УДК: 004.738.5:343.9.02
Biblid 1451-3188, 22 (2023)
Год XXII, бр. 84, стр. 177–192
Изворни научни рад
Рад примљен 26. 7. 2023. године
Рад одобрен 10. 10. 2023. године
DOI: https://doi.org/10.18485/iipe_ez.2023.22.84.10

САЈБЕР БЕЗБЕДНОСТ *vs*. ПРИВАТНОСТ – ОПШТА РАЗМАТРАЊА И ОСНОВИ ЗАШТИТЕ

*Драгана ПЕТРОВИЋ**

Апстракт: Данас се у свету на различитим нивоима воде озбиљне расправе о могућностима модерних информационо-комуникационих технологија (ICT), али и о њиховим нежељеним последицама. За обичног човека, „нов" начин комуникације преко интернета и мобилне телефоније истовремено је лак, једноставан, брз, нужан – постаје чињеница његовог свакодневног живота. Штавише, савремено доба подразумева интернет као једно од главних средстава комуникације. Уколико се користи „како треба", представља изобиље информација на готово сваку тему и доноси многе бенефите. Уз разноврсну количину прикупљених података с лакоћом посредује у стицању нових знања и обликовању животног стила. У тој перспективи, живот у интернет мрежи постаје све више простор подложан манипулацијама и злоупотребама. Списак злоупотреба је дуг – од напада на туђу приватност, прогањања, сајбер мобинга, вршњачког насиља, сексуалног узнемиравања и насиља, трговине људима и људским органима и др. На тај начин, појава нових технологија значајно угрожава право на приватност. Последњих година право на приватност у највећој мери доводи се у везу са подацима о личности. Право на приватност и заштита личних података спада у ред основних људских права. Будући да се ради о темељном праву

* Институт за упоредно право, Београд. E-mail: d.petrovic@iup.rs.

Рад је настао као резултат научноистраживачког рада Института за упоредно право који финансира Министарство науке, технолошког развоја и иновација Републике Србије према Уговору о реализацији и финансирању научноистраживачког рада НИО у 2023. години (евиденциони број: 451-03-47/2023-01/200049 од 3. 2. 2023).

човека и грађанина, основ његове заштите у нашем законодавству садржан је, пре свега, у Уставу, Закону о заштити података (ЗЗЛП) и Кривичном законику (чл 146. Неовлашћено прикупљање личних података). Циљ рада је да се допринесе научној расправи у тој области.

Кључне речи: Сајбер безбедност, сајбер криминал, приватност, заштита података о личности, нормативни оквири

1) УВОД

Одмах, на почетку, морамо се сложити да је данас бескорисно памтити податке из историје, математике, уметности, књижевности итд. Сваки „комплекс" у добијању информације редуциран је само на два клика на интернету. Све смо зависнији од интернета и на задовољство многобројних корисника широм света, та модерна технологија сваким даном постаје све доступнија и једноставнија за употребу. Већина нас има паметне мобилне телефоне, рачунаре, таблете, друштвене мреже, СМС поруке, видео снимке, слике. Може се запазити да нове технологије постају наша екстерна меморија. Оне су увелико загосподариле нашим животима и спонтаном комуникацијом. Својом свеприсутношћу прекриле су „микроструктуре свакодневног живота све до човекове приватности и присности, чак и до његовог сна". Интернетска друштвена мрежа Фејсбук, 4. марта ове године, прославила је свој 18. рођендан. Његових 2,8 милијарде месечно активних корисника широм света потврдило је да је у питању један од најатрактивнијих медијских феномена с почетка овог миленијума (2010–2019), глобално.[1] Да, реч је о глобалном феномену – укидају се просторна, регионална, етничка и друга ограничења – и тако свет прераста у глобалну заједницу, а интернет у информациону супер саобраћајницу.[2] Истиче се да је он постао технолошки, социјални, медијски, политички, али и правни феномен. То „мноштво" одједном делује као несагледива стихија. Нема сумње да на данашњем степену развоја тренутно није могуће постићи потпуну сигурност информационог система. Зато је потребно пружити апсолутну и делотворну заштиту ако дође до

[1] Фејсбук је осмислио Mark Zuckenberg, бивши студент са Харварада (са пријатељима). У почетку је био намењен само студентима тог универзитета који су путем ове мреже међусобно комуницирали и размењивали информације. Касније су му се прикључили многи други универзитети, средње школе, велике корпорације широм света и др. Кад је чувена компанија Мајкрософт купила 1,6 одсто акција у Фејсбуку за 240 милиона долара, а вредност сајта процењена на петнаест милијарди долара, постало је јасно да се родио глобални феномен, а његов идејни творац – најмлађа особа на Форбсовој листи најбогатијих људи на свету. Године 2021. Фејсбук мења име у МЕТА. Видети: Андреј Дилигенски, Драган Прља, *Фејсбук, заштита података и судска пракса*, Институт за упоредно право, Београд, 2018, стр. 9.

[2] Интернет: https://www.michalsons.com/focus-areas/cybercrime-law, 14.10.2021.

његове злоупотребе (крађа идентитета, преваре, тероризам, пиратерија, говор мржње, интернет вандализам, злоупотреба фотографија, патолошка зависност од коришћења интернета и др.).[3] Како нас је снажна динамика промена захватила на овом терену, технизација међуљудске комуникације усвојила је нове методе, и то тако да постоји само један начин – потпуна замена стварности за „стварност" из интернетске мреже. Најважнији модни детаљ је постао мобилни телефон. Новом тренду масовног и опсесивног коришћења овог уређаја произвођачи се врло брзо прилагођавају, увлачећи кориснике без отпора у своје мреже до патолошке зависности (оруђе „великог брата").[4] Реч је о неповратном процесу – модерна интернет технологија свуда се угнездила и није поштедела ниједан ниво људске делатности и човекове личности.[5] Све је учинила огољеним и јавним. Интернет технологија је довела до поништавања свега оног што чини човеково најинтимније „приватно власништво". Из перспективе света у коме живимо, са наглим развојем мрежних дигиталних технологија, право на приватност, па тиме и заштита података о личности, озбиљно су доведени у питање. Као да су повреде приватности и незаконите обраде личних података постале неизбежна карактеристика модерног интернет пејзажа.[6] То је реалност у којој се тренутно налазимо. Али, упоредо са оваквом опомињујућом реалношћу расту и напори у правцу развоја законске регулативе на међународном и националном нивоу – све у циљу да се ефикасно реши питање њихове заштите, да се та заштита појача и прошири.[7] Јер, сасвим разумљиво, промене на сцени употребе модерних информационо-комуникационих технологија и негативни ефекати које оне производе захтевају и промене у реаговању на угрожавање овог, једног од најважнијих људских права.[8]

---

[3] Sarah Summers, "EU Criminal Law and the Regulation of Information and Communication Technology", *Bergen Journal of Criminal Law and Criminal Justice*, no. 1/2015, pp. 48–60.

[4] Richard Stallman, „Mobilni telefoni su Staljinov san", B92. Интернет: http://www.b92.net/tehnopolis/vesti.php?yyyy=2011&=038nav_id=499267, 19.7.2012.

[5] Интернет: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199680832.001.0001/oxfordhb-9780199680832-e-65, 24.3.2022.

[6] Dragan Prlja, Mario Reljanović, "Sybercrime – Comparative experiences", *Strani pravni život*, no. 3/2009, pp. 163–164.

[7] Интернет: https://www.michalsons.com/blog/what-is-it-law-ict-law-or-cyber-law/286, 17.12.2021.

[8] Наташа Мрвић Петровић, „Споразумно признање кривице у дигиталном окружењу", у: Јелена Костић, Марина Матић Бошковић (урс.), *Дигитализација у казненом праву и правосуђу*, Институт за упоредно право, Институт за криминолошка и социолошка истраживања, Правосудна академија, Београд, 2022, стр. 155.

2) КРИМИНАЛ, БЕЗБЕДНОСТ И ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ

Као што се лако може приметити, „сајбер безбедност“ и „заштита информација“ су постале веома популарне речи у нашем свакодневном животу, нарочито после пандемије изазване корона вирусом. Организације, владе, финансијске институције и други субјекти изложени су сталним сајбер претњама. Средства сајбер напада „ у рукама“ сајбер криминалаца сваким даном постају све софистицираниja, чиме се повећава ризик од угрожавања сајбер безбедности. То је темељно питање, централни проблем – апсолутна супротност у смислу да оно што може да се употреби у корист друштва може да се употреби и на његову штету. Према Форбсу, у 2019. години и појединци и бизнис компаније изгубиле су преко 3,5 милијарди долара од сајбер криминала. У том периоду, Федерални истражни биро *(FBI*) регистровао је 467.361 пријаву за сајбер криминал.[9] Ово се све догађа четири деценије након појаве интернета, који је, поновимо, у почетку представљао само лабаво повезан систем компјутера који су користили телефонске линије као средства комуникације. Шездесетих година прошлог века америчка војска је користила ову компјутерску мрежу спремајући се за евентуалне нуклеарне нападе. Данас, интернет представља извор несагледивог броја најразличитијих информација и посебну врсту дигиталне енциклопедије. У свему томе што је добро има и онога што је деструктивно и рушилачко, оно што повећава рањивост савременог друштва. Наиме, са невероватно брзим развојем дигиталне технологије и информационих система, у корак је ишао и упадљиво брзи развој ове врсте криминалитета. Уз експанзију броја корисника интернета повећао се и број хакера, међу њима и број веома талентованих професионалаца који продају стручно знање ономе ко понуди најбољу цену. Реч је о особама које су способне да неопажено „провале“ и искористе системе за убацивање вируса, терорисање, брисање фајлова, креирање технолошког хаоса и сл. Међу супарничким земљама постоји сајбер-шпијунажа која представља опасност по националну безбедност. Свака врста класичних типова криминалитета добија одговарајући простор, има свој појавни облик и у сајбер простору: сајбер-секс, сексуално узнемиравање, силовање, отмица деце, дечија порнографија и сл. Оно што је посебно забрињавајуће је чињеница да се већини злочина учињених на овакав начин не може ући у траг, што њиховим учиниоцима омогућава да слободно владају у свом царству криминалитета. Сајбер криминал се описује као криминалитет будућности, јер обухвата и криминалитет и компјутерску технологију и информационе системе. Он угрожава безбедност милиона

[9] Интернет: https://www.eccu.edu/blog/cybersecurity/the-role-of-cyber-laws-in-cybersecurity/, доступно 13.10.2022.

људи широм света, а посебно су рањиви војни компјутерски системи због могућег изазивања ратних сукоба (војна безбедност). То чини сајбер криминал потенцијално опаснијим и од употребе биолошког и хемијског оружја.[10] Ова врста „провалника" може да обезбеди приступ контролним системима готово сваке компаније на свету и то са најудаљеније географске тачке. Мете могу да буду и банке, међународни финансијски центри и берзе, што може да доведе до губљења поверења у економски систем (економска безбедност). Наш свакодневни живот може да буде прекинут сајбер нападима на електричне и гасне системе итд. Из овог упућивања, сајбер безбедност не може да се посматра одвојено од безбедности у стварном свету.[11] У овом контексту, штете које настану као резултат сајбер напада су врло стварне и проузрокују стварне последице у физичком свету.[12] Као таква, сајбер безбедност постаје саставни део наших свакодневних живота и више се не може разликовати од општег концепта безбедности. „Она се мора доживљавати као природна потреба да заштитимо себе и своје институције, осећајући је суштински као део нашег размишљања и поступања."[13] То је разлог зашто је сајбер безбедност, настала као ограничена и специфична грана права која се односи на заштиту рачунарске опреме и система као и информација које се чувају и „путују" са њима, у тој мери напредовала.[14] Повреде података представљају нападе на сајбер безбедност које директно тангирају право на приватност и заштиту података. Из овакве формулације можда може да се препозна идеја да су сајбер безбедност и безбедност информација и приватност података „заменљиви" појмови, али између њих постоје важне разлике.[15] Шта је сајбер безбедност? Сајбер безбедност или безбедност информација подразумева мере предузете за заштиту рачунара или рачунарског система од неовлашћеног приступа хакера. Снажна политика сајбер безбедности штити сигурне, критичне или осетљиве

[10] Dragana Petrović, "General characteristics of the basic concept of terrorism", *Strani pravni život,* no 4/2020, p. 8, 14.

[11] Садмир Каровић, Марина М. Симовић, „Кривичноправно супротстављање вискотехнолошком – компјутерском криминалитету: савремени изазови, дилеме, перспективе", у: Јелена Костић, Марина Матић Бошковић (урс.), *Дигитализација у казненом праву и правосуђу*, Институт за упоредно право Београд, Институт за криминолошка и социолошка истраживања Београд, Правосудна академија, Београд, 2022, стр. 47–50.

[12] Интернет: https://www.rnids.rs/%D0%BE-%D0%BD%D0%B0%D0%BC%D0%B0/%D1%81%D0%B0%D1%98%D0%B1%D0%B5%D1%80-%D0%B1%D0%B5%D0%B7%D0%B1%D0%B5%D0%B4%D0%BD%D0%BE%D1%81%D1%82, 13.10.2022.

[13] Интернет: https://www.ictsecuritymagazine.com/notizie/cybersecurity-law-una-panoramica-sulla-disciplina-nazionale-e-comunitaria-in-tema-di-sicurezza-informatica/, 13.10.2022.

[14] *Ibid.*

[15] Интернет: https://amtrustfinancial.com/blog/small-business/cybersecurity-vs-data-privacy, 10.10.2022.

податке и спречава да ови „дођу у руке“ злонамерних трећих страна.[16] Шта је приватност података? Но, пре детаљнијег одговора на конкретно постављено питање, учинимо пар напомена која се тичу овог компликованог проблема. Веронис *(Varonis)* дефинише приватност података као врсту „безбедности информација која се бави правилним руковањем подацима који се тичу сагласности, обавештења, осетљивости и регулаторних питања“.[17] У будућности, друштво ће бити принуђено на један другачији концепт размишљања који ће повећати и сложеност истрага и превенцију злочина, док ће истовремено продубљивати регулаторне изазове. Како је сајбер криминал постао неизбежна карактеристика „интернет пејзажа“, конструктивно управљање и развој система (темељно и стратешки) за ублажавање претњи, постали су императиви.[18] Управо, излагање о сајбер безбедности и заштити информација (у кратким цртама), послужило нам је да нас уведе у наредни део текста и омогући да се фокусирамо на неке друге важне аспекте заштите приватности. У склопу наведене расправе, подвући ћемо још једном – приватност и заштита података представљају неодвојива питања за безбедност на интернету. Заштита података је законски механизам који обезбеђује приватност.[19]

3) ЈЕДНОБРАЗНОСТ У ПРИМЕНИ ПРАВА НА МЕЂУНАРОДНОМ НИВОУ

Појам и тенденције

Још у првом написаном чланку о појму и садржини приватности из 1890. године, правници Семјуел Д. Ворен *(Samuel D. Warren)* и Луис Бредис *(Louis Bradeis)* ово право дефинисали су као *“right to be alone”*.[20] У таквом тумачењу

---

[16] *Ibid.*

[17] *Ibid.*

[18] Интернет: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780199680832.001.0001/oxfordhb-9780199680832-e-65, 24.10.2022.

[19] Интернет: https://www.rnids.rs/%D0%BE-%D0%BD%D0%B0%D0%BC%D0%B0/%D1%81%D0%B0%D1%98%D0%B1%D0%B5%D1%80-%D0%B1%D0%B5%D0%B7%D0%B1%D0%B5%D0%B4%D0%BD%D0%BE%D1%81%D1%82, 13.10.2022.

[20] „Право на приватност“, као појам о коме се и данас толико дискутује, постојало је и у старим културама, у кинеској, код Хебрејаца, старих Грка и Римљана. Прво га помиње Аристотел у свом делу *Политика*, раздвајајући приватну и јавну сферу. Међутим, иако су у старој Грчкој и Риму познавали приватност, у њеној примени се није „ишло“ на начин како је ми данас познајемо. Тек се раним хришћанством и пропагирањем молитви у тишини, право и потребе на спокојство и неометања у интими, приватност у правом смислу те речи добија на значају. Видети: Душан Поповић, Марко Јовановић, „Право интернета – одабране теме“, Правни факултет у Београду, 2017, стр. 123–125.

се препознаје шире значење овог појма – које подразумева право особе да сама изабере „изолацију од присуства других ако то жели и право да буде заштићена од праћења у приватном окружењу као што је властити дом".[21] У уобичајеној свакодневној комуникацији, термин приватност се употребљава за означавање нечега што је лично, поверљиво, неслужбено, скровито, затворено за јавност.[22] У овој перспективи, приватно се може посматрати као оно што је супротно јавном. Унутар приватне сфере, појединац има право да буде недоступан другима у стварима које их се не тичу (да се тиме уопште не баве), то је заштићени простор (из ког је свако друго лице физички и психички искључено).[23] Унутар приватне сфере појединац је слободан од уплива и мешања других, препуштен себи, својим осећањима, потребама или хировима. На овај начин, приватно подразумева успостављање физичких граница уласка трећих лица у лични простор појединца. У назначеним формулацијама појма приватности избија, дакле, његов основни смисао и суштина која подразумева заштиту моралног и физичког интегритета, право на избор одговарајућег стила и начина живота, интеракцију између људи и др.[24] Нормативно регулисање ове области на међународном нивоу, започело је усвајањем Универзалне декларације о људским правима – УН (чл. 12) из 1948. године, Конвенције за заштиту људских права и основних слобода, познатије као Европска конвенција о људским правима (чл. 8) из 1950. године, Међународног пакта о грађанским и политичким правима (чл. 17) из 1966. године.[25] Посебно треба поменути Европску конвенцију о људским правима која чланом 8. „на велика врата" уводи право на приватност међу основна људска права: „Свако има право на поштовање свог приватног и

[21] Вида М. Вилић, „Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета", докторска дисертација, Правни факултет Универзитета у Нишу, 2016, стр. 20.

[22] Caroline Kennedy, Ellen Alderman, *The Right to Privacy* Knopf Doubleday Publishing Group, New York, 1997, pp. 20–23.

[23] Владимир В. Водинелић, *Грађанско право, Увод у грађанско право и општи део грађанског права,* Правни факултет Универзитета Унион и ЈП Службени гласник, Београд, 2020, стр. 259.

[24] Не постоји једна опште прихватљива, универзална дефиниција појма права приватности. Концепт приватности може да се сагледа и интерпретира из различитих углова (позиција). Видети: Susan B. Barnes, *A privacy paradox: Social networking in the United States*, First Monday, vol. 11, no. 9/2006. Интернет: http://firstmonday.org/article/viev/1394/1312. 14.10.2021; Вида М. Вилић, *op. cit.,* стр. 20.

[25] Видети: Universal Declaration of Human Rights – the United Nations, 1948; Конвенција за заштиту људских права и основних слобода, познатија као Европска конвенција о људским правима, отворена је за потписивање у Риму 4. новембра 1950. године и ступила је на снагу 3. септембра 1953. године. Међународни пакт о грађанским и политичким правима, Генерална скупштина Уједињених нација. Резолуција 2200А (XXI) од 16. децембра 1966. године.

породичног живота, дома или преписке".[26] Европски суд за људска права у Стразбуру утврдио је да се односним чланом пружа заштита у комуникацији путем интернета, *e-mail* комуникацији, *online* праћењу интернет комуникације. Прецизно установљавајући поменуте облике заштите, суд је ставио акценат на заштиту података о личности која је управо обухваћена означеним чланом. Укратко, заштита се односи на податке о целокупном психичком и физичком интегритету човека (од имена, порекла, здравственог стања, сексуалне оријентације, до потенцијално осетљивих података, као нпр. *IP* адресе интернет корисника).[27] На нивоу Европске уније од изузетног значаја су Повеља о основним правима Европске уније, која чланом 8. регулише право на заштиту података о личности, док се чланом 7. посебно предвиђа заштита приватног и породичног живота, и Конвенција о заштити појединаца у погледу аутоматске обраде личних података.[28] Данас је законодавство ЕУ ослоњено на два најважнија прописа: *General Data Protection Regulation* (EU) GDPR 2016/679, која је заменила Директиву 95/46/ЕЦ и Директиву 2002/58/ЕЦ.[29] На неки начин, важећа ePrivacy Директива је претходница данашњег општег акта, као и предлог нове

[26] Европска конвенција о људским правима, Савета Европе (1949) о заштити слобода и права, усвојена у Риму, Италија, 4. новембра 1950. године.

[27] Овде је потребно приметити да већ ст. 2. истог члана Конвенције ограничава дејство овог права узимајући у обзир јавни интерес и интерес других лица. Видети: Душан Поповић, Марко Јовановић, *op. cit.,* стр. 127.

[28] Повеља о основним правима Европске уније (CFR) уграђује одређена политичка, социјална и економска права за грађане и становнике Европске уније (ЕУ) у законе ЕУ. Направљена је на основу Европске конвенције и свечано проглашена 7. децембра 2000. од стране Европског парламента, Већа министара и Европске комисије. Чл. 8. Заштита личних података прописује: „1. Свако има право на заштиту података о својој личности; 2. Такви подаци морају бити обрађени поштено за (унапред) одређену сврху и на основу информисаног пристанка особе или на неком другом легитимном основу уређеном законом. Свако има право да приступи прикупљеним подацима о својој личности и има право да затражи њихову исправку; 3. Поштовање ових правила подлеже контроли независног органа." Конвенција за заштиту појединаца у погледу аутоматске обраде личних података је споразум Савета Европе из 1981. године који штити право на приватност појединаца, узимајући у обзир све већи проток података о личности који су подвргнути аутоматској обради.

[29] "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 (General Data Protection Regulation) (Text with EEA relevance)", *OJ* L 119, 4.5.2016, pp. 1–88; "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", *OJ* L 281, 23.11.1995, pp. 31–50; "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)", *OJ* L 201, 31.7.2002, pp. 37–47.

ePrivacy Regulation, која би заправо требало да буде *lex specialis* у односу на GDPR.[30] Пажњу скрећемо на горе поменуту Директиву 95/46/ЕЦ, која је у битном одредила, „трасирала пут" за даљи развој правних прописа ЕУ у области заштите података и права приватности – све до *General Data Protection Regulation*. У том оквиру, ради се о најзначајнијој директиви, како због тога што се дугогодишња судска пракса темељи на њој тако и због тога што остале директиве представљају надоградњу како би се омогућила њихова примена у области електронских комуникација.[31] Значај Директиве 95/46/ЕЦ желимо да нагласимо и чињеницом да је она послужила као основа за нову GDPR. Дакле, да поновимо, реч је о најважнијим документима на међународном нивоу, чије су одредбе инкорпорисане касније у сва национална кривична права земаља потписница и земаља које су ратификовале означена документа.[32] Ово право помиње се у преко 150 националних устава у свету.[33] Устав Србије не дефинише експлиците право на приватност, али то чини на начин да гарантује права и слободе кроз које се оно остварује, па у том контексту штити достојанство и слободан развој личности, неповредивост психичког интегритета, неповредивост стана, као и тајност писама и других средстава општења.[34] Међутим, тај ниво реаговања је другачији када је у питању заштита личних података, јер Устав чл. 42. изричито даје посебне гаранције: „Зајамчена је заштита података о личности (ст. 1). Прикупљања, држање, обрада и коришћење података о личности уређују се законом (ст. 2). Забрањена је и кажњива употреба података о личности изван сврхе за коју су прикупљени, у складу са законом, осим за потребе вођења кривичног поступка или заштите безбедности Републике

[30] "Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)", COM/2017/010 final - 2017/03 (COD) Brussels, 10.1.2017.

[31] Наташа Томић, Далибор Петровић, „Друштвено умрежавање и заштита приватности корисника интернета", у: Миодраг Бакмаз, Небојша Бојовић, Дејан Марковић, Владанка Аћимовић-Распоповић (урс.), *Зборник радова XXVII симпозијума о новим технологијама у поштанском и телекомуникационом саобраћају*, *Postel*, Саобраћајни факултет, Београд, 2009, стр. 95–97.

[32] Андреј Дилигенски, Драган Прља, *op.cit.,* стр. 10.

[33] "Right to Privacy". Интернет: https://cic.gov.in/sites/default/files/Right%20to%20Privacy%20and%20RTI%20by% 20Aditya%20Verma%20%20%281%29%20%281%29.pdf, 30.3.2018.

[34] Устав Републике Србије, *Службени гласник Републике Србије*, бр. 98/2006, 16/2022; Одлука о проглашењу Уставног закона за спровођење Акта о промени Устава Републике Србије – Амандмани I–XXIX: *Службени гласник Републике Србије*, бр. 115/2021. Пажњу привлачи чињеница да је Актом о промени Устава Републике Србије из 1888. године, загарантована неповредивост стана и тајност писама и телеграфских депеша. Видети: Чланове 23, 25, 40 и 41. Устава РС.

Србије, на начин предвиђен законом (ст. 3). Свако има право да буде обавештен о прикупљеним подацима о својој личности, у складу са законом, и право на судску заштиту због њихове злоупотребе (ст. 4)". У овом сегменту заштите људских права и слобода, наш Устав је озбиљно водио рачуна о решењима Закона о заштити података о личности из 2018. године (даље ЗЗПЛ), а која су послужила као основ приликом његове израде. Под утицајем *GDPR*-а, Србија је у новембру 2018. године, усвојила ЗЗПЛ, којим је уз извесна мања одступања прихватила принципе и вредности *GDPR*-а, чиме је несумњиво увела неупоредиво више стандарде заштите података о личности.[35] Практично преузимање решења из *GDPR*-а, са ефектима стварног „подизања" заштите података о личности на један виши ниво, представља значајан корак напред у усавршавању нашег законодавства.

Кривичноправна заштита података о личности у КЗС

Чак и они који о информационо-комуникационим технологијама имају површна и половична знања, схватају да је кривичноправна проблематика употребе и заштите од злоупотребе информација о појединцу, од изузетног значаја. Из претходног разматрања, право на приватност укључује и право на личне информације у вези са прибављањем, чувањем, употребом, откривањем, увидом или обезбеђењем од трећих лица и приказивања преко интернета итд. С друге стране, све већа употреба интернета и друштвених мрежа, као и коришћење компјутерске технике у свакодневном животу, повећава могућност њихове злоупотребе, а са подацима који се неовлашћено прибављају злоупотребом информационих система може се на разне начине манипулисати. Масовност ових злоупотреба попримила је огромне размере, а непосредне штете су несагледиве.[36] Овде треба посебно подцртати да се улажу огромни напори на сузбијању тих појава, како у Републици Србији тако и у свету.[37] У том контексту, регулисање кривичноправне заштите података о личности у нашем законодавству извршено је прописивањем и санкционисањем кривичног дела „неовлашћено прикупљање личних података". Ово дело представља новину у КЗ РС из 2005. године, систематизованог у глави XIV под називом, „Кривична дела против слободе и права човека и грађанина". Реч је, дакле, о новој инкриминацији коју је из перспективе промењених ситуација, нових захтева и конфликта интереса, било оправдано унети у законски текст. Одредба чл. 146. КЗС гласи:

---

[35] Сања Прља, „Право на заштиту личних података", *Страни правни живот*, бр. 1/2018, стр. 92, 96.

[36] Интернет: https://cadmus.eui.eu/handle/1814/23296, 27.3.2022.

[37] Драган Прља, Звонимир Ивановић, Марио Рељановић, *Кривична дела високотехнолошког криминала*, Институт за упредно право, Београд, 2011, стр. 77–80.

(1) „Ко податке о личности који се прикупљају, обрађују и користе на основу закона неовлашћено прибави, саопшти другом или употреби у сврху за коју нису намењени, казниће се новчаном казном или затвором до једне године.

(2) Казном из ст. 1. овог члана казниће се и ко противно закону прикупља податке о личности грађана или тако прикупљене податке користи.

(3) Ако дело из ст. 1. овог члана учини службено лице у вршењу службе, казниће се затвором до три године."[38]

Треба имати у виду да се ради о кривичном делу бланкетног карактера, што значи да су за његово потпуно разумевање и примену неопходне одредбе одговарајућих других пописа, конкретно већ поменутог Закона о заштити података (ЗЗПЛ), који је почео да се примењује августа 2019. године. У даљем наставку текста биће указано на рад органа који су задужени за примену наведених и других норми у предметима из ове области у Републици Србији. Наш особен приступ разматрању односног проблема делом ће се базирати и на овој анализи. Наравно, само у мери у којој ће нас то довести дубљем разумевању кључних проблема и изазова у примени кривичноправне заштите овог – једног од оних права за која кажемо да се налази у средишту људске слободе!? Па, да ли су механизми кривичноправне заштите од повреде овог права делотворни у Републици Србији и какви су ефекти усвајања и усаглашавања са новим ЗЗПЛ у погледу судске заштите и санкционисања кршења права која овај закон гарантује (после прве године примене).[39] Укратко, пред судовима у Србији (14 основних судова), у периоду од 2015. до јула 2020. године, формирано је укупно 28 предмета за кривично дело из чл. 146 КЗ – 26 предмета покренута су по приватном тужбама, док су преостала 2 покренута по оптужном акту надлежног јавног тужилаштва.[40] У шест случајева донето је решење о одбацивању тужбеног захтева, у 13 случајева донето је решење о одбијању, у два случаја донето је решење о обустави поступка, два предмета су окончана осуђујућом пресудом, у четири случаја донета је ослобађајућа пресуда, док је у једном суд преиначио пресуду и одбио оптужбу против окривљеног лица. И даље: међу предметима који су окончани ослобађајућом пресудом један предмет покренут је по оптужном акту јавног тужилаштва, а три по приватној тужби. Пажњу привлачи и чињеница да су међу предметима који су окончани осуђујућом пресудом,

[38] Кривични законик, *Службени гласник Републике Србије,*, бр. 85/2005, 88/2005 - испр., 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 и 35/2019.

[39] Дамјан Милеуснић и др., „Приватност и заштита података о личности у Србији, Анализа одабраних секторских прописа и њихове примене", у: Урош Мишљеновић (ур.), *Партнери за демократске промене Србија* (Партнери Србија), Београд, 2021, стр. 12.

[40] *Ibid.*

донете **две** условне осуде.[41] Већ само површан поглед на ову статистику, показује као „на длану" да је за кривично дело – Неовлашћено прикупљање личних података – упадљиво мали број поступака покренут пред судовима у Републици Србији. Наиме, број од 28 предмета у овој материји од 2015. године, у изразитој је несразмери са учесталошћу кршења права на заштиту података у истом периоду, ослањајући се на резултате претходне анализе – на само две осуђујуће пресуде за чл. 146 КЗ, и то условне, није се ни могуће изјаснити о томе да ли је казнена политика судова за ово кривично дело блага или оштра. Као основни разлог зашто је овако лоша (поражавајућа) статистика или, ако хоћемо, зашто су механизми заштите личних података у тој мери „подбацили", може да се наведе чињеница да пред кривичним одељењима судова у Србији „још увек није стигао предмет са значајном повредом приватности, било у погледу озбиљности последица по оштећеног, било у погледу броја оштећених". Овим се, свакако, не пребацује одговорност на судове, већ недостатак таквог приступа треба потражити, пре свега, изван судова имајући у виду надлежност за конкретне поступке.[42] Полазећи од горе поменутог, један од разлога може се наћи и у малом броју поступака које иницира јавно тужилаштво, тј. малом броју оптужница које јавна тужилаштва упућују судовима. Ради илустрације: у посматраном периоду који обухвата више од пет година, само у два предмета се у улози тужиоца појављује надлежно јавно тужилаштво.[43] Да закључимо: У погледу заштите појединца и његове приватности, изостаје адекватна правна заштита за оштећене – жртве злоупотребе података о личности. Испоставило се, нажалост, да у овим, по много чему безобзирним временима, кривичноправна заштита оштећенима због повреда из чл. 146. није ни ефикасна, ни делотворна.[44] „Досежући" до правог објашњења овакве, крајње негативне праксе, акценат је на томе да ниједна кривична пријава Повереника за информације од јавног значаја и заштиту података о личности, поднета у претходних пет година, није добила свој епилог. Исто тако, највећи број поднетих кривичних пријава за односно кривично дело се пред јавним тужилаштвима окончава застарелошћу поступка или без икаквог исхода, што у пракси обесмишљава кривично-судску заштиту због злоупотребе података о личности, како то гарантује Устав.[45]

---

[41] *Ibid.*

[42] *Ibid.*

[43] Види о томе опширније: *Ibid.,* стр. 20–28.

[44] Дамјан Милеуснић и др., *op. cit.,* стр. 30, 31.

[45] Златко Петровић, „Кривичноправна заштита података о личности у Републици Србији", LAWLife портал за право и привреду. Интернет: https://lawlife.rs/index.php/pravo/144-krivicnopravna-zastita-podataka-o-licnosti-u-republici-srbiji, датум приступа 24.6.2023.

4) ИЗВОРИ

Barnes, Susan B., "A privacy paradox: Social networking in the United States", *First Monday*, vol. 11, no. 9/2006. Интернет: http://firstmonday.org/article/view/1394/1312. 14.10.2021.

Дилигенски, Андреј, Прља, Драган, *Фејсбук, заштита података и судска пракса*, Институт за упоредно право, Београд, 2018.

"Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", *OJ* L 281, 23.11.1995.

"Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)", *OJ* L 201, 31.7.2002.

„Европска конвенција о људским правима", Савета Европе (1949) о заштити слобода и права, усвојена у Риму, Италија, 4. новембра 1950. године.

Каровић, Садмир, Симовић, Марина М., „Кривичноправно супротстављање вискотехнолошком – компјутерском криминалитету: савремени изазови, дилеме, перспективе", у: Јелена Костић, Марина Матић Бошковић (урс.), *Дигитализација у казненом праву и правосуђу*, Институт за упоредно право Београд, Институт за криминолошка и социолошка истраживања Београд, Правосудна академија Београд, 2022.

Kennedy, Caroline, Alderman, Ellen, *The Right to Privacy,* Knopf Doubleday Publishing Group, New York, 1997.

„Конвенција за заштиту људских права и основних слобода", познатија као Европска конвенција о људским правима, отворена је за потписивање у Риму 4. новембра 1950. године и ступила је на снагу 3. септембра 1953. године.

„Међународни пакт о грађанским и политичким правима", Генерална скупштина Уједињених нација. Резолуција 2200A (XXI) од 16. децембра 1966. године

Милеуснић, Дамјан и др., „Приватност и заштита података о личности у Србији, Анализа одабраних секторских прописа и њихове примене", у: Урош Мишљеновић (ур.), *Партнери за демократске промене Србија* (Партнери Србија), Београд, 2021.

Мрвић Петровић, Наташа, „Споразумно признање кривице у дигиталном окружењу", у: Јелена Костић, Марина Матић Бошковић (урс.), *Дигитализација у казненом праву и правосуђу*, Институт за упоредно право, Институт за криминолошка и социолошка истраживања, Правосудна какдемија, Београд, 2022.

Petrović, Dragana, "General characteristics of the basic concept of terrorism", *Strani pravni život*, no 4/2020.

Петровић, Златко, „Кривичноправна заштита података о личности у Републици Србији", LAWLife портал за право и привреду. Интернет: https://lawlife.rs/index.php/pravo/144-krivicnopravna-zastita-podataka-o-licnosti-u-republici-srbiji, 24.6.2023.

Поповић, Душан, Јовановић, Марко, *Право интернета – одабране теме,* Правни факултет у Београду, 2017.

"Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)", COM/2017/010 final - 2017/03 (COD) Brussels, 10.1.2017.

Prlja, Dragan, Reljanović, Mario, "Sybercrime – Comparative experiences"*, Strani pravni život*, no. 3/2009.

Прља, Сања, „Право на заштиту личних података", *Страни правни живот,* бр. 1/2018.

Прља, Драган, Ивановић, Звонимир, Рељановић, Марио, *Кривична дела високотехнолошког криминала,* Институт за упредно право, Београд, 2011.

"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 (General Data Protection Regulation) (Text with EEA relevance)", *OJ* L 119, 4.5.2016.

Stallman, Richard, „Mobilni telefoni su Staljinov san", B92. Интернет: http://www.b92.net/tehnopolis/vesti.php?yyyy=2011&=038nav_id=499267, 19.07.2012.

Summers, Sarah, "EU Criminal Law and the Regulation of Information and Communication Technology", *Bergen Journal of Criminal Law and Criminal Justice*, no. 1/2015.

Томић, Наташа, Петровић, Далибор, „Друштвено умрежавање и заштита приватности корисника интернета", у: Миодраг Бакмаз, Небојша Бојовић, Дејан Марковић, Владанка Аћимовић-Распоповић (урс.), *Зборник радова XXVII симпозијума о новим технологијама у поштанском и телекомуникационом саобраћају*, *Postel,* Саобраћајни факултет, Београд, 2009.

Вилић, Вида М., „Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета", докторска дисертација, Правни факултет Универзитета у Нишу, 2016.

Водинелић, Владимир В., *Грађанско право, Увод у грађанско право и општи део грађанског права,* Правни факултет Универзитета Унион и ЈП Службени гласник, Београд, 2020.

5) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Раздобље од краја деведесетих година прошлог века обележио је грандиозни развој информационо-комуникационих технологија (*ICT*). Интернет и друштвене мреже су, без претеривања, постале део нашег свакодневног живота, „ушле" у сваки део људског бића, у сваки његов ген. Процес је жив, ради се о његовом драстичном успону. Централно место у том процесу има чип, односно микрочип или бит. Преко њега се долази до биочипа, до вештачке интелигенције, роботизације, дигиталне комуникације итд. Живимо у свету у коме се огроман број података, филмова, слика и других материјала размењује, поставља на профилима и чини јавно доступним – једном речи, претвара у податке који представљају нови капитал. У том контексту, сајбер криминал и сајбер безбедност привлаче све већу пажњу, како због значаја критичне информационе структуре за националну економију и безбедност тако и због интеракције политика које се баве осетљивим *ICT* правима, као што су приватност и заштита података. Управо је то разлог што су, не тако давно, у наш правни систем уведени закони који на нов и свеобухватан начин третирају ову комплексну и веома динамичну проблематику. Из те перспективе, понуђени су одговори на широк спектар питања у вези са заштитом података, права на приватност, права на слободу мишљења и изражавања, слободу интернета као медија и др. Најважнији, из аспекта наше теме, у фокусу се нашао ЗЗПЛ (који је фактички преведена верзија *GDPR*-а). Судска заштита гарантована овим законом обухвата право лица на које се подаци односе на покретање: управног спора, парничног спора (тужба за заштиту права и тужба за накнаду штете), као и прекршајног поступка. ЗЗПЛ, међутим, не третира кривичноправну судску заштиту у случају „злоупотребе података о личности", попут појединих закона који прописују кривична дела из области коју уређују. Уместо тога, ова заштита је регулисана Кривичним закоником, који у чл 146. прописује кривично дело – Неовлашћено прикупљање личних података. Како ово дело има бланкетни карактер, за разматрање појмовног одређења, тј. потпуног разумевања његовог смисла и суштине, било је неопходно са ове опште позиције „прећи" на посебну теоријску интерпретацију која произилази из ЗЗПЛ-а. С обзиром на то да је наш КЗ имплементирао норме међународног права, с једне стране је постигао да се у свему суштински испуне преузете обавезе, а, с друге стране, испоштују уобичајени кривичноправни стандарди, као и да се примене решења која одговарају потребама нашег друштва и правног система. Међутим, ослањајући се на резултате анализе постојеће праксе (која је послужила као основ за овакав

закључак), право на приватност и заштита података о личности у мери у којој они у примени показује своју објективност и делотворност, тек треба да се унапреде, како у јавном тако и у приватном сектору.

CYBER SECURITY *vs.* PRIVACY: GENERAL CONSIDERATIONS AND GROUNDS FOR PROTECTION

Abstract: Today, there are serious discussions in the world at different levels about the possibilities of modern information and communication technologies (ICT), but also about their unwanted consequences. For an ordinary person, the "new" way of communicating via the Internet and mobile telephony is at the same time easy, simple, fast, and necessary; it becomes a fact of his daily life. Moreover, modern times include the Internet as one of the main means of communication. If used "properly", it represents an abundance of information on almost any topic and brings many benefits. With a diverse amount of collected data, it easily mediates the acquisition of new knowledge and lifestyle shaping. In this perspective, life on the Internet network is increasingly becoming a space subject to manipulation and abuse. The list of abuses is long, from attacks on other people's privacy to persecution, cyber mobbing, peer violence, sexual harassment and violence, trafficking in human beings and human organs, etc. In this way, the emergence of new technologies significantly threatens the right to privacy. In recent years, the right to privacy has mostly been associated with personal data. The right to privacy and protection of personal data is one of the most basic human rights. Since it is a fundamental human and citizen right, the Constitution, the Data Protection Act (DPA), and the Criminal Code (Article 146, Unauthorised Gathering of Personal Data) serve as the foundation for its protection under our legal system. The aim of the work is to contribute to the scientific debate in that area.

Keywords: Cyber security, cyber crime, privacy, personal data protection, normative frameworks.