Маст. Марија Милојевић, истраживачица - сарадница
Правног факултета Универзитета у Крагујевцу

УДК: 347.724:004.738.5:343
DOI: 10.46793/XXIv-14.195M

ДИГИТАЛНЕ УСЛУГЕ И КРИВИЧНО ПРАВО*

Резиме

Процеси као што су глобализација и дигитализација већ увелико обликују животе целокупне светске популације и задиру у све сфере модерног друштва. У овом раду аутор анализира утицај дигиталног сектора[1] *на област кривичног права. Анализа је урађена на свеобухватан начин имајући у виду како процедурално тако и супстанционо кривично право, али и утицај дигитализације на, са кривичним правом повезане области као што су криминалистика, извршење кривичних санкција, криминологија и др. Показаће се да развој и уплив дигиталних услуга у сферу кривичног права неупитно доноси велике бенефите који се огледају у увођењу и функционисању система е-правосуђа, новим начинима прикупљања доказа, коришћењу информатичког система у поступку извршења кривичних санкција, у коришћењу вештачке интелигенције ради побољшања предвиђања криминалитета и др. Са друге стране, развој информатичког друштва са собом носи и велике изазове у виду појаве нових кривичних дела („cyber crime"-рачунарска кривична дела), нових начина за извршење постојећих кривичних дела (нпр. дечја порнографија), као и изазова у погледу заштите права на приватност и личних података појединца, у погледу извештавања о злочинима... Из наведених разлога, неопходна је константна едукација свих професионалаца – судија, тужилаца, полицајаца, криминалиста као и криминолога, пенолога како би правосудни систем успешно одговорио на постојеће и будуће изазове дигиталног окружења.*

Кључне речи: *дигиталне услуге, е-правосуђе, дигитални доказ, вештачка интелигенција, сајбер криминалитет, систем извршења кривичних санкција, предвиђање криминалитета.*

---

* Рад је написан у оквиру Програма истраживања Правног факултета Универзитета у Крагујевцу за 2023. годину који се финансира из средстава Министарства, науке, технолошког развоја и иновација Републике Србије.

[1] Према Уредби ЕУ 2022/1925 о праведним тржиштима са могућношћу неограничене тржишне утакмице у дигиталном сектору и измени директива 2019/1937 и 2020/1828 од 2022. године, чл. 2, ст. 4, дигитални сектор је: „Сектор производа и услуга који се пружају путем или помоћу услуга информацијског друштва".

1. Дигитализација и кривично правосуђе

Под дигитализацијом правосуђа подразумева се процес претварања аналогних података из неког судског или јавнотужилачког предмета (материјалних доказа и других докумената, фотографија, табела, видео и аудио записа) у дигиталне податке који ће се даље користити на бржи и једноставнији начин (у виду неког компјутерског програма, нпр. у *„pdf“* или *„mp4“* формату).[2] Са њим повезан појам е-правосуђа шири је и под истим се подразумева „коришћење информационих и комуникационих технологија ради побољшања приступа правди, повећања сарадње између правних органа, јачања правосудног система и унапређења правних институција и опште администрације закона“[3]. Не улазећи у теоријска разматрања, аутор је појмове користио како синониме, подразумевајући под њима скуп дигиталних услуга које се спроводе под окриљем суда или тужилаштва (и других органа) пре, током и након кривичног поступка у циљу модернизације његовог тока и лакшег постизања његове сврхе.[4]

Остављајући по страни теоријске дилеме, аутори који пишу о овој проблематици слажу се да дигитализација у правосуђу доноси многобројне користи- „у правосуђу као саставном делу друштвеног живота, дигитализација је неопходна јер подразумева ефикасније правосуђе, бржу комуникацију, и смањење трошкова..“[5] Такође, у међународним документима истиче се да законски и подзаконски акти, као и судска пракса треба да буду лако доступни[6], што се у пракси остварује применом е-правосуђа.

Теоретичари често истичу период пандемије *COVID-19* као пресудан у погледу схватања значаја дигитализације у свим сферама друштва а посебно у функционисању правосудног система.[7] Овај период помиње се као прекретница у функционисању правосуђа и у документима ЕУ где се

[2] Дузлевски, И., *Значај дигитализације у кривичном праву*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022, стр. 60.

[3] Димовски, Д., *Бенефити коришћења е-правосуђа у кривичним стварима*, LXII Саветовање Српског удружења за кривичноправну теорију и праксу, Златибор, 2023, стр. 749.

[4] Термин е-правда- „*e-justice*“ егзистира у праву ЕУ и под њиме се подразумева: „широк спектар иницијатива, укључујући коришћење е-поште, попуњавање онлајн захтева, пружање онлајн информација (укључујући судску праксу), коришћење видео-саслушања и конференција, онлајн праћење регистрације и напретка предмета и способност судија или других доносилаца одлука да електронски приступе информацијама“. Према: *Handbook European law relating to access to justice*, https://echr.coe.int/document/handbook_access_justice_eng.pdf, приступљено: 10.10.2023. стр. 177-178.

[5] Самуилов, Ј., *Дигитализација правосуђа у Републици Србији, примена у пракси и изазови*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022, стр. 71.

[6] *E-nabling sustainable development: lessons from e-justice programming in Kyrgyzstan*, International Development Law Organization, Rome, 2018, стр. 4.

[7] Види: Дузлевски, И., *нав. дело*, стр. 60 и Самуилов, Ј., *нав. чланак*, стр. 73, 85.

примећује да су, „бројне државе чланице предузеле мере за ублажавање утицаја пандемије и успеле поновно покренути судске расправе захваљујући социјалном дистанцирању или видеоконференцијским техникама“[8]. Наглашава се и да је пандемија у бројним државама чланицама подстакла дигитализацију судских поступака.[9] У ЕУ важност тзв. *e-justice* подигнута је на завидан ниво постојањем Европског *e-justice* портала, који, између осталог, омогућава појединцима да покрећу прекограничне спорове мале вредности и реализују платне налоге електронским путем у складу са секундарним правом држава чланица.[10] Значај дигитализације препознат је и у раду Савета Европе, где је у оквиру делања Европске комисије за ефикасност правосуђа донет Акциони план 2022-2025 под називом: „Дигитализација за бољу правду“.

У овом поглављу ћемо изложити важеће законске одредбе којима је предвиђена могућност употребе дигиталних средстава и технологије у кривичном поступку, те на који начин они доприносе унапређењу поступка. Посебно ћемо се бавити појмом дигиталног доказа као и његовим специфичностима у односу на традиционални појам доказа.

1.1. Примена технологије у кривичном поступку - нормативни оквир

У праву РС значај дигитализације препознат је доношењем Стратегије развоја дигиталних вештина у Републици Србији за период од 2020.-2024. године[11]. Стратегија се у свом Посебном циљу 2 концентрише на унапређење основних и напредних дигиталних вештина за све грађане што је посебно важно као предуслов за реализацију несметаног приступа суду појединца као део права на правично суђење. За област кривичног правосуђа значајна је Стратегија развоја правосуђа за период 2020–2025. године у којој је, као један од стратешких приоритета, препознато даље подизање нивоа ефикасности

[8] Комуникација комисије Европском парламенту, вијећу, Европском господарском и социјалном одбору и одбору регија COM/2020/580 final, Извештај о владавини права за 2020.годину, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52020DC0580, приступљено: 10.10.2023, Увод.

[9] *Исто*, увод.

[10] *Handbook European law relating to access to justice*, https://echr.coe.int/document/handbook_access_justice_eng.pdf, приступљено: 10.10.2023, стр. 178.

[11] Стратегија одражава континуитет и наслања се на Дигиталну агенду за Србију коју чине Стратегија развоја информационог друштва у Републици Србији до 2020. године и Стратегија развоја електронских комуникација у Републици Србији од 2010. до 2020. године, а заједно са Стратегијом развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године, представља стратешки оквир за повећање приступа грађана и привреде информационим и комуникационим технологијама, унапређење отворености и доступности интернета и стварање информационог друштва, између осталог, и развојем е-правосуђа.

правосудног система кроз развијање ИТ система у правосуђу са циљем постизања модерног е-правосуђа. Као посебан циљ Стратегије наведен је развој е-правосуђа и то кроз „даље унапређење е-сервиса унутар правосуђа, чиме би се обезбедио приступ правди, повећање квалитета поступања и одлучивања, ефикасно управљање предметима, статистичко праћење и извештавање о раду правосуђа, и транспарентност рада правосудних органа“[12].

У нашој земљи је, још доношењем Законика о кривичном поступку установљен нормативни оквир за примену информационих технологија и дигиталних сервиса у кривичном поступку. Међутим, требало је времена да поједини е-алати заживе у пракси; законом дате могућности стидљиво се примењују.[13] Разлози за такво поступање леже првенствено у изостанку финансијске потпоре, „недостаје довољно добра техничка опрема и услови, при чему се овде мисли на добре и квалитетне рачунаре, штампаче, довољан број скенера, али и посебно оне опреме који би служили за дигитално фотографисање, скенирање, видео и аудио снимање“[14]. Са друге стране се јавља и проблем обучености кадрова за коришћење техничке опреме и учешће у дигитализацији уопште.[15]

Нормативни оквир као основ примене е-правосуђа састоји се из неколико скупа одредби. То су:

1) одредбе којима се регулише транспарентност рада правосуђа и омогућава приступ правди, информисање грађана и њихова комуникација са органима поступка (коришћење е-поште, пружање онлајн информација и онлајн праћење регистрације и напретка предмета);

2) одредбе које се односе на комуникацију међу самим органима поступка у виду ефикасног управљања предметима, статистичког праћења и електронског приступа и размене докумената међу органима поступка;

3) одредбе које се тичу заштите сведока коришћењем аудио-визуелних средстава и техничких средстава за прикривање идентитета;

4) одредбе које се тичу посебних доказних радњи (тајни надзор комуникације, тајно праћење и снимање и рачунарско претраживање података).

1) Главни предуслов за реализацију права појединца на приступ суду је информисаност учесника у поступку. То се постиже одредбама о достављању писмена и организовањем интернет страница тужилаштава и судова у Републици Србији и портала где се грађани могу информисати о току

[12] Стратегија развоја правосуђа за период 2020–2025. године, (Сл. гласник РС, бр. 101 од 17. јула 2020, 18 од 11. фебруара 2022.), Део 4-Визија и циљеви Стратегије.

[13] Види: Милојевић, М., *Пружање услуга Центра за социјални рад у кривичном поступку*, Зборник радова: Садашњост и будућност услужног права, Крагујевац, 2022, стр. 897-915. У раду се наводи да је први форензички интервју са дететом вођен је у просторијама Центра за социјални рад „Свети Сава“ у Нишу 2021. године, иако су за то постојале законске могућности знатно раније.

[14] Самуилов, Ј., *нав. чланак*, стр. 75-76.

[15] *Исто*, стр. 76.

предмета, али и о структури, организацији органа и важећим прописима. У одредбама Законика о кривичном поступку предвиђено је да се достављање може вршити и на огласној табли или интернет страници органа поступка, али уз сагласност лица коме се достављање има извршити и преко пуномоћника за пријем писмена, путем поштанског фаха или електронске поште.[16] Законик предвиђа могућност подношења електронског поднеска, односно да писмени поднесак може бити састављен и у облику електронског документа који је снабдевен електронским потписом подносиоца, те је наведено да се овакав поднесак подноси органу поступка путем електронске поште, а орган поступка мора без одлагања подносиоцу да потврди електронским путем пријем поднеска, док о електронском поднеску орган поступка саставља службену белешку.[17]

2) У судовима и тужилаштвима записници и други поднесци чувају се у електронском облику. Судским пословником предвиђено је да се записници састављају и штампају по правилу коришћењем ИКТ или писаћом машином[18], а од 2010. године је у функцији електронски уписник *LIBRA* у којем се налазе поднесци скенирани по предметима и приказани у електронском облику, са којима се могу упознати и странке на посебном порталу Министарства правде који је основан ради праћења тока предмета. У јавним тужилаштвима се, по правилу, у раду користе информационо-комуникационе технологије за обраду текста, вођење евиденција, обраду и прикупљање статистичких података за електронску размену података, рачуноводствене послове, као и за праћење прописа, судске и јавнотужилачке праксе.[19] У појединим тужилаштвима се употребљава врста електронског уписника *SAPO* али је она ограничена само на неколико тужилаштава у Републици Србији, јер иако су сви тужиоци били у обавези да током 2021. године прођу обуку, примена овог програма још увек, уопште није заживела.[20] Законом је предвиђена могућност тонског или оптичког снимања извођења доказне или друге радње, као и снимање на главном претресу.[21] Такође, успостављен је Правосудни информациони систем у 2017. години чији је циљ повећање ефикасности судских поступака повезивањем базе података државних и правосудних органа и разменом

[16] Чл. 242 ст. 3 Законика о кривичном поступку (Сл. гласник РС, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021- одлука УС и 62/2021-одлука УС).
[17] *Исто*, чл. 230.
[18] Чл. 125а ст. 3 Судског пословника (Сл. гласник РС, бр. 110/2009, 70/2011, 19/2012, 89/2013, 96/2015, 104/2015, 113/2015 - испр., 39/2016, 56/2016, 77/2016, 16/2018, 78/2018, 43/2019, 93/2019 и 18/2022).
[19] Чл. 86 ст. 1 Правилника о управи у јавним тужилаштвима (Сл. гласник РС, бр. 110/2009,87/2010,5/2012,54/2017,14/2018 и 57/2019).
[20] Самуилов, Ј, *нав. чланак*, стр. 77.
[21] Чл. 236 Законика о кривичном поступку (Сл. гласник РС, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021- одлука УС и 62/2021-одлука УС).

електронских докумената који скраћују време које је иначе потребно за доставу писмена у папирном облику.

3) Употреба дигиталних и техничких средстава у области заштите предвиђена је у оквиру посебних мера заштите сведока. Мере специјалне заштите сведока се односе на одредбе ЗКП-а којима је регулисан процесни положај посебно осетљивих сведока и заштићеног сведока.[22] Орган поступка може одлучити да се посебно осетљиви сведок испита употребом техничких средстава за пренос слике и звука, испитивање се спроводи без присуства странака и других учесника у поступку у просторији у којој се сведок налази.[23] Статус заштићеног сведока обухвата примену мера посебне заштите сведока чија је сврха да обезбеде да се истоветност заштићеног сведока не открије јавности. У том смислу, за испитивање сведока могу да се користе технички уређаји за пренос и промену слике и звука, може се вршити испитивање из посебне просторије уз промену гласа сведока и др.

4) У Законику о кривичном поступку за одређена кривична дела предвиђене су посебне доказне радње: тајни надзор комуникације, тајно праћење и снимање, симуловани послови, рачунарско претраживање података, контролисана испорука и прикривени иследник. Заједничко за све доказне радње је употреба технологије (прикривеном иследнику може бити одређено да употреби техничка средства за фотографисање или тонско, оптичко или електронско снимање). Како се оваквим доказним радњама знатно задире у приватност осумњичених лица а путем њих се може доћи до деликатних информација прописани су строги услови за њихово одређивање.[24]

1.2. Дигитални докази

Развој дигиталног тржишта довео је до нове врсте доказа који се користе у кривичном поступку- дигиталних доказа. О овом институту издвојено је посебно поглавље јер је међународна стручна и научна јавност њему посветила посебну пажњу доношењем бројних међународних докумената и детаљном анализом кроз израду научних радова. Савет Европе је у 2013. години издао Водич о електронским доказима. Овај водич представља најважнији споредни алат који се користи у вези са електронским доказима. Треба издвојити и Стандардне оперативне процедуре за прикупљање, анализу и презентацију

[22] Тешовић, О., Миловановић, И., *Заштита сведока у кривичним поступцима и примена технологије*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022, стр.177.

[23] Чл. 104 ст. 2 Законика о кривичном поступку.

[24] Одређују се за само за таксативно набројана кривична дела уколико се на други начин не могу прикупити докази за кривично гоњење или би њихово прикупљање било знатно отежано. Спис са посебним доказним радњама носи ознаку степена тајности, а постоје и посебне одредбе о уништавању материјала и о случајном налазу.

дигиталних доказа донете 2019. године од стране тела Савета Европе-Канцеларије за програм сајбер криминалитета.

Дигитални докази су први пут били споменути и регулисани у оквиру Будапештанске Конвенције о кибернетичком криминалитету из 2001.године. Иако је конвенција донета како би европска заједница одговорила на изазов повећаног раста тзв. сајбер криминала, суштински је, између осталог, регулисала начин прибављања и чувања дигиталних доказа иако их нигде није прецизно дефинисала. Аутори сматрају да је најчешће употребљавана дефиниција дигиталних доказа у академској и стручној литератури дефиниција из 2012. године садржана у Смерницама за идентификацију, прибављање и чување дигиталних доказа Међународне организације за стандарде према којој су дигитални докази информације или подаци, који се чувају или преносе у бинарном облику, а на које се може ослонити као на доказ.[25] Доказ се, у традиционалном смислу, дефинише као чињеница, којом се утврђује постојање спорних правно релевантних чињеница у кривичном поступку.[26] Дигитални или електронски доказ је само врста доказа у ширем смислу имајући у виду да докази могу бити: посредни и непосредни, доказ о личности, форензички доказ, писани и статистички доказ, ослобађајући доказ, доказ сведочења и по чувењу, физички доказ, доказ-претпоставка... Међутим ова подела нема јасне границе па тако електронски доказ може бити и форензички, ослобађајући или документарни. Такође, можемо разликовати доказе који су по својој природи форензички или физички али за чије се прибављање могу користити дигитална средства (нпр. докази прикупљени употребом дронова - отисци прстију, трагови крви...) од дигиталних доказа који представљају информације у дигиталном облику. Оно што треба нагласити када су у питању дигитални докази и разлог зашто се посебно проучавају и за њих донесе посебна правила је тај што се за сведочење, материјалне и физичке доказе сматра да су директнији, лакши за прикупљање, чување и очување, показивање, интерпретацију и конфронтацију. За електронске доказе то није случај: по природи их је теже прибавити и чувати, нестални су, означени датумом- роком важења, често су изузетно обимни а све манипулације њима захтевају стручно и специјализовано знање. Тешко је доказати њихово порекло, аутентичност и интегритет.[27] Оно што додатно отежава њихово прикупљање и чување је то што лако могу променити локацију и садржај, могу се складиштити на више извора- интернет претраживачу, рачунару, преносним меморијама, тзв. *cloud*-у

[25] Муртезић, А., *Дигитални докази: шта доноси други додатни протокол уз Будимпештанску конвенцију?*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022, стр. 90.

[26] Стевановић, Ч., Ђурђић, В., *Кривично процесно право – општи део*, Ниш, 2006, стр. 228, Радуловић, Д., *Кривично процесно право*, Подгорица, 2009, стр. 158.

[27] Види: *Cybercrime and Electronic Evidence*, https://help.elearning.ext.coe.int/enrol/index.php?id=5526, стр. 7-8, приступљено: 23.10.2023.

(емајл се може наћи и на компјутеру пошилаоца као и на компјутеру примаоца), могу бити изложени рачунарским вирусима..

Из наведених разлога, приликом прикупљања и чувања дигиталних доказа морају се поштовати одређена правила, а свако правило одговара својству које доказ мора имати да би се сматрао валидним и релевантним: прихватљивост, аутентичност, комплетност, поузданост прикупљања процедуре и анализе које не смеју довести у питање аутентичност и истинитост доказа и уверљивост.[28] Будапештанском конвенцијом предвиђена је хитна заштита похрањених рачунарских података, регулисан је налог за доставу као и претрес и одузимање сачуваних компјутерских података. Посебна пажња усмерена је ка прикупљању података о промету у стварном времену и пресретању података.

2. Кривично материјално право у савременом друштву

Утицај дигиталних технологија протеже се и на област кривичног материјалног права, а најизраженији печат модерно друштво оставило је, нажалост, на посебни део кривичног права резултирајући појавом нових кривичних дела и нових облика (видова испољавања) већ постојећих противправних понашања. Међутим, пораст броја комплексних кривичних дела посредно је резултирао успостављање и ојачање међународне сарадње у кривичним стварима првенствено међу европским државама што свакако представља позитиван начин борбе против високотехнолошког криминалитета који врло често прелази границе двеју или више земаља. Конвенција о високотехнолошком криминалу предвидела је успостављање међународне сарадње у предметним питањима тако што ће „стране једна с другом сарађивати у најширем могућем обиму у складу с одредбама овог поглавља, примењујући релевантне међународне инструменте међународне сарадње у кривичним стварима, споразуме склопљене на основу јединственог или реципрочног законодавства и домаћег права, у сврху спровођења истрага или поступака поводом кривичних дела везаних за компјутерске системе и податке или у сврху прикупљања доказа о кривичном делу у електронском облику“[29]. Упоредо са развојем високотехнолошког криминала развија се и реакција међународне заједнице која константно мора ићи у корак са најсавременијим тенденцијама. У складу са тим Интерпол је у Сингапуру 2014. године отворио Глобални комплекс за иновације чији су главни елементи: иновативна истраживања и развој како би се побољшали форензички капацитети и базе података посебно у погледу идентификације злочина и починилаца; одговор на

[28] Муртезић, А., *нав. чланак*, стр. 91-92.

[29] Поглавље 3, Одељак 1, Део 1, чл. 23 Конвенције о високотехнолошком криминалу из 2001. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documen-tId=0900001680081561, приступљено: 10.10.2023.

захтев за полицијским тренингом и побољшањем капацитета полиције базираног на технологијама и иновацијама, као и побољшање капацитета Интерпола за пружањем 24/7 оперативне подршке полицији у различитим временским зонама и већој удаљености са већом мобилношћу него раније.[30]

Савремено друштво, развој дигиталних услуга и дигиталног тржишта, поред свих бенефита, са собом доноси и пораст и развој криминалитета. Реч је о појави високотехнолошког (информатичког, рачунарског, кибернетичког или сајбер) криминалитета. На тај начин нека већ постојећа, класична, општа, конвенционална кривична дела добијају нове облике или видове испољавања, али се јављају и нове инкриминације којима се повређују или угрожавају заштићена добра, вредности и интереси других физичких или правних лица, па и читавих држава, односно међународне заједнице у целини.[31] Неки аутори тако разликују рачунарски криминалитет у ужем и рачунарски криминалитет у ширем смислу.[32] Европа је 2001. године реаговала на овај тип криминалитета доношењем Конвенције о високотехнолошком криминалу у Будимпешти у оквиру Савета Европе. У Кривичном Законику Републике Србије[33] из 2005. године рачунарска кривична дела регулисана су у посебној глави „Кривична дела против безбедности рачунарских података“. Уз Конвенцију о високотехнолошком криминалу донет је Допунски протокол о криминализовању аката расистичке и ксенофобичне природе која су учињена посредством рачунарских система 2005. године у Стразбуру и управо се у овом протоколу регулишу противправна понашања која спадају у сајбер криминалитет у ширем смислу - ради се о вршењу специфичних кривичних дела извршених из расистичких и ксенофобних понуда (зло)употребом дигиталних технологија- рачунара. И сама Будимпештанска конвенција схвата

[30] Интернет сајт Интерпола, https://www.interpol.int/News-and-Events/News/2010/INTERPOL-Global-Complex-in-Singapore-to-enhance-and-strengthen-policing-worldwide, приступљено: 25.10.2023.

[31] Јовашевић, Д., *Појам и карактеристике рачунарских кривичних дела*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022, стр. 2.

[32] Рачунарски криминалитет у ужем смислу - свако незаконито (противправно) понашање које је усмерено на електронске операције против сигурности рачунарских система и рачунарских података који се у њима обрађују (прављење и убацивање рачунарских вируса, хакинг, пиратство, рачунарска саботажа, рачунарска шпијунажа, рачунарске преваре и крађа рачунарских услуга) и б) рачунарски криминалитет у ширем смислу - свако незаконито (противправно) понашање које је везано за или у односу на рачунарски систем и рачунарску мрежу, укључујући и такав криминалитет какво је незаконито поседовање, нуђење и дистрибуирање информација преко рачунарских система и рачунарских мрежа. Види: Бабић, М., *Међународно кривично право*, Бања Лука, 2011, стр. 89-94, Вестби, Ц., *Међународни водич за борбу против компјутерског криминалитета*, Београд, 2004, стр. 214-223.

[33] Сл. гласник РС, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94 /2016 и 35/2019.

високотехнолошки криминал у ширем смислу - Поглавље II - мере које треба да се предузму на националном нивоу, Део 1 - Материјално кривично право, Одељак 3 - Дела у вези са садржајем- односи се на регулисање дела у вези са дечјом порнографијом (производња, дистрибуција, нуђење или чињење доступним дечије порнографије, набављање дечије порнографије преко рачунарског система, за себе или за друго лице као и поседовање дечије порнографије у рачунарском систему или на медијумима за чување рачунарских података); Одељак 4 - Дела у вези са кршењем ауторских и сродних права - регулише кршење ауторских и сродних права тј. прописује да свака држава уговорница треба да усвоји законодавне и друге мере, неопходне да би се као кривично дело у домаћем праву прописало кршење ауторских и сродних права дефинисаних у законима те стране уговорнице „када су та дела учињена добровољно, у обиму који их квалификује да имају комерцијални карактер и преко рачунарског система“. У посебној глави „Кривична дела против безбедности рачунарских података“- прописана су рачунарска кривична дела у ужем смислу: Оштећење рачунарских података и програма, Рачунарска саботажа, Прављење и уношење рачунарских вируса, Рачунарска превара, Неовлашћени приступ заштићеном рачунару, рачунарској мрежи и електронској обради података, Спречавање и органичавање приступа јавној рачунарској мрежи, Неовлашћено коришћење рачунара или рачунарске мреже, Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података.[34]

Треба напоменути да је, поред препознавања и законског регулисања рачунарских кривичних дела као таквих а затим и њиховог санкционисања, од практичне важности за појединца (можда и најважнија) сама превенција дигиталног криминалитета. Превенција, откривање и расветљавање компјутерског криминала захтева посебан приступ и континуирано увођење нових метода, стално усавршавање стручних квалификација криминалиста и, на крају, али не и најмање важно, ближа сарадња са спољним стручњацима (приватни сектор).[35] Међутим, аутори наглашавају да је за поједина рачунарска кривична дела превенција готово немогућа.[36] Имајући на уму да се дигитално

[34] У Глави 18-Кривична дела против полне слободе у чл. 185б регулисано је кривично дело- Искоришћавање рачунарске мреже или комуникације другим техничким средствима за извршење кривичних дела против полне слободе према малолетном лицу.

[35] Brvnišťan, M., *Cybercrime and possibilities of prevention*, Proceedings of the scientific conference with international participation Current challenges of computer crime prevention held on 21 March 2018 at the Academy of Police Force in Bratislava, Bratislava: Academy of Police Force, 2018, стр. 34.

[36] Код злоупотребе платних картица превенција је готово немогућа- може се састојати само у настојању да појединци користе сигурне и верификоване системе за плаћање као и да купују од сигурних продаваца; код кривичног дела у вези са нелегалним копијама ауторских дела на вебсајтовима једина могућа превенција је предвиђање кривичних

тржиште услугама развило до тог ступња да је постало готово неопходно у свим сферама живота, да су дигитални финансијски инструменти све бројнији (куповина платним картицама преко интернета, онлајн клађење, трговина криптовалутама, мобилне апликације банака и оне које служе за платни промет), сувишно је говорити о уздржавању а понајмање о забрани поменутих активности.

3. Утицај дигиталних услуга на остала питања и области повезане са кривичним правом

Поред утицаја које дигитализација има на кривични поступак у виду употребе е-правосуђа, разних дигиталних средстава и услуга у току поступка као и у виду појаве нове врсте доказа-дигиталних доказа, на кривично материјално право који се огледа у појави новог облика криминалитета - сајбер криминалитета о чему је већ било речи у претходним поглављима, неопходно је навести неке дигиталне услуге и средства која су, директно или индиректно, повезана са кривичним правом. Њихова повезаност огледа се у томе да се користе у, са кривичним правом повезаним наукама и дисциплинама.

У САД, технолошки напредак користи се за предвиђање криминалних понашања што увелико може допринети превенцији криминалитета. Универзитет у Хјустону радио је на развоју алгоритама који обезбеђују континуирано праћење ради процене активности и предвиђају појаву сумњивих и криминалних понашања преко мреже камера.[37] Овај алгоритам се такође служи анализом одеће, скелетне структуре, покрета, као и предвиђања правца за идентификацију појединаца од интереса путем више камера и слике.[38]Превенцији криминалитета служи и апликација Амбер Алерт која је дана 25. 10. 2023. године почела са радом у Републици Србији под називом „Пронађи ме“ која под одређеним законским условима покреће механизам проналаска несталих лица који се састоји од објављивања фотографија и описа несталих малолетних лица путем медија прекидањем програма на сваких 30 минута, на аеродромима, аутопутевима, на аутобуским и железничким станицама и другим прометним местима као и слањем порука корисницима

санкција за оваква противправна понашања; и код ширења лажних информација путем вебсајтова и имејлова превенција је непостојећа- починилац најчешће верује у истинитост својих тврдњи. Према: Blazek, R., *The new forms of digital criminality in Slovakia and fight against them*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022, стр. 25-27.

[37] Rigano, C., *Using artificial intelligence to address criminal justice needs*, National Institute of Justice Journal/Issue No. 280, January 2019, стр. 5, https://www.ojp.gov/pdffiles1/nij/252038.pdf, приступљено: 25.10.2023.године.

[38] *Learning Models for Predictive Behavioral Intent and Activity Analysis in Wide Area Video Surveillance* at the University of Houston, NIJ award number 2009-MU-MU-K004.

мобилних мрежа.[39]Увођењем видео надзора почетком 60-тих година прошлог века почео је процес секуритизације у свету који се сматра важним механизмом ситуационе превенције.[40] Видео надзор користи се и у криминалистици приликом идентификације лица од интереса за предистражне и истражне органе.

Под утицајем друштвено-економских чинилаца измењена је и феноменологија криминалитета чиме је и криминологија као наука претрпела одређене измене. Са већим присуством високе технологије у свакодневном животу дошло и до трансформације криминалних прилика и понашања.[41] Криминалне активности су постале глобалне, дистрибутивне и информационализоване.[42]

Употреба технологије у великој мери утицала је на област криминалистике. Ласерско скенирање и виртуелно - 3Д окружење места користи се за обезбеђивање доказа са места злочина, за потребе извођења увиђаја и реконструкције. У Хонг Конгу, виртуелна реалност коришћења је приликом суђења за смрт студента, што би било корисно у циљу предочења чињеница и приближавања поротницима како се конкретни догађај одиграо.[43] 3Д техника форензичке анализе коришћена је и код нас за анализу случаја убијених топчидерских војника коју је спровео Центар за форензичка истраживања, као и у случају убиства Јелене Марјановић од стране стручног саветника форензичара Ненада Шипке. Све чешће су у употреби и дронови у криминалистичким истраживањима, пре свега у спровођењу увиђаја, али и у другим криминалистичким радњама, нарочито претраживању лица места након што је догађај завршен или у надзору још активног догађаја.[44]

У погледу извршења кривичних санкција примена дигитализације евидентна је како у погледу ванзаводских, тако и заводских санкција и мера. Код ванзаводских мера примењује се електронски надзор, док је код заводских

[39] Систем неће бити активиран за свако дете чији је нестанак пријављен, већ само када постоји сумња да је жртва кривичног дела. Нити ће бити активиран ако се процени да објављивање информација о детету може да угрози сигурност детета и омете рад полиције. Обавезно ће бити активиран у случајевима нестанка деце до седам година, као и деце са сметњама у развоју до 18 година. Говор министра полиције Братислава Гашића на представљању система, извор: https://www.bbc.com/serbian/cyr/srbija-67210992, приступљено: 25.10.2023.

[40] Стевановић, А., *Улога вештачке интелигенције у контроли криминалитета*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022, стр. 349, 353.

[41] *Исто*, стр. 350.

[42] Wall, S. D., *Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime*, The European Review of Organised Crime. No. 2/2015., стр. 86.

[43] Димовски, Д., *нав. чланак*, стр. 758.

[44]Дураковић, А. и др., *Употреба доказа прикупљених дроновима у криминалистичким истраживањима*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022, стр. 99.

мера уведен Софтвер за евиденцију лица лишених слободе предвиђен Стратегијом развоја система извршења кривичних санкција у Републици Србији за период 2021-2027. године. Дигитализација је присутна и код вршења надзора у заводима за извршење кривичних санкција као и код ресоцијализације осуђеника[45].

4. Вештачка интелигенција и кривично право

Вештачка интелигенција издвојена је у посебно поглавље јер потенцијално може да утиче на све сфере савременог друштва. Њена примена може потпуно изменити кривични поступак каквим га познајемо, алгоритми вештачке интелигенције своју примену могу наћи у предвиђању криминалитета, приликом доношења судских одлука, предвиђању успеха у преткривичном поступку, у погледу обраде великог броја правних докумената; развој вештачке интелигенције може ићи толико далеко и изнедрити појаву робот-судија и адвоката а то је само врх леденог брега јер будућност дефинитивно са собом носи многи тога што још не можемо да предвидимо.

Према једној општеприхваћеној дефиницији, вештачка интелигенција је део науке о рачунарима, која се бави креирањем таквих рачунарских система који су способни да поседују карактеристике које асоцирају на људско понашање[46]. Није прошло много времена од када су научници схватили да вештачку интелигенцију могу употребити у области права и правде. Употребу вештачке интелигенције у праву можемо повезати са појмом предвидиве правде (енг. *Predictive Justice*) који је новијег датума, настао пре свега развојем рачунарских метода обраде великог обима података и подразумева могућност предвиђања исхода судског поступка или неке његове фазе применом математичких алгоритама заснованих на обради великог обима доступних података, односно претходних одлука.[47]

У Сједињеним Америчким Државама користи се алгоритам заснован на вештачкој интелигенцији *(COMPAS)* који процењује степен ризика по опасност заједнице осуђеника у поступку одлучивања о условном отпусту. У

[45] У августу 2020. године, Министарство правде Владе Републике Србије саопштило је да су осуђеници у десет казнено-поправних установа почели да користе програме „Скајп“ (Skype) и „Вајбер“ (Viber) за контакт са члановима својих породица у циљу додатне психосоцијалне подршке током пандемије коронавируса. Извор: https://www.srbija.gov.rs/vest/482074/osudjenici-koriste-skajp-i-vajber-za-kontakt-sa-porodicom-to-kom-pandemije.php, приступљено: 25.10.2023.

[46] Russel, S., Norvig, P., *Artificial Intelligence: A Modern Approach*, 2 ed. N.J:Prentice Hall, 2010, стр. 1034.

[47] Тоскић Цветиновић, А., Тошић, М., *Примена вештачке интелигенције у правосуђу– перспективе и изазови*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022, стр. 319.

претходном поглављу већ је поменуто коришћење сличних алгоритама у САД за процену криминалног понашања користећи камере видео надзора.

Када су у питању алати вештачке интелигенције, у пракси се све више употребљава *ChatGPT* као вештачком интелигенцијом генерисан четбот који има приступ широком спектру речи из речника, докумената и информација и на основу тога има могућност да пружа смислене одговоре на, наизглед, бесконачан број тема. Евидентно је да своју примену може наћи у раду правних практичара тако што ће повећати продуктивност и ефикасност, побољшати комуникацију, смањити трошкове и омогућити приступ широком спектру правних и стручних извора[48] што ће даље омогућити правницима да приступе већем броју информација него што би то био случај помоћу традиционалног истраживања. Апликација постоји и у облику *Law ChatGPT*- специјализована за питања из области права. *ChatGPT* је употребљен и приликом доношења судске одлуке[49] мада то са собом отвара бројна питања и контроверзе[50]. Не само да се вештачка интелигенција користи приликом креирања судских одлука већ и саме судије могу бити генерисани путем вештачке интелигенције. Тако, и споровима мале вредности у Естонији и Канади у улози судије поступају ентитети вештачке интелигенције. У Пекингу 2019. године уведен је Интернет суд у коме ради судија створен вештачком интелигенијом - ентитет женског лика и гласа. Међутим, евидентно је да се у конкретним случајевима радило о потреби суда да се растерети у ситуацији претрпаности предметима, ситуација у погледу одлучивања о кривичним стварима далеко је комплекснија. Ни професија адвоката не представља изузетак. Један вид четбота - апликација *DoNotPay* састоји се из бесплатног пружања услуга клијентима који немају финансијских могућности да ангажују адвоката али се углавном користи за решавање спорова из потрошачког права. Иако је било речи о пројекту у коме би „ВИ Адвокат“ имао своју премијеру на суду где је било планирано да заступани помоћу смартфона генерише своју одбрану а да ће му одговори на правна питања бити путем слушалица саопштавани. Од овог пројекта се у међувремену одустало[51], а са правом можемо да кажемо да је поступање ВИ

[48] Види: https://www.allens.com.au/insights-news/insights/2023/02/ChatGPT-in-law/, приступљено: 25.10.2023.

[49] Колумбијски судија је своју одлуку генерисао помоћу *ChatGPT-a* у случају аутистичног детета коме је осигурање требало да покрије трошкове лечења, https://www.theguardian.com/technology/2023/feb/03/colombia-judge-chatgpt-ruling, приступљено: 26.10.2023.

[50] Ради се, пре свега, о питању правичности и тзв. осећаја за правду који разликује људе од машина, затим о утицају вештачке интелигенције на поштовање људских права, на једнакост странака, могућност дискриминације, право на приватност, заштиту и безбедност података. Види: Тоскић Цветиновић, А., Тошић, М., *нав. чланак*, стр. 332-336.

[51] Види: https://www.npr.org/2023/01/25/1151435033/a-robot-was-scheduled-to-argue-in-court-then-came-the-jail-threats, приступљено: 26.10.2023.

судија и адвоката, бар у области кривичног права, још увек резервисано за даљу и неизвесну будућност.

5. Закључак

Широк спектар дигиталних услуга све се више користи у домену кривичног права и са њим повезаним гранама и дисциплинама. Утицај дигитализације у овој области вишеструк је и комплексан и не може се дефинисати као у потпуности позитиван или негативан. Оно око чега се можемо сложити је да је употреба технологије евидентно неизбежна у свим сферама кривичног права.

У кривичном поступку употреба е-правосуђа и дигиталних средстава уопште знатно олакшава, убрзава и чини економичним поступак изрицања кривичне санкције, али комплексност техничких средстава захтева константну едукацију и стручност свих професија неопходних за функционисање правосудног система. „...Савремене технологије, могу се применити и у сврхе просперитета постојећих правосудних система, тј. могу допринети експедитивности и ефикасности судских поступака, као и правичнијим, надасве објективније одмереним одлукама.“[52] Правосудни системи неких земаља далеко су одмакли у коришћењу техничких средстава. Разматра се увођење бар кодова којима би се било која информација уградила у шифру, којој се затим може приступити скенирањем путем паметних уређаја.[53] У САД се у преткривичном поступку користе посебне софтверске апликације за предвиђање вероватноће успеха у преткривичном поступку (*The Public Safety Assessment - PSA*), У Пекингу од 2019. године ради „парнични услужни центар“ у коме поступа судија- продукт вештачке интелигенције, у Индији унапређен је систем електронске комуникације грађана и органа правосуђа и регулисана могућност подношења електронског поднеска... Евидентно је да правна пракса у нашој земљи још дуго неће бити на том нивоу и да ће, ако некада дође до примене неких од наведених института, претходно морати да дође до промене закона и опсежне припреме запослених за такво поступање. Наша правна традиција другачија је и јединствена, томе говори у прилог чињеница да је пракса судова да за време пандемије одрже онлајн кривична суђења преко апликације *Skype* изазвала озбиљне контроверзе; део стручне јавности је замерао да је овакво суђење у супротности са нормативним оквиром, док је други део стручне јавности пледирао у његову одбрану.[54]

---

[52] Муњић, Ј., *Поједини аспекти имплементације савремених софтверских решења у правосудни систем и утицај дигитализације на правосуђе и адвокатуру*, Зборник радова: Правна регулатива услуга у националним законодавствима и праву Европске уније, Крагујевац, 2023, стр. 473.

[53] У питању су Сједињене Америчке Државе према: Димовски, Д., *нав. чланак*, стр. 755.

[54] *Исто*, стр. 755-756.

Највећи негативни нуспроизвод технолошких достигнућа је појава сајбер криминала. Тас на ваги изједначава се применом технолошких достигнућа у погледу превенције и предвиђања криминала, као и у области криминалистичке технике.

Претерана употреба технологије може изазвати супротан ефекат. Право на приступ суду може бити угрожено појединцима који не користе савремене технологије у довољној мери.[55] Са друге стране, Министарство Правде Уједињеног Краљевства добило је признање међународне заједнице за интерактивни водич „Ти буди судија“ у коме се грађанима приближава доношење пресуда и одлука од стране суда; сматра се да ће визуелизација процеса одлучивања олакшати приступ правди.[56] Употреба виртуелне реалности у кривичном поступку може бити превише скупа, посебно имајући у виду наше услове где већина судова није опремљена ни посебним техничким средствима и просторијама за снимање слике и звука.[57] Све речено односи се и на употребу дигиталних доказа у кривичном поступку- њихова употреба кључна је у борби против све учесталијих рачунарских кривичних дела, међутим њихово прикупљање и чување компликовано је, није јефтино и захтева завидна знања и вештине.

Комплексно је питање употребе вештачке интелигенције у области кривичног права што је детаљно изложено у делу о вештачкој интелигенцији. На тлу Европе дуго времена није долазило до консензуса о овом питању. Инструменти који су предвиђени за регулацију вештачке интелигенције углавном су у вези са заштитом података о личности (Европска етичка повеља о коришћењу вештачке интелигенције у правосуђу Европске комисије за ефикасност правосуђа (СЕПЕЖ – “ЦЕПЕЈ”) из децембра 2018. године, Смернице о вештачкој интелигенцији и заштити података о личности Савета Европе из 2019. године, Општа уредба о заштити података ЕУ из 2016. године). Искорак напред десио се када је Европски парламент 14. јуна 2023. године изгласао своју преговарачку позицију након две године расправе о Предлогу закона о вештачкој интелигенцији. Акт још увек није ступио на снагу, а

[55] Од кључне важности је да савремена технолошка решења постоје упоредо са традиционалним системима, Суд правде Европске уније у својим одлукама потврдио је да за појединце може бити немогуће да остваре своја права уколико се правосуђу може приступити само електронским путем. *Handbook European law relating to access to justice, Наведено дело,* стр. 180. Види: *CJEU, Joined cases, C-317/08, C-318/08, C-319/08 and C-320/08, Rosalba Alassini v. Telecom Italia SpA, Filomena Califano v. Wind SpA, Lucia Anna Giorgia Iacono v. Telecom Italia SpA and Multiservice Srl v. Telecom Italia SpA,* 18 March 2010, para. 58.

[56] *Handbook European law relating to access to justice, Наведено дело,* приступљено: 25.10.2023, стр. 180.

[57] У свету се виртуелна реалност употребљава приликом чувања доказа са места злочина, како би се што реалније стекао утисак о одиграном злочину и сагледао догађај из више перспектива.

предвиђања су да ће се то десити почетком 2025. године. У Акту о вештачкој интелигенцији се прави разлика између система „неприхватљог ризика“ и система „ограниченог ризика“ у које спада и *ChatGPT* где су први начелно недозвољени док су други начелно дозвољени ако имају ознаку „*AI generated*“. Без обзира на то што су први системи неприхватљиви јер на недозвољен начин „бодују“ и класификују људе на основу њиховог понашања, статуса и карактеристика, ипак се дозвољава употреба тих система у ситуацијама као што су трагање за несталом децом, идентификација осумњичених злочинаца и спречавање терористичких претњи.[58]

Marija Milojević, LL.M., Research Associate
Faculty of Law, University of Kragujevac

DIGITAL SERVICES AND CRIMINAL LAW

Summary

Processes such as globalization and digitalization are already greatly shaping the life of the entire world population and encroaching on all spheres of modern society. In this paper, the author analyzes the impact of the digital sector on the field of criminal law. The analysis was done in a comprehensive way, taking into account both procedural and substantive criminal law, but also the impact of digitalization on criminal law related areas such as criminalistics, enforcement of criminal sanctions, criminology, etc. It will be shown that the development and influence of digital services in the sphere of criminal law undoubtedly brings great benefits, which are reflected in the introduction and functioning of the e-justice system, new ways of gathering evidence, the use of IT systems in the procedure for the execution of criminal sanctions, and the use of artificial intelligence to improve the prediction of criminality. etc. On the other hand, the development of the information society brings with it great challenges in the form of the appearance of new criminal acts ("cyber crime" - computer criminal acts), new ways of committing existing criminal acts (e.g. child pornography), as well as challenges in terms of protection the right to privacy and personal data of an individual, in terms of reporting crimes... For the above reasons, constant education of all professionals - judges, prosecutors, police officers, criminalists as well as criminologists, penologists - is necessary in order for the

[58] Види: https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready -to-negotiate-first-ever-rules-for-safe-and-transparent-ai, приступљено:26.10.2023.

judicial system to successfully respond to the existing and future challenges of the digital environment.

Key words: *digital services, e-justice, digital evidence, artificial intelligence, cybercrime, criminal sanctions enforcement system, crime prediction.*

Литература

Blazek, R., *The new forms of digital criminality in Slovakia and fight against them*", Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022.

Brvnišťan, M., *Cybercrime and possibilities of prevention*, Proceedings of the scientific conference with international participation Current challenges of computer crime prevention held on 21 March 2018 at the Academy of Police Force in Bratislava, Bratislava: Academy of Police Force, 2018.

Бабић, М., *Међународно кривично право*, Бања Лука, 2011.

Вестби, Ц., *Међународни водич за борбу против компјутерског криминалитета*. Београд, 2004.

Димовски, Д., *Бенефити коришћења е-правосуђа у кривичним стварима*, LXII Саветовање Српског удружења за кривичноправну теорију и праксу, Златибор, 2023.

Дузлевски, И., *Значај дигитализације у кривичном праву*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022.

Дураковић, А., и др., *Употреба доказа прикупљених дроновима у криминалистичким истраживањима*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022.

Јовашевић, Д., *Појам и карактеристике рачунарских кривичних дела*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022.

Милојевић, М., *Пружање услуга Центра за социјални рад у кривичном поступку*, Зборник радова: Садашњост и будућност услужног права, Крагујевац, 2022.

Муњић, Ј., *Поједини аспекти имплементације савремених софтверских решења у правосудни систем и утицај дигитализације на правосуђе и адвокатуру*, Зборник радова: Правна регулатива услуга у националним законодавствима и праву Европске уније, Крагујевац, 2023.

Муртезић, А., *Дигитални докази: шта доноси други додатни протокол уз Будимпештанску конвенцију?*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022.

Радуловић, Д., *Кривично процесно право*, Подгорица, 2009.

Rigano, C., *Using artificial intelligence to address criminal justice needs* , National Institute of Justice Journal / Issue No. 280, January 2019, https://www.ojp.gov/pdffiles1/nij/252038.pdf, приступљено: 25.10.2023.

Самуилов, Ј., *Дигитализација правосуђа у Републици Србији, примена у пракси и изазови*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022.

Стевановић, А., *Улога вештачке интелигенције у контроли криминалитета*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022.

Стевановић, Ч., Ђурђић, В., *Кривично процесно право – општи део*, Ниш, 2006.

Тешовић, О., Миловановић, И., *Заштита сведока у кривичним поступцима и примена технологије*, Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022.

Тоскић Цветиновић, А., Тошић, М., *Примена вештачке интелигенције у правосуђу– перспективе и изазови* Зборник радова: Дигитализација у казненом праву и правосуђу, Београд, 2022.

Wall, S. D., *Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime*, The European Review of Organised Crime, No. 2/2015.

Правни извори

A digital future for Europe, https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe/, приступљено: 12.10.2023.

Artificial Intelligence Act, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html, приступљено: 12.10.2023.

Акциони план 2022-2025 „*Дигитализација за бољу правду*“, Европска комисија Савета Европе за ефикасност правосуђа, CEPEJ(2021)12Final, https://rm.coe.int/cepej-2021-12-en-cepej-action-plan-2022-2025-digitalisation-justice/1680a4cf2c, приступљено: 10. 10. 2023.

Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32022D2481, 12.10.2023.године;

Директива ЕУ 2018/1972 о Европском законику електронских комуникација, Сл. лист ЕУ, Л 321 од 17. 12. 2018.

E-nabling sustainable development: lessons from e-justice programming in Kyrgyzstan, International Development Law Organization, Rome, 2018.

Законик о кривичном поступку (Сл. гласник РС, бр. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021- одлука УС и 62/2021-одлука УС);

Интернет сајт Интерпола, https://www.interpol.int/News-and-Events/News/2010/INTERPOL-Global-Complex-in-Singapore-to-enhance-and-strengthen-policing-worldwide, приступљено:25.10.2023.

Комуникација комисије Европском парламенту, вијећу, Европском господарском и социјалном одбору и одбору регија COM/2020/580 final, Извештај о владавини права за 2020.годину, https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52020DC0580, приступљено: 10.10.2023.

Кривични Законик (Сл. гласник РС, бр. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94 /2016 и 35/2019).

Правилник о управи у јавним тужилаштвима (Сл. гласник РС, бр. 110/2009,87/2010,5/2012,54/2017,14/2018 и 57/2019).

Standard Operating Procedures for the collection, analysis and presentation od electronic evidence, Cybercrime Programme Office- Council of Europe, (https://www.coe.int/en/web/octopus/request-form, available upon request), 2019.

Стратегија развоја дигиталних вештина у Републици Србији за период од 2020.-2024.године, донета 2020. (Сл. гласник РС, бр. 21/2020 и 8/2023);
Стратегија развоја електронских комуникација у Републици Србији од 2010. до 2020. године, Сл. гласник РС, бр, 68/10,
Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020.године, Сл. гласник РС, бр. 53/17.
Стратегија развоја информационог друштва у Републици Србији до 2020. године, Сл. гласник РС, бр. 51/10.
Стратегија развоја правосуђа за период 2020–2025. године, (Сл. гласник РС, бр. 101 од 17. јула 2020, 18 од 11. фебруара 2022.),
Судски пословник (Сл. гласник РС, бр. 110/2009, 70/2011, 19/2012, 89/2013, 96/2015, 104/2015, 113/2015 - испр., 39/2016, 56/2016, 77/2016, 16/2018, 78/2018, 43/2019, 93/2019 и 18/2022).
Уредба ЕЗ бр. 861/2007 Европског парламента и Већа о увођењу европског поступка за спорове мале вредности од 11.07.2007.
Уредба ЕУ 2022/1925 о праведним тржиштима са могућношћу неограничене тржишне утакмице у дигиталном сектору и измени директива 2019/1937 и 2020/1828, Сл. лист ЕУ, Л 265 од 27. 10. 2022.
Handbook European law relating to access to justice, https://echr.coe.int/document/handbook_access_justice_eng.pdf, приступљено: 10.10.2023.
The Council of Europe, Electronic Evidence Guide, https://www.coe.int/en/web/octopus/request-form (available upon request), 2013.
CJEU, Joined cases, C-317/08, C-318/08, C-319/08 and C-320/08, Rosalba Alassini v. Telecom Italia SpA, Filomena Califano v. Wind SpA, Lucia Anna Giorgia Iacono v. Telecom Italia SpA and Multiservice Srl v. Telecom Italia SpA, 18 March 2010.
Council of Europe, Convention on Cybercrime (CETS No 185), Budapest, November 23, 2001. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documen-tId=0900001680081561, приступљено: 10.10.2023.
Cybercrime and Electronic Evidence, https://help.elearning.ext.coe.int/enrol/index.php?id=5526, приступљено: 23.10.2023.