

Јована М. Бановић¹
Универзитет у Београду, Факултет безбедности
Београд (Србија)

Ивана М. Радисављевић²
Универзитет у Београду, Правни факултет
Београд (Србија)

342.738:004.056
004.738.5:351.083.8
Прејледни научни рад
Примљен 12/02/2025
Измењен 28/02/2025
Прихваћен 28/02/2025
doi: [10.5937/socpreg59-56730](https://doi.org/10.5937/socpreg59-56730)

ПРИВАТНОСТ, ЗАШТИТА ПОДАТАКА О ЛИЧНОСТИ И ДИГИТАЛНО ДОБА – ЈЕДАН (КРИВИЧНО)ПРАВНИ „ОМНИБУС“

Сажетак: Устав Републике Србије штити право на приватност кроз неколико аспеката. Европска конвенција о заштити људских права и основних слобода, такође. Закон о заштити података о личности, усвојен 2018. године, матични је у овој области. Кривични законик, у складу са *ultima ratio* карактером кривичног права, штити ове податке када дође до најозбиљнијих повреда, а у складу са Законом о кривичном поступку. Међутим, све ово поприма другачију, „дигиталну“ димензију са свакодневном експанзијом науке, технике и иновативних средстава општења, снимања и слично. Разумљиво, ова тенденција захтева извесна прилагођавања, како у самим прописима, тако и у њиховом тумачењу и примени. Ауторке ће у овом раду настојати да укажу на битне одредбе поменутих прописа и њихово садашње и будуће разумевање у контексту дигиталног друштва, са нарочитим освртом на кривично-правне домете. Све се то додатно усложњава развојем вештачке интелигенције која, по својој природи, подразумева употребу велике количине података. Циљ рада је да лоцира неке од круцијалних елемената у заштити права на приватност, а посебно оних који се тичу података о личности који су најнепосредније везани за човека, и отвори питање потенцијалних законодавних измена.

Кључне речи: приватност, подаци о личности, неовлашћено прикупљање, неовлашћено снимање, кривичноправна заштита

УВОДНА РАЗМАТРАЊА

Различити домаћи и међународни документи посредно или непосредно препознају приватност као основно људско право које представља право појединца или групе појединаца да заштите свој приватни живот и приватно окружење, укључујући и информације о себи. Савремено дигитално доба овај појам нужно проширује тако да обухвата и приватност у дигиталном окружењу („е-приватност“) и, штавише,

¹ jovana.banovic@fb.bg.ac.rs; <https://orcid.org/0009-0007-6324-487X>

² ivana.radisavljevic@ius.bg.ac.rs; <https://orcid.org/0000-0003-1445-707>

сугерише да га треба посматрати као независно право које заслужује правну заштиту само по себи (Romansky & Noninska, 2020, 5288–5289).

Устав Републике Србије („Службени гласник РС“, бр. 98/2006 и 115/2021, у даљем тексту: Устав), за разлику од Европске конвенције за заштиту људских права и основних слобода (објављене са додатним протоколима у „Службеном листу СЦГ – Међународни уговори“, бр. 9/2003, 5/2005 и 7/2005 – испр. и „Службени гласник РС – Међународни уговори“, бр. 12/2010 и 10/2015, у даљем тексту: ЕКЉП), познаје право на приватност, али га не формулише тако експлицитно као што то чини помениути документ Савета Европе. Наиме, чл. 8. ЕКЉП дефинише „право на поштовање приватног и породичног живота“. Оно обухвата четири сегмента, и то: приватни живот, породични живот, дом и преписку, које пак није увек тако лако раздвојити (Beširević i dr., 2017, str. 160). Српски Устав, са друге стране, ова четири фрагмента разрађује у више појединачних одредаба, а за тему нашег рада најважнији су чл. 41. и 42. Њима се штите тајност писама и других средстава општења и подаци о личности.

Матични закон у области заштите података је Закон о заштити података о личности („Службени гласник РС“, бр. 87/2018, у даљем тексту: ЗЗПЛ) и он, у најширем смислу, уређује прикупљање, држање, обраду и коришћење ових података у сврхе за које су намењени, те низ правила с циљем спречавања њихове злоупотребе. Неповредивост тајности писама и других средстава општења се даље непосредније регулише инкриминацијама из чл. 142, 143. и 144, а података о личности чланом 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 и 94/2024, у даљем тексту: КЗ). Ово нису једина кривична дела којима се штити право на приватност, па су у том смислу релевантна и кривична дела из чл. 138а (прогањање), 141. (неовлашћено откривање тајне) и 145. (неовлашћено објављивање и приказивање туђег списка, портрета и снимка) (више о томе: Milošević, 2021, str. 124–126). Како ћемо се у овом раду бавити подацима о личности у контексту права на приватност, то ће кривично дело из чл. 146. КЗ бити основни предмет обраде.

У сваком случају, заштита података се раније третирао као део права на приватност, а данас је задобила обресе самосталног концепта (Blume, 2010, str. 153), па чак и засебне гране права (Andonović & Prlja, 2020, str. 54). У том смислу ћемо фокус рада усмерити превасходно на податке о личности, премда то неспорно подразумева и право на приватност.

Када је у питању дигитална „околина“, вреди истаћи да је сада већ чувена Уредба 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, у даљем тексту: GDPR) узела у обзир интернет окружење кроз регулисање „права на заборав, одн. брисање“ из чл. 17 GDPR.³ А које су специфичности заштите података у дигиталној ери?

³ Право на заборав се дефинише као „право да се захтева уклањање личних података са веб-сајтова или претраживача, посебно када су ти подаци нерелевантни, застарели, штетни или нарушавају приватност или достојанство појединца“ (Gill, Redeker, Gasser, 2015, str. 8). Њиме се даје могућност појединцу да захтева ограничени приступ прошлим информацијама које шкоде његовим садашњим и будућим интересима, брисањем или изменом таквих података.

(СТАРИ) ИЗАЗОВИ НОВОГ ДОБА

Пред сам крај прошлог миленијума, Берман и Малиган (Berman & Mulligan) објавили су донекле револуционаран рад у којем су указали на то да интернет, тада још „у настајању“ за ширу популацију, даје нову визуру проблему заштите приватности. Они су препознали три кључне тачке на овом плану, и то: пораст стварања и прикупљања података; глобализацију информација и њихово ширење; недостатак централизоване контроле над заштитом података (Berman & Mulligan, 1999, str. 554–556). И после четврт века, ови проблеми не само да су актуелни већ су и додатно усложњени константним развојем и доступношћу како интернета, тако и друге дигиталне технологије која ствара практично нови социјални оквир људског деловања.⁴

Неспорно је да подаци „одлазе у етар“ непосредном вољном радњом лица на које се односе (нпр. унећемо податке о личном имену, адреси, јединственом матичном броју итд. приликом регистрације за добијање картице за попусте у омиљеној радњи или куповини полисе осигурања приликом одласка на зимовање). Међутим, велики број података се свакодневно прикупља, не толико без наше воље, колико без наше свести о томе, или још прецизније – без обраћања пажње (нпр. сигурносне камере, некада са јасним упозорењем да је простор под видео-надзором, а некада и без њега; потом, мапе кретања приликом коришћења GPS уређаја који су доступни на готово сваком мобилном уређају; употреба „паметних уређаја“ у домаћинству којима се управља путем WiFi конекције на даљину; биометријски подаци за „откључавање“ мобилних телефона и слично (о постојећем правном и стварном стању у овим областима, више у: Petrović, 2024; Ružić, 2024).

Интернет је „планета без граница“, те се ови подаци практично могу наћи у сваком делу света па чак, сликовито говорећи – и испод њега. Такав је пример употребе *deer* и *dark web*-а, на којима се незаконито може трговати различитим ресурсима (људи, оружје, дрога...), па и личним подацима. Примера ради, да би се заобилазле мере усмерене на спречавање прања новца, а које подразумевају потпуну идентификацију корисника услуга, могу се купити посебни KYC (*Know Your Customer*) Kits с циљем избегавања „познавања“, односно откривања стварног корисника. У овом „сету“ неретко се могу набавити скоро комплетни подаци о личности који су некада измишљени, а често и стварни, али украдени (Elliptic, 2024, str. 27)⁵.

Ово право се родило управо са развојем технологије и комуникационих средстава, а такав став је заузео и Европски суд за људска права. Више о томе: *Case of Hurbain v. Belgium*, Application no. 57292/16, July 4th, 2023, §191 et seq.

⁴ Можемо казати да су данас доступне технологије које су у време настанка цитираног рада практично биле у домену научне фантастике. Илустративан је пример из филма „Пети елемент“ из 1997. године у којем су летећи аутомобили приказани као уобичајено превозно средство. Такве аутомобиле још увек немамо, али се увелико развијају и користе тзв. аутономна возила. О неким питањима одговорности за незгоде у којима учествују самовозећи аутомобили, више у: Banović, 2023, str. 41–43. Штавише, у Републици Србији је од 2. 12. 2023. године у примени Правилник о условима за обављање аутономне вожње („Службени гласник РС“, бр. 104/23) чији је превасходни предмет уређења процедура издавања дозволе за тестирање (sic!) аутономног возила.

⁵ Интересантно је да је у наведеном приручнику као пример једне понуде за куповину, поред података о продавцу и цени, постављена и фотографија личне карте издате у Републици

Када је у питању недостатак централизоване контроле заштите података, GDPR је значајно допринео унификацији ових правила. И српски ЗЗПД је донесен по узору на GDPR и тзв. Полицијску директиву (Directive /EU/ 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA). Поменули смо да новелирањем и овај акт кудикамо прати савремене развојне токове, међутим, и појединачне земље морају да узимају у обзир свеопшти дигитални развој.

Заштита података, поред нормативних, све више подразумева и техничка унапређења. Тако се, примерице, развој интернета може описати кроз три фазе: *read* (Web1) – *read, write* (Web2) – *read, write, own* (Web3). Речју, у првој фази, интернет је био дизајниран тако да омогући корисницима само конзумирање постојећег, али не и креирање новог садржаја. Друга фаза је обележена стварањем друштвених мрежа (Facebook, Google, Wikipedia...) и давањем могућности корисницима да креирају садржај (тзв. *user generated content*). Овакав механизам је резултирао добровољним постављањем великог броја података који су се похрањивали на већим серверима, а потом довели и до једног феномена који се зове „циљана реклама усмерена ка конкретном кориснику“. На овај начин се прикупља и чува огроман број информација о појединцима, што отвара простор и за одређене злоупотребе.⁶ У основи таквих незаконитих деловања јесте управо централизовани систем на којем се чувају сви ти подаци који се остављају или прикупљају. Када су, кроз експанзију дигиталне имовине, потврђене све иновативне предности блокчејн технологије, тада се развија идеја по којој би и интернет треће генерације – Web3, могао да почива на децентрализацији. То би значило да велике платформе попут Google, Amazon и сл., не би биле „апсолутне господарице“ мноштва података, већ би то био сам корисник као њихов сопственик (*owner*) (Stackpole, 2022).

Управо због тога, у наставку рада ћемо се позабавити неовлашћеним прикупљањем података у различитим формама.

Србији са, уистину, делимично заштићеним подацима (вероватно услед непознавања језика и ћириличног писма, својеручни потпис је остао видљив, па би се на тај начин идентитет особе чија је лична карта „завршила“ на тржишту могао одредити).

⁶ Нпр. Суд правде Европске уније је донео пресуду у поступку *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés* (CNIL) и утврдио повреду права на приватност услед недостатка транспарентности где Гугл није јасно и разумљиво објаснио корисницима како се њихови подаци прикупљају и обрађују; потом, недовољности информација када подаци о обради нису били лако доступни, па су корисници морали да пролазе кроз више корака да би добили кључне информације о коришћењу њихових података; и на концу, неадекватне сагласности за персонализоване огласе јер Гугл није прибавио валидну сагласност корисника за обраду њихових података у сврху персонализације огласа, будући да она није била довољно специфична и једнозначна. Judgment of the Court (Grand Chamber) of 24 September 2019, available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:62017CJ0507>

КРИВИЧНО ПРАВО У ДРУШТВУ „НА КЛИК“

Кривично материјално и процесно право, као уосталом и друге гране права, нужно треба да прате развој дигиталног друштва и са њиме се усклађују у одговарајућој мери. Мада законодавне интервенције учињене у протеклој деценији не иду у прилог томе, кривично материјално право је мање динамична грана права у којој сувише честе измене нису пожељне. У том смислу, када су у питању поједина кривична дела чија се обележја све више премештају у дигитално окружење, ипак има места изменама како би се избегле недозвољене аналогije у тумачењу у ситуацијама када конкретна норма недостаје. Наш фокус ће примарно бити на „дигиталним аспектима“ кривичног дела из чл. 146. КЗ, а у одређеној мери и чл. 143. истог законика.

Неовлашћено прикупљање личних података (чл. 146. КЗ)

Кривично дело из наслова ове целине рада садржи по један основни, посебни и тежи облик. Извршилац основног облика може бити било ко ко предузме неку од три алтернативно прописане радње: неовлашћено прибављање, саопштавање другом, или употреба података у сврху за коју нису намењени. Објект извршења кривичног дела су подаци о личности који се прикупљају, обрађују и користе на основу закона. То су подаци који се законито налазе у поседу руковооца или обрађивача (њихове дефиниције садржи ЗЗПЛ у чл. 4. ст. 1. тач. 8. и 9), али који предузимањем једне од наведених радњи извршења доспевају до непозваног лица (Milošević, 2022, str. 65). С обзиром на чињеницу да се данас велики број података складишти и преноси у дигиталној форми (Mandić, Putnik & Milošević, 2017, str. 25), појавни облици овог кривичног дела су све „дигиталнији“⁷.

Хипотетички говорећи, подаци о личности се у оваквом окружењу могу прибавити на различите начине. Нпр. хаковањем база података, тј. неовлашћеним приступом рачунарским системима, што се најчешће чини уношењем рачунарских вируса; издвајањем података из „cloud“ система – кроз неовлашћен приступ налазима на платформама за складиштење података (Google Drive, Dropbox) ради преузимања или копирања података о личности; бесконтактно скенирање с циљем прибављања података са личних докумената или платних картица помоћу уређаја који бежично читавају податке. Дакле, овде је реч о подацима који су претходно законито прикупљени, али их из базе у којој су законито складиштени неко неовлашћено прибавља. Ово су примери у којима је сам начин прибављања података кажњив, без обзира на околност да ли је реч о подацима о личности, или није. Стога, битно је истаћи да се на овај начин истовремено могу учинити и друга кривична дела, па у кривичноправном смислу (најчешће) говоримо о правом стицају, будући да се истим понашањима

⁷ Осим тога, могућности обраде велике количине података се континуирано шире са развојем вештачке интелигенције, па и у системима у којима се рукује са нарочито осетљивим подацима. Тако се нпр. данас вештачка интелигенција користи за анализу правних докумената, уговора, судске праксе, доказа итд., како би се олакшали и убрзали правни саобраћај и судски поступци (Matić Bošković, 2024, str. 482–483).

нападају различити објекти заштите. У обзир тако долазе превасходно кривична дела из групе против безбедности рачунарских података⁸ (прављење и уношење рачунарских вируса, неовлашћен приступ заштићеном рачунару, рачунарској мрежи и електронској обради података... (о томе видети и код: Putnik, Milošević, Cvetković, 2022, стр. 331), против имовине (превара), против државних органа (лажно представљање). Треба међутим приметити да се ова кривична дела највећма гоне по службеној дужности, док се кривично дело из чл. 146. ст. 1. и 2. КЗ гони по приватној тужби, тако да оно и у овим случајевима води „самосталан процесни живот“ па материја стицаја није од нарочитог практичног значаја.

Радња саопштавања је посебно актуелизована са развојем друштвених мрежа које омогућавају рапидно ширење информација са којима се велики број људи упознаје у кратком року. Имајући у виду да је податак о личности сваки податак који се односи на физичко лице чији је идентитет одређен или одредив, непосредно или посредно, посебно на основу ознаке идентитета, као што је име и идентификациони број, података о локацији, идентификатора у електронским комуникационим мрежама или једног, односно више обележја његовог физичког, физиолошког, генетског, менталног, економског, културног и друштвеног идентитета (чл. 4. ст. 1. тач. 1. ЗЗП), индикативно је која количина информација може бити саопштена у смислу ове радње. То може бити учињено објављивањем фотографија, видео-записа, текстова или гласовних порука у којима су садржани ови подаци – лик, број, глас итд.

Радња употребе у сврху за коју подаци нису намењени унеколико је специфичнија што такве податке о личности имаалац држи овлашћено, прибавио их је законито, али их даље користи противно закону. Разлика између ове и претходних радњи се увиђа тек довођењем у везу са циљем коришћења предметних података. Нпр. обрађивач података, радећи у јавнобележничкој канцеларији, законито обрађује податке о личном имену, матичном броју, адреси становања, прометовању непокретностима итд. у вези са послом који обавља, путем званичног информационог система. Међутим, када он те податке искористи како би их ставио на располагање инвеститору с циљем ширења његовог посла, тј. да би инвеститор тим лицима нудио новоизграђене станове, тада можемо говорити о овој радњи извршења.

Мада је спорно да ли је реч о другом основном облику или посебном облику, дело из ст. 2. постоји када се противно закону прикупљају подаци о личности грађана или тако прикупљени подаци користе. У односу на облик из чл. 146. ст. 1. КЗ, радња извршења се састоји у незаконитом прикупљању података о личности. У једном временском односу, радња прикупљања претходи радњи извршења из ст. 1, односно радњи прибављања. Наиме, прибављање се врши у односу на већ законито прикупљене податке (ст. 1), а незаконито прикупљање је иницијално противно прописима (ст. 2).

Овде су, ипак, спорне две ствари. Прва, да ли су „неовлашћено“ прибављање (чл. 146. ст. 1. КЗ) и „противно закону“ (чл. 146. ст. 2. КЗ) синоними? И друга, да ли се објекат радње другог облика (посебног) односи само на податке о личности у смислу

⁸ Подаци о личности се могу прибавити и пресретањем комуникације. Интересантно је да међународни документи предвиђају кажњивост ових радњи у домену високотехнолошког криминала, док то није случај са нашим важећим Кривичним закоником који је иначе углавном усклађен са тим инструментима (Delić, 2021, стр. 327; Milošević, 2022, стр. 171, fn. 55).

ЗЗПЛ или је реч о „квалификованим“ подацима о личности више грађана, тј. да ли се језички ради о множини (Lazarević, 2011, str. 553)? Мишљења смо да јесте реч о синонимима, нарочито јер се ради о бланкетном кривичном делу (Milošević, 2021, str. 119). Међутим, у првом ставу, незаконитост имамо тек на другом кораку – подаци су законито ту (први корак), али се њима неовлашћено рукује (други корак), док у другом ставу та незаконитост делује већ са првим кораком – подаци нису законито у поседу, па последично, ни свака друга радња не може бити законита (мада је реч о правилу имовинског права, чини се сврсисходним приметити да и овде делује принцип „што се грбо роди, вријеме не исправи“). Друга спорна ствар, чини се, не представља питање језичког тумачења граматичког броја, већ просто неспретне правне формулације и упитног законодавног мотива инкриминисања. Слично као код првог облика, кроз незаконито прикупљање података о личности, могу се остварити и елементи неких других кривичних дела. Нпр. креирањем лажних апликација или интернет страница које опонашају званичне сервисе, а које корисници користе за унос својих личних података; социјалним инжењерингом кроз навођење на откривање података о личности итд.

За оба облика овог кривичног дела прописана је новчана казна или казна затвора до једне године, што сугерише да је реч о лакшем делу, па у обзир долази примена блажих кривичних санкција или института попут дела малог значаја или опортунитета кривичног гоњења.

Тежи облик овог кривичног дела постоји уколико дело из чл. 146. ст. 1. КЗ учини службено лице у вршењу службе, што за последицу има могућност кажњавања затвором у трајању до три године. За разлику од основног и посебног облика, гоњење се предузима *ex officio*. Интересантно је да се тежи облик не односи на чл. 146. ст. 2. КЗ, иако су ова лица и те како у фактичкој могућности да у већ наведеном смислу незаконито прикупљају податке. Релевантан облик кривице код сва три облика је умишљај, при чему у неким случајевима можемо говорити о постојању стварне или правне заблуде као основа искључења кривице (Milošević, 2021, str. 118).

Чини нам се да ове дилеме нису нешто што се може решити самим тумачењем прописа. Овде је ипак потребна детаљнија анализа овог кривичног дела и, након тога, адекватна законодавна интервенција. Ово особито важи јер се поједини прекршаји из ЗЗПЛ који садржи „млађе“ норме од чл. 146. КЗ, који није мењан од 2006. године, поклапају са обележјима овог кривичног дела. То је, на концу, једна правно неодржива ситуација која подрива правну сигурност и захтева системско усклађивање прописа (више о томе: Milošević, 2021, str. 119–121).

О неовлашћеном прислушкивању и снимању (чл. 143. КЗ) са освртом на „дигитални“ доказни значај

Основни облик кривичног дела из наслова овог дела рада постоји уколико се посебним уређајима неовлашћено прислушкује или снима разговор, изјава или какво саопштење, који том лицу нису намењени, као и, што је посебан облик, уколико се омогући непозваном лицу да се упозна са разговором, изјавом или саопштењем који су неовлашћено прислушкивани, односно тонски снимани. Прописана је новчана

казна или затвор од три месеца до три године. Објекат радње овог кривичног дела су разговори, изјаве или саопштења, дакле, не подаци о личности као такви, већ један шири облик који их посредно може садржати. Битно је истаћи и то да се ово дело чини уз употребу посебних уређаја за слушање и снимање. За нашу тему је посебно индикативно то што се кроз аудио и видео записе, који настају као предмет извршења кривичног дела, може доћи у посед и одређених података о личности. Због тога се и овде поставља питање односа овог и кривичног дела из чл. 146. КЗ. Премда је реч о истом групном заштитном објекту (слободе и права човека и грађанина), ради се о посве другачијој инкриминацији. Сходно томе, а како се и за ово кривично дело гони по приватној тужби, могуће је замислити да таква приватна тужба обухвати оба дела. Тежи облик постоји уколико је дело из чл. 143. ст. 1. и 2. КЗ учинило службено лице у вршењу службе, за које је предвиђена казна затвора од шест месеци до пет година, и гони се по службеној дужности.

Шта је „дигитално“ у овом кривичном делу? Пре свега, само средство извршења, тј. електронски уређаји за снимање. Потом, и начини извршења и продукти тако створеног садржаја. Ипак, оно што представља нарочито занимљиву тему јесте могућност коришћења снимљеног садржаја као доказа у кривичном поступку (Lazić & Radisavljević, 2018, стр. 381–386; Milošević, 2021, стр. 123–124). Употреба овако начињених доказа није неспорна, иако тумачења и судска пракса иду у прилог допуштености њиховог коришћења под одређеним условима (нпр. упозорењем да се одређено лице снима). Отуда се у предлогу потоњих измена Законика о кривичном поступку (Нацрт Законика о кривичном поступку, <https://www.mpravde.gov.rs/sekcija/53/radne-verzije-propisa.php>) управо поставило питање тзв. Дигиталних доказа. Њима је у чл. 139а предложено правило по којем се: фотографије или тонски, односно тонски и оптички снимци, настали и прибављени у складу са овим закоником, могу користити као доказ и на њима се може заснивати одлука суда. Са друге стране, уколико се ради о фотографијама или тонским, односно тонским и оптичким снимцима који не спадају у поменуто правило, они се могу користити као доказ у кривичном поступку, само онда када се окривљени налази на фотографији или снимку, односно ако је његов глас забележен на снимку. Следствено томе, тзв. Аматерски снимци би се у случају усвајања ових измена неспорно могли користити као доказ.

Оно што пак додатно компликује ова питања јесу предложене измене КЗ управо у домену чл. 143. КЗ (Нацрт Кривичног законика, <https://www.mpravde.gov.rs/sekcija/53/radne-verzije-propisa.php>). Наиме, њима је предложено брисање синтагме „који му нису намењени“, што имплицира да би кривично дело чинио свако ко користи посебне уређаје за снимање, без обзира на то да ли је учесник у њима или није, као и неvezано од тога да ли на тај начин „прибавља доказни материјал“ о извршењу кривичног дела. Нејасан је однос предложених материјалних и процесних одредаба о овом питању. Бланкетни карактер и овог кривичног дела, због речи „неовлашћено“, могао би указати на специфичан основ искључења противправности који се налази у процесном закоником. Такође, на пољу материјалног кривичног права могли бисмо теоријски говорити и о неком виду поступања у нужној одбрани, ако снимањем настојимо да одбијемо истовремени и противправни напад на неко наше правом заштићено добро.

Јасно је да се овој проблематици мора придати одговарајући значај и приступи јој правно и друштвено одговорно, посебно јер смо окружени све већим бројем уређаја који истовремено снимају и обрађују прикупљене податке, уз могућност идентификације и праћења особа. Наравно, права мера се налази на „пола пута“ између потребе за безбедношћу и могућих кршења права на заштиту приватности.

ЗАКЉУЧАК

Свеопшти научни и технички напредак нужно мења постојећи поредак у свим областима битисања – друштвеном, политичком, правном, технолошком итд. То се лепо уочава на промењеном разумевању па и редефинисању приватности, како правно, тако и стварно. Отуда приватност не обитава само „у четири зида“, па ни на „четири стране света“, већ постоји у једном вишедимензионалном простору какав је дигитални. Стога се све више говори о концепту тзв. е-приватности, који је помало и контрадикторан јер је површина коју обухвата дигитална околина све само не „приватна“. То не значи да се „интима“ не може заштитити ни на који начин, али ипак захтева новије и суптилније механизме. Све то сасвим добро видимо на примеру прикупљања и обраде података о личности, на бази којих многе ствари о појединцу постају лако сазнатљиве. Због тога је њихова заштита посебан изазов.

Примарни механизми заштите леже на човеку и његовој свести о значају података о личности, те неговању безбедносне културе у дигиталном окружењу. Штету насталу злоупотребом података о личности донекле може да санира тзв. право на заборав (брисање) података, које се иначе налази у зачетку разматрања употребе података у интернет окружењу. Како ни то није увек довољно, то се прибегава кривичноправној реакцији. Улога кривичног права ни овде не одступа од традиционалних постулата ове гране права, односно, његове супсидијарне заштитне улоге, тј. *ultima ratio* карактера. Дакле, када заштита блажим средствима остане без ефекта, ваља активирати кривичноправни апарат. Оно што је проблематично јесте то што ни „стављање у погон“ кривичног права не може сасвим ефикасно да сузбије негативне ефекте података који су већ „угледали светлост дигиталног дана“.

Кривично дело неовлашћеног прикупљања личних података из чл. 146. КЗ представља инкриминацију којом се пружа појачана заштита употреби података о личности. С обзиром на прописану казну, реч је о лакшем делу па се чини да кривични законодавац ово противправно понашање не третира једнако друштвено опасним као што се то чини у матичним прописима и њиховим казним одредбама. Ипак, треба имати на уму да је ово решење из 2006. године, а да је важећи ЗЗПЛ на снази од 2018. године и, у том смислу, прати европске трендове. Видели смо да постоје поједине недоследности у законском опису овог кривичног дела. Оне се превасходно односе на нормативну редакцију чл. 146. ст. 2. КЗ, па и на његов мотив инкриминисања, а због могућих преклапања радњи извршења са онима из чл. 146. ст. 1. КЗ. На овај налаз додатно утиче и чињеница да се тежи облик из ст. 3. не односи на противзаконито прикупљање или коришћење података о личности грађана. Ова питања су оцењена као вредна даље научне обраде, али и будућих законодавних измена.

Мада је кривично дело неовлашћеног прислушкивања и снимања из чл. 143. КЗ анализирано у мањој мери, оно може бити од значаја у домену употребе тзв. дигиталних доказа, а то је и правац у којем се креће и реформа кривичног процесног законодавства. И ту постоје извесне нејасноће о којима се мора водити рачуна приликом усвајања предлога нових решења (нпр. колизија материјалноправних и процесноправних одредаба).

Коначно, „на почетку беше реч“, у средини – интернет, а на крају, чини се, потреба за проналажењем прав(н)е мере између „аналогне“ и „дигиталне“ приватности у савременом друштву.

Jovana M. Banović¹
University of Belgrade, Faculty of Security Studies
Belgrade (Serbia)

Ivana M. Radisavljević²
University of Belgrade, Faculty of Law
Belgrade (Serbia)

PRIVACY, PERSONAL DATA PROTECTION AND THE DIGITAL AGE – A (CRIMINAL) LAW “OMNIBUS”

(Translation *In Extenso*)

Abstract: The Constitution of the Republic of Serbia safeguards the right to privacy through several aspects, as does the European Convention on Human Rights and Fundamental Freedoms. The cornerstone in this area is the Law on Personal Data Protection from 2018. In line with the *ultima ratio* principle of criminal law, the Criminal Code protects these data when the most severe violations occur, pursuant to the Criminal Procedure Code. However, with the daily expansion of science, technology, and innovative means of communication and recording, this takes on a different, “digital” dimension. Naturally, this trend calls for certain adjustments in regulations, as well as in their interpretation and application. In this paper, the authors aim to highlight key provisions of the aforementioned regulations and their current and future interpretation within the context of digital society, with a particular focus on criminal law aspects. This complexity is further amplified by the development of artificial intelligence, which inherently relies on the use of vast amounts of data. The aim of this paper is to identify some of the critical elements in the protection of privacy rights, particularly those related to personal data most closely linked to individuals, and to raise the question of potential legislative amendments.

Keywords: privacy, personal data, unauthorized collection, unauthorized recording, criminal law protection

INTRODUCTORY CONSIDERATIONS

Different national and international documents directly or indirectly recognize privacy as a fundamental human right which implies the right of an individual or a group of individuals to protect their private life and private environment, including information about themselves. Today’s digital age inevitably expands this concept so that it also encompasses privacy in digital setting (“e-privacy”) and, moreover, suggests that it should

¹ jovana.banovic@fb.bg.ac.rs; <https://orcid.org/0009-0007-6324-487X>

² ivana.radisavljevic@ius.bg.ac.rs; <https://orcid.org/0000-0003-1445-707>

be observed as an independent right that deserves legal protection in itself (Romansky & Noninska, 2020, 5288–5289).

The Constitution of the Republic of Serbia (“Official Gazette of the RS”, No. 98/2006 and 115/2021, hereinafter: the Constitution), unlike the European Convention on Human Rights and Fundamental Freedoms (published with additional protocols in “Official Gazette of Serbia and Montenegro – International Contracts”, No. 9/2003, 5/2005 and 7/2005 – corrected, and “Official Gazette of the RS – International Contracts”, No. 12/2010 and 10/2015, hereinafter: European Convention), recognizes the right to privacy, but does not formulate it so explicitly as the aforementioned document of the Council of Europe. In fact, Article 8 of the European Convention defines “the right to respect of private and family life”. It includes four segments as follows: private life, family life, home and correspondents, but they are not easily separated (Beširević et al., 2017, p. 160). The Serbian Constitution, on the other hand, elaborates these four fragments in several individual provisions, the most relevant of which for the topic of our paper are Articles 41 and 42. They protect the confidentiality of letters and other means of communication and personal data.

The cornerstone law in the field of data protection is the Law on Personal Data Protection (“Official Gazette of the RS”, No. 87/2018) which, in broadest terms, regulates the collection, storage, processing and use of these data for their intended purposes, as well as a number of rules aimed at preventing data abuse. Inviolability of the confidentiality of letters and other means of communication are further regulated more directly by incriminations from Articles 142, 143 and 144, and of personal data in Article 146 of the Criminal Code (“Official Gazette of the RS”, 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). These are not the only criminal offences which protect the right to privacy and, in those terms, of relevance are also the criminal offences from Article 138a (persecution), Article 141 (unauthorized disclosure of secret) and Article 145 (unauthorized publication and display of documents, portraits and recordings) (for more information, see: Milošević, 2021, pp. 124–126). Since in this paper we will deal with personal data within the context of the right to privacy, the criminal offence from Article 146 of the Criminal Code will be the main subject matter.

In any case, data protection used to be treated as part of the right to privacy, while today it has assumed the contours of an independent concept (Blume, 2010, p. 153), and even of a separate branch of law (Andonović & Prlja, 2020, p. 54). In that respect, the focus of our paper will be mainly directed towards personal data, although it indisputably implies the right to privacy as well.

Speaking of digital “setting”, it should be emphasized that now already famous 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, hereinafter: GDPR), takes into account the Internet setting through regulating the “right to erasure, i.e., the right to be forgotten” from Article 17 of GDPR.³ And what are the specific features of data protection in the digital age?

³ The right to be forgotten is defined as “the right to request the removal of personal data from websites or browsers, particularly when such data are irrelevant, obsolete, harmful or violating an individual’s privacy or dignity” (Gill, Redeker, Gasser, 2015, p. 8). This right entitles an individual to request limited access to previous information which harm his/her present and future interests through erasure or

(OLD) CHALLENGES OF THE NEW AGE

At the very end of the previous millennium, Berman & Mulligan published a somewhat revolutionary paper in which they indicated that the internet, at the time still in the “creation stage” for broader population, gave a new perspective to the issue of privacy protection. They recognized three key points at this level, namely: increasing generation and collection of data; information globalization and spread; the lack of centralized control over data protection (Berman & Mulligan, 1999, pp. 554–556). After a quarter of the century, these problems are not only current but even further compounded by the constant development and accessibility both of the internet and of other digital technologies creating a practically new social framework of human action.⁴

Data indisputably “go into the ether” through direct and willing action of the person they refer to (e.g., we will enter data about personal name, address, Unique Master Citizen Number etc. when registering for a discount card in a favourite shop or when purchasing an insurance policy before going on a skiing trip). However, a large amount of data is collected on a daily basis not so much without our consent as without our being aware of it or, more precisely – without our paying attention to it (e.g., security cameras, sometimes with a clear warning that the space is under video-surveillance, and sometimes without it; our movement while using GPS devices which are available on almost all mobile devices; the use of “smart gadgets” in households, which are operated through WiFi remote connection, biometric data for “unlocking” mobile phones etc.; for more information about the current legal and real situation in these fields, see: Petrović, 2024; Ružić, 2024).

The internet is “a planet without borders” and these data can be found practically in any part of the world and even – graphically speaking – underneath it. It is illustrated by the use of the *deep web* and *dark web*, where it is possible to trade illegally with various resources (people, weapons, drugs...), and even personal data. For instance, to avoid measures directed at preventing money laundering, which imply complete identification of the service user, it is possible to buy special KYC (*Know Your Customer*) Kits with the aim of avoiding the identification, or disclosure of the real user. In this “set”, it is often possible to obtain almost all personal data that have been made up, and often the real ones which have been stolen (Elliptic, 2024, p. 27)⁵.

modification of such data. This right emerged exactly with the development of technology and means of communication, while the same attitude is taken by the European Court of Human Rights. For more information, see: Case of Hurbain v. Belgium, Application no. 57292/16, July 4th, 2023, §191 et seq.

⁴ We can say that today there are available technologies which were practically in the domain of science fiction at the time of the preparation of the cited paper. There is also an illustrative example from the film “Fifth Element” from 1997, in which flying cars are shown as an ordinary means of transport. We still do not have cars like that, but so-called autonomous vehicles are being developed and used on a large scale. For more about certain matters of responsibility for accidents involving self-driving cars, see: Banović, 2023, pp. 41–43. In fact, since 2 December 2023, the Republic of Serbia has applied the the Regulation on the Conditions for Autonomous Driving (“Official Gazette of the RS”, No. 104/23), the main subject of which is the regulation of procedures of issuing the testing licence (sic!) for an autonomous vehicle.

⁵ It is interesting that in the aforementioned manual there is an example of a purchase offer which, in addition to the data about the seller and the prince, there is also a photograph of the ID issued in

Speaking of the lack of centralized control of data protection, GDPR has significantly contributed to the unification of these rules. Serbia's Law on Personal Data Protection was also enacted after the model of GDPR and the so-called Police Directive (Directive /EU/ 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA). We have mentioned that, owing to its revision, this act largely follows modern development trends, but individual countries must also take into account general digital development.

Data protection, apart from normative advancements, increasingly implies technical advancements as well. Therefore, for example, the development of the internet may be described through three stages: *read (Web1) – read, write (Web2) – read, write, own (Web3)*. Namely, in the first stage, the internet was designed so as to enable users to use only the existing content, but not to create new content. The second stage is characterized by the creation of social networks (Facebook, Google, Wikipedia...) and by providing users with the opportunity to create their own content (so-called *user generated content*). This mechanism resulted in voluntary placement of a large amount of data which were stored on larger servers and then led to a phenomenon known as “targeted advertising directed at a specific user”. In this manner, a large amount of information about individuals is collected and stored, which opens up the space for certain abuses as well.⁶ In the essence of these unlawful activities is exactly the centralized system on which all those collected or supplied data are stored. When, through the expansion of digital property, all innovative advantages of blockchain technology were acknowledged, the idea developed according to which the third-generation internet – *Web3*, could rely on decentralization. It would mean that large platforms such as Google, Amazon etc. would not be “absolute masters” of a multitude of data, but it would be the user himself as the data owner (Stackpole, 2022).

This is exactly why in the paper below we will deal with unauthorized data collection in various forms.

the Republic of Serbia, although with partly concealed data (probably due to the unfamiliarity with the language and the Cyrillic script, the signature remained visible, and that is how the identity of the ID owner “ending up” in the market could be determined).

⁶ For example, the Court of Justice of the European Union passed its judgment in the case *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)* and established the violation of the right to privacy due to the lack of transparency, where Google did not clearly and comprehensibly explain to its users how their data were collected and processed; moreover, insufficient information was given when data about processing were not easily accessible, so users had to take several steps to get key information about the use of their data; finally, the consent for personalized ads was inadequate because Google had not obtained the user's consent for processing personal data for the purpose of ad personalization, since it was not sufficiently specific and unique. Judgment of the Court (Grand Chamber) of 24 September 2019, available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:62017CJ0507>.

CRIMINAL LAW IN “CLICK” SOCIETY

Criminal substantive and procedural law, just as all other branches of law, must follow the development of digital society and adjust to it to an appropriate extent. Although legislative interventions performed in the previous decade are not in favour of this, criminal substantive law is a less dynamic ranch of law in which too frequent amendments are not desirable. In that respect, when it comes to individual criminal offences the characteristics of which are increasingly transferred into digital setting, there is still room for amendments in order to avoid forbidden analogies in interpretation in those situations when a specific norm is missing. Our focus will be primarily on “digital aspects” of the criminal offence from Article 146 of the Criminal Code, and, to a certain extent, from Article 143 of this Code.

Unauthorized collection of personal data (Article 146 of the Criminal Code)

The criminal offence from the title of this segment of the paper can have its main, special and graver form. The offender of the main form may be anyone who undertakes any of the three stipulated acts: unauthorized acquisition, disclosure to others, or the use of data for unintended purposes. The object of the commission of the criminal offence are personal data which are collected, processed and used in compliance with the law. Those are data which are legally owned by the handler or processor (their definitions are provided in the Law on Personal Data Protection, Article 4, Paragraph 1, Items 8 and 9), but which, due to the execution of one of the above-listed acts, reach an uninvited person (Milošević, 2022, p. 65). Having in mind the fact that today a large amount of data is stored and transferred in a digital form (Mandić, Putnik & Milošević, 2017, p. 25), the manifestation forms of this criminal offence are increasingly becoming “more digital”⁷.

Hypothetically speaking, personal data in this setting may be obtained in different ways. For example, by hacking data bases, i.e., through unauthorized access to computing systems, which is most often done by entering computer viruses; by singling data out from “cloud” systems – through unauthorized access to accounts on data storage platforms (Google Drive, Dropbox) for the purposes of downloading or copying personal data; contactless scanning aimed at acquiring data from personal documents or payment cards with the aid of devices for wireless data reading. Therefore, these are data which were legally collected earlier, but which are now obtained by someone without authorization from the base in which they are legally stored. These are examples in which the very method of obtaining data is subject to punishment, regardless of the circumstance whether those are personal data or not. That is why it is important to emphasize that in this manner it is also possible to commit other criminal offences, so in criminal law terms we (most frequently) speak about joinder of offences, since same acting attacks different objects of protection. That is why this refers primarily to the criminal offences from the group directed against the

⁷ Moreover, possibilities for processing large amounts of data are constantly increasing with the development of artificial intelligence, even in the systems which handle particularly sensitive data. Therefore, artificial intelligence is used today, for example, for the analysis of legal documents, contracts, case law, evidence etc. in order to facilitate and accelerate legal traffic and court proceedings (Matić Bošković, 2024, pp. 482–483).

security of computer data⁸ (creating and introducing computer viruses, unauthorized access to protected computers, computer networks and electronic data processing etc. (for more information, see: Putnik, Milošević, Cvetković, 2022, p. 331), those offences directed against property (fraud), against state bodies (false impersonation). However, it should be noted that these criminal offences are mostly prosecuted *ex officio*, while the criminal offence from Article 146, Paragraphs 1 and 2 of the Criminal Code is processed in a private lawsuit, so that even in these cases it has “an independent procedural life”, and the matter of joinder of offences is of no particular practical significance.

The act of disclosure has become increasingly relevant with the development of social networks which enable rapid spread of information that can become known to a large number of people in a short period. Having in mind that personal data are any data referring to a natural person whose identity is determined or determinable, directly or indirectly, particularly on the basis of identity marks, such as name and identification number, location data, identifiers in electronic communication networks, and of one and/or several features of the person's physical, physiological, genetic, mental, economic, cultural and social identity (Article 4, Paragraph 1, Item 1 of the Law on Consumer Protection), the amount of information that can be disclosed in terms of this act is indicative. It may be done by posting photographs, video-clips, texts or voice messages containing these data – person's appearance, number, voice etc.

The act of using data for unintended purposes is somewhat more specific because the owner of such personal data is authorized to keep them, has obtained them legally, but subsequently uses them against the law. The difference between this act and the previous acts is perceived only when connected with the purpose of using the given data. For example, the data processor who works in a public notary's office, legally and by using the official information system, processes data about someone's name, identification number, address, real estate deals etc. in relation to the business activity. However, when the data processor uses those data to make them available to an investor, with the aim of expanding the investor's business operations, i.e., enabling the investor to offer newly-built apartments to those people, it can be defined as a commission of this act.

Although it is disputable whether this refers to the second main form or to a separate form, the offence from Paragraph 2 exists when citizens' personal data are collected unlawfully and when the data collected in this manner are used. In relation to the form pursuant to Article 146, Paragraph 1 of the Criminal Code, the committed act refers to unlawful collection of personal data. In a time relationship, the act of collection precedes the act of commission from Paragraph 1, i.e., the act of collection. In fact, collection is performed in relation to the already legally collected data (Paragraph 1), while unlawful collection is initially against the regulations (Paragraph 2).

However, two things are contentious here. First, are “unauthorized” collection (Article 146, Paragraph 1 of the Criminal Code) and “unlawful” collection (Article 146, Paragraph 2 of the Criminal Code) synonymous? Second, does the object of the act of the second

⁸ Personal data can also be obtained by intercepting communication. It is interesting that international documents stipulate the criminal character of these activities in the domain of high-technology crime, while it is not the case with our applicable Criminal Code, although it is otherwise harmonized with these instruments (Delić, 2021, p. 327; Milošević, 2022, p. 171, fn. 55).

(special) form refer only to personal data in terms of the Law on Personal Data Protection, or are those “qualified” personal data of several citizens, i.e., is it plural in linguistic terms (Lazarević, 2011, p. 553)? We believe that these are synonyms, particularly because it is a blanket criminal offence (Milošević, 2021, p. 119). However, in Paragraph 1, unlawfulness appears only in the second step – data are legally there (first step), but their handling is unlawful (second step), while in Paragraph 2, this unlawfulness begins with the first step – data are not legally owned and, consequently, no other action can be legal (although this refers to the property right rule, so it is purposeful to note that here we also have the principle of “something that is born wrong cannot be corrected with time”). Another contentious thing does not seem to be the matter of the language interpretation of grammatical singular/plural, but simply of an awkward legal formulation and a questionable legislative motive of incrimination. Similarly to the first form, through illegal collection of personal data, it is possible to realize the elements of some other criminal offences, e.g., by creating fake applications or web pages which emulate official services, and which are used for entering personal data; through social engineering by encouraging users to disclose personal data etc.

For both forms of this criminal offence, there is a stipulated fine or prison sentence of up to one year, which suggests that it is a minor offence, so that it is possible to apply more lenient criminal sanctions or institutes, such as an offence of minor significance or an opportunity of criminal prosecution.

A graver form of this criminal offence exists in case the offence from Article 146, Paragraph 1 of the Criminal Code is committed by an official *ex officio*, which consequently leads to the possibility of imprisonment of up to three years. Unlike the man and the special form, prosecution is undertaken *ex officio*. It is interesting that the graver form does not refer to Article 146, Paragraph 2 of the Criminal Code, although these persons definitely have the factual possibility of collecting data illegally in the above-mentioned terms. A relevant form of guilt in all three forms is intention, whereas in some cases we can speak of the existence of real or legal illusion as the basis for excluding guilt (Milošević, 2021, p. 118).

These dilemmas do not seem as something that may be resolved solely by interpreting the regulations. Here, a detailed analysis of the criminal offence is necessary, including an adequate legislative intervention afterwards. This is particularly valid because some violations defined in the Law on Personal Data Protection, which contain “more recent” norms than Article 146 of the Criminal Code (unamended since 2006), coincide with the characteristics of this criminal offence. Finally, it is a legally unsustainable situation which undermines legal security and calls for systematic harmonization of regulations (for more information, see: Milošević, 2021, pp. 119–121).

About unauthorized wiretapping and recording (Article 143 of the Criminal Code) with a focus on “digital” evidential significance

The main form of the criminal offence from the title of this segment exists if special devices are used for unauthorized wiretapping or recording a conversation, statement or any announcement not intended for the person doing it, as well as, in a special form, if an uninvited person is enabled to learn about a conversation, statement or announcement

previously heard in an unauthorized way, i.e., previously recorded. There is a stipulated fine or a prison sentence from three months to three years. The object of this criminal offence are conversations, statements or announcements – not personal data as such, but a broader form which may contain them indirectly. It is also important to emphasize that this offence is committed by using special devices for listening and recording. Particularly indicative for our topic is the fact that through audio and video recordings made as the object of the criminal offence it is possible to obtain certain personal data as well. That is why here a question arises about the relationship of this criminal offence and the criminal offence from Article 146 of the Criminal Code. Although this refers to the same group object of protection (people's and citizens' rights and freedoms), incrimination is completely different. Accordingly, since this criminal offence is also prosecuted in a private lawsuit, it is possible to imagine that the private lawsuit may include both offences. The graver form exists if the offence from Article 143, Paragraphs 1 and 2 of the Criminal Code is committed by an official *ex officio*, and imprisonment from six months and five years, and prosecution *ex officio* are prescribed.

What is “digital” in this criminal offence? First of all, the means of commission itself, i.e., electronic recording device(s). Furthermore, the methods of commission and products of the content generated in that manner. Nevertheless, what is a particularly interesting topic is the possibility of using the recorded content as evidence in criminal proceedings (Lazić & Radisavljević, 2018, pp. 381–386; Milošević, 2021, pp. 123–124). The use of the evidence made in this way is not indisputable, although interpretations and case law are in favour of allowing their use under certain conditions (e.g., warning that a certain person is being recorded). Hence, the proposal of subsequent amendments to the Criminal Procedure Code (Draft Criminal Procedure Code, <https://www.mpravde.gov.rs/sekcija/53/radne-verzije-propisa.php>) raises the very question of so-called digital evidence. These amendments propose a rule in Article 139a according to which photographs or sound and/or optical recordings, made in line with this Code, may be used as evidence and as a foundation of the court decision. On the other hand, if those are photographs or sound and/or optical recordings which do not belong to the category of this rule, they can be used as evidence in criminal proceedings only when the suspect is in the photograph or on the recording, i.e., if his/her voice has been recorded. Consequently, if these amendments are adopted, so-called amateur recordings might indisputably be used as evidence.

What complicates these issues further are the proposed amendments to the Criminal Code exactly in the domain of Article 143 of the Criminal Code (the Draft Criminal Code, <https://www.mpravde.gov.rs/sekcija/53/radne-verzije-propisa.php>). In fact, they propose deleting the syntagm “unintended to that person”, which implies that the criminal offence would be committed by anyone using special recording devices, no matter whether they participate or not, and no matter whether in that manner “evidential material is acquired” about the commission of the criminal offence. There is an unclear relationship between proposed substantive and procedural provisions about this matter. The blanket character of this criminal offence as well, because of the word “unauthorized”, might point to a specific foundation for excluding unlawfulness contained in the Criminal Procedure Code. Moreover, in the field of criminal substantive law, it is also possible to speak theoretically about a form of acting in self-defence, if by recording we try to refuse a simultaneously unlawful attack to our legally protected good.

It is clear that it is necessary to give appropriate significance to this issue and deal with it with legal and social responsibility, particularly because we are surrounded by an increasing number of devices which simultaneously record and process collected data, with the possibility of identifying and tracking people. Of course, the right measure is “somewhere halfway” between the need for security and potential violations of the right to privacy protection.

CONCLUSION

General scientific and technical progress inevitably changes the existing order in all areas of life – social, political, legal, technological etc. It is properly seen in the modified understanding and even redefinition of privacy, both legally and in practice. Hence, privacy does not exist only “between four walls” or on “four sides of the world”, but also in multidimensional space, or digital space. That is why we pay more attention to the concept of so-called e-privacy, which is slightly contradictory because the area covered by digital setting is all but “private”. This does not mean that “intimacy” cannot be protected at all, but it still requires more novel and subtle mechanisms. It can be perfectly seen in the example of collecting and processing personal data, on the basis of which it is possible to find out easily many things about an individual. That is why their protection is a special challenge.

Primary mechanisms of protection rely on man and his awareness of the significance of personal data, and on the cultivation of security culture in digital setting. The harm caused by the abuse of personal data can be to a certain extent alleviated by the so-called right to be forgotten, i.e., the right to data erasure, which is in the beginning stage of considering the use of data in the internet setting. Since it is not always enough, it is necessary to resort to a criminal law response. The role of criminal law does not deviate from traditional postulates of this branch of law, or its subsidiary protective role, i.e., *ultima ratio* character. Therefore, when protection with more lenient means makes no effect, it is necessary to activate the criminal law apparatus. What is problematic is that not even “putting criminal law in operation” cannot completely efficiently suppress negative effects of data which “have already seen the light of digital day”.

The criminal offence of unauthorized collection of personal data from Article 146 of the Criminal Code is an incrimination which provides greater protection to the use of personal data. Having in mind the prescribed punishment, it is a minor offence, and the criminal legislator does not seem to treat this contradictory behaviour as equally socially dangerous as in the case of basic regulations and their penal provisions. However, it should be taken into account that this decision is from 2006, while the applicable Law on Personal Data Protection has been in force since 2018 and, in that respect, it follows European trends. We have noticed certain inconsistencies in the legal description of this criminal offence. They mainly refer to the normative revision of Article 146, Paragraph 2 of the Criminal Code, including its motive of incrimination, due to potential overlapping of the acts with those from Article 146, Paragraph 1 of the Criminal Code. This finding is further affected by the fact that the graver form pursuant to Paragraph 3 does not refer to unlawful collection or use of citizens' personal data. These matters are assessed as worthy of further scientific processing, as well as of future legislative amendments.

Although the criminal offence of unauthorized wiretapping and recording from Article 143 of the Criminal Code has been analyzed to a smaller extent, it may be significant in the domain of the use of so-called digital evidence, and that is also the direction in which the reform of criminal procedural legislation is going. There are also certain unclear things which must be taken into account when adopting proposals of new solutions (e.g., collision of substantive-legal and procedural-legal provisions).

Finally, “in the beginning there was a word”, in the middle – the internet and, at the end, apparently, the need for finding the right (legal) measure between “analogous” and “digital” privacy in modern society.

REFERENCES / ЛИТЕРАТУРА

- Andonović, S., Prlja, D. (2020). *The Basics of Personal Data Protection Rights*. Beograd: Institut za uporedno pravo, Službeni glasnik. [In Serbian]
- Banović, J. (2023). “Professional Negligence” – Criminal Law Response to Professional Risks. In: N. Stekić, M. Milošević (eds.). *Proceedings from the 2nd Memorial Scientific Conference “Predrag Marić”*, 33–45. Beograd: Univerzitet u Beogradu – Fakultet bezbednosti. [In Serbian]
- Berman, J., Mulligan, D. (1999). Privacy in the Digital Age: Work in Progress. *Nova Law Review*, 23 (2), 549–583. Available at: <https://nsuworks.nova.edu/nlr/vol23/iss2/2>
- Beširević, V. et al. (2017). *Commentary on the Convention for the Protection of Human Rights and Fundamental Freedoms*. Beograd: Službeni glasnik. [In Serbian]
- Blume, P. (2010). Dana Protection and Privacy – Basic Concepts in a Changing World. *Scandinavian Studies in Law*, 151–164. Available at: <https://www.scandinavianlaw.se/pdf/56-7.pdf>
- Case of Hurbain v. Belgium, Application no. 57292/16, July 4th, 2023 Available at: <https://hudoc.echr.coe.int/eng?i=001-225814>
- Constitution of the Republic of Serbia (“Official Gazette of the Republic of Serbia”, No. 98/2006 and 115/2021). [In Serbian]
- 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]
- Delić, N. (2021). *Criminal Law – Special Part*. Beograd: Univerzitet u Beogradu – Pravni fakultet. [In Serbian]
- Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
- Draft on Criminal Code of Serbia, Available at: <https://www.mpravde.gov.rs/sekcija/53/radne-verzije-propisa.php> [In Serbian]
- Draft on Criminal Procedure Code of Serbia, Available at: <https://www.mpravde.gov.rs/sekcija/53/radne-verzije-propisa.php> [In Serbian]
- Elliptic (2024). Preventing Financial Crime in Cryptoassets. *Typologies Report 2023*.

- European Convention for the Protection of Human Rights and Fundamental Freedoms (ratified with additional protocols in the “Official Gazette of Serbia and Montenegro – International Agreements”, No. 9/2003, 5/2005, and 7/2005 – corrected, and the “Official Gazette of the RS – International Agreements”, No. 12/2010 and 10/2015). [In Serbian]
- 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)
- Gill, L., Redeker, D., Gasser, U. (2015). Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights. *The Berkman Center for Internet and Society at Harvard University, Research Publication* (15), 1–26. Available at: <https://ssrn.com/abstract=2687120> or <http://dx.doi.org/10.2139/ssrn.2687120>
- Judgment of the Court (Grand Chamber) of 24 September 2019. Available at: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:62017CJ0507>
- Law on Personal Data Protection (“Official Gazette of the Republic of Serbia”, No. 87/2018. [In Serbian]
- Lazarević, Lj. (2011). *Commentary on the Criminal Code*. Beograd: Pravni fakultet Univerziteta Union. [In Serbian]
- Lazić, D., Radisavljević, I. (2018). Legal Importance of Amateur Audio and Video Recordings. *Godišnjak Fakulteta bezbednosti*, (1), 371–389. Available at: <https://scindeks-clanci.ceon.rs/data/pdf/1821-150X/2018/1821-150X1801371X.pdf> [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. M. (2024). Impact of artificial intelligence on practicing judicial professions. *Sociološki pregled*, LVIII (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]
- Petrović, Z. (2024). Video Surveillance and Personal Data Protection in the Republic of Serbia. *Savremene studije bezbednosti*, (1), 57–82. doi: [10.5937/ssb2401057P](https://doi.org/10.5937/ssb2401057P). Available at: <https://fb.bg.ac.rs/download/zbornici/SSB-1-2024-FB.pdf> [In Serbian]
- Putnik, N. R., Milošević, M. M., Cvetković, V. N. (2022). Ransomware as a Security Threat – Social and Criminal Legislation Aspects. *Sociološki pregled*, 56 (1), 328–353. doi: [10.5937/socpreg56-36845](https://doi.org/10.5937/socpreg56-36845)
- Romansky, P., Noninska, S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, 17 (5), 5288–5303. doi: [10.3934/mbe.2020286](https://doi.org/10.3934/mbe.2020286)
- Ružić, N. (2024). Facial Recognition Technology, and the Rights and Freedoms – Case of the Republic of Serbia. *Savremene studije bezbednosti*, (1), 83–101. doi: [10.5937/ssb2401083R](https://doi.org/10.5937/ssb2401083R). Available at: <https://fb.bg.ac.rs/download/zbornici/SSB-1-2024-FB.pdf> [In Serbian]
- Stackpole, T. (2022). What Is Web3? Your guide to (what could be) the future of the internet. *Harvard Business Review*. Available at: <https://hbr.org/2022/05/what-is-web3>