennett) и Чен (Chan) указују на постојање емпиријске, концептуалне и епистемолошке потребе да криминологија, односно криминологи, пружи објашњења средине у којој дигиталне технологије све више обављају кључне улоге. То подразумева не само контекст њиховог коришћења у сврху извршења кривичних дела већ и као својеврсних плурализованих платформи кроз које се свет злочина свакодневно презентује јавности. Последица тога је мобилисање заједница и афективно реаговање на криминална понашања, криминалне догађаје, али и сличне реакције органа формалне контроле који предузимају званичне мере контроле криминала (Smith et al., 2017, str. 269).

Повезаност технолошког развоја и криминалитета се може пратити кроз одређене фазе, које су истовремено и етапе у развоју криминолошког проучавања дигиталног криминалитета. Условно се тај комплетан период може поделити у три основне фазе, односно временске оквири: „предвећ” ера током 80-их до раних 90-их година 20. века, ера „глобалног веба” од 90-их година 20. века до раних 2000-их, и ера „друштвеног веба” од средине 2000-их до данас (Stratton et al., 2017, str. 19).

Криминологија је у оквиру „предвећ” ере препознала околност да раширена доступност рачунара и електронски складиштених података, у комбинацији са интерно умреженим радним станицама и dial-in везама, чини да су владе, корпорације и образовне институције постале подложније новим облицима криминала путем злоупотребе технологије (Stratton et al., 2017, str. 19). Током тог периода је постало јасно и да је поменути технолошки развој пружио нове злочиначке могућности радозналим адолесцентима који су у доколици развили и раширили компјутерске вирусе и црве чиме су изазвали поремећај дигиталних система (Dupont & Whelan, 2021, str. 78–79).

Током 90-их година 20. века, са развојем компјутерске технологије и појавом интернета, криминологија се почела, у оквиру својих истраживања, бавити проблематиком компјутерског и сајбер криминала што је подразумевало анализу онога што се из данашње перспективе може назвати конвенционалним компјутерским криминалитетом. Међутим, процес дигитализације који се убрзано развија, утиче и на експанзију и разноврсност вршења кривичних дела у дигиталном простору, односно кроз употребу достигнућа дигиталне технологије. Појава рачунарске мреже, уређаја, апликација и онлајн платформи обликовала је све аспекте људске активности што је иновативним преступницима отворило простор за нове прилике за вршење кривичних дела (Dupont & Whelan, 2021, str. 79).

Стратон (Stratton), Пауел (Powell) и Камерон (Cameron) предлажу проширење традиционалног теоријског оквира компјутерске односно дигиталне криминологије, заснованог искључиво на теоријама које служе објашњењу конвенционалног криминалитета⁶. Истиче се значај експанзије и ревитализације криминолошке мисли која би могла бити инспирисана кроз анализу развоја друштвених, критичких и технолошких

⁶ Традиционални теоријски оквир у криминологији заснива се превасходно на позитивистичким теоријама које се примарно баве факторима криминалитета, односно објашњењу узрочности злочина попут различитих социолошких теорија: теорија о учењу, теорија друштвеног притиска или теорија диференцијалне асоцијације, употпуњене са неким новијим приступима у оквиру новијих криминолошких теорија, попут теорије рационалног избора или теорије рутинске активности.

теорија изван саме криминологије односно традиционално сродних дисциплина⁷. С тим у вези, указује се на важност дебате унутар саме криминологије како би се изашло из конвенционалних оквира бављења сајбер криминалом ка ширем контексту истраживања злочина и правде у дигиталном добу (Stratton et al., 2017, стр. 18).

Посебан сегмент у којем би било пожељно да дигитална криминологија оствари свој пун потенцијал је проблематика кршења људских права кроз повреду права на приватност у дигиталном простору и заштити личних података у вези са тим. Игњатовић тако ставља замерку на Јашанкарово објашњење о домаћају сајбер криминологије у којем управо изоставља тај сегмент (Ignjatović, 2019, стр. 96). Дигитални или сајбер злочини често укључују кршење личних и осетљивих информација, што доводи до забринутости за приватност и заштиту података. У том сегменту би се могао пронаћи простор и за интензивнију сарадњу криминологије и кривичног права где би емпиријска криминолошка анализа различитих модалитета кршења људских права у дигиталном простору омогућила даљи развој кривичноправне регулативе кроз потпуније и прецизније дефинисање одговарајућих инкриминација.

Један од горућих проблема који тражи бољу кривичноправну реакцију, који је као феномен препознат на глобалном плану, тиче се осветничке порнографије. Посебно се истиче забринутост због одсуства одговарајућег законског оквира у вези са тим, упркос томе што се у различитим дебатама то препознаје као битан задатак (Walker & Sleath, 2017). С тим у вези се јавља и проблем прецизног дефинисања феномена, што отежава систематично прикупљање података о размерама виктимизације, али је чињеница да је реч о распрострањеној појави.

Виктимолошка димензија дигиталног криминалитета и кривичноправна заштита

Питање виктимолошке димензије дигиталног криминалитета завређује посебну пажњу. С обзиром на то да проучавање учинилаца и њихових карактеристика не може бити коначно ако се не укључи перспектива жртве, онда је јасно колико сложени задатак представља разматрање свих поменутих елемената криминалног феномена у једном значајно другачијем оквиру него пре. Имајући у виду присутност већине људи у дигиталном простору и самим тим подложност исте те већине различитим злоупотребама, може се рећи да је виктимолошка перспектива дигиталне криминологије веома комплексна.

Иако смо мишљења да је свеобухватна анализа криминалног феномена најбољи могући пут у разумевању свих појединачних перспектива, па и виктимолошке, можда би вредело размишљати и о развоју посебног правца унутар виктимологије, тзв. дигиталне виктимологије која би се посебно бавила појавним облицима виктимизација у дигиталном простору, карактеристикама жртава као и последицама по

⁷ Углавном се истиче спектар дисциплина које су традиционално сродне криминологији: психологија, социологија, медицина, биологија, антропологија, право, економија и друге. Ипак, изазов проучавања криминалитета у дигитално доба захтева укључивање и другачијих промишљања.

жртве таквих облика криминалног деловања. Та идеја није свакако нова, поједини аутори говоре о сајбер виктимологији (Cyber Victimology) (Jaishankar, 2020; Debarati, 2021) и њеном значају. Даље развијање те основне идеје подразумева анализу виктимизације у сајбер простору, која има своје посебне карактеристике које се у одређеној мери разликују од виктимизације у физички стварном простору. Сајбер виктимизација се уклапа у категорију контекстуалне рањивости, односно перспективу која се концентрише на интеракцију жртве са „виктимогеним окружењем“ као кључним фактором (Agustina, 2015, str. 39) која своје базично теоријско објашњење проналази у теорији рутинске активности која подразумева постојање три битна елемента: мотивисане преступнике, погодне мете и одсуство оспособљених заштитника од преступа (Cohen & Felson, 1979, наведено према: Ignjatović, 2019, str. 88). С обзиром на неминовну изложеност појединаца у виртуелном простору и подложност различитим облицима виктимизације, и с тим повезане веома мотивисане преступнике, акценат сајбер или дигиталне виктимологије би требало да буде побољшање заштите од сајбер виктимизације кроз увођење одговарајућих процедура у сајбер простору које воде ка бољем остваривању превенције.

Кад је реч о превенцији сајбер или дигиталног криминалитета и самим тим бољој контроли рањивости у виртуелном простору, изузетно важну превентивну улогу имају носиоци друштвене реакције на криминалитет, у оба своја облика испољавања, неформалном и формалном.

НЕФОРМАЛНА И ФОРМАЛНА ДРУШТВЕНА РЕАКЦИЈА НА КРИМИНАЛИТЕТ У ДИГИТАЛНОЈ ЕРИ

Друштвена реакција на злочин и криминалитет се може испољити, с једне стране, у неформалној реакцији друштвене заједнице, а с друге подразумева формалну реакцију на исте појаве, односно тиче се активности свих органа задужених за сузбијање криминалитета чије је деловање јасно и прецизно регулисано у одговарајућем законском оквиру.

Процес дигитализације донео је одређене промене у начину испољавања како неформалне тако и формалне реакције на криминалитет и задатак дигиталне криминологије је да расветли, колико је могуће, специфичности како једног тако и другог облика реаговања, уочи предности и недостатке „дигитализоване“ реакције и истакне их у дебатама које би се бавиле том проблематиком.

Посматрајући из угла неформалне реакције друштва на злочин и криминалитет, односно свих оних механизма којима друштво подстиче своје чланове на конформизам⁸ (Ignjatović, 2019, str. 16), у савременим оквирима постоји пуно могућих начина како се та неформална реакција остварује коришћењем средстава дигиталне технологије.

Данас је постало уобичајено да се све снима и да се готово у реалном времену поставља на различите дигиталне платформе и друштвене мреже што се потом брзином светлости шири захваљујући медијима. Међу тим снимцима се налазе и они који потенцијално указују на нечије противправно понашање. Реакција грађана која

⁸ Конформизам је прихватање општепотврђених и прихваћених норми понашања.

потом уследи има карактер неформалне друштвене реакције којом се изражава бес, љутња, прекор због учињеног дела, али њен основни и крајњи циљ је активирање органа формалне контроле у чијој надлежности се налази предузимање одговарајућих корака како би се иницирао и спровео формални механизам утврђивања евентуалне одговорности појединаца. Ипак, такав вид реакције јавности неретко представља манифестацију моралне панике као појаве која се више деценија описује у криминолошкој литератури (Cohen, 1972; Goode & Ben-Yehuda, 2009; Ilić, 2017; Tompson, 2003) и која се превасходно повезује са активношћу медија. Морална паника укратко подразумева пренаглашену реакцију јавности на одређене појаве које се перципирају као претња установљеном систему вредности, одређују се јасни и прецизни носиоци те претње, тзв. непријатељи друштва (folk devils) и тражи брза и ефикасна реакција доносилаца одлука, односно оних механизма који се могу готово тренутно активирати и деловати. Та брза реакција најчешће није најбоље решење јер у сфери кривичноправног реаговања и из угла циљева кажњавања најважнији аспект је и даље превенција.

Без обзира на многе негативне стране, најважнији облик неформалне реакције на криминалитет заснива се на улози медија. Свеprisутност различитих медијских форми у свакодневном животу је потврда да се сви важни друштвени процеси региструју од стране медија и изазивају одређену реакцију јавности. Неформална друштвена реакција подразумева и притисак јавности у вези са одређеним криминално-политичким питањима. Сведоци смо да се врло често код нас доносе новеле у области кривичног законодавства, уколико се у јавности створи утисак да су одређене измене у том смислу неопходне, како би се нпр. смањила стопа неког криминалитета, најчешће у сфери насилничког (попут кривичних дела против полне слободе или у случају насиља у породици), па се у том смислу пооштравају прописане казне или се уносе неке измене у општем делу кривичног законодавства.

Имајући у виду такву савремену тенденцију, задатак дигиталне криминологије је да истражи у коликој мери јавност показује заинтересованост за уношење одређених измена у сфери кривичноправне заштите права на приватност и заштите личних података у дигиталној сфери. С тим у вези, још једно важно питање је и колико је развијена свест грађана о размерама и карактеристикама дигиталних злочина и да ли се довољно чини у погледу едуковања шире јавности о свим потенцијалним ризицима који постоје у виртуелном свету.

Полазећи од првог циља, задатак криминолога у оквиру дигиталне криминологије је да у складу са правилима „криминологије производње вести” (Barak, 1994) допринесе скретању пажње јавности на значај континуираног унапређивања кривичноправне регулативе у овој области (за разлику од неких других области где се претерало са интервенционизмом), с обзиром на њену очигледну динамичност. Усклађивање домаћег кривичног законодавства са неким најважнијим међународним документима у тој области је важан корак у хватању укоштац са изазовима дигиталног криминалитета, посебно у сфери заштите података о личности као важном аспект приватног живота (Milošević, 2022, стр. 64). С тим у вези, треба истаћи да су одредбе кривичног дела неовлашћено прикупљање личних података из члана 146. Кривичног законика („Службени гласник РС”, бр. 85/2005, 88/2005 – испр., 107/2005 – испр.,

72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 i 94/2024) усклађене са Општом уредбом о заштити података о личности ЕУ (General Regulation [EU] 2016/679 of the European Parliament and the Council of Europe)⁹ која нема само локални већ превасходно глобални значај.

Други важан задатак „дигиталног криминолога” би подразумевао едукацију шире јавности о феноменолошким, етиолошким и виктимолошким карактеристикама дигиталног криминалитета како би се подизала свест о присутности и размерама тог феномена, али и оспособљавали грађани да боље препознају опасности које вребају у дигиталном окружењу. Чињеница је да многи грађани својевољно, путем интернета, омогућавају приступ својим личним подацима и тиме стварају погодно тло за различите злоупотребе и манипулације (Mandić, Putnik, Milošević, 2017). С друге стране, неки облици недозвољеног понашања у дигиталном простору нису довољно препознати у свести људи, али ни у кривичним законодавствима, попут поменуте осветничке порнографије, јер је значајно присутан став који окривљује жртве и подржава стереотипна уверења, а то све делује као препрека делотворној законодавној акцији (Harper, Smith, Fido, 2022, str. 778).

Савремени оквир сузбијања различитих облика криминалитета кроз активности органа формалне социјалне контроле подразумева, између осталог, и примену одређених дигиталних инструмената који олакшавају и убрзавају поједине процесе у односу на ранији период. Та констатација важи за све поменуте органе, како полицију тако и тужилаштво, али и за судове. Такође, не сме се заборавити ни значај дигитализације у оквиру система извршења кривичних санкција, посебно када је у питању систем извршења кривичних санкција заводског карактера. Без амбиције да се на овом месту поброје сви могући облици дигитализације на којима се заснивају активности органа формалне контроле, идеја је да се укаже на неке најосновније аспекте примене дигитализације у реализацији формалне реакције на злочин и криминалитет.

Дигитализација несумњиво олакшава рад органа формалне контроле што се може манифестовати нпр. у полицијском раду како проактивном тако и реактивном, попут ситуација када је потребно пронаћи осумњичена лица. У свакодневном животу, у многобројним активностима, остављамо неки дигитални траг што омогућава поменутиим органима да применом својих овлашћења дођу до информације о лицу/има с циљем лишења слободе или позивању ради сведочења, односно генерално у сврхе откривања и доказивања кривичних дела. Један од сегмената коришћења дигиталних алата од стране органа гоњења односи се на прогнозирање кретања криминалитета и активности појединих група па чак и конкретних појединаца. Критичари такве праксе тврде да превише ослањање на предиктивне алгоритме може угрозити претпоставку невиности, због чињенице да би појединци могли бити предмет појачаног надзора или чак хапшења на основу предвиђања њихове вероватноће да ће учинити злочин. С тим у вези, постоје примери где предиктивни дигитални полицијски алати нису успели да испуне неопходне стандарде неутралности, што доводи до забринутости у погледу легалности и етичности поступања (Matić Bošković, 2024, str. 484).

⁹ Општа уредба је усвојена 27. априла 2016. године и тиче се заштите физичких лица у односу на обраду података о личности, и о слободном кретању таквих података, као и стављању ван снаге Директиве 95/46/ЕЗ.

Простор у којем се несумњиво може користити дигитализација у пракси органа формалне контроле тиче се развоја дигиталне форензике која своју примену посебно налази у сфери сузбијања дигиталног односно високотехнолошког криминала како је то, у складу са позитивноправном терминологијом, дефинисано у члану 2. Закона о организацији и надлежности државних органа у сузбијању високотехнолошког криминала („Službeni glasnik RS“, br. 61/05, 104/09, 10/23 i 10/23 – dr. zakon¹⁰). Високотехнолошки криминал је још само један назив за разноврстан спектар кривичних дела који подразумева коришћење дигиталне технологије (Bodrožić, 2013). То су кривична дела за чије сузбијање је неопходно установити посебну организацију надлежних органа гоњења¹¹. Свакако активност посебно установљених служби и одељења у оквиру постојећих органа гоњења не може се замислити без унапређења посебног, дигиталног, вида форензичке праксе. Поменућемо само неке од разлога зашто је то тако: „може се рећи да готово да не постоји ниједна већа организација на свету која није претрпела компромитовање свог система захваљујући нападима, затим нажалост системи за детекцију напада на систем и антивирусни програми нису решили безбедносне проблеме али и околност да постоји велики број умрежених рачунара намењених дистрибуцији нелегалних садржаја и пиратерији” (Korać, Prlja, Diligenski, 2016, стр. 12).

Задатак дигиталне криминологије би превасходно требало да буде анализа колико примена дигитализације у различитим аспектима функционисања органа формалне социјалне контроле омогућава бољу ефикасност у раду поменутих органа уз оствареност принципа на којима се заснива поступање са лицима која се појављују у кривичном поступку, а посебно оних принципа који имају заштитну улогу. Прикупљање и коришћење дигиталних доказа покреће многа важна питања која се превасходно тичу заштите приватности и индивидуалне слободе појединаца (Stratton et al., 2016, стр. 26).

С друге стране, уколико је епилог поступка изрицање неке кривичне санкције, онда се отвара питање примене дигитализације у извршењу појединих кривичних санкција, при чему акценат не треба примарно да буде на корисности коју дигитализација доноси систему извршења кривичних санкција као таквом, већ како дигитализација помаже осуђеницима у процесу остваривања сврхе извршења односно реализацији циља кажњавања. Примера ради, остваривање ресоцијализације као сврхе извршења казне затвора се у савременим оквирима не може замислити без увођења дигитализације. То је посебно битно због потребе прилагођавања затвореника условима дигитализованог живота на слободи, али и ради ефикаснијег деловања на

¹⁰ Високотехнолошки криминал представља вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику. Под производима у електронском облику посебно се подразумевају рачунарске програми и ауторска дела која се могу употребити у електронском облику.

¹¹ Служба за борбу против високотехничког (очигледно термиолошка грешка законодавца) криминала у оквиру Министарства унутрашњих послова, Посебно одељење за борбу против високотехнолошког криминала у оквиру Вишег јавног тужилаштва и Одељење за борбу против високотехнолошког криминала у оквиру Вишег суда у Београду у првом степену.

чиниоце криминалног понашања који су довели до чињења дела (Плић, 2024). Такође, не треба занемарити ни значај дигитализације као вид помоћи осуђеницима приликом остваривања неких њихових права. У случају немогућности реализације непосредног контакта осуђеника са члановима породице то се може надоместити употребом различитих дигиталних помагала што доприноси јачем ресоцијализирајућем ефекту на осуђенике (Плић & Бановић, 2022, стр. 191–194) или у случају остваривања права осуђеника на образовање (Barros, Monteiro, Leite, 2023).

ЗАКЉУЧНА РАЗМАТРАЊА

Без обзира на све предности дигиталне технологије у савременом свету и оптимистична очекивања да ће она превасходно представљати решење за оскудицу знања и препреке у слободном изражавању (Vajdijantan, 2018, стр. 33), никако не смемо занемарити озбиљне ризике који нас вребају у развијеном дигиталном простору. Иако су нам, захваљујући разним дигиталним алатима, доступне многе информације о поменутих ризицима, због сталног боравка у дигиталном свету нисмо их довољно свесни, о чему говори чињеница да су дела која можемо сврстати у дигитални криминалитет у сталном порасту.

Задатак дигиталне криминологије је да препознаје нове али и модификоване постојеће облике криминалног понашања који се развијају у измењеним условима функционисања савременог дигиталног друштва. Препознавање тих образаца свакако није довољно уколико то не прати с једне стране одговарајућа кривичноправна реакција односно нормативно препознавање понашања која би требало инкриминисати. Иако генерално не треба претеривати са кривичноправном интервенцијом, у овој области је та активност и те како пожељна како би се правовремено и адекватно одговорило на изазове дигиталног криминалитета. С друге стране, учовање одступајућих понашања у дигиталном простору треба да прати истовремена едукација грађана у вези са опасностима које вребају у том простору и предузимање адекватних мера заштите, односно превенције, како би се ризик од виктимизације свео на најмању могућу меру.

Посебан задатак у превенцији дигиталног криминалитета имају органи формалне контроле, који морају да усавршавају своја знања и методе које примењују у откривању и доказивању дела дигиталног криминалитета.

Не треба занемарити позитивну страну дигитализације у раду поменутих органа, посебно полиције, с обзиром на то да су се захваљујући достигнућима дигиталне технологије побољшали услови разјашњавања различитих облика криминалитета. Дигитализација је од вишеструког значаја и у систему извршења кривичних санкција јер омогућава да се неки циљеви извршења лакше и ефикасније остваре уколико се на адекватан начин искористе.

Понављамо констатацију са почетка рада да је ово моменат када посебно долази до изражаја потреба сарадње различитих дисциплина, са акцентом на мултидисциплинарној сарадњи која би, поред традиционалних криминолошких дисциплина, обухватила неке нове, с циљем бољег препознавања и сузбијања дела дигиталног криминалитета.

Aleksandra Z. Ilić¹
University of Belgrade, Faculty of Security Studies
Belgrade (Serbia)

Ivana P. Bodrožić²
University of Criminal Investigation and Police Studies
Belgrade (Serbia)

Mladen M. Milošević³
University of Belgrade, Faculty of Security Studies
Belgrade (Serbia)

SOCIAL RESPONSE TO CRIME IN THE DIGITAL ERA – THE IMPORTANCE OF DIGITAL CRIMINOLOGY AND CRIMINAL LEGISLATION

(Translation *In Extenso*)

Abstract: Modern life based on digitalization significantly influences the characteristics of crime, which is the focus of digital criminology as a specific approach to studying criminal phenomena in the digital era. Given the complexity of the phenomenon, the paper emphasizes the importance of considering the aforementioned issue in all dimensions. The victim's perspective is particularly highlighted due to the importance of preventing victimization in the digital space, which is closely related to the issue of adequate criminal law response. The authors point out the importance of continuous monitoring of research results on the state of digital crime, especially in the context of recognizing and incriminating new forms of criminal behaviour. In the digital era, the social response to crime is also transforming, in both of its forms: informal and formal. Analyzing individual aspects of both forms of social response, the authors point out both the positive and negative sides of this transformation.

Keywords: social response, digital crime, digital criminology, criminal legislation, criminal law protection

INTRODUCTORY CONSIDERATIONS

Digitalization is present in everyday life of people in different segments of functioning in both private and business settings. We are in the digital era which shapes the physiognomy of various social phenomena. Availability of numerous digital tools and their permanent

¹ aleksandra.ilic@fb.bg.ac.rs; <https://orcid.org/0000-0001-7298-2347>

² ivana.bodrozic@kpu.edu.rs; <https://orcid.org/0000-0001-5010-7832>

³ mladen.milosevic@fb.bg.ac.rs; <https://orcid.org/0000-0001-8978-3475>

improvement, as well as the presence of a large number of people in the digital space, are the factors which substantially influence the characteristics of the modern criminal phenomenon. We may still hide behind the framework of what constitutes the traditional approach to the analysis of the criminal phenomenon, but it is true that there has been a digital and/or “big data” shift in criminology. Digital media, both those considered “hard”, or “material”, and the other ones, “soft”, or “non-material”, have a more significant performance, i.e., role, in the structure and experience of social life and relations among people (Smith, Bennett, Chan, 2017, p. 263).

Complete understanding of all the novelties in the digital sphere and their effect on the way of manifesting the criminal phenomenon implies a comprehensive analysis of all important factors shaping it. It is not enough merely to deal with the profile or set of characteristics of typical perpetrators of digital criminal offences, but it is also necessary to include the victim's perspective, as well as consider social response to crime within the context of the digital era in which live. This is the period of extremely developed media; information is quickly transmitted and, in certain cases, commission of some criminal offences provoke turbulent response of the public which, thanks to these media, has the power to influence the acting of law-enforcement bodies. On the one hand, this opens up the question of the limits of the public's influence on the operations of those bodies, but also reflects the reality of the modern world, or the manner of its functioning.

The traditional framework of dealing with the criminal phenomenon is no longer sufficient, but there is a growing need for some novel approaches and explanations, which would have not only theoretical, but also practical importance. The cooperation of all criminal disciplines, especially criminology and criminal law, seems to be more necessary than ever in order to respond optimally to challenges of suppressing what will be called digital crime in this paper. Given the complexity of that task, it seems best to unify all its aspects within a separate approach in criminology which we will refer to as “digital criminology”.

RELATION BETWEEN CRIMINOLOGY AND CRIMINAL LAW PROTECTION IN THE DIGITAL SPHERE

The need for developing and applying a special criminological approach based on the identification and overall analysis of the effects of digital technology in various aspects of the criminal phenomenon manifestation has crystalized a new direction in criminological thought, which in the past few years has been called mainly digital criminology (Smith, Moses, Chan, 2017; Stratton, Powel, Cameron, 2016). Some other authors tend to prefer the term cyber criminology (Grabosky, 2016; Dupont, Whelan, 2021), and even the term computer criminology (Berk, 2013; Brantingham, 2011).

As a dynamic scientific discipline and a criminal science, criminology deals with multidisciplinary and interdisciplinary research of the criminal phenomenon as a complex phenomenon consisting of several interrelated elements: crime, perpetrator, victim, criminality and society's response to criminal behaviour (Ignjatović, 2019, p. 15, 16). Within its dealing with the aforementioned whole of the subjects, or some of its elements, criminological research may have three dimensions: phenomenological, etiological and

victimological which, in this order, they imply the analysis of manifestation forms and characteristics of various forms of crime, the research of their causality⁴, or more precise conditionality and, finally, the victim's perspective.

In its development, criminology has encountered a number of challenges, such as attempts to fragment it as a whole into several criminological disciplines, depending on the main criterion of such classification, for example the influence of the monocausal approach in explaining the causality of crime which had been dominant chiefly in the early stages of criminological thought within the positivist orientation.⁵ By overcoming the positivist framework, as the only possible and legitimate framework in the context of treating the explanation of the criminal phenomenon and including more recent theoretical perspectives, social response theories and novel criminological theories, a different approach has been reached in the development of criminology disciplines which emphasize current tendencies in the commission of criminal offences and/or the modern framework of resolving the problems of crime where, among other factors, there is an increasing domination of digitalization in various forms.

Although everything has occurred slowly, with time it has become clear that traditional approaches to researching the criminal phenomenon must be adapted to the changing conditions of life which have brought about changes both in the context of commission of the already existing and well-known criminal offences, but also to the emergence of some new, previously unknown forms of criminal acting. "The basic sociological thesis manifested within the complexities of the digital era is that, concurrently with unstoppable process of digitalization development in all segments of life, we witness the same accelerated mutation, from analogous to electronic and digital forms of deviant behaviour and crime at the global level" (Sandywell, 2010, p. 42).

One of the main questions to be posed within considering the research subject of digital criminology is how to define digital crime and/or digital criminal offence. The analysis of the literature about criminal offences committed by the use of modern technology shows an incomplete picture and definition of those criminal offences committed in the sphere of digital technology or through the use of digital technology, which is corroborated by the quite diverse terminology that may be found: "electronic crime", "computer crime", "crime committed through the use of computer technology", "high-technology crime", "cybercrime" etc. (Rakhmanova & Pinkevich, 2020, p. 195). Some authors also use the term "internet

⁴ Although in all aspects of life, as well as scientific dealing with various phenomena, it is common to use the term "causality", i.e., that every phenomenon has its cause(s), it makes an impression that a certain phenomenon, regardless of its specific characteristics, is affected by certain factors whose influence can be precisely measured. However, that level of exactness and precision is reserved for scientific disciplines in which it is possible to reach such a conclusion, for example natural and technical sciences, while in the sciences about man and society, including criminology itself, these conclusions must not be drawn. We may speak only about the probability of action of a factor, or about a stronger or weaker influence in the given case.

⁵ Dealing with causality after the model of exact scientific disciplines, e.g., different natural sciences has made certain authors, such as Lombroso, highlight precisely determined factors of criminal behaviour as the cause of committing criminal offences, which at one moment led to the separation of the creation of narrow disciplines within criminology which deal only with the isolated factors and their influence on the commission of criminal offences.

crime" (Furnell, 2010; Jewkes & Yar, 2010). Internet Web and cyberspace are described as the "Wild West" of new forms of crime organized at the global level (Sandywell, 2010, p. 39). The places where digital crimes are committed are the virtual setting, the parallel universe and, in those terms, computer data, digital systems or social media are used for the commission of specific crimes (Rakhmanova & Pinkevich, 2020, p. 195).

Transferring numerous life activities into the virtual space, i.e., their modification under the influence of unstoppable processes within the digital era, has changed people, including those individuals who took the road of committing criminal offences. Certain already existing factors have adjusted or are adjusting to the permanently changed circumstances. In the same vein, new circumstances have produced some new factors which, perhaps due to the digital framework of the course of life in general, have opted for a road of law violation. "An offender grotesquely deforms his real image when introducing himself on the network, changes normal interactions among people and, consequently, traditional forms of crime, in such a manner that it becomes necessary to modify the existing criminological and dogmatic categories when the same criminal offences are analyzed" (Agustina, 2015, p. 39).

To that end, one of the most important challenges of digital criminology is becoming familiar with the characteristics of the perpetrators of crime offences whose criminal activities are primarily based on such digitalization. Given the diversity and complexity of criminal typology, criminal motives and profiles of the perpetrators in the digital space, some authors distinguish economic, social and political cybercrime (Agustina, 2015, p. 49). Criminological findings to date, although still important, must be completed with the modern framework of reflecting on this issue.

Some authors point out that criminology must develop digital specialization which examines the multilayered role of digital technologies as intersectional and transformative media in the sphere of crime and justice (Smith et al., 2017). Special momentum in the development of the idea about a new branch of criminology occurred due to the spread of the internet as a global web for communication and exchange of information. Therefore, Jaishankar points out that the development of the internet, apart from the aforementioned changes in the sphere of interpersonal communication, has also led to the emergence of a new form of crime whose study entails the development of a new branch of criminology. Through a multidisciplinary approach, that branch would integrate findings of different scientific disciplines which might be called to contribute, from their own perspective, to understanding crimes in the cyberspace, as well as their influence on the physical space (Jaishankar, 2007; according to: Ignjatović, 2019, p. 96). It is implied that the criminological approach is multidisciplinary, but with the development of the idea of cyber or digital criminology, the list of already acknowledged scientific disciplines which have something to offer in the context of analyzing crime conditionality would also include some new scientific disciplines, such as the internet science, or Informatics and Computing.

Smith, Bennett and Chan point to the existence of an empirical, conceptual and epistemological need for criminology, i.e., criminologists, to provide an explanation of the setting in which digital technologies increasingly play key roles. This implies not only the context of their use for the purpose of committing criminal offences, but also as specific pluralized platforms through which the world of crime is presented to the public on a daily basis. The consequence is the mobilization of communities and affective response

to criminal behaviours, criminal events, as well as similar responses of the formal control bodies which undertake official measures of crime control (Smith et al., 2017, p. 269).

The relation of technological development and crime may be monitored through certain stages, which are at the same time stages in the development of the criminological research of digital crime. Conditionally speaking, this whole period may be divided into three main stages or timeframe: “pre-web” era during the 1980s and the early 1990s, “global web” era from the 1990s to the early 2000s, and “social web” era since mid-2000s to date (Stratton et al., 2017, p. 19).

In the “pre-web” era, criminology recognized the circumstance that the widespread availability of computers and electronically stored data, in combination with internally networked workstations and dial-in connections, made governments, corporations and educational institutions more vulnerable to new forms of crime through technology abuse (Stratton et al., 2017, p. 19). During that period, it also became clear that the aforementioned technological development provided new criminal possibilities to curious adolescents who in their spare time developed and spread computer viruses and malware, thus causing a disturbance in digital systems (Dupont & Whelan, 2021, p. 78, 79).

During the 1990s, with the development of computer technology and the emergence of the internet, criminology began, within its field of research, to deal with the issues of computer and cybercrime, which implied the analysis of what, from today’s perspective, may be called conventional computer crime. However, the digitalization process which is increasingly accelerated also leads to the expansion and diversity of criminal offences committed in the digital space, i.e., through the use of digital technology achievements. The emergence of the computer network, devices, applications and online platforms shaped all aspects of human activity, which opened new space to innovative offenders for new opportunities for committing criminal offences (Dupont & Whelan, 2021, p. 79).

Stratton, Powell and Cameron propose expanding the traditional theoretical framework of computer and/or digital criminology, based exclusively on the theories which serve to explain conventional crime⁶. The emphasis is on the importance of the expansion and revitalization of criminological thought that might be inspired through the analysis of the development of social, critical and technological theories outside criminology itself, or its traditionally related disciplines⁷. In that respect, the importance of debate is emphasized within criminology itself in order to go beyond the conventional frameworks of dealing with cybercrime towards a broader context of researching crime and justice in the digital era (Stratton et al., 2017, p. 18).

A special segment in which it would be desirable that digital criminology should realize its full potential is the issue of human rights violation through the violation of the

⁶ The traditional theoretical framework in criminology is chiefly based on the positivist theories which primarily deal with the factors of crime, or with explaining the causality of crimes like different sociological theories: learning theory, social pressure theory, or differential association theory, supplemented by some novel approaches within more recent criminological theories, such as rational choice theory or routine activity theory.

⁷ Mostly emphasized is the range of disciplines traditionally related to criminology: psychology, sociology, medicine, biology, anthropology, law, economics etc. However, the challenges of studying crime in the digital era calls for including other considerations as well.

right to privacy in the digital space and personal data protection in relation to it. Therefore, Ignjatović objects to Jaishankar's explanation of the range of cyber criminology from which this very segment is omitted (Ignjatović, 2019, p. 96). Digital or cybercrimes often involve the violation of personal and vulnerable information, thus leading to concerns about data privacy and protection. In that segment, some room could also be found for a more intensive cooperation between criminology and criminal law, where empirical criminological analysis of different modalities of human rights violation in the digital space would ensure further development of criminal law regulations through a more complete and precise definition of corresponding incriminations.

One of the burning problems that requires better criminal law response, which has been recognized as a phenomenon at the global level, refers to revenge pornography. Of particular concern is the absence of an adequate legal framework in relation to it, despite being recognized as an important task in various debates (Walker & Sleath, 2017). In that respect, a problem also arises in precise definition of the phenomenon, which compounds systematically collecting data about the actual proportions of victimization, but it is a fact that it is a widespread phenomenon.

The victimological dimension of digital crime and criminal law protection

The question of the victimological dimension of digital crime deserves special attention. Having in mind that the research of perpetrators and their characteristics cannot be final without including the victim's perspective, it is clear what a complex task it is to consider all the aforementioned elements of the criminal phenomenon in a framework completely different from earlier. Given the presence of the majority of people in the digital space and, thus, their being subject to various abuses, it may be said that the victimological perspective of digital criminology is rather complex.

Although, in our opinion, a comprehensive analysis of the criminal phenomenon is the best possible path in understanding all individual perspectives, including the victimological one, perhaps it is worth considering the development of a separate direction withing victimology, the so-called digital victimology, which would deal particularly with the manifestation forms of victimizations in the digital space, the characteristics of victims, as well as the consequences of these forms of criminal action. This idea is by no means new because some authors already speak about Cyber Victimology (Jaishankar, 2020; Debarati, 2021) and its importance. Further development of this basic idea implies the analysis of victimization in cyberspace, which has its special characteristics to a certain extent different from victimization in the physically real space. Cyber victimization fits into the category of contextual vulnerability, i.e., perspective concentrated on the interaction of the victim with the "victimogenic setting" as a key factor (Agustina, 2015, p. 39) that finds its basic theoretical explanation in the routine activity theory which implies the existence of three major elements: motivated perpetrators, suitable targets and the absence of competent protectors from offences (Cohen & Felson, 1979, according to. Ignjatović, 2019, p. 88). Since individuals are inevitable exposed in the virtual space and subject to various forms of victimization, as well as the related and quite motivated offenders, the emphasis of cyber

or digital victimology should be on improving protection from cyber victimization through introducing adequate procedures in the cyberspace towards better realization of prevention.

As for the prevention of cyber or digital crime and, thus, better control of vulnerability in cyberspace, an extremely important and, thus, better control of vulnerability in the virtual space, an extremely important preventive role is played by the bearers of social response to crime, in both forms of its manifestation, informal and formal.

INFORMAL AND FORMAL SOCIAL RESPONSE TO CRIME IN THE DIGITAL ERA

Social response to crime and criminality may be manifested, on the one hand, in the informal response of the social community and, on the other hand, it implies formal response to the same phenomena, i.e., it refers to the activity of all bodies in charge of suppressing crime, whose acting is clearly and precisely regulated in a corresponding legal framework.

The digitalization process has caused certain changes in the manner of manifesting both informal and informal responses to crime, and the task of digital criminology is to clarify, to the greatest possible extent, the specific features of both forms of response, to perceive the advantages and disadvantages of “digitalized” response and to emphasize them in the debates dealing with that issue.

From the perspective of society’s informal response to crime and criminality, i.e., all those mechanisms by which society encourages its members to conformism⁸ (Ignjatović, 2019, p. 16), in modern frameworks there are many possible ways of realizing this informal response by using digital technology instruments.

Nowadays it has become common to record everything and post it in real time on different digital platforms and social media, and then this information is spread at the speed of light thanks to the media. These recordings include those which potentially indicate someone’s unlawful behaviour. The ensuing citizens’ response has the character of informal social response which expresses fury, anger and reproach because of the committed offence, but its main and ultimate goal is the activation of the formal control bodies which are in charge of undertaking adequate measures in order to initiate and implement the formal mechanism of determining potential responsibility of individuals. However, this form of public response is often a manifestation of moral panic as a phenomenon which has been described in the criminological literature for decades (Cohen, 1972; Goode & Ben-Yehuda, 2009; Ilić, 2017; Tompson, 2003) and is mainly related to the media activity. In short, moral panic is the exaggerated reaction of the public to certain phenomena perceived as a threat to the established system of values, while clear and precise bearers of that threat are identified, the so-called folk devils, and quick and efficient response is requested from decision-makers, i.e. the mechanisms that may be activated and start acting almost immediately. Such rapid response is most often not the best solution because, in the sphere of criminal law response and from the perspective of the goals of punishment, the most important aspect is still prevention.

Regardless of its many negative sides, the most important form of informal response to crime is based on the role of the media. The omnipresence of different media forms in

⁸ Conformism is the assumption of generally confirmed and accepted norms of behaviour.

everyday life is the proof that all important social processes are registered by the media and cause certain response in the public. Informal social response also implies the public pressure regarding certain criminal-political issues. We quite often witness the novelties in the sphere of criminal legislation in our country if the impression is made in the public of the indispensability of certain changes so as to, for example, reduce the rate of certain crime, most often in the sphere of violence (e.g., criminal offences against gender freedom or family violence). In that respect, the stipulated punishment is made more stringent or certain amendments are made to the general part of criminal legislation.

Having in mind this modern tendency, the task of digital criminology is to examine the extent to which the public shows its interest in certain amendments in the sphere of criminal law protection of the right to privacy and personal data protection in the digital sphere. In that respect, another important question is also how developed citizens' awareness is of the proportions and characteristics of digital crimes and whether there are sufficient activities in terms of educating broader public about all potential risks in the virtual world.

Starting from the first goal, the criminologist's task within digital criminology is to contribute, in line with the rules of "newsmaking criminology" (Barak, 1994), to drawing public attention to the importance of continued improvement of criminal law regulations in this sphere (in contrast to some other spheres which have exaggerated with interventionism), given its obvious dynamics. Harmonizing national criminal legislation with some of the most important international documents in that sphere is an important step in coming to grips with the challenges of digital crime, particularly in the sphere of personal data protection as an important aspect of private life (Milošević, 2022, p. 64). In that respect, it should be emphasized that the provisions about the criminal offence of unauthorized personal data collection from Article 146 of the Criminal Code ("Official Gazette of the Republic of Serbia", No. 85/2005, 88/2005 – corrected, 107/2005 – corrected, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 and 94/2024) have been aligned with the EU General Data Protection Regulation (General Regulation [EU] 2016/679 of the European Parliament and the Council of Europe)⁹ which local, but also mainly global significance.

The second important task of the "digital criminologist" would imply educating broader public about the phenomenological, etiological and victimological characteristics of digital crime in order to raise awareness of the presence and proportions of that phenomenon, as well as enabling citizens to recognize better the dangers lurking in the digital setting. In fact, many citizens willingly, via the internet, enable access to their personal data, thus creating a fertile soil for various abuses and manipulations (Mandić, Putnik, Milošević, 2017). On the other hand, some forms of prohibited behaviour in the digital space are not sufficiently recognized either in people's consciousness or in criminal legislations, for example, aforementioned revenge pornography, because there is a rather present attitude of accusing victims and supporting stereotypical beliefs, which constitutes an obstacle in effective legislative action (Harper, Smith, Fido, 2022, p. 778).

The modern framework of suppressing various forms of crime through activities of the formal social control bodies implies, *inter alia*, the application of certain digital instruments

⁹ The General Regulation was adopted on 27 April 2016 and refers to the protection of natural persons in terms of personal data protection, but also the free movement of such data, as well as declaring Directive 95/46/E3 as no longer valid.

which facilitate and accelerate some processes in comparison to the earlier period. This statement refers to all the above-listed bodies – the police, the prosecutor's office as well as the courts. Moreover, the importance of digitalization within the system of must not be forgotten, particularly in terms of the system of the institutional-type criminal sanctions execution. Without an ambition to list in this place all possible forms of digitalization on which activities of the formal control bodies are based, the idea is to point to some of the most basic aspects of digitalization application in achieving formal response to crime and criminality.

Digitalization indisputably facilitates the work of the formal control bodies, which may be manifested, for example, in the police work, both proactive and reactive, in the situations when suspects must be found. In everyday life, in many activities we leave a digital trace, which enables the aforementioned bodies to exercise their authority and reach information about a person/persons aimed at deprivation of freedom or invitation for the purpose of testifying, or generally for the purpose of identifying and proving criminal offences. One of the segments of the use of digital tools by law-enforcement bodies refers to predicting the movement of crime and activities of certain groups and even specific individuals. The critics of this practice claim that excessive reliance on predictive algorithms may threaten the presumption of innocence, due to the fact that individuals might be the subject of increased surveillance or even arrest based on the predicted probability of their commission of crime. In that respect, there are examples where predictive digital police tools have not managed to meet necessary standards of neutrality, which leads to concerns about legality and ethics of acting (Matić Bošković, 2024, p. 484).

The space in which digitalization may be of indisputable use in the practice of the formal control bodies refers to the development of digital forensics and its application primarily in the sphere of suppressing digital and/or high-technology crime as defined, in line with positive law terminology, in Article 2 of the Law on the Organization and Competences of Government Authorities Combating Cyber Crime ("Official Gazette of the Republic of Serbia", No. 61/05, 104/09, 10/23 i 10/23 – other law¹⁰). Cybercrime is yet another name for a variety of offences implying the use of digital technology (Bodrožić, 2013). Those are criminal offences the suppression of which needs the establishment of a special organization of competent prosecution bodies¹¹. The activity of the specially established services and departments within the existing prosecution bodies can certainly not be imagined without the improvement of a special digital form of forensic practice. We will mention only several reasons for it: "It may be said that there has almost no larger organization in the world that has not undergone the compromising of the system due to attacks; moreover, the systems for detecting attacks to the system and antivirus programs have not resolved security problems, while there is also a large number of networked computers intended for the distribution of illegal content and piracy" (Korać, Prlja, Diligenski, 2016, p. 12).

¹⁰ High-tech crime is the commission of criminal offences in which the object or instrument of commission includes computers, computer systems, computer networks, computer data, as well as their products in material and electronic forms. The products in electronic form particularly refers to computer programs and copyrighted works which may be used electronically.

¹¹ The Service for Combatting High-Technical (obviously the legislator's terminological error) Crime within the Ministry of Interior Affairs, the Special Department for Combatting High-Technology Crime within the Higher Public Prosecutor's Office, and the Department for Combatting High-Technology Crime within the Higher Court in Belgrade in the first instance.

The task of digital criminology should mainly be to analyze to what extent the application of digitalization in different aspects of the functioning of the formal social control bodies enables better efficiency in the work of these bodies, while observing the principles on which the treatment of the persons appearing in criminal proceedings is based, particularly those principles with a protective role. Collecting and using digital evidence raises many important questions which mainly refer to the protection of personal privacy and individual freedoms (Stratton et al., 2016, p. 26).

In contrast, if the epilogue of the proceedings is a criminal sanction, the question arises of the question of applying digitalization in the execution of certain criminal sanctions, whereas the emphasis should not be primarily on the usefulness brought by digitalization to the system of criminal sanctions execution as such, but on how digitalization helps convicts in the process of fulfilling the purpose of execution and/or achievement of the punishment goal. For example, achieving resocialization as the purpose of the prison sentence in modern frameworks cannot be imagined without introducing digitalization. It is particularly important because of the need to adjust prisoners to the conditions of the digitalized life in freedom, as well as of more efficient acting on the criminal behaviour factors which initially led to the commission of the offence (Ilić, 2024). Moreover, the importance of digitalization should not be ignored either as a form of aid to convicts in the exercise of some of their rights. In the case of impossibility of realizing direct contact between convicts and their family members, it can be compensated by the use of various digital aids, which contributes to a stronger resocialization effect on convicts (Ilić & Banović, 2022, pp. 191–194) or, in the case of convicts' exercise of their right to education (Barros, Monteiro, Leite, 2023).

FINAL CONSIDERATIONS

Despite all the advantages of digital technology in the modern world and the optimistic expectations of their being the main solution to the lack of knowledge and barriers in free expression (Vajdijanatan, 2018, p. 33), we must not ignore serious risks lurking in the developed digital space. Although, thanks to various digital tools, plenty of information about the aforementioned risks is available to us, we are not sufficiently aware of them because of our constantly being present in the digital world, which is corroborated by the fact that the offences that may be categorized as digital crime are constantly on the rise.

The task of digital criminology is to recognize new, as well as modified forms of criminal behaviour developing in the modified conditions of modern digital society's functioning. Recognizing these patterns is certainly not sufficient if it is not accompanied, on one side, by adequate criminal law response and/or normative recognition of behaviours that should be incriminated. Although, in general, there is no need for exaggerated criminal law intervention, in this sphere such activity is extremely desirable in order to react to the challenges of digital crime in a timely and adequate manner. On the other hand, the perception of deviating behaviours in the digital space should at the same time be accompanied by citizens' education about the dangers lurking in that space and undertaking adequate protection and/or prevention measures in order to reduce the victimization risk to the minimum.

A special task in the prevention of digital crime is assumed by the formal control bodies which must specialize their knowledge and methods applied in identifying and proving digital crime offences.

The positive side of digitalization must not be ignored in the work of the above-listed bodies, particularly of the police, since the conditions of clarifying various form of crime have been improved thanks to digital technology achievements. Digitalization also has multiple significance in the system of criminal sanctions execution, ensuring easier and more efficient achievement of some execution goals provided that they are adequately used.

We will once again repeat the statement from the beginning of the paper that this is the moment when the need for the cooperation of various disciplines is particularly pronounced, with a focus on multidisciplinary cooperation that would, apart from traditional criminological disciplines, also encompass some new ones, with the aim of better identification and prevention of digital crime offences.

REFERENCES / ЛИТЕРАТУРА

- Agustina, R. J. (2015). Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect. *International Journal of Cyber Criminology (IJCC)*, 9 (1), 35–54. doi: [10.5281/zenodo.22239](https://doi.org/10.5281/zenodo.22239)
- Barak, G. (1994). Media, Society and Criminology. In: G. Barak (ed.). *Media, Process, and the Social Construction of Crime: studies in Newsmaking Criminology*, 3–45. New York: Garland Publishing
- Barros, R., Monteiro, A., Leite, C. (2023). Learning with digital technologies in prison: a scoping review. *Digital Education Review*, 43, <https://revistes.ub.edu/der>
- Berk, R. (2013). Algorithmic criminology. *Security Informatics*, 2 (5). <https://doi.org/10.1186/2190-8532-2-5>
- Bodrožić, I. (2013). Criminal offences with elements of high-tech crime. *Bezbednost*, 55 (2), 142–157. Available at: https://hdl.handle.net/21.15107/rcub_jakov_546
- Brantingham, P. L. (2011). Computational Criminology. In: *European Intelligence and Security Informatics Conference*, 3. Athens: IEEE Computer Society. doi: [10.1109/eisic.2011.79](https://doi.org/10.1109/eisic.2011.79)
- Cohen, S. (1972). *Folk Devils and Moral Panics: The Creation of the Mods and Rockers*. Oxford: Routledge
- Criminal Code (“Official Gazette of the Republic of Serbia”, No. 85/05, 88/05, 107/05, 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19 and 94/2024). [In Serbian]
- Debarati, H. (2021). *Cyber Victimology: Decoding Cyber-Crime Victimisation*. New York: Routledge
- Dupont, B., Whelan C. (2021). Enhancing relationships between Criminology and cyber-security. *Journal of Criminology*, 54 (1), 76–92. doi: [10.1177/00048658211003925](https://doi.org/10.1177/00048658211003925)
- General Data Protection Regulation – GDPR (Regulation [EU]) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Goode, E., Ben-Yehuda, N. (2009). *Moral Panics: The Social Construction of Deviance*. Chichester: Wiley-Blackwell

- Furnell, S. (2010). Hackers, viruses, and malicious software. In: Y. Jewkes, M. Yar (eds.). *Handbook of Internet Crime*, 38–66. Devon: Willan Publishing
- Harper, A. G., Smith, L., Leach, J., Daruwala, A. N., Fido, D. (2023). Development and Validation of the Beliefs About Revenge Pornography Questionnaire. *Sexual Abuse*, Vol. 35 (6), 748–783. doi: [10.1177/10790632221082663](https://doi.org/10.1177/10790632221082663)
- Ignjatović, Đ. (2019). *Criminology*. Beograd: Univerzitet u Beogradu – Pravni fakultet.
- Ilić, A. (2017). *Media and Crime: criminological aspects*. Beograd: Univerzitet u Beogradu – Pravni fakultet. Available at: <https://nardus.mpn.gov.rs/handle/123456789/9158> [In Serbian]
- Ilić, A. (2024). The influence of digital technology on the reduction of re-offending and rehabilitation of convicts. In: M. Milošević, N. Stekić (eds.). *The third memorial conference "Predrag Marić"* (book of abstracts), 16. Beograd: Univerzitet u Beogradu – Fakultet bezbednosti. Available at: <https://newsimrdproject.fb.bg.ac.rs/rez/rez35.pdf> [In Serbian]
- Ilić, A., Banović, B. (2022). Digitalization in the system of execution of criminal sanctions in the Republic of Serbia. In: J. Kostić, M. Matić-Bošković (eds.). *Digitalization in Penal Law and Judiciary*, 185–200. Beograd: Institut za uporedno pravo; Institut za kriminološka i sociološka istraživanja. doi: [10.56461/zr_22.dukpp.14](https://doi.org/10.56461/zr_22.dukpp.14). [In Serbian]
- Jaishankar, K. (2020). Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology. *An International Perspective on Contemporary Developments in Victimology*, 3–19. https://doi.org/10.1007/978-3-030-41622-5_1
- Jewkes, Y., Yar, M. (2010). Forms of Internet Crime. In: Y. Jewkes, M. Yar (eds.). *Handbook of Internet Crime*, 167–172. Devon: Willan Publishing
- Korać, V., Prlja, D., Diligenski, A. (2016). *Digital Frensics*. Beograd: Centar za nove tehnologije Viminacium; Arheološki Institut Beograd; Institut za uporedno pravo. Available at: <https://iup.rs/wp-content/uploads/2021/05/2016-Digitalna-forenzika-Korac-Prlja-Diligenski.pdf> [In Serbian]
- Law on the Organization and Competences of Government Authorities Combating Cyber Crime ("Official Gazette of the Republic of Serbia", No. 61/05, 104/09, 10/23 and 10/23 – other law). [In Serbian]
- Mandić, G., Putnik, N., Milošević, M. (2017). *Data protection and social engineering - legal, organizational and security aspects*. Beograd: Univerzitet u Beogradu – Fakultet bezbednosti [In Serbian]
- Matić Bošković, M. (2024). Impact of artificial intelligence on practicing judicial professions. *Sociološki pregled / Sociological Review*, 58 (3), 481–499. doi: [10.5937/socpreg58-51385](https://doi.org/10.5937/socpreg58-51385)
- Milošević, M. (2021). Personal Data Protection in Criminal Law. *Revija za kriminologiju i krivično pravo*, (2), 113–130. doi: [10.47152/rkkp.59.2.7](https://doi.org/10.47152/rkkp.59.2.7) [In Serbian]
- Milošević, M. (2022). *Criminal Law – Special Part: Selected Offenses for Security Studies*. Beograd: Univerzitet u Beogradu – Fakultet bezbednosti. [In Serbian]
- Rakhmanova, E. N., Pinkevich T. V. (2021). Digital Crime Concept. *Advances in Economics, Business and Management Research*, 138, 193–196. Available at: https://www.researchgate.net/publication/341348757_Digital_Crime_Concept
- Ramirez-Thompson, E. R. (2020). *Computer and Criminal Justice*. College of DuPage Press. Available at: <https://cod.pressbooks.pub/crimj1165/front-matter/title-page/>

- Sandywell, B. (2010). On the globalisation of crime: the Internet and new criminality. In: Y. Jewkes, M. Yar (eds.). *Handbook of Internet Crime*, 38–66. Devon: Willan Publishing
- Smith D. J. G., Moses, B. L., Chan, A. (2017). The challenges of doing criminology in the big data era: towards a digital and data-driven approach. *The British Journal of Criminology*, 57 (2), 259–274. <https://doi.org/10.1093/bjc/azw096>
- Stratton, G., Powell, A., Cameron, R. (2016). Crime and Justice in Digital Society: Towards a 'Digital Criminology'?. *International Journal for Crime, Justice and Social Democracy*, 6 (2), 17–33. doi: [10.5204/ijcjsd.v6i2.355](https://doi.org/10.5204/ijcjsd.v6i2.355)
- Tompson, K. (2003). *Moral Panics*. Beograd: CLIO. [In Serbian]
- Vajdiđanatan, S. (2018). *Antisocial Media*. Beograd: CLIO. [In Serbian]
- Walker, S., Sleath, E. (2017). A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media. *Aggression and Violent Behavior*, 36 (1), 9–24. doi: [10.1016/j.avb.2017.06.010](https://doi.org/10.1016/j.avb.2017.06.010)