Тијана Леваков Вермезовић,*
Студент докторских студија
Правни факултет Универзитета у Београду

ПРЕГЛЕДНИ НАУЧНИ ЧЛАНАК
doi:10.5937/zrpfni1674249L
UDK: 343.4:004.738.5

Рад примљен: 30.09.2016.
Рад прихваћен: 27.11.2016.

ЗАШТИТА ПРАВА НА ПРИВАТНОСТ КАО ДРУШТВЕНИ ИМПЕРАТИВ ДИГИТАЛНОГ ДОБА КОЛИКО СМО РАЊИВИ?

Апстракт: *У раду се сагледавају начини угрожавања приватности појединаца у дигиталном свету са фокусом на кривичноправну заштиту коју пружа постојећи међународни и национални правни оквир и пракса Европског суда за људска права у овој области. Значај спровођења оваквог истраживања је велики, с обзиром на то да живимо у свету електронских комуникација у којем нико није анониман. Развој информационо-комуникационих технологија, поред бројних предности, донео је и бројне изазове у свим сферама модерног живота. Од како је интернет постао глобални форум, појединци постају мета бројних увреда, клевета и претњи и о њима се објављују информације, или медији за које они нису дали сагласност. Пракса показује да је ефективно сузбијање и контрола незаконитог понашања на интернету, те кажњавање учинилаца, на ембрионалном нивоу. Како би се пружила адекватна заштита оштећенима кривичним делима којима се директно угрожава њихова приватност у дигиталном свету, неопходно је креирати нове моделе и приступе у решавању овог проблема.*

Кључне речи: *приватност, лични подаци, електронска комуникација, интернет, високотехнолошки криминал, информациона безбедност.*

1. Увод

Модерне дигиталне технологије постале су незаобилазан чинилац у свим сферама друштва. Развојем информационих система долази до трансформације традиционалног друштва у информатичко друштво, вршећи велики утицај на начин на који је друштво организовано, на економске и друштвене односе, на односе појединаца и начин њихове

* tijana.levakov.vermezovic@gmail.com

комуникације. Милијарде корисника интернета путем популарних друштвених мрежа, сервиса за слање и примање електронске поште, апликација и програма за слање текстуалних, видео и графичких порука и других активности на рачунарима и „smart" телефонима[1] чине доступним неслућено много информација и електронских података о себи, што може бити злоупотребљено у криминалне или друге сврхе, а колатерална штета је управо приватност појединца. Разлози за малициозно коришћење рачунара могу бити бројни, као на пример прибављање противправне имовинске користи, вређање, узнемиравање, осветољубивост, доказивање, шала, вршење тероризма, изазивање панике и нереда или просто modus operandi за извршење неког другог кривичног дела.

Сам концепт приватности није прецизно дефинисан и у себи обухвата читав низ веома важних друштвених вредности и то право на слободу мисли и духа, право човека да живи на начин на који жели, право да има контролу над сопственим телом и личним подацима о себи, слободу од неовлашћеног видео-надзора, фотографисања и праћења комуникација, право на интиму породичног живота и дома, право на достојанство, углед и част и право на успостављање и неговање односа са другим људима, нарочито у емоционалној сфери, ради развијања и задовољења сопствене личности (Пауновић, Кривокапић, Крстић, 2014: 181). Једну од ранијих дефиниција овог права формулисала је америчка јуриспруденција крајем XIX века као право да се буде остављен на миру – eng. *right to be left alone* (Прља, Рељановић, Ивановић, 2012: 95). Начин на који одређујемо сам оквир приватности суштински утиче и на то како обликујемо законска решења појединих проблема. То је од изузетног значаја за информатичко доба које нас суочава са бројним веома сложеним проблемима приватности и изазива велике поремећаје у систему друштвених вредности (Solove, 2002: 1088).

Веома брз развој информационих система поставио је велики изазов пред законодавне, управне и друге државне органе, као и пред целу међународну заједницу, да правним прописима регулишу ову област. „Решавање питања приватности и безбедности у електронским комуникацијама захтева свеобухватан приступ, укључивање широког круга заинтересованих и усаглашавање многих, често различитих потреба и интереса". (Slijepčević, 2016: 41)

Разликују се кривична дела у којима се рачунари појављују као средство извршења и као објекат извршења, а затим и кривична дела у чијем се начину извршења појављују елементи незаконитог коришћења интернета.

1 Справа која у себи обухвата мобилни телефон и ручни рачунар.

У овом раду ће фокус бити на правној заштити која се пружа појединцима оштећеним кривичним делима којима се значајно угрожава њихово право на приватност у дигиталном свету, а чији основни облици се у складу са Кривичним закоником Републике Србије[2] гоне по приватној тужби, што ствара велике проблеме у пружању заштите основним правима и слободама грађана. Рад ће укратко указати и на одређене радње које у нашем кривичном праву нису прописане као кажњиве радње, а значајно задиру у сферу приватности појединаца, као што су ухођење и крађа идентитета до момента док се не изврши неко друго прописано кривично дело.

2. Начини угрожавања приватности

Веома су бројни начини угрожавања приватности појединаца путем интернета. Најозбиљнији облици су квалификовани као кривична дела, док за друге може да се тражи накнада штете у парничном поступку. Међутим, последице незаконитог коришћења интернета могу за појединце бити веома озбиљне и манифестовати се у друштвеној осуди, губитку поштовања, пријатеља, партнера, посла, немогућности да се заснује радни однос, дискриминацији на послу, осећају срама и страха, ухођењу, узнемиравању, физичком и психичком злостављању, нарушавању здравља, а у најтежим случајевима могу да доведу и до покушаја самоубиства, посебно код млађих особа или емотивно нестабилних личности.

Најчешћи начин угрожавања приватности путем интернета је управо увреда[3], која је кривично дело против части и угледа, односно људског достојанства. Радња се састоји у изјави којом се омаловажава друго лице у виду псовке, погрдних и вулгарних израза или негативног вредносног суда (Стојановић, 2009: 424). Последице по појединца могу бити велике јер такву изјаву путем интернета сазнаје велики број људи.

Изношењем личних и породичних прилика које су такве природе да је у интересу породице не буду познате другим људима, а односе се на одређена лична својства, карактерне црте, навике, стил живота, породичне односе, сексуалну оријентацију и болести, може се нанети велика штета части или угледу појединца и такође је кажњиво у законодавству Републике Србије (Стојановић, 2009: 431).[4]

2 Кривични законик, *Сл. гласник РС, б*р. 85/05, 88/05 – испр., 107/05 – испр., 72/09, 111/09, 121/12, 104/13 и 108/14, у даљем тексту КЗ.

3 Чл. 170 КЗ, прописано као кривично дело увреда.

4 Чл. 172 КЗ, прописано као кривично дело изношење личних и породичних прилика неког лица.

Забрањено је и неовлашћено, без знања и пристанка овлашћеног лица, отварање и сазнавање садржине електронске поште или поруке и саопштавање другом или служење садржином која је сазната на тај начин[5]. Поруке на телефонима и електронска пошта су веома рањиви на неовлашћене приступе вештих корисника рачунара и могу бити хаковане[6]. Веома популаран у данашње време, а путем мобилних телефона или програма за дописивање, постао је „sexting", односно размењивање интимних порука сексуалног садржаја. Неовлашћен приступ било ког лица овим порукама је веома инвазиван за слободу комуникације.

Приватност значајно може да се угрози и неовлашћеним прислушкивањем и снимањем које се врши посебним уређајима, нарушавајући на тај начин пре свега слободу несметаног изражавања.[7] Најчешће се прислушкују мобилни телефони.

Објављивањем неовлашћено прибављеног, или овлашћено прибављеног али без сагласности објављеног или приказаног, фотографског, филмског, видео или другог снимка лица на којег се снимак односи може осетно да се задре у лични живот.[8] Осетно задирање у приватни живот би свакако било снимање нагих лица или нечијих сексуалних активности, што суд цени у сваком појединачном случају, док у другим ситуацијама лице које сматра да му је на тај начин угрожена приватност може да тражи заштиту у парничном поступку (Стојановић, 2009: 395). Модерним технологијама се пружају неслућене могућности задирања у приватни живот појединца на овај начин, јер се путем интернета овакве фотографије и видео-записи могу учинити доступним милионима корисника. Сви записи који се праве путем модерних фотоапарата, веб камере, а најчешће путем „smart" телефона доступни су у информатичком свету, и често се неовлашћено дистрибуирају.[9] Чак се јављају и осветнички анонимни

5 Чл. 142 КЗ, прописано као кривично дело повреда тајности писма и других пошиљки.

6 Хаковати – незаконито и без ауторизације приступити компјутерској датотеци или мрежи (The Free Dictionary by Farlex, Retrieved 7, July 2016 from http://www.thefreedictionary.com/hack)

7 Чл. 143 КЗ, прописано као кривично дело неовлашћено прислушкивање и снимање.

8 Чл.144–145 КЗ, прописано као неовлашћено фотографисање и неовлашћено објављивање и приказивање туђег списа, портрета и снимка.

9 У истраживању које је спровела Холи Јакобс, уочено је да је преко 53,3% хетеросексуалних парова делило интимну фотографију опсценог садржаја са другом особом, а ЛГБТ популација 74,8% (Bambauer 2014: 2027). Холи Јакобс је била жртва осветничке порнографије и сада води кампању за криминализацију осветничке порнографије и сматра је врстом сексуалног злостављања. В. Cyber Civil Rights Initiative, visited 9, November 2016: https://www.cybercivilrights.org/.

порнографски сајтови, са великим бројем неовлашћено постављених интимних фотографија и видео-записа углавном жена, најчешће од стране повређених бивших партнера[10]. Ови сајтови су незаконити и уклањају се, али је штета за многе тада већ ненадокнадива. Потребно је радити на превенцији и на едукацији корисника о начинима заштите њихових електронских датотека и не правити медије интимног садржаја, али и тражити нове моделе за ефикаснију заштиту. Велики је број земаља[11] које су криминализовале осветничку порнографију тако што су прописале да кривично дело представља свако копирање, репродуковање, дељење или излагање сексуалних експлицитних слика или видеа путем интернета без писане сагласности особе на запису.

Неовлашћено прибављање, саопштавање другом или употребљавање у сврху за коју нису намењени података о личности који се прикупљају, обрађују и користе на основу Закона о заштити података о личности противно је Кривичном закону Републике Србије.[12] Лични подаци су веома осетљиве природе и лако се могу злоупотребити и користити за извршење другог кривичног дела. Данас велики број правних лица путем својих интернет сајтова и апликација на телефонима прибавља и обрађује разне личне податке, често и без сагласности корисника, а грађани нису упознати са ризиком који носи одавање оваквих података.

У правном систему Републике Србије сајбер ухођење и крађа идентитета нису прописани као самостална кривична дела. Ухођење или прогањање би представљало континуирано праћење и узнемиравање друге особе. Према Европској комисији, ухођење би требало да буде укључено у Кривични законик Европске уније.[13] Ухођење је веома друштвено опасно дело, које нарушава основна права на слободу кретања, комуникације, води психичком злостављању и осећају страха, а може довести и до силовања

10 Први такав веб сајт је био „IsAnyoneUp?“, а оснивач је био Хантер Мур. Сајт је угашен у априлу 2012. године.

11 34 земље Сједињених Америчких Држава, Филипини, Израел, Аустралија, Канада (Revenge Porn. *Wikipedia,* visited 6 July 2016. https://en.wikipedia.org/ wiki/Revenge_porn)

12 Чл. 146 Закона о заштити података о личности, *Сл. гласник РС*, бр. 97/08,104/09 – др. закон, 68/12 – одлука УС и 107/12, кривично дело неовлашћено прикупљање личних података

13 Енглеска и Велс, Белгија, Холандија, Немачка, Малта, Ирска, Аустрија, Италија, Шкотска су прописале ухођење као кривично дело (EU Commission Stalking document. Retrieved 4, July 2016 from: http://ec.europa.eu/justice/news/consulting_public/0053/contributions/organisations/Unregistered/net_for_surviving_stalking_en.pdf).

и убиства.[14] Сајбер ухођење је само софистицирани облик ухођења уз помоћ информационе технологије. Предлог Закона о изменама и допунама Кривичног законика од 9. 11. 2016. године предвиђа чланом 10 увођење новог члана 138а у Кривични законик који би прописивао кривично дело прогањање. Исти Предлог чланом 15 предвиђа и увођење кривичног дела полно злостављање кроз увођење новог члана 182а у Кривични законик. Овим делима пружиће се додатна заштита појединцима од малициозних понашања путем интернета и гониће се по службеној дужности. Међутим, остаје да се види какав одговор ће дати судска пракса услед свих тешкоћа у њиховом доказивању у случајевима радње извршења дела путем интернета, као и у разграничењу од неких других горе поменутих кривичних дела. Крађа идентитета је још један облик понашања који може бити средство извршења бројних других кривичних дела као што су превара, фалсификовање и др. Састоји се углавном од неовлашћеног прибављања или коришћења информација о идентитету другог лица.[15] Ово може подразумевати и прибављање идентификационих података као што су име, датум рођења, адреса становања и слично друге особе, без његовог знања и одобрења, а најлакше се извршава управо путем рачунара.[16] Веома је често коришћење лажних непостојећих идентитета на интернету или неовлашћено прављење туђег профила.

3. Међународноправна заштита права на приватност

Право на поштовање приватног и породичног живота гарантовано је бројним међународним правним инструментима усвојеним под окриљем Уједињених нација. Члан 12 Универзалне декларације[17] прописује да нико не сме бити изложен произвољном мешању у његову приватност, породицу, дом или преписку, нити нападима на част или углед. Свако има право на

14 У Уједињеном краљевству 1,2 милиона жена и 900.000 мушкараца се уходи сваке године (EU Commission Stalking document, Retrieved 4, July 2016 from: http://ec.europa.eu/justice/news/consulting_public/0053/contrib utions/organis at i ons/Unregistered/net_for_surviving_stalking_en.pdf)

15 Council of Europe, *T-CY GuidanceNote #4 identity Theft and phishing in relation to fraud*, Retrieved 10, July 2016 from http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY_ 2013_8E_ gui da nceNote4_id%20theft_V8.pdf

16 Занимљив је податак да друштвена мрежа „Facebook" броји преко милијарду корисника који пружају велику количину информација о себи и то 90,8% профила садржи слику корисника, 87,8% објављује свој датум рођења, 39,9% има постављен број телефона, 50,8% наводи место пребивалишта, 62,9% поставља у ком су личном статусу. (Gross, Acquisti, 2005: 5)

17 Универзална декларација, усвојена и проглашена Резолуцијом Генералне скупштине бр. 217 (III) од 10. 12. 1948.

заштиту закона против оваквог мешања или напада. На универзалном нивоу под окриљем Уједињених нација није донета Конвенција која се бави питањима високотехнолошког криминала.

За нашу земљу веома су значајни регионални инструменти усвојени од стране Савета Европе. Најзначајније место заузима Европска конвенција за заштиту људских права и основних слобода[18] (у даљем тексту Европска конвенција), којом се у члану 8, ст. 1 гарантује свакоме право на поштовање свог приватног и породичног живота, дома и преписке. Како је фокус овог рада на заштити права на приватност путем информационих система, од великог значаја је и Конвенција о високотехнолошком криминалу која је усвојена у Будимпешти 23. 11. 2001. године[19] јер је у њој препозната неопходност заједничке казнене политике у сврху заштите друштва од сајберкриминала и има за циљ спречавање дела усмерених против поверљивости, интегритета и доступности компјутерских система, мрежа и компјутерских података, као и спречавање злоупотребе тих система, мрежа и података. Оно што је од посебног значаја за заштиту приватности појединаца је да се обим процедуралних одредаба Конвенције[20] односи на било које кривично дело почињено путем компјутерских система. Члан 18 Конвенције овлашћује надлежне органе да нареде сваком лицу на територији чланице да преда одређене рачунарске податке које поседује, односно који су под његовом контролом, као и да нареде пружаоцу услуге да преда податке о свом претплатнику. Подаци о претплатнику/ кориснику неке електронске услуге су потребни да би се идентификовале услуге и за њу везане техничке мере које су коришћене или се користе о стране корисника, а ради утврђивања идентитета особе о којој се ради[21].

Смернице за сарадњу између полиције и пружаоца интернет услуга на сузбијању високотехнолошког криминала донете на глобалној конференцији у оквиру Савета Европе предлажу успостављање формалног партнерства између њих.[22]

---

18 Закон о ратификацији Европске конвенције за заштиту људских права и основних слобода, *Сл. лист СЦГ – Међународни уговори*, бр. 9/03, 5/05 и 7/05 – испр. и *Сл. гласник РС – Међународни уговори*, бр. 12/10.

19 Закон о потврђивању Конвенције о високотехнолошком криминалу, *Сл. гласник РС*, бр. 19/09.

20 *Idem*, чл. 14–21.

21 Para. 178 Council of Europe, *Explanatory Report to the Convention on Cybercrime (ETS No. 185)*, Retrieved 4, July 2016 from https://ccdcoe.org/sites/default/files/documents/CoE-011123-Explanatory ReportTo TheConventionOnCybercrime.pdf

22 Para. 8 и 13 Council of Europe, *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime* (2008) retrieved 11, November 2016 https://

Компаративном анализом се уочава да се праву на приватност пружа универзална заштита, али да о механизмима те заштите која се пружа у оквиру информационих технологија још увек не постоји сагласност на универзалном нивоу. Нагласак је на превентивној заштити и на међународној сарадњи за извршење озбиљнијих кривичних дела извршених употребом рачунара, али се још увек нису изнашли модели заштите приватности појединца на свакодневном нивоу, нити јасни механизми прикупљања доказа, с обзиром на иностране елементе ових дела.

4. Пракса Европског суда за људска права

Постоји богата пракса Европског суда за људска права у вези са угрожавањем приватности појединаца у вези члана 8 ЕКЉП, међутим, иста није толико обимна када се ради о угрожавању приватности појединаца путем интернета.[23] Најпознатији такав случај је К.У. против Финске[24] који говори о дванаестогодишњем дечаку који је постао мета бројних педофила због постављања огласа сексуалне природе о њему на интернет сајту за упознавање од стране непознатог учиниоца. Отац дечака није био у могућности да покрене поступак ни против кога јер је у то време у Финској регулатива била таква да није дозвољавала полицији нити судовима да захтевају од пружаоца услуга интернета да идентификују особу која је поставила оглас. Суд је утврдио да одређена дела захтевају кривичне санкције и установио да држава није успела да испуни позитивну обавезу да пружи заштиту физичком и психичком интегритету детета, дајући предност заштити анонимности на интернету.[25] Суд је такође установио да је концепт физичког и менталног интегритета заштићен као аспект приватног живота под чланом 8 ЕКЉП, као и да анонимност и поверење на интернету не сме навести државе да одбију да пруже заштиту правима потенцијалних жртава, поготово када су у питању рањиве групе.[26] Држава је у обавези да усвоји мере које ће обезбедити поштовање приватног живота у сфери међусобних односа појединаца, односно да обезбеди ефикасну кривично-правну регулативу (спроводи ефикасну кривичну

rm.coe.int/CoERMPublicCommon SearchServices /DisplayDCTMContent?documentId=090 00016802fa3ba

23 V. Case-law of the European Court of Human Rights. Retrieved 2, July 2016 from: *http:// www.echr.coe.int /Documents/Research_report_internet_ENG.pdf.* 47–57.

24 K.U. v. Finland [2009], ECHR, 6–14.

25 *Idem*, para. 48.

26 *Idem*, para. 43, 46.

истрагу) и да криминализује овакву врсту понашања.[27] Суд је прихватио да у светлу разних потешкоћа са којима се суочава модерно друштво, позитивне обавезе државе морају бити интерпретиране на начин да не наметну немогуће или диспропорционални терет на власти или у овом случају на законодавца.[28]

Генерални принципи ЕСЉП-а који се тичу слободе изражавања на интернету и односу са другим слободама појединца најбоље се виде у пресуди Делфи АС против Естоније.[29] Случај се тицао одговорности портала за вести и коментаре појединаца, који је у конкретном случају био увредљиве и вулгарне садржине, садржао је претње и вређао људско достојанство. У параграфу 110 Суд је запазио да интернет пружа платформу за слободу изражавања, која је загарантована Конвенцијом, али клевете и друге врсте очигледно незаконитог говора, укључујући и говор мржње и говор који подстиче насиље, могу бити невероватном брзином проширени и могу, понекад, трајно остати у интернет свету. Због тога се мора изнаћи равнотежа између два заштићена права прокламована чланом 8 (заштита приватног живота) и чланом 10 (права на слободу изражавања) Конвенције. Мора постојати одговорност за клевете и друге врсте незаконитих изјава, те се успоставити ефективно правно средство за кршење личних права.[30]

Велики број одлука Суда се односи на заштиту личних података.[31] Тако је Суд у случају Миткус против Латвије[32], у ком се подносилац представке жалио да је новински чланак обелоданио информацију да је заражен ХИВ-ом и објавио његову слику, и у случају Алкаја против Турске[33], у којем је штампа објавила адресу становања познате личности, нашао повреду члана 8 ЕКЉП, односно да је дошло до повреде права на приватан живот, као и у другим случајевима.

27 *Idem*, para. 46.

28 *Idem*, para. 48.

29 Case Delfi AS v. Estonia [2015], ECHR, para. 10–32.

30 *Idem*, para 110.

31 V. European Court of Human Rights, *Personal Data Protection.* Retrieved 5, July 2016. from http://echr.coe.int/ Documents/FS_Data_ENG.pdf

32 Mitkus v. Latvia [2012], ECHR, para. 4–48.

33 Alkaya v. Turkey [2012], ECHR, para. 5–12.

Такође, велики број одлука Суда[34] односи се и на заштиту приватног живота, пре свега личног портрета у којима је Суд установио повреду члана 8 ЕКЉП[35].

Иако ове одлуке нису у директној вези са коришћењем интернета, исте би се аналогно могле применити и на такве ситуације, пре свега имајући у виду да данас објављивање нечије слике или личних података у вестима или у новинама значи и објављивање на интернету, односно у електронској верзији, а да су извор информација медијима често управо друга физичка лица.

5. Правна регулатива у Републици Србији

Право на приватност је у нашој земљи загарантовано највишим правним актом Уставом Републике Србије, на тај начин што се прокламује неприкосновено право на људско достојанство, право на слободан развој личности, неповредивост тајности писама и других средстава комуницирања, заштита података о личности и др.[36]

Од значаја за заштиту приватности путем информационих технологија је свакако Закон о електронским комуникацијама[37], којим се уређују између осталог услови и начин за обављање делатности у области електронских комуникација, надлежности државних органа у области електронских комуникација, заштита права корисника и претплатника, безбедност и интегритет електронских комуникационих мрежа и услуга, тајност електронских комуникација, законито пресретање и задржавање података и др.[38] Међусобна права и обавезе оператора и корисника уређују се уговором у писаној форми који поред других обавезних елемената садржи и одредбе о поступању са подацима о личности. Пресретање електронских комуникација којим се открива садржај комуникације, као и приступ задржаним подацима нису допуштени без пристанка корисника, осим на одређено време и на основу одлуке суда, ако је то неопходно ради вођења кривичног поступка или заштите безбедности Републике Србије, на начин

34 Case Von Hannover v. Germany [2004], ECHR, para. 11–20; Case Peck v. the United Kingdom [2003], ECHR, para. 8–34.

35 European Court of Human Rights, *Right to the Protection of One's Image*, Retrieved 5, July 2016. from http://echr.coe.int/Documents/FS_Own_image_ENG.pdf

36 Чл. 23, 41 и 42 Устава Републике Србије, *Сл. гласник РС*, бр. 98/06.

37 Закон о електронским комуникацијама, *Сл. гласник РС*, бр. 44/10, 60/13 – одлука УС и 62/14.

38 *Idem*, чл. 3.

предвиђен законом.[39] Оператер је дужан да задржане податке чува 12 месеци од дана обављене комуникације и то у изворном облику.[40]

Поступак у којем се пружа заштита појединцима у ситуацијама када им је повређено неко од права приватности кривичним делом регулисано је Закоником о кривичном поступку[41] и Законом о полицији[42]. Како се основни облици горе поменутих кривичних дела гоне по приватној тужби, јавни тужилац неће поступати по кривичним пријавама за ова дела, односно исте ће одбацивати. Да би се покренуо поступак по приватној тужби, потребно је да постоје одређени докази који би указивали да постоји оправдана сумња да је одређено лице учинило кривично дело. Оштећени као тужилац нема права која припадају јавном тужиоцу као државном органу, те он не може рачунати на помоћ државних органа у прикупљању доказа[43]. Оштећени као тужилац има право да ангажује адвоката да га заступа, али су његове услуге скупе. Адвокат има права да од државних органа, установа, предузећа и других организација тражи и благовремено добије информације, списе и доказе који су у њиховом поседу или под њиховом контролом, али то право је знатно уже од оних којима располаже јавни тужилац[44] и није обавезујуће (Ilić, Majić, Beljanski, Trešnjev, 2016: 215). Приватна тужба се подноси у року од три месеца од дана када је оштећени сазнао за кривично дело и осумњиченог[45]. Овај рок се не подудара са роком застаре кривичног гоњења, који је веома кратак за кривична дела која су у фокусу овог рада, с обзиром на то да се исти рачуна према висини и врсти казне које су прописане за иста, а које су ниске.[46] Наведено указује да је за приватног тужиоца, у ситуацији када су предметна кривична дела извршена коришћењем информационих технологија, поготово у ситуацијама када је непознат починилац дела, често практично немогуће да благовремено покрене поступак, идентификује учиниоца и обезбеди доказе за вођење кривичног поступка, а касније исти и да спроведе.

39 *Idem*, чл. 126.

40 *Idem*, чл. 128.

41 Законик о кривичном поступку, *Сл. гласник РС*, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 и 55/2014, у даљем тексту ЗКП.

42 Закон о полицији, Сл. гласник РС, бр. 6/2016.

43 Члан 19 ЗКП и чл. 9 Закона о јавном тужилаштву, *Сл. гласник РС*, бр. 116/2008, 104/2009, 101/2010, 78/2011 – др. закон, 101/2011, 38/2012 – одлука УС, 121/2012, 101/2013, 111/2014 – одлука УС, 117/2014 и 106/2015.

44 Чл. 36 Закона о адвокатури, *Сл. гласник РС*, бр. 31/2011 и 24/2012 – одлука УС.

45 Чл. 65 ЗКП.

46 Чл. 103, ст. 1, т. 6 и 7 КЗ.

Грађанин којем је угрожено неко од личних или имовинских права може да се обрати полицији ради заштите тог права, ако у конкретном случају није обезбеђена друга правна заштита и ако је угрожавање тог права у вези са његовом личном и имовинском безбедношћу.[47] Међутим, имајући у виду ограниченост капацитета полицијских органа, они неће пружати помоћ оштећенима за дела која се гоне по приватној тужби, с обзиром на то да Закон о полицији говори о могућности, не о обавези.[48] Чак и уколико би се дошло до податка ко је власник интернет протокол адресе, па затим и физичке адресе са које је извршена незаконита радња, потребно би било прикупити обавештења од свих корисника рачунара са те адресе и обезбедити електронске и друге доказе који указују на одређеног учиниоца. За свако од ових дела би била потребна велика оперативна помоћ полиције.

Велики проблем представља и слабо познавање информационих технологија приватних лица, истражних органа и суда. Да би могли докази да се користе у електронском облику, неопходно је обезбедити њихов интегритет, односно очувати изворни садржај и комплетност податка, како би се спречиле различите злоупотребе. Такође, подаци морају да буду доступни и употребљиви на захтев овлашћених лица онда када су им потребни у сврху судског поступка. Мора им се обезбедити аутентичност, односно могућност да се провери и потврди да је податке створио или послао онај за кога се тврди да је ту радњу извршио, као и непорецивост, односно способност доказивања да се догодила одређена радња или да је наступио одређени догађај.[49]

Велики изазов у вези кривичних дела употребом информационе технологије је управо међународни карактер истих, с обзиром на то да се седишта фирми које су власници веб сервера или пружаоци интернет услуга који могу да пруже податке о починиоцу често налазе у иностранству[50], због

47 Чл. 30 и 35 Закона о полицији, *Сл. гласник РС*, бр. 6/2016.

48 Према речима заменика начелника Одељења за борбу против високотехнолошког криминала Драгана Јовановића, у Одељење за борбу против високотехнолошког криминала готово сваког дана дође двоје или троје грађана да се пожале како им је неко нешто написао на Фејсбук профилу, увредио их, називао њих или њима ближње погрдним именима, стављао непримерене фотографије и слично, али да „Полиција нажалост тиме не може да се бави", те да, када би полицајци реаговали на сваку злоупотребу и пријављивали је Фејсбуку, било би их вероватно више стотина хиљада дневно, а ФБИ би по цео дан само издавао податке о корисницима Фејсбука. Извор: Магазин Време бр.1009, *Мрачна страна Фејсбука,* Преузето 6. маја 2010. са http://www.vreme.com/cms/view.php?id=929661.

49 Чл. 2, ст. 1, т. 5–8 Закона о информационој безбедности, *Сл. гласник РС,* бр. 6/2016.

50 Седишта већине правних лица које су власници најпопуларнијих друштвених мрежа и веб сајтова као што су „Facebook", „Instragram", „Twitter", „Gmail" су у Сједињеним

чега је неопходно тражити међународноправну помоћ, која представља дуготрајан и скуп поступак. Отежавајућу околност представља и чињеница да се прописи о заштити приватности разликују, те је за сада немогуће такву помоћ добити осим у случајевима тешких кривичних дела. (В. Прља, Рељановић, Ивановић, 2012: 95–104)

Приватност се може штитити и у парничном поступку у складу са Законом о парничном поступку[51], али проблеми у доказивању основаности тужбеног захтева су исти као у кривичном поступку.

Имајући у виду све наведено, може се констатовати да је Република Србија прихватила највеће међународне стандарде у предметној области. Међутим, анализирајући пресуду Европског суда за људска права К.У. против Финске, уочава се правна празнина, односно читава једна област у којој су, иако загарантована, права појединца веома угрожена.

6. Закључак

На основу свега изнетог у раду, потврђује се хипотеза рада да заштита која се пружа појединцима у погледу њихових права на приватност када су иста угрожена путем информационих технологија није у потпуности ефикасна и да је потребно изнаћи нове моделе како би се ова права заштитила.

Предметни рад указује на озбиљност сваке злоупотребе која се врши на интернету, путем рачунарских система. Имајући у виду тежину последице на приватна лица, степен угрожавања њихове приватне сфере, неопходно је извршити измене и допуне Законика о кривичном поступку на тај начин што ће се прописати да је полиција дужна да, уколико су кривична дела за која се поступак води по приватној тужби извршена путем информационо-комуникационих система, асистира у помоћи идентификовања учиниоца на захтев оштећених, као и у прикупљању и обезбеђењу тако прибављених доказа у електронском облику. Уколико би полиција сматрала да нема елемената кривичног дела, могла би писмено одбити да поступи по таквом налогу оштећеног / приватног тужиоца, али на то решење би исти морали да имају право на приговор Основном јавном тужилаштву, које би, уколико усвоји приговор, могло да нареди полицији да прибави тражену информацију, односно да поступи по налогу оштећеног. Такође, судије би приликом одмеравања казне за ова кривична дела као отежавајућу околност морале да цене чињеницу да су иста извршена путем интернета/

Америчким Државама.

51 Закон о парничном поступку, *Сл. гласник РС*, бр. 72/11, 49/13 – одлука УС, 74/13 – одлука УС и 55/14.

рачунара, имајући у виду велику друштвену опасност ових дела. Једино на тај начин ће Р. Србија испунити своје позитивне обавезе у складу са чланом 8 Европске конвенције за заштиту људских права и основних слобода.

У кораку са развојем права, требало би сајбер прогањање и крађу идентитета прописати као кривична дела у Кривичном законику Републике Србије.

Потребно је спровести обуку и унапредити људске и техничке капацитете полиције и јавног тужилаштва за истрагу кривичних дела у којима се као објекат или средство извршења кривичних дела јављају рачунари. Посебна пажња би требало да се усмери на обезбеђивање доказа у електронском облику за потребе спровођења кривичног поступка.

Неопходно је успоставити ближу сарадњу између држава и приватних предузећа у борби против криминала употребом информационе технологије.

Важно је побољшати међународну сарадњу и увести ефикасне и адекватне процедуре путем којих би истражни органи могли да захтевају од страних власти да без одлагања сакупе и обезбеде доказе. Веома је важно, имајући у виду горе наведене препреке за прикупљање доказа, закључити билатерални уговор са Сједињеним Америчким Државама, где се налазе седишта фирми које су власници најпопуларнијих друштвених мрежа и интернет сајтова, путем којег би се превасходно омогућила, па потом и убрзала, процедура прибављања доказа.

И за крај, повећању информационе безбедности могу да допринесу континуиране едукације свих актера информатичког друштва о неизлагању претераним ризицима на рачунарима и интернету и ефикасним начинима заштите личних података, као и јавних профила на друштвеним мрежама.

Литература

Bambauer, D. (2014). Exposed. *Minnesota Law Review.* 98. 2025–2102.

Gross, R., Acquisti A. (2005). Information Revelation and Privacy in Online Social Networks (The Facebook case). Retrieved 3, May 2016. from http://www.heinz.cmu.edu/~acquisti/pa pers/privacy-facebook-gross-acquisti.pdf. 5.

EU Commission Stalking document. Retrieved 4, July 2016 from: http://ec.europa.eu/justice/news/ consulting_public/0053/contributions/organisations/Unregistered/net_for_surviving_stalking_en.pdf.

European Court of Human Rights. *Personal Data Protection*. Retrieved 5, July 2016. from http://echr.coe.int/Documents/FS_Data_ENG.pdf.

European Court of Human Rights. *Right to the Protection of One's Image*. Retrieved 5, July 2016. from http://echr.coe.int/Documents/FS_Own_image_ENG.pdf.

Закон о адвокатури. *Сл. гласник РС*. Бр. 31(2011) и 24(2012) – одлука УС.

Закон о електронским комуникацијама. *Сл. гласник РС.* Бр. 44(2010), 60(2013) – одлука УС и 62(2014).

Закон о заштити података о личности. *Сл. гласник РС.* Бр. 97(2008),104(2009) – др. закон, 68(2012) – одлука УС и 107(2012).

Закон о информационој безбедности. *Сл. гласник РС.* Бр. 6(2016).

Закон о јавном тужилаштву. *Сл. гласник РС.* Бр. 116(2008), 104(2009), 101(2010), 78(2011) – др. закон, 101(2011), 38(2012) – одлука УС, 121(2012), 101(2013), 111(2014) – одлука УС, 117(2014) и 106(2015).

Законик о кривичном поступку. *Сл. гласник РС.* Бр. 72(2011), 101(2011), 121(2012), 32(2013), 45(2013) и 55(2014).

Закон о парничном поступку. *Сл. гласник РС.* Бр. 72(2011), 49(2013) – одлука УС, 74(2013) – одлука УС и 55(2014).

Закон о полицији. Службени гласник РС. бр. 6(2016).

Закон о потврђивању Конвенције о високотехнолошком криминалу. *Службени гласник РС*. Бр. 19(2009).

Закон о ратификацији Европске конвенције за заштиту људских права и основних слобода, *Сл. лист СЦГ– Међународни уговори*. Бр.9(2003), 5(2005) и 7(2005) – испр. и *Сл. гласник РС – Међународни уговори.* Бр. 12/2010.

Илић, Г., Мајић, М., Бељански, С., Трешњев, А. (2016). *Коментар Законика о кривичном поступку, 6. измењено и допуњено издање*, Београд: Службени гласник. 215.

Кривични законик. *Сл. гласник РС*. Бр. 85(2005), 88(2005) – испр., 107(2005) – испр., 72(2009), 111(2009), 121(2012), 104(2013) и 108(2014).

Магазин Време. Бр. 1009. *Мрачна страна Фејсбука*. Преузето 6. маја 2010. са http://www.vreme.com/cms/view.php?id=929661.

Пауновић М., Кривокапић Б., Крстић И. (2014). *Међународна људска права*. Београд: Правни факултет Универзитета у Београду. 181.

Прља, Д., Рељановић М., Ивановић З. (2012). *Интернет право.* Београд: Институт за упоредно право. 95.

Revenge Porn. *Wikipedia*. Visited 6, July 2016. https://en.wikipedia.org/ wiki/ Revenge_porn.

Слијепчевић Љ. (2016). Право на приватност у домаћим и међународним прописима с освртом на интернет. *Гласник Адвокатске коморе Војводине*. 1(76). 41.

Solove, D. (2002). Conceptualizing Privacy. *California Law Review*. Vol. 90. 1087–1155.

Стојановић З. (2009). *Коментар Кривичног законика*. Београд: Службени гласник. 431, 395, 424.

The Free Dictionary by Farlex. Retrieved 7, July 2016 from http://www.thefree-dictionary .com/hack.

Универзална декларација, усвојена и проглашена Резолуцијом Генералне скупштине бр. 217 (III) од 10. 12. 1948.

Устав Републике Србије. *Сл. гласник РС*. Бр. 98(2006).

Case Alkaya v. Turkey, Application No. 42811/06, Judgment of 9. October 2012.

Case Von Hannover v. Germany, Application No. 59320/00, Judgment of 24, June 2004.

Case Delfi AS v. Estonia, Application No. бр. 64569/09, Judgment of 16, June 2015.

Case K.U. v. Finland, Application No. 2872/02, Judgment of 2, March 2009.

Case-law of the European Court of Human Rights. (2015). Retrieved 2, July 2016 from: *http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf.* 47–57.

Case Law of the European Court of Human Rights Concerning the Protection of Personal Data. (2013). Retrieved 3, July 2016 from: https://www.coe.int/t/dghl/standardsetting/dataprotection/ Judgments/DP%202013%20Case%20Law_Eng_FINAL.pdf .

Case Mitkus v. Latvia, Application No. 7259/03, Judgment of 2, October 2012.

Case Peck v. the United Kingdom, Application No. 44647/98, Judgment of 28, January 2003.

Council of Europe. *Explanatory Report to the Convention on Cybercrime (ETS No. 185).* Retrieved 4, July 2016 from: https://rm.coe.int/CoERMPublicCommonSearchServices/Display DCTMContent?documentId=09000016800cce5b.

Council of Europe. *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime* (2008) Retrieved 11, November 2016 from https://rm.coe.int/ CoERMPublicCommonSearchServices/Display-DCTMContent?documentId=09000016802fa3ba.

Council of Europe. *T-CY GuidanceNote #4 identity Theft and phishing in relation to fraud*. Retrieved 10, July 2016 from http://www.coe.int/t/dghl/cooperation/economiccrime/Source/ Cybercrime/TCY/TCY%202013/T-CY_2013_8E_ gui da nceNote4_id%20theft_V8.pdf.

Cyber Civil Rights Initiative. Visited 9, November 2016. https://www.cybercivilrights.org/.

Tijana Levakov Vermezović,
Faculty of Law, Univeristy of Belgrade

THE PROTECTION OF THE RIGHT TO PRIVACY AS THE SOCIAL IMPERATIVE OF DIGITAL AGE: How vulnerable are we?

Summary

The paper examines various forms of jeopardizing the privacy of individuals in digital world, with specific focus on criminal protection provided by current international and national legal framework and the jurisprudence of European Court of Human Rights. The significance of conducting this scientific research is essential considering that we live in the era of electronic communications in which no one is anonymous. Development of information and communication technologies has brought, among its many advantages, various challenges in all spheres of modern life. Since the Internet has become the global forum, individuals have been increasingly target of countless insults, defamation and threats; moreover, numerous personal information or media get published without consent. The practice shows that effective suppression and control of illegal behavior on the Internet and punishing the perpetrators is at the rudimental level. In order to provide proper protection for the victims of criminal offenses committed against their privacy in the digital world, it is necessary to create new models and approaches to solving this problem.

Keywords*: right to privacy, protection of personal data and communictions in digital form, Internet, criminal offences against rights and freedoms of man and citizen.*