INSTITUT ZA UPOREDNO PRAVO
INSTITUTE OF COMPARATIVE LAW
INSTITUT ZA KRIMINOLOŠKA I SOCIOLOŠKA ISTRAŽIVANJA
INSTITUTE OF CRIMINOLOGICAL AND SOCIOLOGICAL RESEARCH
PRAVOSUDNA AKDADEMIJA
JUDICIAL ACADEMY

VII MEĐUNARODNI NAUČNI SKUP
VII International Scientific Thematic Conference

DIGITALIZACIJA U KAZNENOM PRAVU I PRAVOSUĐU

Digitalization in Penal Law and Judiciary

Urednici/Editors:

Jelena Kostić
Marina Matić Bošković

Tematski zbornik radova međunarodnog značaja
Thematic Conference Proceedings of International Significance

BEOGRAD, novembar 2022.
BELGRADE, november 2022

INSTITUT ZA UPOREDNO PRAVO
INSTITUTE OF COMPARATIVE LAW
INSTITUT ZA KRIMINOLOŠKA I SOCIOLOŠKA ISTRAŽIVANJA
INSTITUTE OF CRIMINOLOGICAL AND SOCIOLOGICAL RESEARCH
PRAVOSUDNA AKDADEMIJA
JUDICIAL ACADEMY

VII MEĐUNARODNI NAUČNI SKUP
VII International Scientific Thematic Conference

DIGITALIZACIJA U KAZNENOM PRAVU I PRAVOSUĐU

Digitalization in Penal Law and Judiciary

Urednici/Editors:

Jelena Kostić
Marina Matić Bošković

Tematski zbornik radova međunarodnog značaja
Thematic Conference Proceedings of International Significance

BEOGRAD, novembar 2022.
BELGRADE, november 2022

VII MEĐUNARODNI NAUČNI SKUP
DIGITALIZACIJA U KAZNENOM PRAVU I PRAVOSUĐU

VII International Scientific Thematic Conference
Digitalization in Penal Law and Judiciary

Izdavač/Publisher:
Institut za uporedno pravo
(Institute of Comparative Law)
Institut za kriminološka i sociološka istraživanja
(Institute of Criminological and Sociological Research)

Za izdavača / For the Publisher:
Prof. dr Vladimir Čolović
Dr Ivana Stevanović

Recenzenti/Reviewers:
Prof. dr Ioana Vasiu (Romania)
Dr Jovan Ćirić (Serbia)
Prof. dr Dražen Cerović (Montenegro)

Radni jezici konferencije / Official Languages:
engleski i srpski / English and Serbian

Priprema za štampu / Prepress:
Branimir Trošić

Štampa / Printed by:
„Tri O d.o.o.", Aranđelovac

Tiraž/Copies:
200

ISBN 978-86-80186-92-4 (IUP)

ISBN 978-86-80756-52-3 (IKSI)

DOI: https://doi.org/10.56461/ZR_22.DUKPP

Zbornik je nastao kao rezultat naučnoistraživačkog rada Instituta za uporedno pravo koji finansira Ministarstvo prosvete, nauke i tehnološkog razvoja RS prema Ugovoru o realizaciji i finansiranju naučnoistraživačkog rada NIO u 2022. godini (evidencioni broj 451-03-68/2022-14/200049).

This Collection of Papers was created as a result of the scientific research work of the Institute of Comparative Law, funded by the Ministry of Education, Science and Technological Development of the Republic of Serbia under the Contract on the Realization and Financing of Scientific Research work of SRO in 2022 (record number 451-03-68/2022-14/200049).

Sadržaj / Table of Contents

PREDGOVOR

Poslednjih decenija digitalizacija je sve prisutnija u svim društvenim sferama kao proces koji vodi unapređenju efikasnosti, standardizacije usluga i povećanja pristupa, pa nije zaobišla ni oblast pravosuđa. Digitalizacija pravosuđa obuhvata sve oblike digitalnih tehnologija, od složenih sistema upravljanja predmetima do inovativnih aplikacija i upotrebe elektronske komunikacije. Inicijative za digitalizaciju uključuju redefinisanje poslovnih procesa, automatizaciju, prikupljanje podataka, integraciju sistema, online rešavanje sporova, elektronsko podnošenje pismena, sudski proces na daljinu, kao i tehnologije koje se koriste za digitalizaciju, skladištenje i omogućavanje pristupa pravnim dokumentima i dokazima. Pored navedenog, aplikacije i alati za komunikaciju i neposrednu razmenu podataka sa korisnicima predstavljaju takođe deo procesa digitalizacije pravosuđa. Pandemija uslovljena virusom COVID-19 pokazala je ranjivost institucija koje se oslanjaju na analogne operacije, predmete u štampanom obliku i neposredan kontakt. Pravosudni sistemi širom sveta, posebno su osetili ove izazove tokom pandemije. Međutim, prilikom sprovođenja digitalizacije pravosuđa često se fokus usmerava na nove tehnologije i procese, umesto na cilj digitalizacije a to je uticaj na pristup pravdi, jednakost i zaštitu ljudskih prava.

U kaznenom pravu, digitalizacija je posebno uticala na proces prikupljanja dokaza i njihovog izvođenja. Danas se veliki broj krivičnih dela vrši korišćenjem digitalnih tehnologija. To nisu samo dela protiv bezbednosti računarskih podataka, već i krivična dela koja spadaju u finansijski kriminalitet. Prikupljanje digitalnih dokaza predstavlja poseban izazov zbog lakoće i brzine kojom mogu biti uklonjeni ili premešteni, kao i prekogranične saradnje koja je neophodna ukoliko su podaci pohranjeni kod pružalaca usluga čije se sedište nalazi u drugoj državi. Radi njihovog dokazivanja neophodno je da pripadnici organa unutrašnjih poslova, javni tužioci i sudije poseduju adekvatan nivo znanja kako bi blagovremeno prikupili dokaze od značaja za sprovođenje krivičnog postupka.

Zanimljiva je činjenica da se u svetu danas koriste sudije roboti i algoritmi za izricanje sudskih presuda. Između ostalog digitalizacija je prisutna i tokom izvršenja sankcija. Međutim, to istovremeno aktuelizuje brojna pitanja koja se pre

svega tiču zaštite ljudskih prava, a posebno prava na pravično suđenje i zaštitu procesnih prava osumnjičenih i okrivljenih.

Na brojna pitanja koja se mogu javiti u vezi sa primenom digitalizacije u kaznenom pravu i pravosuđu nastojali smo da damo odgovore na VII Međunarodnoj naučnoj konferenciji u organizaciji Instituta za uporedno pravo, Instituta za kriminološka i sociološka istraživanja i Pravosudne akademije iz Beograda. Ovogodišnja konferencija okupila je veliki broj naučnika i praktičara iz Portugala, Brazila, Savezne Republike Nemačke, Austrije, Hrvatske, Slovačke Republike, Češke Republike, Grčke, Rumunije, Bosne i Hercegovine i Republike Srbije. Oni su u svojim radovima pokušali da daju odgovore na pitanja koja su aktuelizovana procesom digitalizacije pravosuđa. Poseban značaj ovoj konferenciji daje njen međunarodni karakter. Na osnovnu razmene iskustava u procesu digitalizacije različitih zemalja, moguće je potražiti odogovore za rešavanje nedoumica koje postoje u praksi.

Beograd, 5. decembar 2022.

Dr Jelena Kostić
Dr Marina Matić Bošković

PREFACE

Over the recent decades, digitalization has been increasingly present in all social spheres as a process that leads to the improvement of efficiency, standardization of services and increased access and it has not circumvented the field of justice. Digitalization of justice includes all forms of digital technologies, from complex case management systems to innovative applications and the use of electronic communication. Digitalization initiatives include redesign of business process, automation, data collection, system integration, online dispute resolution, electronic filing, remote litigation, and technologies used to digitize, store, and provide access to legal documents and evidence. In addition to the above, applications and tools for communication and direct exchange of data with users are also part of the process of digitalization of the judiciary. The COVID-19 pandemic has shown the vulnerability of institutions that rely on analogue operations, paper base work, and in person contacts. Judicial systems around the world have particularly felt these challenges during the pandemic. However, when implementing the digitalization of justice, the focus is often directed to new technologies and processes, instead of the goal of digitalization, which is the impact on access to justice, equality and protection of human rights.

In criminal law, the digitalization of society has particularly affected the process of gathering evidence and its presentation. Today, many crimes are committed using digital technologies. These are not only crimes against the security of computer data, but also crimes that fall under financial crimes. The collection of digital evidence is a particular challenge due to the ease and speed with which it can be destroyed or moved, as well as the cross-border cooperation that is necessary if the data is stored with service providers whose headquarters are in another country. To prove them, it is necessary that members of investigative bodies, specifically police, public prosecutors, but also judges possess an adequate level of knowledge to timely collect evidence of importance for the implementation of criminal proceedings.

It is an interesting fact that robot judges and algorithms are used in the world today to adopt court verdicts. Among other things, digitalization is also

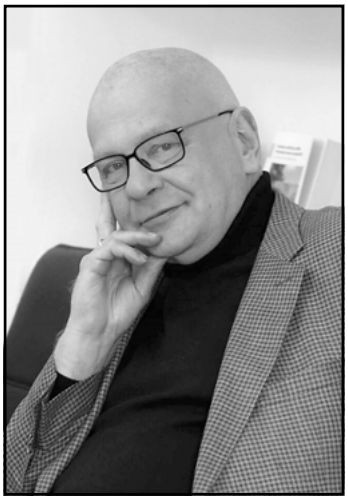
present during the execution of sanctions. However, at the same time, it actualizes numerous issues that primarily concern the protection of human rights, especially the right to a fair trial and the protection of the procedural rights of suspects and accused.

We tried to provide answers to numerous questions that may arise in connection with the application of digitalization in criminal law and justice at the VII International Scientific Conference organized by the Institute for Comparative Law, the Institute for Criminological and Sociological Research and the Judicial Academy from Belgrade. This year's conference brought together many members of academia and practitioners from Portugal, Brazil, the Federal Republic of Germany, Austria, Croatia, the Slovak Republic, the Czech Republic, Greece, Romania, Bosnia and Herzegovina and the Republic of Serbia. In the articles, authors tried to provide answers to the questions that were raised by the process of digitalization of the judiciary. The special importance of this conference is given by its international character. Based on the exchange of experiences in the digitalization process of different countries, it is possible to find answers to solve the doubts that exist in practice.

Belgrade, December 5th, 2022

Jelena Kostić, PhD
Marina Matić Bošković, PhD

In memoriam: dr Jovan Ćirić (1960-2022)



Pred sam izlazak ovog zbornika, sve nas je zatekla vest o smrti našeg dragog dr Jovana Ćirića – Ćire. Naš dragi prijatelj i kolega uveličao je svojim prisustvom našu međunarodnu konferenciju, a čiji je rezultat ovaj zbornik naučnih radova. Zahvaljujući njemu u septembru 2016. godine, u Vršcu je održana prva naučna konferencija u organizaciji Instituta za uporedno pravo i Instituta za kriminološka i sociološka istraživanja u saradnji sa Pravosudnom akademijom. Tada je počela višegodišnja uspešna saradnja navedenih institucija u organizaciji tematskih naučnih konferencija. Ovogodišnja međunarodna naučna konferencija "Digitalizacija u kaznenom pravu i pravosuđu" je nastavak te saradnje. Dr Jovan Ćirić je kako kao autor, tako i kao recenzent dao značajan doprinos kvalitetu zbornika radova predstavljenih na naučnim konferencijama Instituta za uporedno pravo i Instituta za kriminološka i sociološka istraživanja, a u saradnji sa Pravosudnom akademijom.

Ćirin odlazak predstavlja odlazak jednog vrsnog pravnika i još bolje osobe. Ono što ga čini velikim jeste činjenica da je nazavisno od funkcije i pozicije, ostao pre svega čovek – uvek tu za prijatelje, uvek tu da podrži mlade ljude bez rezerve i uvek iskren. Takvih ljudi danas nema mnogo, a od ponedeljka 12.12.2022. godine taj broj je još manji.

Ćiro, neka ti je večna slava i hvala ti na svemu.

Right before the release of this collection of papers, we were all caught by the news of the death of our dear Dr Jovan Ćirić – Ćira. Our friend and colleague attended international conference, the result of which is this Collection of scientific papers. Thanks to him, in September 2016, the first scientific conference was held in Vršac organized by the Institute of Comparative Law and the Institute of Criminological and Sociological Research in cooperation with the Judicial Academy. Then the multi-year successful cooperation of the mentioned institutions in the organization of thematic scientific conferences began. This year's international scientific conference "Digitalization in criminal law and justice" is a continuation of that cooperation. Dr Jovan Ćirić, both as an author and as a reviewer, made a significant contribution to the quality of the Collections of papers presented at the scientific conferences of the Institute for Comparative Law and the Institute of Criminological and Sociological Research, and in cooperation with the Judicial Academy.

What makes him a great man is the fact that regardless of his function and position, he remained above all a man - always there for friends, always there to support young people without reservation and always honest. There are not many such people today, and from Monday 12.12.2022. that number is even smaller.

Dear Ćiro, you will be greatly missed and thank you for everything.

DOI: https://doi.org/10.56461/ZR_22.DUKPP.01

POJAM I KARAKTERISTIKE RAČUNARSKIH KRIVIČNIH DELA*

Dragan Jovašević**

Poslednjih decenija se u sistemu postojećih, opštih, klasičnih krivičnih dela javljaju novi oblici ili vidovi ispoljavanja, ako se njihova radnja izvršenja preduzima uz pomoć, posredstvom, korišćenjem ili upotrebom računara, računarskih sistema, odnosno računarske mreže. Istovremeno se javljaju nova, do sada nepoznata, krivična dela koja se vrše na ovaj način. Svi ovi oblici protivpravnih delatnosti uz pomoć računara, kojima se povređuju ili ugrožavaju prava, interesi ili dobra drugih fizičkih ili pravnih lica, čine sistem računarskih krivičnih dela. U pozitivnom zakonodavstvu, koje se zasniva na bazi međunarodnih standarda, propisana su brojna računarska krivična dela o čijoj sadržini, karakteristikama i elementima u pravnoj teoriji još uvek ne postoji jedinstveno shvatanje. Upravo se u radu izlažu osnovne karakteristike računarskih krivičnih dela u pravnoj teoriji, međunarodnim dokumentima i domaćem krivičnom zakonodavstvu.

KLJUČNE REČI: *računari, krivično delo, protivpravnost, međunarodni dokumenti, zakon.*

* Ovaj rad je rezultat istraživanja na projektu koji finansira Pravni fakultet Univerziteta u Nišu: "Odgovornost u pravnom i društvenom kontekstu" u periodu 2021-2025.godine.

** Doktor pravnih nauka, redovni profesor Pravnog fakulteta Univerziteta u Nišu.
E-mail: *jovas@prafak.ni.ac.rs*

UVOD

Digitalizacija danas predstavlja neumitni pratilac ljudskog života, ali i života celog društva-države. Stoga je logično da je upotreba digitalnih sredstava, opreme ili mreža svakodnevno prisutna u svim oblastima prava i pravosuđa, a posebno u oblasti kaznenog prava. Velike su digitalne mogućnosti u svakodnevnom životu na svim nivoima, ali se time povećava i opasnost od zloupotrebe gotovo svih vrsta digitalnih tehnologija. U takvim slučajevima se javljaju tzv. računarska krivična dela (kako ih zakon naziva), iako se u teoriji, praksi i uporednom zakonodavstvu javljaju i drugi nazivi: kompjuterska, informaciona, elektronska, sajber, visokotehnološka ili informatička krivična dela.

Na bazi relevantnih međunarodnih standarda univerzalnog (OUN) i regionalnog karaktera (Savet Evrope) u nizu država, pa tako i u Srbiji, je poslednjih decenija izričito propisana krivična odgovornost fizičkih i pravnih lica za različita nedozvoljena, protivpravna ponašanja (činjenja ili nečinjenja) koja su preduzeta (zlo)upotrebom računarskih (kompjuterskih, informatičkih, informacionih, sajber) podataka, sistema, mreža ili uređaja. Na taj način neka već postojeća, klasična, opšta, konvencionalna krivična dela dobijaju nove oblike ili vidove ispoljavanja, ali se javljaju i nove inkriminacije kojima se povređuju ili ugrožavaju zaštićena dobra, vrednosti i interesi drugih fizičkih ili pravnih lica, pa i čitavih država, odnosno međunarodne zajednice u celini.

Usvajanjem Zakona o izmenama i dopunama Krivičnog zakona Srbije[1] aprila 2003. godine na bazi međunarodnih standarda, donetih u okviru Saveta Evrope, u sistem domaćeg krivičnog prava je po prvi put uvedeno više računarskih krivičnih dela, te su određena pravila o krivičnoj odgovornosti i kažnjavanju njihovih učinilaca u novouvedenoj glavi 16A. Krivičnog zakona pod nazivom: „Krivična dela protiv bezbednosti računarskih podataka". Na taj način se i naša država priključila nizu savremenih država koje se na različite načine (u prvom redu sistemom krivičnih sankcija) pokušavaju efikasno, zakonito i kvalitetno suprotstaviti različitim oblicima i vidovima zloupotrebe računara na štetu prava ili interesa drugih fizičkih ili pravnih lica, pa i opštih, javnih, društvenih dobara. Posle zakonodavne reforme 2005.godine donet je Krivični zakonik Srbije[2] koji u glavi dvadeset sedmoj pod nazivom: ''Krivična dela protiv bezbednosti računarskih podataka'' propisuje brojna računarska krivična dela.

U osnovi ovih zakonskih rešenja se nalazi Konvencija o viokotehnološkom (kibernetičkom, računarskom, informatičkom, sajber kriminalu) - *Convention on Cybercrime*, ETS 185 iz novembra 2001.godine (Budimpešta). Tu su postavljene osnove jedinstvenog evropskog sistema materijalnog (čl.2-23.) i procesnog krivičnog prava u oblasti saradnje država članica u suzbijanju različitih oblika i vidova računarskog kriminaliteta (Pavišić, 2006:261-265). Uz ovu Konvenciju je usvojen i Dopunski protokol o kriminalizovanju akata rasističke i ksenofobične prirode koja su učinjena posredstvom računarskih sistema 2005.godine (Strazbur) koji u čl. 3-7. propisuje takođe krivičnu odgovornost i kažnjivost

[1] *Službeni glasnik Republike Srbije,* br. 39/2003.

[2] *Službeni glasnik Republike Srbije,* br. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94 /2016 i 35/2019.

za zloupotrebu računara u vršenju specifičnih krivičnih dela iz rasističkih i ksenofobičnih pobuda (motiva).

Nešto ranije, krajem 80-tih godina komitet eksperata za računarski (kompjuterski) kriminalitet Saveta Evrope razmatrao je, pod pritiskom brojnih i sve češćih, ali i raznovrsnijih oblika ispoljavanja zloupotrebe računara u sudskoj praksi, brojne probleme koji su vezani za računarski kriminalitet, odnosno njegovo suzbijanje i efikasno otkrivanje i kažnjavanje (Clough, 2010: 151-163). To je rezultiralo donošenjem Preporuke o kriminalitetu vezanom za računare R(89) 9 koju je Savet Evrope usvojio septembra 1989.godine. Ova preporuka je obavezala države članice da u svom nacionalnom zakonodavstvu uspostave sistem odgovornosti (krivična, prekršajna, upravna, građanska) za različite oblike, odnosno vidove ispoljavanja računarskog kriminaliteta (Petrović, Jovašević, 2010: 91-93).

U međunarodnom krivičnom pravu od posebnog značaja, za sprečavanje, odnosno suzbijanje računarskog kriminaliteta su takođe i zaključci Desetog kongresa OUN koji razlikuju dve vrste ovog kriminaliteta (Vestbi, 2004: 214-223): a) računarski kriminalitet u užem smislu - svako nezakonito (protivpravno) ponašanje koje je usmereno na elektronske operacije protiv sigurnosti računarskih sistema i računarskih podataka koji se u njima obrađuju (pravljenje i ubacivanje računarskih virusa, haking, piratstvo, računarska sabotaža, računarska špijunaža, računarske prevare i krađa računarskih usluga i b) računarski kriminalitet u širem smislu - svako nezakonito (protivpravno) ponašanje koje je vezano za ili u odnosu na računarski sistem i računarsku mrežu, uključujući i takav kriminalitet kakvo je nezakonito posedovanje, nuđenje i distribuiranje informacija preko računarskih sistema i računarskih mreža (Babić, 2011:89-94).

U osnovi najznačajnijeg međunarodnog akta regionalnog karaktera koji uređuje oblast sprečavanja, odnosno suzbijanja računarskih krivičnih dela - Konvencije o visokotehnološkom kriminalu, nalaze se prethodno donete preporuke kao što su (Jovašević, Ikanović, 2015: 116-118): 1) Preporuka broj R (85) 10 o praktičnoj primeni Evropske konvencije o uzajamnoj pomoći u krivičnim predmetima u pogledu pružanja međunarodne krivičnopravne pomoći pri presretanju komunikacija, 2) Preporuka broj R (88) 2 o piratstvu na polju autorskih i srodnih prava, 3) Preproruka broj R (87) 15 koja propisuje upotrebu ličnih podataka u oblasti delatnosti policije, 4) Preporuka broj R (95) 4 o zaštiti ličnih podataka na području telekomunikacionih usluga sa posebnim osvrtom na ulogu telefonije, 5) Preporuka broj R (89) 9 o računarskom kriminalu koja daje smernice nacionalnim organima u pogledu definisanja pojedinih računarskih krivičnih dela i 6) Preporuka broj R (95) 13 o problemima krivičnog procesnog prava koji su vezani za informatičku tehnologiju (Koševaliska, Maksimova, 2020: 121-125).

1. EVROPSKI STANDARDI I RAČUNARSKA KRIVIČNA DELA

Konvencija o visokotehnološkom kriminalu polazi od činjenice da je cilj Saveta Evrope da postigne što veće jedinstvo među svojim članicama, priznajući vrednost unapređenja saradnje sa drugim državama, uverene u potrebu da se, kao prioritetna, sprovodi

zajednička politika u borbi za zaštitu društva od visokotehnološkog kriminaliteta, pa čak, između ostalog, usvajanjem odgovarajućeg zakonodavstva, kao i unapređivanjem međunarodne saradnje (Pavlović, Vučić, 2017:98-104). Pri tome je Savet Evrope kao regionalna politička i bezbednosna organizacija svestan dubokih promena koje je donela digitalizacija, konvergencija i stalna globalizacija računarskih mreža (Kouch, 2016: 161-175).

Upravo zato su države zabrinute zbog visoko ispoljenog rizika da se računarske mreže i elektronske informacije mogu koristiti i za izvršenje brojnih, kako već postojećih "arhaičnih" krivičnih dela, kako dela iz oblasti opšteg, klasičnog, konvencionalnog kriminaliteta, tako i brojnih novih, do sada nepoznatih, krivičnih dela (Cullen, 1997: 211-215). S druge strane, dokazi koji se odnose na takva krivična dela, a koji se upotrebljavaju u odgovarajućim krivičnim postupcima od strane za to nadležnih državnih organa mogu biti sačuvani i preneseni, odnosno vidljivi upravo preko takvih računarskih mreža ili sistema elektronske obrade podataka (Čejović, Vučković, Vučković, 2001: 118-121).

Konvencija o visokotehnološkom kriminalu predstavlja osnovni izvor evropskog krivičnog prava ili sistema međunarodnih standarda za sprečavanje i suzbijanje računarskog kriminaliteta u državama na evropskom kontinentu. Ona u prvom poglavlju (član 1.) pod nazivom: "Upotreba termina" određuje osnovne pojmove vezane za računarski kriminalitet. Prema ovim rešenjima, računarski sistem označava svaki uređaj ili grupu međusobno povezanih ili zavisnih uređaja, od kojih jedan ili više njih, na osnovu programa, vrši automatsku obradu podataka. Računarski podatak je, s druge strane, svako predstavljanje činjenica, informacija ili koncepata u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju. Konačno, podatak o saobraćaju označava svaki računarski podatak koji se odnosi na komunikaciju preko računarskog sistema, proizvedenu od računarskog sistema koji je deo lanca komunikacije, a u kojoj su sadržani podaci o poreklu, odredištu, putanji, vremenu, datumu, veličini, trajanju ili vrsti predmetne usluge.

Poglavlje drugo Konvencije o visokotehnološkom kriminalu: "Mere koje treba da se preduzmu na nacionalnom nivou", u prvom delu pod nazivom: "Materijalno krivično pravo" propisuje pojedina računarska krivična dela, koja treba da propišu pojedina nacionalna krivična zakonodavstva uz obezbeđenje vrste i mere kazni (Moore, 2005: 114-127). Na ovom mestu su postavljene solidne pravne osnove za inkriminaciju pojedinih ponašanja u vezi ili povodom zloupotrebe računara, računarskih podataka ili računarskih sistema u krivičnom zakonodavstvu država članica Saveta Evrope. Stoga su brojna rešenja prisutna u uporednom krivičnom zakonodavstvu, koja su zasnovana na ovim standardima, u većoj ili manjoj meri unificirana, odnosno standardizovana (Stojanović, Delić, 2013: 252).

Konvencija razlikuje sledeće grupe računarskih krivičnih dela. To su: a) krivična dela protiv poverljivosti, celovitosti i dostupnosti računarskih podataka i sistema, b) krivična dela u vezi sa računarima, c) krivična dela u vezi sa sadržajem i d) krivična dela u vezi sa kršenjem autorskih i srodnih prava. U sistem krivičnih dela protiv poverljivosti, celovitosti i dostupnosti računarskih podataka i sistema spadaju sledeća krivična dela: a)

nezakonit pristup (član 2.), b) nezakonito presretanje (član 3.), c) ometanje podataka (član 4.), d) ometanje sistema (član 5.) i e) zloupotreba uređaja (član 6.). Drugu grupu međunarodnih računarskih krivičnih dela predstavljaju: "Krivična dela u vezi sa računarima". To su: a) falsifikovanje u vezi sa računarima (član 7.) i b) prevara u vezi sa računarima (član 8.) (Čejović, 2006: 211-214). U trećoj grupi međunarodnih računarskih krivičnih dela pod nazivom: "Krivična dela u vezi sa sadržajem" se nalaze krivična dela u vezi sa dečijom pornografijom (član 9.). Konačno, u odredbi člana 10. opisana su: "Krivična dela u vezi sa kršenjem autorskih i srodnih prava". Za računarska krivična dela, pojedina nacionalna krivična zakonodavstva u smislu člana 13. Konvencije propisuju različite vrste kazni kao "delotvorne, proporcionalne i odvraćajuće sankcije", koje uključuju lišavanje slobode za fizička lica, odnosno novčanu kaznu za pravna lica (Ambos, 2018: 171-184).

Pored neposredne radnje izvršenja, kojom su ostvarena obeležja bića konkretnog računarskog krivičnog dela, odeljak peti Konvencije: "Drugi oblici odgovornosti i sankcije" propisuje u članu 11. odgovornost za posebne, specifične oblike ispoljavanja navedenih krivičnih dela. To su (Petrović, Jovašević, Ferhatović, 2016: 189-194): a) pokušaj krivičnog dela – umišljajno (sa namerom) započinjanje izvršenja nekog od računarskih krivičnih dela, bez prouzrokovanja krivičnopravno relevantne posledice i b) saučesništvo u obliku: 1) pomaganja – kao namerno, umišljajno doprinošenje, omogućavanje, olakšavanje, stvaranje uslova ili pretpostavki drugom licu da izvrši neko od navedenih računarskih krivičnih dela i 2) podstrekavanje – kao namerno, umišljajno psihološko uticanje na volju drugog lica u smislu da donese novu ili učvrsti postojeću, nedovoljno čvrstu, kolebljivu odluku za izvršenje nekog od računarskih krivičnih dela (Kareklas, 2009: 94-97).

Pored fizičkih lica, za računarska krivična dela, shodno međunarodnim standardima, treba da odgovaraju i pravna lica (član 12. Konvencije). Za odgovornost pravnih lica je neophodno ispunjenje sledećih uslova (Satzger, 2018: 189-201): a) ako je krivično delo izvršeno u njihovu korist, b) ako je krivično delo izvršilo bilo koje fizičko lice, delujući kao pojedinac ili kao član organa pravnog lica i c) ako fizičko lice ima rukovodeću ulogu u pravnom licu na osnovu: 1) ovlašćenja da zastupa pravno lice, 2) ovlašćenja da donosi odluke u ime pravnog lica i 3) ovlašćenja da vrši kontrolu unutar pravnog lica. Pored toga, odgovornost pravnih lica za učinjeno krivično delo se može uspostaviti u još jednom slučaju - kada je nepostojanje nadzora ili kontrole od strane rukovodećeg fizičkog lica omogućilo (olakšavalo, doprinelo) izvršenje nekog od Konvencijom nabrojanih računarskih krivičnih dela, pod uslovom da je konkretno delo izvršilo fizičko lice u korist upravo tog pravnog lica, na osnovu ovlašćenja pravnog lica (Novoselec, 2009: 56-62). U vezi odgovornosti pravnih lica za računarska krivična dela Konvencija predviđa dva načela. To su: a) odgovornost pravnog lica može biti različito određena kao: krivična, prekršajna, građanska ili administrativna (upravna) i b) odgovornost pravnog lica ne isključuje istovremenu i paralelnu krivičnu odgovornost fizičkih lica koja su neposredno izvršila delo - odgovorno lice (Selinšek, 2006: 145-169).

2. POJAM I ELEMENTI RAČUNARSKIH KRIVIČNIH DELA

Iako domaći pravni sistem Srbije poznaje više računarskih krivičnih dela, sa specifičnim objektom radnje, oblicima ispoljavanja radnje izvršenja, načinom ili sredstvom njihovog izvršenja, te subjektivnim elementima na strani učinioca, ipak se može konstatovati da ova dela imaju i niz zajedničkih, opštih karakteristika. Računar, elektronski prenos ili obrada računarskih podataka, računarski program, računarska mreža i sl.predstavljaju jednu od najznačajnijih tekovina razvoja tehničko-tehnološke civilizacije sveta na početku trećeg milenijuma. No, pored brojnih prednosti koje sobom nosi i ogromne koristi za pojedince, grupe, privredne subjekte, državne organe, pa čak i celokupno čovečanstvo, računar je brzo postao, pa čak i napredovao kao često korišćeno sredstvo za ispoljavanje raznih zloupotreba od strane nesavesnih pojedinaca, grupa, pa i čitavih organizacija. Tako nastaje računarski kriminalitet kao poseban, dinamičan, specifičan, brzo narastajući i gotovo sveprisutan oblik savremenog kriminaliteta po obimu, dinamici, strukturi i osobenostima, te pojavnim oblicima ispoljavanja, kao i karakteristikama ličnosti njihovih učinilaca (izvršilaca ili saučesnika), načinima i sredstvima njihovog izvršenja, prouzrokovanim posledicama, svojstvima oštećenih lica (žrtava) itd. (Dragičević, 1999: 119-124).

U pravnoj teoriji je gotovo opšte prihvaćeno da ovaj vid savremenog kriminaliteta, za razliku od drugih, još uvek ne predstavlja zaokruženu, jedinstvenu i sistematizovanu fenomenološku kategoriju (Završnik, 2015: 95-115). Zato se neretko ističe da je računarski kriminalitet gotovo nemoguće pojmovno odrediti i definisati na jedinstveni, opšte prihvaćeni, ali i sveobuhvatni način. Računarski kriminalitet se javlja samo kao opšta forma (oblik) kroz koju se ispoljavaju različiti oblici već postojeće kriminalne delatnosti pojedinaca, grupa, ali i pravnih lica, upotrebom, uz pomoć, preko ili posredstvom računara (Milosavljević, Grubor, 2009: 167-181). Ovde se radi o starim, arhaičnim krivičnim delima, koja se svrstavaju u opšti, klasičan, konvencionalni kriminalitet (krađa, prevara, utaja, uništenje ili oštećenje tuđe stvari, falsifikovanje - krivotvorenje, sabotaža i sl.). Računar, kompjuter se ovde javlja samo kao novo, specifično, osobeno sredstvo (način) za izvršenje klasičnih, opštepoznatih krivičnih dela.

S druge strane, javljaju se nova računarska krivična dela koja se jedino, isključivo ili pretežno vrše uz pomoć, preko, upotrebom ili posredstvom računara. Ova se dela bez računara uopšte ne mogu izvršiti, što znači da njihovo postojanje i pravna egzistencija bez računara nije moguća. To je kriminalitet koji je primarno upravljen protiv bezbednosti računarskih (informatičkih, informacionih, kompjuterskih) sistema ili tehnologija, odnosno elektronskih sistema za obradu ili prenos računarskih podataka ili programa, bilo u celini, bilo njihovih pojedinih segmenata, delova ili oblasti. Ova se krivična dela vrše na različite načine i različitim sredstvima, najčešće sa različitim namerama ili ciljevima kao subjektivnim elementima ličnosti (što uključuje posebna, specijalna znanja ili veštine iz oblasti računarske, informacione tehnologije) njihovih učinilaca (Zvrlevski, Andononova, Miloševski, 2014: 121-132).

Brojni i različiti načini gotovo svakodnevne upotrebe računara u svim oblastima života, privrede i drugih društvenih delatnosti, kako u pojedinim državama, tako i u

međunarodnoj zajednici su odavno uočene, ali i iskorišćene od strane nesavesnih i zlonamernih pojedinaca ili grupa, kao i pravnih lica. Naime, oni ne biraju situacije, sredstva i načine u pokušaju da pribave, ostvare za sebe ili drugo (fizičko ili pravno) lice protivpravnu imovinsku, materijalnu (ili drugu neimovinsku) korist ili pak da na taj način drugome nanesu bilo kakvu, ali i najčešće, imovinsku štetu (Atanasov, 2021: 181-196). Tako je računar postao često korišćeno sredstvo, oruđe za izvršenje različitih krivičnih dela, uglavnom iz sfere opšteg (uglavnom imovinskog) kriminaliteta. Za različite oblike i vidove zloupotrebe računara u pravnoj teoriji se koriste različiti nazivi kao što su: zloupotreba računara (*computer abuse*), delikti uz pomoć računara (*crime by computer*), kompjuterska prevara (*computer fraud*), informatički kriminalitet, računarski kriminalitet, sajber kriminalitet, tehno kriminalitet itd. (Jovašević, 2011: 639).

Paralelno sa ubrzanom digitalizacijom svih pora društva i ulaskom prvo računara, a potom i interneta u sve oblasti društvenog i privatnog života ljudi, računarski kriminalitet postaje sve više dominantan oblik zloupotreba, kršenja zakona i drugih propisa. Novi, visoko sofisticirani oblici napada, povrede ili ugrožavanja računara, računarskih mreža ili računarskih sistema javljaju se velikom brzinom, te se brzo šire na brojne i različite vidove ljudskog, društvenog, ali i privrednog života. Zapravo, može se reći da su novi oblici, vidovi ispoljavanja ili tipovi računarskog kriminaliteta praktično nepresušni, te da oni prvenstveno zavise samo od mašte malicioznih učinilaca ovih krivičnih dela (Babić, 2009: 187-195).

Računarskim krivičnim delima su propisane različite radnje izvršenja kojima se kažnjava neovlašćeni pristup tuđem računaru (sa ili bez izmene ili prerade računarskih podataka), onesposobljavanje tuđeg računara za rad (fizičko, ako je u vlasništvu pravnog lica, naročito države ili softversko – pravljenjem ili unošenjem računarskih virusa), prevare uz manipulacije računarskim podacima, ometanje elektronske obrade ili prenosa podataka ili računarske mreže (Babić, Marković, 2007: 206). Često se u pravnoj teoriji, pojam računarski kriminalitet zamenjuje pojmom sajber kriminalitet (*Cyber crime*). Ovaj naziv ukazuje na oblik ispoljavanja kriminalnog ponašanja fizičkih ili pravnih lica, kod koga se korišćenje računarske tehnologije i informacionih sistema ispoljava kao način (*modus operandi*) izvršenja krivičnih dela, gde se računar ili računarska mreža upotrebljavaju kao sredstvo ili cilj njihovog izvršenja.

U pravnoj teoriji se mogu uočiti brojna različita pojmovna određenja računarskog kriminaliteta. Prema jednom shvatanju, računarski kriminalitet obuhvata različite delatnosti kojima se narušava bezbednost računarskih podataka, pri čemu se krivična dela u njegovom sastavu vrše pomoću računara, tako da se računar koristi kao sredstvo za njihovo izvršenje. No, ovaj pojam obuhvata i krivična dela koja se sastoje u onespobljavanju računara ili računarskih mreža kod kojih se računar javlja kao objekat napada (Mrvić Petrović, 2005: 322). S druge strane, u okviru računarskog kriminaliteta razlikuje se dve vrste krivičnih dela. To su: a) dela kojima se povređuje sam sistem računarske tehnologije oštećivanjem ili uništenjem računarskih podataka ili programa ili ometa njihovo korišćenje ili se vrši neovlašćeni pristup računarskoj mreži ili samoj elektronskoj obradi podataka i b) dela kod kojih se koristi računarska tehnologija da bi se pomoću nje

vršila druga krivična dela (Đorđević, 2011: 177). Takođe se kao računarski kriminalitet u najširem smislu reči ili kriminalitet vezan za računare (*computer related crime*) smatra vršenje krivičnih dela zloupotrebom računara, odnosno računarskih sistema. To zači da samo vršenje krivičnih dela podrazumeva upotrebu računara ili računarskih sistema kao sredstva ili cilja izvršenja krivčnog dela (Stojanović, Delić, 2013: 251).

Smatramo da se računarski kriminalitet može odrediti kao kriminalitet koji je primarno usmeren protiv bezbednosti digitalnih, informacionih, računarskih sistema, mreža ili podataka, u nameri da se sebi ili drugom pribavi određena korist ili da se drugome nanese kakva šteta. Ovako posmatrano, za računarski kriminalitet se može reći da on predstavlja zbirni naziv za kriminalitet koji se javlja u više različitih oblika i vidova ispoljavanja. Pod ovim se pojmom podrazumeva sveukupnost različitih oblika, vidova i formi ispoljavanja protivpravnih ponašanja fizičkih ili pravnih lica upravljenih protiv bezbednosti računarskih, informacionih i digitalnih sistema u celini ili njihovih pojedinih delova na različite načine i različitim sredstvima u nameri da se sebi ili drugom (fizičkom ili pravnom) licu pribavi kakva korist (imovinske ili neimovinske prirode) ili da se drugome nanese kakva šteta (Jovašević, 2017: 189-192).

3. KARAKTERISTIKE RAČUNARSKIH KRIVIČNIH DELA

Ovako određeni pojam računarskog kriminaliteta ukazuje na njegove osnovne karakteristike (Petrović, Jovašević, Ferhatović, 2016: 211-214). To su, na prvom mestu: a) objekt zaštite - bezbednost računarskih podataka, računarskih mreža ili informacionog sistema u celini ili njegovog pojedinog dela (segmenta) i b) objekt napada – koji je višestruko određen kao: računar, računarski podatak ili računarski virus.

Objekt zaštite (u smislu dobra, vrednosti ili interesa koji se štite krivičnim zakonodavstvom uopšte) kod računarskih krivičnih dela jeste bezbednost računarskih podataka i sistema, odnosno računarske mreže, odnosno efikasno, uredno, kvalitetno, zakonito i blagovremeno funkcionisanje (odvijanje, rad, delovanje) sistema ili mreže automatske obrade podataka. U pravnoj teoriji, ali i u pozitivnom krivičnom zakonodavstvu pojedinih država, danas je uobičajeno da se ova krivična dela obuhvataju pojmom ''računarski ili kompjuterski'' kriminalitet[3]. Zaštitni objekat ovih krivičnih dela je određen kao bezbednost računarskih podataka. Pri tome se kao računarski podaci smatraju podaci koji se unose ili koriste radi nesmetanog rada računara (npr. programi koji su neophodni deo za rad računara), zatim podaci koji se unose radi elektronske obrade ili koji se prenose računarskim mrežama (Mrvić Petrović, 2005: 322). No, postoje i takva krivična zakonodavstava u Evropi (npr.Srbija) koja, pored ovog naziva za krivična dela, upotrebljavaju i pojam ''visokotehnološki'' kriminal[4]. Pod ovim se pojmom podrazumeva vršenje

[3] Ovaj pojam koristi Krivični zakonik Severne Makedonije posle donošenja Zakona o izmenama i dopunama Krivičnog zakonika (*Služben vesnik na Republika Makedonija,* br.37/96, 80/99, 4/2002, 43/2003 i 19/2004).

[4] Pojam, karakteristike, organi krivičnog gonjenja i postupak za krivična dela visokotehnološkog kriminala u Republici Srbiji uređeni su odredbama Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala (*Službeni glasnik Republike Srbije*, br.61/2005).

krivičnih dela kod kojih se kao objekat ili kao sredstvo izvršenja krivičnih dela javljaju računari, računarske mreže, računarski podaci, računarski sistemi, kao i njihovi proizvodi u materijalnom ili elektronskom obliku (Petrović, 2004: 109-115). To uostalom ukazuje da objekt zaštite kod računarskih krivičnih dela proizilazi iz naziva glave zakona (zakonika) u koju su sistematizovana ova krivična dela.

Pored objekta zaštite, materijalno krivično pravo poznaje i objekt napada (napadni ili gramatički objekat) u smislu dobra prema kome je ili na kome se preduzima radnja izvršenja konkretnog krivičnog dela kako bi se zaštitni objekat napao, povredio ili samo ugrozio. Pojedina savremena krivična zakonodavstva (Srbija, Crna Gora, Hrvatska) u samom zakonskom tekstu ("Značenje izraza koji su upotrebljeni u zakonu") pri autentičnom tumačenju daju pojmovno određenje pojedinih zakonskih izraza koji označavaju objekte napada kod računarskih krivičnih dela. Krivični zakonik Srbije u članu 112. određuje pojam i karakteristike objekta napada kod računarskih krivičnih dela. To su (Jovašević, 2017: 189-192): a) računarski podatak, b) računarska mreža, c) računarski program, d) računarski virus, e) računar i 6) računarski sistem.

Tako je računarski podatak svako predstavljanje činjenica, informacija ili koncepta u obliku koji je podesan za njihovu obradu u računarskom sistemu, uključujući i odgovarajući program na osnovu koga računarski sistem obavlja svoju funkciju (tačka 17.), dok računarska mreža predstavlja skup međusobno povezanih računara, odnosno računarskih sistema koji komuniciraju razmenjujući podatke (tačka 18.). Kao računarski program smatra se uređeni skup naredbi koji služi za upravljanje radom računara, kao i za rešavanje određenog zadatka pomoću računara (tačka 19.). S druge strane, računarski virus je računarski program ili drugi skup naredbi koji je unet u računar ili računarsku mrežu, koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka (tačka 20.). Računar je svaki elektronski uređaj koji na osnovu programa automatski obrađuje i razmenjuje podatke (tačka 33.). I konačno, računarski sistem je svaki uređaj ili grupa međusobno povezanih ili zavisnih uređaja od kojih jedan ili više njih, na osnovu programa vrši automatsku obradu podataka (tačka 34.).

Kao ostale karakteristike računarskih krivičnh dela možemo istaći sledeće: a) radnju izvršenja čini poseban, specifičan karakter i priroda protivpravnih delatnosti u vidu činjenja pojedinaca (preduzimanje pozitivne, aktivne radnje), b) posebna znanja, veština, sposobnosti i specijalizacija na strani učinilaca ovih krivičnih dela koja isključuje mogućnost da se svako, bilo koje lice nađe u ovoj ulozi, c) poseban način i sredstvo preduzimanja radnje izvršenja – uz pomoć, posredstvom, preko ili upotrebom (zloupotrebom) računara, d) posledica ovih dela se javlja u dva vida i to kao: 1) povreda, narušavanje rada, delovanja, funkcionisanja računara, računarske mreže ili računarskih sistema i 2) ugrožavanje – prouzrokovanje, stvaranje opasnosti, mogućnosti da dođe do narušavanja funkcinisanja uopšte ili urednog, kvalitetnog, efikasnog funkcionisanja računara, računarske mreže ili računarskih sistema i e) ova se krivična dela vrše od strane lica koje u vreme preduzimanja radnje postupa sa namerom (ciljem) kao subjektivnim elementom. Ova namera ne mora biti ostvarena u svakom konkretnom slučaju,

ali ona mora da upravlja, determiniše, aktivira ponašanje učinioca. Ta se namera može javiti u više oblika ispoljavanja kao: 1) namera pribavljanja za sebe ili drugo (fizičko ili pravno) lice kakve (imovinske ili neimovinske) koristi ili 2) namera nanošenja kakve (imovinske ili neimovinske) štete drugom fizičkom ili pravnom licu (Komlen Nikolić *et al*. 2010: 86-97).

Izvršioci računarskih krivičnih dela predstavljaju specifičnu kategoriju lica. Naime, ova krivična dela teško može da izvrši svako, bilo koje lice. Ovde se radi, uglavnom, o nedelinkventnim i socijalno prilagodljivim, nenasilnim ličnostima. S druge strane, učinioci za vršenje krivičnih dela putem računara moraju da poseduju određena, specijalna, posebna, stručna i praktična znanja, sposobnosti i veštine u domenu digitalne, informatičke i računarske tehnike i tehnologije. Pored toga, mora se raditi o licima kojima su upravo ovakva tehnička sredstva (računari, računarski sistemi, računarski podaci, računarske mreže) dostupna u fizičkom smislu.

Konačno, za računarska krivična dela se može konstatovati da se radi o krivičnim delima koja se vrše prikriveno, potajno, najčešće bez vidljive prostorne i vremenski bliske povezanosti između učinioca dela i oštećenog (pasivnog subjekta). U praksi postoji veća ili manja vremenska razlika između preduzete radnje izvršenja krivičnog dela i vremena nastupanja njegove posledice. Ova se zato krivična dela teško otkrivaju, a još teže dokazuju, dugo vremena ostaju praktično neotkrivena, sve dok oštećeni (fizičko ili pravno lice) ne pretrpi štetu na svojoj imovini (bilo u vidu gubitka, umanjenja postojeće imovine bilo u vidu nemogućnosti ili otežanog uvećanja postojeće imovine). Upravo se zato u pravnoj teoriji često ističe da se ovde radi o kriminalitetu koji brzo i lako menja forme i oblike ispoljavanja, granice među državama, kao i vrstu oštećenog.

Sa aspekta krivice učinioca, može se uočiti da se računarska krivična dela izvršavaju isključivo sa umišljajem (kao najvišim oblikom svesne i voljne upravljenosti učinioca na prouzrokovanje krivičnopravno relevantne posledice u spoljnom svetu). No, pojedina od ovih krivičnih dela se sa aspekta krivice mogu izvršiti samo sa direktnim umišljajem. To je slučaj kod onih krivičnih dela kod kojih učinilac pristupa preduzimanju radnje izvršenja sa posebnom vrstom namere ili cilja koji želi da ostvari na objektu napada (Ranđelović, 2013: 131-143). To može biti dvojaka namera: a) namera učinioca da se sebi ili drugom fizičkom ili pravnom licu pribavi bilo kakva ili pak imovinska (ekonomska, materijalna) korist i b) namera učinioca da drugom (fizičkom ili pravnom) licu nanese bilo kakvu ili pak imovinsku štetu. U tim slučajevima postojanje namere (cilja) učinioca opredeljuje direktan umišljaj kao oblik njegove krivice. Ova namera učinioca mora da kod njega postoji upravo u vreme preduzimanja radnje izvršenja, ali ta namera (cilj) ne mora u svakom konkretnom slučaju da bude i ostvarena.

Računarski kriminalitet takođe karakteriše velika dinamika i izuzetna šarolikost pojavnih oblika, formi i vidova ispoljavanja (Jovašević, 2003: 351-353). To se moglo i očekivati jer se ovde upravo radi o novoj tehnologiji sa velikim mogućnostima primene u širokoj sferi ljudske, društvene, finansijske i privredne delatnosti, te su i mogućnosti zloupotrebe računara svaki dan sve veće. Pored novih pojavnih oblika ranije, već poznatih krivičnih dela koja pod uticajem zloupotrebe kompjutera menjaju tradicionalni, klasični

način, sredstvo i modus ispoljavanja (krađa, prevara, pronevera, falsifikovanje), javljaju se i novi oblici protivpravnog i kažnjivog ponašanja koji ne poznaju granice između država (pravljenje računarskog virusa) (Matijašević, 2013: 75-82).

Radi se o prikrivenim oblicima delovanja pojedinaca ili grupa, koji mogu zahvatiti različite oblasti ljudske, društvene, odnosno privredne delatnosti. S druge strane, često između mesta (distanciono delo), odnosno vremena (temporalno delo) preduzimanja radnje izvršenja, te prouzrokovane posledice na štetu nekog fizičkog ili pravnog lica ne postoji direkna i neposredna povezanost. To ukazuje da se često za krivično delo uopšte i ne zna pre nego što je uopšte nekom licu naneta štetna posledica (Nikolovska, 2013:71-89). S druge strane, ova karakteristika računarskog kriminaliteta znatno otežava otkrivanje, kao i dokazivanje izvršenih krivičnih dela, kao i krivice njihovih učinilaca za što su potrebni posebno obučeni ljudi (sa specijalnim znanjima, veštinama, sposobnostima) u organima krivičnog pravosuđa (policije, tužilaštva i suda), odnosno posebna, visoko sofisticirana tehnika (Bakreski, Milešeska, 2021: 161-174).

Štetne posledice računarskih krivičnih dela su velike i ispoljavaju se u nastupanju imovinske štete za druga fizička ili pravna lica (ponekad i za celu državu), u gubitku poslovnog ugleda, gubitku poverenja u sigurnost, poverljivost, tačnost, urednost, kvalitet i istinitost računarskog poslovanja i uopšte računarskih podataka, opasnosti od zloupotrebe po slobode i prava čoveka i građana na razne načine, odavanje lične, poslovne i drugih vidova tajni i sl.

ZAKLJUČAK

Uz sve veću prisutnost digitalizacije u svim sferama društvenog života, sve češće dolazi do njene zloupotrebe. Tako se poslednjih decenija u okviru opštih, klasičnih krivičnih dela javljaju novi pojavni oblici ili vidovi ispoljavanja u slučaju preduzimanja njihove radnje izvršenja uz pomoć, korišćenjem računara, računarskih sistema ili računarske mreže. Istovremeno se javljaju nova, do sada nepoznata, krivična dela koja se vrše na ovaj način. Svi ovi oblici protivpravnih delatnosti uz pomoć računara, kojima se povređuju ili ugrožavaju prava, interesi ili dobra drugih fizičkih ili pravnih lica, čine sistem računarskih krivičnih dela.

Na bazi brojnih međunarodnih dokumenata donetih poslednjih decenija u okviru Saveta Evrope, a posebno na bazi Konvencije o visokotehnološkom kriminalu (2001.) uspostavljene su pravne osnove za nacionalna zakonodavstva za propisivanje pojedinih računarskih krivičnih dela, sa sistemom krivičnih sankcija, te pravilima o odgovornosti fizičkih i pravnih lica za njih. Stoga su brojna rešenja prisutna u uporednom krivičnom zakonodavstvu, koja su zasnovana na ovim standardima, u većoj ili manjoj meri unificirana, odnosno standardizovana.

U pravnoj teoriji postoje različita pojmovna određenja računarskih krivičnih dela. Računarski kriminalitet, kao zbirni naziv, se može odrediti kao kriminalitet koji je primarno usmeren protiv bezbednosti informacionih (kompjuterskih, računarskih)

sistema, mreža ili podataka, u nameri da se sebi ili drugom pribavi određena korist ili da se drugome nanese kakva šteta. To je, dakle, sveukupnost različitih oblika, vidova i formi ispoljavanja protivpravnih ponašanja fizičkih ili pravnih lica upravljenih protiv bezbednosti računarskih, informacionih i kompjuterskih sistema u celini ili njihovih pojedinih delova na različite načine i različitim sredstvima, posredstvom, korišćenjem računara ili računarskih sistema u nameri da se sebi ili drugom (fizičkom ili pravnom) licu pribavi kakva korist (imovinske ili neimovinske prirode) ili da se drugome nanese kakva šteta. Kao objekt zaštite javlja se bezbednost računarskih podataka, računarskih mreža ili informacionog sistema u celini ili njegovog pojedinog dela (segmenta), dok je objekt napada višestruko određen kao: računar, računarski podatak ili računarski virus.

U ostale karakteristike računarskih krivičnh dela spadaju: a) radnju izvršenja čini poseban, specifičan karakter protivpravnih delatnosti činjenja pojedinaca (preduzimanje pozitivne, aktivne radnje), b) učinioca karakterišu posebna znanja, veštine, sposobnosti i specijalizacije, c) radnja izvršenja se preduzima na poseban način - uz pomoć, posredstvom, putem, preko ili upotrebom (zloupotrebom) računara, d) posledica dela se javlja kao: 1) povreda, narušavanje rada, delovanja, funkcionisanja računara, računarske mreže ili računarskih sistema i 2) ugrožavanje – prouzrokovanje, stvaranje opasnosti, mogućnosti da dođe do narušavanja funkcinisanja uopšte ili urednog, kvalitetnog, efikasnog funkcionisanja računara, računarske mreže ili računarskih sistema i e) radnja izvršenja se preduzima sa određenom namerom (ciljem) kao subjektivnim elementom: 1) namera pribavljanja za sebe ili drugo (fizičko ili pravno) lice kakve (imovinske ili neimovinske) koristi ili 2) namera nanošenja kakve (imovinske ili neimovinske) štete drugom fizičkom ili pravnom licu.

LITERATURA

1. Ambos, K. (2018) *European criminal law.* Cambridge: Universitet Press.
2. Atanasov, R. (2021) *Priračnak za zaštitata od izmami i kompjuterski kriminal*. Skopje: Prosvetno delo.
3. Babić, M., Marković, I. (2007) *Krivično pravo, Posebni deo.* Banja Luka: Pravni fakultet.
4. Babić, M. (2011) *Međunarodno krivično pravo.* Banja Luka: Pravni fakultet.
5. Babić, V. (2009) *Kompjuterski kriminal*. Sarajevo: Rabic.
6. Bakreski, O., Milešeska, T. (2021) *Bezbednosta na informaciite i kritičnata infrastruktura*. Skopje: Direkcija za bezbednost.
7. Clough, J. (2010) *Principles of Cybercrime*. Cambridge: University Press.
8. Cullen, P. (1997) *Computer crime, Law and the Internet, regulating Syberspace*. Oxford: Universitet Press.
9. Čejović, B. (2006) *Međunarodno krivično pravo, Opšti i posebni deo*. Beograd: Dosije.

10. Čejović, B., Vučković, B., Vučković, V. (2011) *Međunarodno krivično pravo*. Tivat: FMS.
11. Dragičević, D. (1999) *Kompjuterski kriminal i informacijski sustavi*. Zagreb: Informator.
12. Đorđević, Đ. (2011) *Krivično pravo, Posebni deo*. Beograd: Kriminalističko-policijska akademija.
13. Emm Kareklas, S. (2009) *Priručnik za krivično pravo Evropske unije*. Beograd: Institut za uporedno pravo.
14. Jovašević, D. (2003) *Komentar Krivičnog zakona Republike Srbije sa sudskom praksom*. Beograd: Nomos.
15. Jovašević, D. (2011) *Leksikon krivičnog prava*. Beograd: Službeni glasnik.
16. Jovašević, D., Ikanović, V. (2015) *Međunarodno krivično pravo*. Banja Luka: Univerzitet Apeiron.
17. Jovašević, D. (2017) *Krivično pravo, Posebni deo*. Beograd: Dosije.
18. Komlen Nikolić, L. *et al.* (2010) *Suzbijanje visokotehnološkog kriminala*. Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca.
19. Koševaliska, O., Maksimova, E. (2020) *Megunarodno kazneno pravo*. Štip: Univerzitet Goce Delčev.
20. Kouch, J. (2016) *Cyber Crime*. Praha: CZ NIC.
21. Matijašević, J. (2013) *Krivičnopravna regulativa računarskog kriminaliteta*. Novi Sad: Pravni fakultet za privredu i pravosuđe.
22. Milosavljević, M., Grubor, G. (2009) *Istraga kompjuterskog kriminaliteta*. Beograd: Singidunum Univerzitet.
23. Moore, R. (2005) *Cyber Crime*. New York: Lexis Nexis.
24. Mrvić Petrović, N. (2005) *Krivično pravo*. Beograd: Službeni glasnik.
25. Nikolovska, S. (2013) *Metodika na istražuvanje kompjuterska kriminaliteta*. Skopje: Fakultet na bezbednost.
26. Novoselec, P. (2009) *Uvod u gospodarsko kazneno pravo*. Zagreb: Pravni fakultet.
27. Pavišić, B. (2006) *Kazneno pravo Vijeća Evrope*. Zagreb: Golden marketing.
28. Pavlović, Z., Vučić, M. (2017) *Međunarodno krivično pravo*. Novi Sad: Pravni fakultet za privredu i pravosuđe.
29. Petrović, B., Jovašević, D. (2010) *Međunarodno krivično pravo*. Sarajevo: Pravni fakultet.
30. Petrović, B., Jovašević, D., Ferhatović, A. (2016) *Krivično pravo 2*. Sarajevo: Pravni fakultet.
31. Petrović, S. (2004) *Kompjuterski kriminal*. Beograd: Vojnoizdavački zavod.
32. Ranđelović, D. (2013) *Visokotehnološki kriminal*. Beograd: Kriminalističko policijska akademija.
33. Satzger, H. (2018) *International and European criminal law*. Munchen: CH Beck.
34. Selinšek, Lj. (2006) *Gospodarsko kazneno pravo*. Ljubljana: GV Založba.
35. Stojanović, Z., Delić, N. (2013) *Krivično pravo, Posebni deo*. Beograd: Pravna knjiga.

36. Vestbi, Dž. (2004) *Međunarodni vodič za borbu protiv kompjuterskog kriminaliteta*. Beograd: Produktivnost.
37. Završnik, A. (2014) *Kibernetska kriminaliteta*. Ljubljana: IUS Software, GV Založba.
38. Zvrlevski, M., Andononova, S., Miloševski, V. (2014) *Priračnik za kompjuterski kriminal.* Skopje: OSCE.

Pravni izvori

1. Krivični zakonik Republike Srbije (*Službeni glasnik Republike Srbije,* br. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94 /2016 i 35/2019).
2. Krivični zakonik Severne Makedonije (*Služben vesnik na Republika Makedonija,* br.37/96, 80/99, 4/2002, 43/2003 i 19/2004).
3. Zakon o izmenama i dopunama Krivičnog zakona Srbije (*Službeni glasnik Republike Srbije,* br. 39/2003).
4. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala (*Službeni glasnik Republike Srbije*, br. 61/2005).

CONCEPT AND CHARACTERISTICS OF COMPUTER CRIMES

In recent decades, new forms or types of their manifestations have appeared in the system of existing, general, classic criminal offenses, if their act of execution is undertaken with the help, mediation, use or use of computers, computer systems or computer networks. At the same time, new, hitherto unknown, crimes are being committed in this way. All these forms of illegal activities with the help of computers, which violate or endanger the rights, interests or property of other natural or legal persons, constitute a system of computer crimes. Positive legislation, which is based on international standards, prescribes a number of computer crimes, the content, characteristics and elements of which are still not understood in legal theory. The paper presents the basic characteristics of computer crimes in legal theory, international documents and domestic criminal law.

KEYWORDS: *computers, crime, illegality, international documents, law.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.02

THE NEW FORMS OF DIGITAL CRIMINALITY IN SLOVAKIA AND FIGHT AGAINST THEM*

Radovan Blazek**

The article should introduce the new forms of digital criminality that were noticed in the Slovak Republic in the last years. The article presents the methods of conducting these types of criminality and the vulnerability of victims in these cases. Main focus is concerned on the different methods of internet and mobile communication frauds together with new forms of missuses of credit cards and internet payments. The article presents real cases from Slovakia based on the author's practice of the prosecutor at the District Office of the Prosecutor in the town Malacky, Slovakia. The article also focuses on the specific problems connected with investigation of this criminality in Slovak Republic, on the digital evidence and forms of international cooperation in gathering the electronic evidence, the problems of "European Investigation Order" and other forms of international tools that could be used for securing the evidence from the countries that are not the members of EU. The last part presents the forms of prevention that need to be performed in order to fight against these forms of criminality.

KEYWORDS: *computer crime, fraud, defamation, threats, pornography.*

* This article was supported by the scientific project APVV-19-0102 of the Slovak Research and Development Agency.

** Associate professor, JUDr., PhD., Comenius University, Faculty of Law, Bratislava, Slovakia.

ORCID: https://orcid.org/0000-0003-3091-3399

E-mail: *radovan.blazek@flaw.uniba.sk*

INTRODUCTION

By the term computer crime, we mainly refer to crimes directed against computers, programs and data transmitted via a computer, their misuse or unauthorized access to them, as well as crimes committed with the help of a computer. The literature contains countless definitions of computer crime:

> *"Cybercrime is any illegal, immoral and unauthorized action that involves the misuse of data obtained through computer technology or its alteration."* (Dianiška & Strémy, 2016: 292).

> *"Computer crime can be divided into two groups - crimes committed against computers and crimes committed through computers. In the first case, the computer represents the object of criminal activity, in the second case, it is a tool, while the object is the violation of other, relatively diverse rights."* (Matějka, 2002: 7).

> *"Under the term computer crime (the increasingly used term cybercrime) we understand both crimes directed against computers and indirect computer crime, i.e. crimes committed using a computer, some of its components, or a larger number of separate computers or computers connected to a computer network."* (Brvnišťan, 2018: 26).

> *"Under the term computer crime or cybercrime, it is necessary to understand the conducting of a criminal activity in which a computer figures in a certain way as a sum of technical and software equipment including computer data, or only one of its components, or a larger number of separate computers or connected to a computer network, and that, for example, as the subject of this activity, with the exception of criminal activity, the subject of which are said components as movable things, but not excluding as an instrument of criminal activity."* (Dopita, 2018: 17).

The terminology used to describe cybercrime is still very inconsistent. There is no legal definition of cybercrime, because it is a broad field whose boundaries are not easy to define. Differences persist not only in the labelling of this phenomenon, the content is also understood differently, which mainly contributes to a misunderstanding of the meaning and harmfulness of this type of criminal activity (Kostrecová *et al.* 2010: 1).

Computer crime is currently one of the fastest developing forms of crime, growing in direct proportion to the computerization of society. One of the basic tools for combating it is the Convention on Cybercrime of November 23, 2001.[1] Computers and Internet services are used in the conducting of various criminal activities, mainly related to blackmail, threats, slander, production and distribution of child pornography, drug crimes, frauds, but also criminal offenses in the field of intellectual property.

In this article, cases of computer crimes are analysed, which have been recorded in recent years under the jurisdiction of the District Prosecutor's Office of Malacky, Slovakia.

[1] Announcement of the Ministry of Foreign Affairs of the Slovak Republic published under no. 137/2008 Coll.

1. TYPES OF COMPUTER CRIME

1.1. Online Stores

In this case, the buyer is misled by the seller, who promises to send certain goods or to provide a service after paying the purchase price, while after paying for the goods or services, he does not provide it and keeps the transferred funds. Therefore, there is a suspicion of committing the crime of fraud according to Art. 221 of the Criminal Code of Slovakia.[2]

The commission of this criminal activity is connected with false advertisements for the offer, e.g. of motor vehicles, where real advertisements from other sellers are used and the perpetrators only misuse vehicle identification data, photos, etc.

Subsequently, criminal activity is carried out by using email communication, where the perpetrators try to create the appearance of credibility by sending electronic confirmations of the shipment of goods by a delivery company, which, however, either does not exist or the confirmation is electronically falsified. Alternatively, there are cases where the seller sends scanned personal documents by e-mail to prove his trustworthiness, which turn out to be fake or stolen.

The injured party is misled, while the transaction has the appearance of a trustworthy business for him and he sends the money, while it may also involve communication in a foreign language, sending money abroad to the account of a completely different person than the name of the seller, or to a completely different country than the one where the seller is said to be located.

These frauds are very often easily detectable, and criminal reports in these cases are rejected pointing to the failure to observe the "usual level of caution" on the side of the victims, who, with the vision of a profitable purchase, send funds even to foreigners, communicating in a language other than the nationality they pretend to be, to foreign accounts that do not belong to the seller and risk the loss of their funds, even they must be aware from all available information that the said transaction is risky.

There are also fake websites that pretend to be a real merchant, but on the fake website there are other contact details and other information necessary to make a business transaction. In this way, the perpetrators create the impression that they represent a specific legal entity. The victim is thus misled into believing that he is transacting with a real merchant, but this is not the case. Here it is not always possible to talk about the carelessness of the injured party, because the sites seem to be trustworthy and are difficult to recognize from the sites of real traders.

There are also cases where the same offender operates several fraudulent online stores and offers fictitious goods that, after receiving the money, he does not send to the customer or sends him an imitation of goods that does not meet the required characteristics, especially quality, and is of an incomparably lower price category. After finding

[2] Law no. 300/2005 Coll. The Criminal Code, as amended, hereinafter referred to as "the Criminal Code" or "CC".

out that it is a fraud, customers often express through various communication and review portals that it is a fraudulent business, but many customers who do not read the negative reviews still make purchases through these sites. Only when a number of negative reviews accumulate, the site lose customers, but the perpetrator always creates new websites with new name and a new design, which is relatively simple in the Internet environment and does not require high costs for the perpetrator. Subsequently, the perpetrator creates the impression that it is a different, new merchant and again acquires new customers. These frauds are difficult for consumers to detect, and most of the time consumers recognize them only after the purchase.

The Internet environment creates space for the anonymity of the perpetrators, therefore the detection of the perpetrators in these cases is considerably difficult. When searching for the perpetrator, the flow of data is often monitored and the relevant internet providers and network administrators are cooperated with, but proving that a specific computer was used to commit a crime does not always lead to finding out which specific user used it. It is easier to detect criminals who communicate through their own e-mail addresses, where it is possible to find out the data about the person who set them up, but even in these cases, some servers allow the establishment e-mail box even with false, incomplete or no personal data.

The problem of convicting and punishing the offender is often also the aspect that the offender resides in a country that is not a member of the EU (e.g. Ukraine, Serbia, Moldova) and judicial cooperation with this country is lengthy and difficult and often does not lead to the desired success in detection and the conviction of the perpetrator, and therefore the clarification of this crime becomes more economically demanding than the damage itself in these cases.

1.2. Abuse of Payment Cards

This criminal activity is mainly associated with the purchase of goods via Internet, where the victims record an unwanted transaction on their bank account, while in these cases the bank can provide relevant data on which merchant the payment was sent to, and from the merchant it is subsequently possible to find out to which address the goods were sent to.

The problem of this criminal activity consists in the fact that the ordered goods are mostly delivered by deliverymen as part of their normal work, where they deliver a number of orders per day, while at the time of the investigation they no longer remember the circumstances of the particular delivery and thus cannot even identify the offender who uses it for delivery different addresses, from work to sublet addresses, etc., while subsequently it is not possible to identify a specific person, who may also appear under a false name.

In this case the victim does not have the opportunity to influence the commission of this criminal activity by his caution, because most often the victims are not able to identify how the information necessary for card payment via Internet was "leaked" and

state that they did not lend their cards to anyone, nor did they entrust anyone with the relevant data from the cards. The circumstances under which the perpetrators manage to carry out the mentioned transactions often remain unexplained, because the perpetrators either fail to be identified or refuse to testify.

The latest method of committing this criminal activity is to make phone calls to victims from non-existent numbers, from which an English-speaking person who pretends to be a representative of Microsoft services and convinces the victim that his computer has a virus, it needs to be removed and the necessary maintenance should be carried out on protection against virtual attacks. Subsequently, he instructs the victim over the phone how to proceed when working with his computer, and through remote access, these perpetrators access the computers of the victims, request the provision of their personal data and documents, and subsequently request to pay for the services provided with a payment card, while after entering the payment card data there will be payments in a completely different, much higher amount than was originally announced to the injured party. As a rule, the money is used to open an account on the sites of virtual currency operators and used to buy virtual currency.

The newest form of performing this criminal activity is via What's up communication tool, where the perpetrator writes a message to the injured party, that he/she is interested in buying a thing, that the injured party offers on the internet via "second hand webstores". Then the buyer pretends to send the money on the bank card of the seller and instruct the seller to put the card details in a specific form. However, this action is completely fraudulent and the seller will not receive money, but he will lose the money.

The problem of convicting and punishing the perpetrator is often connected with the aspect that the perpetrator is staying abroad and the investigation of criminal activity must be carried out through international judicial cooperation, which is lengthy and difficult and often does not lead to the desired success in detecting and convicting the perpetrator. It is also about technically proficient criminals who are difficult to trace in a virtual environment, the participation of several persons in the commission of this criminal activity, which is characterized by high sophistication and is represented in all EU states. It is, so to speak, a worldwide problem, and at international working meetings on this type of crime, it has not yet been possible to find an effective means of combating it.

In the agenda of the Malacky District Prosecutor's Office, this crime represents a significant share of the total investigated crime. In 2020, a total of 58 criminal cases were conducted at the Malacky District Prosecutor's Office for the aforementioned crime.

1.3. Misuse of Access Passwords for Illegal Financial Transactions

These actions can take on the dimension of both the crime of theft according to Art 212 CC, but also the crime of Art 219 CC - unauthorized use of payment card. In these cases the perpetrators misuse passwords saved on a computer or mobile phone of their owner, while they borrow these electronic devices for another purpose and then

misuse the saved passwords to access internet banking and transfer funds to their own account. These crimes are relatively easy to detect because it is known to which account the perpetrator transferred the money, also at what time the transaction was made, and the victims usually remember to whom they lent their electronic devices.

1.4. Misuse of Access Passwords for Sending Unsolicited Communications

Usually committing a crime of dangerous threats under Article 360 CC, the criminal offense of damaging the rights of others under Article 375 CC, extortion under Article 189 CC, or criminal offense according to Article 247 CC - unauthorized access to a computer system. We most often encounter this criminal activity in a family environment, where life partners mutually access their e-mail, Facebook accounts or use the same computers with saved passwords, and then after the break-up they use it to fight against each other and make each other wrong reputation.

1.5. Placing Illegally Made Copies of Author's Works on Websites

In Slovakia crime of copyright infringement pursuant to Article 283 CC. These crimes are often reported by various associations and legal entities created for the protection of copyrights, which also provide sufficient information to convict and detect the perpetrator. However, there are also often criminal reports that are not relevant, because copyright protection associations do not have sufficient legal knowledge to be able to clearly identify what constitutes a criminal act and cannot accept the interpretation of legal norms that not every copyright infringement it is also a criminal act.

The criminal proceedings listed in sub-chapters 2.3 to 2.5 are most often reported by the victims and their detection is not problematic, therefore there is not a high latency within this type of criminal activity, but all these cases are rather isolated within the agenda of the Malacky District Prosecutor's Office and occur on average in 5 cases per year.

1.6. Spreading False Information via Emails or Published on Websites

Most often, these actions take on the dimensions of criminal defamation according to Article 373 CC or damage to the rights of others according to Article 375 CC. These acts have been a relatively widespread practice in recent times, when people disseminate information of various kinds, especially about civil servants and public officials, in the Malacky district typical examples are the sending of such information about mayors of municipalities, members of municipal councils or representatives of the municipal administration or local state administration. Perpetrators usually publish such false information on various blogs, Facebook or other communication servers on the basis of dissatisfaction with the decision-making activities of the said authorities, or send them to various recipients, e.g. other state authorities. Another example of such

criminal behaviour is slandering neighbours or family members with whom there are unresolved disputes, especially property disputes, but there are also known cases of parents arguing about child care, etc.

1.7. Email Blackmail

Most often committed by unknown criminals communicating in foreign languages, who recently send a large number of emails about capturing passwords and hacking into the victim's computer system, where, based on these claims, they are asked to send a financial amount in order not to publish their erotic photos or other incriminating materials, which they allegedly downloaded from their computer or made by themselves by remotely controlling their webcam or capturing data about visited websites. Victims, fearing the disclosure of sensitive information, end up repeatedly sending large sums of money to these unknown persons. Similar cases are known throughout the Slovak Republic and in other countries.

1.8. Sexual Crimes and Child Pornography

A new type of crime, which is committed in the virtual world, are crimes of sexual abuse, which can also be carried out via Internet. The amendment to the Criminal Code with effect from 1 August 2013 (amended by Act No. 204/2013 Coll.) included the provisions of Article 201a and 201b CC, which are also intended to punish the actions of offenders who contact a child younger than fifteen years for the purpose of committing the crime of sexual abuse or the production of child pornography via an electronic communication service, e.g. via the Internet (Art. 201a). Also, as the factual basis of sexual abuse, an act by which someone involves a person under the age of 15 in sexual activities without that person directly participating in such activities was added (Art. 201b), which is also possible in the area of Internet, where this person may become a consumer of Internet sex products.

The frequency of these crimes in Malacky district is still small. This is due to the fact that a certain degree of sexual deviation is required for the commission of the mentioned criminal activity, which is not that common, and at the same time, if there are no real meetings and physical contact between the perpetrator and the victim, the detection of this crime is difficult. As with other Internet crimes, anonymity is high in this environment. In most cases, the detection of this criminal activity is only possible if the victim himself confides in his parents, friends or teachers about the said problem. Otherwise, capturing such "criminal" communication in the Internet environment is almost impossible.

Similarly, computers and computer systems are used in the commission of the crimes of production of child pornography according to Art. 368 CC, distribution of child pornography according to Art. 369 CC and possession of child pornography and participation in a child pornography performance according to Art. 370 CC. In the

agenda of the Malacky District Prosecutor's Office, this crime does not represent a significant share of the total investigated crime. In 2020, 2 new criminal cases were registered for the mentioned crimes. This mainly concerns the sending of erotic images of minors among juvenile offenders who consider such sexual objects appropriate for their age, but do not realize the danger and seriousness of their actions when they send such "images" to their friends via electronic communication services. They thereby commit the crime of distributing child pornography according to Art. 369 CC, even if they are often unaware of the criminality of this action.

1.9. Other Crimes

In addition to the above-mentioned crimes, we also rarely encounter the reporting of crimes under Art. 247a CC - unauthorized access to a computer system, under Art. 247b CC - unauthorized access to computer data and under Art. 247c CC - unauthorized interception of computer data. However, unlike the above-mentioned crimes, these represent a high degree of latency, because the injured party is often not able to record these interventions in the tangle of their own electronic information, or records them only after a longer time interval or cannot clearly determine whether the resulting consequence is the result of a criminal act. This type of criminal activity is still relatively difficult to investigate, because within the anonymity of the Internet environment, it is difficult to find out over time who and when made unauthorized interventions in the computer system and, in particular, from where the perpetrator acted and who specifically acted. In 2020, only one new criminal complaint was registered for the mentioned crimes.

Prof. Strémy (Dianiška, & Strémy, 2016: 296) also mentions other criminal acts, which, however, were not dealt with within the agenda of the Malacky District Prosecutor's Office: spreading drug addiction (Art. 174 CC), unauthorized enrichment (Art. 226 CC), operating unfair games and bets (Art. 229 CC), endangering morals (Art. 371 and § 372 CC, unauthorized handling of personal data (Art. 374 CC), support and promotion of groups aimed at suppressing fundamental rights and freedoms (Art. 421 and 422 CC), defamation of a nation, race and belief (Art. 423 CC) and others the facts of the criminal acts listed in the Criminal Code. One of the reasons why proceedings were not recorded according to Art. 421 of the CC in the service district of the Malacky district, it is also the fact that these crimes currently fall under the jurisdiction of the Specialized Criminal Court,[3] but there is no doubt that these proceedings are also a relatively frequent phenomenon on the Internet.

[3] Art. 14 letter o) CC.

2. EVALUATION OF COMPUTER CRIME AND PREVENTION

2.1. Evaluation of Computer Crime

Cybercrime is currently a relatively common phenomenon due to the wide availability of computing technology and at the same time the increase in the number of households connected to the Internet. Also other types of technical means than just computers are being used for this type of crime, i.e. tablets and mobile phones, which further increases the possibility of criminals to access the technical equipment necessary to commit this type of criminal activity.

Mentioned type of crime in general is detected when an Internet provider or network administrator records the illegal behaviour of an Internet user and reports this fact to the law enforcement authorities. In other cases, the victims themselves report this criminal activity. From one's own activity, knowledge about this criminal activity can occur only secondarily, when computer hardware components are seized as part of enforcement actions in connection with other criminal activity, which contain illegal software (child pornography, data that violated copyright). Criminal reports to the public also occur rarely, if the announcer learns that a person from his neighbourhood is committing the above-mentioned criminal activity.

Among the basic causes of cybercrime is the low security awareness of the victims. A person is the one who can most endanger his or others' safety in the cyber environment, by action or inaction. It is also necessary to take into account the basic technical causes of cybercrime, e.g. old and non-updated software, non-use of antivirus programs, insufficient security settings, relative availability of sophisticated technical means for criminals and others. In many cases, inexperienced computer users, due to their technological and security illiteracy, neglect the protection of computers and information and communication tools, or are completely unaware of possible cyber threats. It is obvious that the human factor plays a key role in committing cybercrime, therefore prevention can play an important role in the fight against cybercrime.

2.2. Prevention of Computer Crime

> *"Prevention, as an area that can help the situation, is not yet systematically applied and used in the field of cyber security. It is obvious that the nature of cybercrime requires the implementation of specific preventive measures so that it is possible to effectively prevent the commission of modern forms of criminal activity in cyberspace."* (Brvnišťan, 2018: 27).

In relation to the procedures described in subsection 2.1, the prevention and reduction of this type of crime is essential, especially in the area of raising people's awareness of this type of computer crime. For some, the mentioned form of criminal activity may be obvious, and many people may state that they would never come across the

mentioned frauds. Also for this reason, the number of such proceedings does not even catch up, because criminal reports are rejected citing non-compliance with the so-called "mandatory degree of caution". The so-called "mandatory degree of caution" is an application rule formulated by jurisprudence, the basic principle of which is that everyone should act in such a way as to observe at least the basic rules of prudence and not become a victim of obvious and easily detectable criminal activity.

Nevertheless, it must be remembered that in our society there are also a number of easily vulnerable victims of such crimes, juveniles, persons with certain mental disabilities or persons coming from less developed areas where the computerization of society has not yet reached a sufficient level. It is these persons who then become easy prey for the perpetrators of these crimes. Therefore, it is important to publish the forms of committing this criminal activity in professional and scientific articles, but also in the media, television and newspaper articles, which are more accessible to people. In professional circles, some standard procedures are already almost routine, which the perpetrators use again and again on the victims and abuse the voluntary cooperation of the victims, their inexperience, trust and naivety. A number of identical internet frauds are known all over Slovakia, which show a similar modus operandi and represent de facto partial attacks of the same continuing crime. Despite efforts to inform the victims of these specific attacks, awareness of these acts is apparently still low, as new victims are still appearing. Without the cooperation of the victims themselves, it would not even be possible to commit these crimes. The number of these crimes is a signal that prevention in this area is insufficient.

In relation to the crimes described in subsection 2.2, prevention is almost impossible. The only option is to encourage payment card users and electronic banking users to make transactions only through verified online stores, only through secure payment gateways, and to find out and verify in advance where and how they use their bank card. However, detecting suspicious online stores is much more difficult in this case than it is with the crimes described in subsection 2.1.

In relation to the crimes described in subsection 2.3, it is crucial that users of electronic devices consistently consider saving passwords for Internet banking directly in these devices without the need to re-enter them when logging in. It is convenient not to have to re-enter the password every time when logging in, and it is precisely this convenience of users that is abused by criminals who purposefully look for opportunities to carry out illegal transactions through foreign devices. Their authorized user so often does not keep in mind when handing them over to another person that can easy access to his bank accounts. These transactions are often not even detected by the victims, because some do not sufficiently monitor the movements on their accounts, and if the amounts involved are minimal, the victim may not even notice them in the tangle of other transactions.

Most of the misuse of these computer accounts and passwords in subsection 2.4. comes from the same title - saving passwords to mailboxes on the computer, not locking the computer when the user leaves, and a general careless approach to protecting one's own privacy.

Within the crimes described in subsection 2.5, no other prevention is possible than the threat of criminal penalties for these procedures, which would deter the perpetrators from this type of crime. In this case, it is mostly a generally accepted type of criminal activity, and the public approves it. The perpetrators of this type of crime are mostly ordinary citizens and there are countless of them in the society, therefore they mutually confirm and reinforce the belief that this type of crime is not even a crime and do not attach great importance to it. The attitude of the public, which does not sufficiently condemn this type of crime, is the driving force for other perpetrators to commit this type of criminal activity. Based on the above, the prevention of this criminal activity is to increase the clarity of this criminal activity and exemplary punishments of its perpetrators, in order to reduce the number of those who dare to commit this criminal activity.

Almost no prevention is also possible for the acts described in subsection 2.6. Perpetrators commit this crime believing that they are in the right, believing that they are only justly venting their righteous anger at the wrongdoing of others. The problem is often in the subjective perception of various life situations by the perpetrators, who perceive things in a distorted way and thus put themselves in danger of prosecution when they start sharing their distorted view publicly with others on the Internet. Unfortunately, the Internet is a public place where posts on social networks and websites is almost uncontrollable. The innumerable number of websites does not allow effective control over their content. Also, within the Internet, there is no way to exclude unwanted users who will post various negative information on the network. Since each perpetrator of this type of criminal activity can log-in from another place, from another computer, under a different name, the fight against this crime is almost impossible. And due to the overwhelming subjectivity of the perpetrators' perception of reality, the possible threat of criminal punishment is also insufficient, because the perpetrators are often subjectively convinced that their actions are not criminal.

In the cases described in subsection 2.7, prevention is similar to the cases according to subsection 2.1. It is not possible to immediately jump in and trust all the information that someone sends in the form of electronic communication, and it is necessary to rationally evaluate before the initial threat whether this threat is real and whether it is even possible for the perpetrator to have the information that he claims to have. Of course, there are also rare cases of real blackmail via e-mail communication, when the perpetrator threatens with things that he is capable of carrying out. But this form of blackmail is rather rare. Email extortions have the character of fraud rather than real blackmail.

The conduct mentioned in subsections 2.8 and 2.9 is hard to be detected due to the anonymity of Internet, therefore it is not even possible to discourage their perpetrators, because they commit them knowingly that they cannot be detected. Therefore, prevention in this area also fails.

CONCLUSION

This article summarizes the current most frequent actions of criminals carried out within the Internet. As mentioned above, suppressing and punishing this type of crime is currently quite difficult. Potentially every Internet user can become a perpetrator of any of the listed crimes. However, there are too few law enforcement agencies for all these crimes to be detected, investigated, and then the perpetrators identified and punished fairly and effectively. It is also necessary to emphasize that the method of committing this criminal activity as well as its detection and documentation often requires information technology education, which members of the police forces and prosecutors do not have.

> *"The prevention, detection and clarification of computer crime requires a special approach and the continuous introduction of new methods, the constant improvement of the professional qualifications of criminalists and, last but not least, closer cooperation with external experts (private sector)."* (Brvnišťan, M. 2018, p. 34).

It is always necessary to cooperate with experts in the field of informatics, to request expert opinions, because most often law enforcement authorities do not have sufficient knowledge in this scope. Such investigations take 6 to 12 months due to their complexity. In the Slovakia there are not enough experts with whom law enforcement authorities can cooperate, therefore they are overworked and cannot provide the desired outputs in the required quality and ontime. There are not enough policemen and prosecutors to prosecute the mentioned criminal activity, but there are even fewer technicians who could clearly prove and document this criminal activity.

For this type of criminality, it is necessary to focus more on prevention than on repression. Successful prevention and citizens' awareness of the existence of these illegal actions can significantly reduce the number of these crimes and victims affected by them.

REFERENCES

1. Act No. 300/2005 Coll. Criminal Code, as amended.
2. Brvnišťan, M. (2018) "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, 26-37.
3. Convention on computer crime of November 23, 2001, no. 137/2008 Coll.
4. Dianiška, G., Strémy, T., Vráblová, M. *et al.* (2016) *Criminology*, 3rd updated and supplemented edition. Pilsen: Aleš Čeněk, s.r.o.
5. Dopita, T. (2018) *Computer data - their securing and use in criminal proceedings*,
6. Kostrecová, E., Jókay, M., Kostrec, M. (2010) *Computer crime*, Bratislava: Slovak Technical University.
7. Matějka, M. (2002) *Computer crime*, Prague: Computer Press.

NOVI OBLICI DIGITALNOG KRIMINALITETA U SLOVAČKOJ I NJIHOVO SUZBIJANJE

U ovom radu predstavljeni su novi oblici digitalnog kriminaliteta koji su prisutni u Slovačkoj poslednjih godina. U radu je ukazano na način vršenja krivičnih dela koja spadaju u navedeni vid kriminaliteta, kao i na ugroženost žrtava njihovim posledicama. Glavni fokus je na različitim vrstama prevara na inernetu i sredstvima mobilne komunikacije, kao i na novim oblicima zloupotrebe kreditnih kartica i internet plaćanja. U radu su predstavljeni stvarni slučajevi iz Slovačke koji su zabeleženi u praksi Okružnog tužilaštva u gradu Malacki u Slovačkoj. Autor se u radu osvrće na specifične probleme u vezi sa sprovođenjem istrage za ovu vrsu kriminaliteta, na digitalne dokaze i oblike međunarodne saradnje u prikupljanju elektronskih dokaza, probleme u vezi sa sprovođenjem "elektronskog naloga za istragu", kao i na druge oblike međunarodnih akata koji bi se mogli koristiti za obezbeđivanje dokaza od zemalja koje nisu članice Evropske unije. U poslednjem delu rada, autor ukazuje na metode prevencije koje je neophodno primeniti u cilju suzbijanja digitalnog kriminaliteta.

KLJUČNE REČI: *kompjuterski kriminalitet, prevara, kleveta, pretnje, pornografija.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.03

FALSIFIKOVANJE I ZLOUPOTREBA BEZGOTOVINSKIH INSTRUMENATA PLAĆANJA I EVROPSKI STANDARDI

Zoran Pavlović*

Opšta društvena digitalizacija i dinamične promene življenja, uz sve veću upotrebu i rasprostranjenost „pametnih" telefona, sa mnogim različitim sadržajima koje nude, dovode do pojave novih relacija između banaka, kupaca i prodavaca, koje se odnose na savremena poslovanja sa platnim karticama. Plaćanja se obavljaju, nezavisno od toga da li se radi o tradicionalnom ili on line poslovanju, a savremeno bankarstvo je u stalnoj potrazi za što optimalnijim načinom plaćanja uz korišćenje novih tehnoloških i komunikacionih rešenja. Transakcije platnim karticama su česta meta za izvršenje krivičnih dela, što nije izazov samo za zakonodavca da postavi pravni okvir zaštite, već i za organe otkrivanja i judikaturu. Evropski standardi koji se formulišu nastoje da odgovore na te izazove, što zahteva i implementaciju u domaće zakonodavstvo. Direktiva Evropskog parlamenta i Saveta 2019/713/EU o borbi protiv prevara i falsifikovanja u vezi s bezgotovinskim sredstvama plaćanja upravo pruža osnov za zaštitu bezgotovinskih instrumenata plaćanja, u skladu sa zahtevima koji se postavljaju u vezi sa plaćanjima danas i kaznenopravnom reakcijom u domaćem zakonodavstvu.

KLJUČNE REČI: *platne kartice, rizik plaćanja, informatički kriminalitet.*

* Doktor pravnih nauka, redovni profesor Pravnog fakulteta Univerziteta Privredna akademija u Novom Sadu, Professor et dr h. c. Univerziteta u Pečuju, Mađarska. E-mail: *zoran.pav@hotmail.com*

UVOD

Savremene modele platnih usluga danas nemoguće je zamisliti bez platnih kartica, bilo kontaktnih ili bezkontaktnih, koje su danas skoro u potpunosti potisnule upotrebu gotovog novca i/ili čekova. Iako je prvi elektronski transfer novca telegrafom *via* Western Union zabeležen još 1860.godine, još dugo nakon toga je upotreba platnih kartica pripadala sferi naučne fantastike i tehnoloških predviđanja. Na Ruzveltovoj predsedničkoj fotografiji u Beloj kući iz 1933.vidi se i naslov knjige E. Belamija iz 1888.godine „Pogled unazad" (Immerwahr, 2021). To je priča o čoveku koji je zaspao 1887. i probudio se 2000. u elektrificiranom gradu, uz muzičke emisije, u društvu gde se više ne koristi gotov novac već - kreditne kartice! U Sjedinjenim Državama 19. veka Belamijev utopijski roman Pogled unazad bio je posle Čiča Tomine kolibe najprodavanija knjiga u prvim godinama izdanja.[1]

Ipak, nešto manje od veka trebalo je da prođe od 1888. da bi se bezgotovinski način plaćanja roba i usluga kao rezultat tehnološkog i digitalnog razvoja utvrdio kao oblik plaćanja. Futurističku ideju oživeo je Franc McNamara stvaranjem Diners kluba kao instrument plaćanja za poslovne ljude, sa Corporate Card kojom bi mogli brzo da prikažu svoj finansijski kredibilitet (Pavlović, 2006: 164).

Platne usluge izvršene platnim karticama danas su u EU najrašireniji oblik platnih usluga. I upravo zbog toga su kao takve vrlo često izazov i meta mnogim pojedincima i organizovanim kriminalnim grupama, koji kroz falsifikovanje i zloupotrebe ovih sredstava plaćanja ostvaraju veliku protivpravnu imovinsku korist. Komad plastike na kome se nalazi sredstvo za identifikaciju u obliku potpisa ili slike postao je tako izuzetno često sredstvo falsifikovanja. Od *skimminga* ili kopiranja podataka sa magnetne trake bankarske kartice, koji se kopiraju najčešće na bankarskim automatima, preko zloupotrebe POS (*point of sales terminals*) aparata putem manipulacija i falsifikovanja istih, do krađe identiteta. Naime, *phishing* se sa sve širom primenom globalnog virtuelnog autoputa - Interneta sa preuzimanjem ličnih podataka i slanjem prevarnih e-mailova pretvorio u profitabilan posao za mnoge izvršioce IKT krivičnih dela. Putem *pharminga*, odnosno zloupotrebom internet domena (umesto google.com postavlja se na primer google.org kao lažna stranica) žrtva se preusmerava na lažnu *web* stranicu, gde se onda vrši preuzimanje novca kroz lažnu transakciju (Clough: 2015).

U bankarskom sektoru Srbije se pojavljuju ovakve zloupotrebe, pa je Narodna banka Srbije identifikovala lažnu internet stranicu pod nazivom DinaKartica - Srbija, na kojoj se traži ostavljanje podataka i preduzela mere radi sprečavanja prevarne aktivnosti i otkrivanje počinilaca krivičnog dela. Narodna banka Srbije je saopštila da se stranica lažne kartice nalazi na adresi: www.dinakartica.com i da koristi ime i logo sistema DinaCard. Na lažnoj stranici od korisnika Dina kartica, u sklopu promotivne akcije,

[1] https://www.nytimes.com/1988/01/17/books/looking-back-at-looking-backward-we-have-seen-the-future-and-it-didn-t-work.html, [21.10.2022.].

https://archive.nytimes.com/www.nytimes.com/books/00/12/24/bookend/bookend.html, [21.10.2022.].

zahteva se da ostave podatke s platne kartice.[2] Ovo je bila dvostruka zloupotreba oglašene stranice, imajući u vidu da se radi o prikupljanju podataka o platnoj kartici ali i ličnih podataka, ugrošavajući i ljudsko pravo na privatnost.

Prevare sa internet bankarstvom, kreditnim (platnim) karticama i krađom identitteta su se dodatno počele usavršavati zbog sve šire upotrebe sigurnijih kreditnih kartica sa čipom. Dakle, radi se o krivičnim delima zloupotrebe i falsifikovanja platnih kartica kod plaćanja gde u stvari nije potrebno ni prikazati karticu u njenom fizičkom obliku.[3]

Sve ovo uslovilo je u okvirima Evropske unije stalno jačanje pravnog okvira unapređenja mera za sprečavanje ovih vrsta zloupotreba. Prvi korak u zaštiti platnih usluga bila je Okvirna odluka Saveta 2001/413/PUP o borbi protiv prevara i falsifikovanja bezgotovinskih sredstava plaćanja.[4] Kao takva Direktiva je bila na određeni način sa svojim rešenjima implementirana i u nacionalno zakonodavstvo Srbije jer je i ranijim krivičnim zakonom RS imala neka krivična dela koja su odgovarala onima propisanima u Okvirnoj odluci (Pavlović, 2006). Od tada do danas došlo je do mnogih promena u stvarnom životu i načinima plaćanja robe i usluga. Kupovina preko interneta, mobilni novčanici, kriptovalute, elektronski novac i druga visokotehnološka dostignuća doprinela su prekograničnom širenju zabranjenih radnji sa bezgotovinskim sredstvima plaćanja, što višestruko povećava izazove u otkrivanju, dokazivanju, gonjenju, nadležnostima ali i presuđivanju kod zloupotreba i falsifikovanja bezgotovinskih instrumenata i oblika plaćanja.

Funkcionalna zajednica digitalnog društva nije moguća bez sveobuhvatnijeg pravnog instrumenta koji bi služio prvo prevenciji, a onda i represiji u odnosu na krivična dela prevare, zloupotrebe i falsifikovanja bezgotovinskih instrumenata plaćanja. Sam naslov rada ima za cilj da odredi predmet analize, ali ne i da se ograniči na jedno krivično delo i krivičnopravnu zaštitu bezgotovinskih oblika plaćanja, već da analizom relevantnih evropskih standarda, ponudi temu za razgovor o unapređenju pravne zaštite.

Ali, krenimo redom.

1. JEDAN PRIMER I NEKOLIKO PITANJA

Tokom avgusta 2018.godine su pred američkim pravosuđem optužena trojica ukrajinskih državljana, kao članovi hakerske grupe FIN7 (Carbanak ili Cobalt). U optužnici je navedeno da je grupa FIN7 ukrala više od 15 miliona brojeva platnih kartica sa više od 6000 POS (point-of-sale) terminala, na više od 3600 lokacija. Optuženi su zarađivali od prodaje podataka o platnim karticama na Dark Webu. Optužbe su se odnosile na krivična dela izvršena protiv američkih kompanija, ali je grupa jednako hakovala i kompanije u Velikoj Britaniji, Australiji i Francuskoj.

[2] https://www.euronews.rs/biznis/biznis-vesti/42178/narodna-banka-srbije-upozorila-gradane-na-prevaru-sa-laznim-dina-karticama-ne-ostavljate-licne-podatke/vest, [2.10.2022.].

[3] https://what-europe-does-for-me.eu/, [2.10.2022.].

[4] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32001F0413.

Svi napadi bi započinjali tako što su hakeri slali *spear* fišing emailove svojim ciljevima. Emailovi su navodno slali legitimni poslovni partneri ili saradnici a oni su sadržali priloge sa malicioznim softverom. Grupa je bila veoma kreativna, a posebno kada su bili u pitanju *spear* fišing emailovi. Na primer, grupa je često ciljala službe za podršku korisnicima kako bi upala u veće korporacije. Često su pozivali i tvrdili da imaju problema sa određenom uslugom ili proizvodom, a kasnije bi emailom slali maliciozni dokument predstavniku podrške za korisnike, tvrdeći da dokument sadrži detalje o problemu.

Kada bi hakeri dobili pristup sistemima, a posebno sistemima banaka, izabrali bi jedan od tri načina na koji su krali novac. Prvi je podrazumevao koordinaciju sa grupama pomagača (*money mule*), izbacivanje novca iz bankomata u unapred određenom satu i danu. Pomagači bi pokupili novac, i pošto bi uzeli svoj deo, ostatak novca je završavao u rukama članova grupe FIN7. Drugi način je podrazumevao da grupa prebacuje novac sa legitimnih računa na svoje račune ili račune pomagača, koji bi onda ispraznili račune na bankomatima ili koristili račune za kupovinu skupih proizvoda i pranje novca. Treće, izvršioci krivičnih dela bi koristili pristup internoj mreži banke kako bi veštački uvećali saldo na računima koje bi pre toga otvorili pomagači, bez prenosa sredstava sa drugih računa. Mule bi kasnije ispraznile ove veštački napunjene račune. Nešto od "zarađenog" novca, grupa je prala preko kriptovaluta ali su koristili i pripejd kartice povezane sa novčanicima kriptovaluta, kojima su kupovali robu kao što su luksuzni automobili, umetnički predmeti ili kuće.[5]

Ovako opisana aktivnost transnacionalne organizovane kriminalne grupe, koja je radila u izvornom sastavu od 2013. do 2018. godine (a prema izveštajima EUROPOLa te aktivnosti traju i dalje, sa drugim izvršiocima), pokazuju da se razvija novi oblik kriminaliteta u vezi sa bezgotovinskim instrumentima plaćanja, što uključuje i mere za borbu protiv IT kriminaliteta, bez čega nema ni nacionalne ni evropske bezbednosti. Osim kao bezbednosna sajber pretnja na kritičnu infrastrukturu, ova krivična dela predstavljaju branu razvoju digitalnog tržišta. To vodi jačanju nepoverenja korisnika u bezbednost bezgotovinskih instrumenata plaćanja, što posledično vodi padu prometa i gubicima.[6]

Samo pravovremenom reakcijom na ovakve zabranjene radnje, dobrim zakonodavnim okvirom i prekograničnom saradnjom moći će se ovakve posledice smanjivati ili svesti na minimum. Rešenja iz Okvirne odluke nisu dala odgovor na pitanja vezana za nadležnost, mehanizam za informisanje javnosti i zahteve za prijavljivanje prevara sa bezgotovinskim instrumentima plaćanja. Sve ovo, motivisalo je Evropski parlament i Savet za donošenje nove Direktive 2019.godine.

[5] https://www.informacija.rs/Sajber-hronika/SAD-optuzile-clanove-grupe-Carbanak-za-kradju-15-miliona-kreditnih-kartica.html, [22.10.2022.].

[6] https://www.europol.europa.eu/media-press/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain, [22.10.2022.].

2. DIREKTIVA 2019/713/EU

2.1. Opšte karakteristike

Direktiva dopunjava Okvirnu odluku i Direktivu EP i Saveta (2013/40/EU), jer ranija rešenja precizira, uključujući pored klasičnih oblika falsifikovanja i prevara u vezi sa instrumentima plaćanja sada i digitalne falsifikate i prevare, sredstava koja nisu u fizičkom obliku. Neki krivična dela su zastarela, kao što su ona u vezi sa euro-čekovima. Predviđa se prekogranična saradnja, kazne za fizička lica koja izvrše krivična dela određena su sa minimumom i maksimumom, predviđa se *on line* razmena informacija između država, ali i *on line* prijava prevara ove vrste. Posebna zaštita predviđena je za žrtve ovih krivičnih dela u odnosu na negativne posledice i drugo. Direktiva predviđa da će Komisija do 31. maja 2023. EP i Savetu podneti izveštaj o nacionalnim usklađenostima zakonodavstava sa Direktivom, a za još 3 godine i izveštaj o uspostavljanju *on line* sistema za prijave krivičnih dela i za pomoć i podršku žrtvama.

2.2. Krivična dela iz Direktive

Krivična dela su u Direktivi podeljena u tri grupe. U prvoj su krivična dela prevara i falsifikovanja platnih kartica u fizičkom obliku, drugu čine krivična dela istih koji nisu u fizičkom obliku, kao što su virtuelne valute, e-novčanici i sl., a treću čine krivična dela koja su u vezi sa informatičkim sistemima. Sama Direktiva vrši razlikovanje bezgotovinskih instrumenata plaćanja u fizičkom i nefizičkom obliku.

Prvo krivično delo iz prve gruge inkriminacija odnosi se na prevarnu upotrebu bezgotovinskih instrumenata plaćanja, a koja se sastoji u upotrebi ukradenog ili na drugi način nezakonito prisvojenog ili stečenog bezgotovinskog instrumenta plaćanja s ciljem prevare i uptrebi lažnog ili falsifikovanog bezgotovinskog instrumenta plaćanja u cilju prevare. To krivično delo može se izvršiti samo sa umišljajem, i za njega Direktiva propisuje maksimalnu kaznu zatvora u trajanju od najmanje dve godine. Drugo krivično delo odnosi se na izvršenje „a) krađe ili drugog nezakonitog prisvajanja bezgotovinskog instrumenta plaćanja koji je u fizičkom obliku, b) pravljenja lažnog ili falsifikovanog bezgotovinskog instrumenta plaćanja koji je u fizičkom obliku u cilju prevare, c) posedovanja ukradenog ili na drugi način nezakonito prisvojenog ili napravljenog bezgotovinskog instrumenta plaćanja koji je u fizičkom obliku radi upotrebe u cilju prevare, kao i d) pribavljanje za sebe ili druge, uključujući primanje, prisvajanje, kupovinu, prenos, uvoz, izvoz, prodaju, prevoz ili distribuciju ukradenog, lažnog ili falsifikovanog bezgotovinskog instrumenta plaćanja koji je u fi zičkom obliku radi upotrebe u cilju prevare". To krivično delo odnosi se na protivpravno raspolaganje tuđim platnim karticama. Direktiva za krivična dela iz tačke a) i b) maksimalnu kaznu zatvora u trajanju od najmanje dve godine, a za radnje iz tačke c) i d) maksimalnu kaznu zatvora u trajanju od najmanje jedne godine.

Krivična dela iz druge grupe inkriminacija (čl. 5. Direktive) odnose se na prevare s bezgotovinskim instrumentima plaćanja u nefizičkom obliku. Pri tome je Direktiva odredila definiciju bezgotovinskog instrumenta plaćanja, kao „zaštićeni uređaj, predmet ili zapis ili njihovu kombinaciju, osim zakonskih sredstava plaćanja, koji može ali i ne mora biti u fizičkom obliku, a koji korisniku omogućava, samostalno ili u vezi s postupkom, odnosno nizom postupaka, transfer novca ili ekvivalentne vrednosti, uključujući i digitalna sredstva razmene".

Sam pojam bezgotovinskog instrumenta plaćanja u kontekstu ovih krivičnih dela podrazumeva mogućnost stvarnog transfera novca, novčane vrednosti ili aktivirati platni nalog. To znači da se ne može smatrati nezakonitim samo nezakonito prisvajanje mobilne aplikacije za plaćanje, ako se nema adekvatna šifra za pristup.

U odnosu na izvršenja ovih krivičnih dela bezgotovinskim instrumentom plaćanja treba da se ostvari funkcija plaćanja. Također, za postojanje tih krivičnih dela nije relevantno o kojoj se količini novca radi.

Oblici izvršenja krivičnog dela u vezi sa bezgotovinskim instrumentom plaćanja u nefizičkom obliku jesu: „a) nezakonito sticanje bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku, ili zloupotrebu bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku, b) pravljenje ili falsifikovanje bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku u svrhu prevare, c) držanje nezakonito stečenog, napravljenog ili falsifikovanog bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku radi upotrebe u svrhu prevare, bar ako je u trenutku držanja instrumenta poznato njegovo nezakonito poreklo, d) nabavljanje za sebe ili druge, uključujući prodaju, prenos i distribuciju ili stavljanje na raspolaganje nezakonito stečenog, napravljenog ili falsifikovanog bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku radi upotrebe u cilju prevare." Za oblike tog krivičnog dela pod a) i b) Direktiva normira maksimalnu kaznu zatvora u trajanju od najmanje dvije godine, a za oblike izvršenja pod c) i d) maksimalnu kaznu zatvora u trajanju od najmanje jedne godine.

U treću grupu inkriminacija prema čl. 6. Direktive ulaze krivična dela u vezi s prevarama sa ifnormatičkim sistemima, i to umišljajni prenos ili prouzrokovanje prenosa novca, novčane vrednosti ili kriptovaluta i time uzrokovanje nezakonitog gubitka imovine za drugoga u cilju sticanja nezakonite koristi za izvršioca ili nekog drugog ako je izvršeno: a) neovlašećenim sprečavanjem ili ometanjem funkcionisanja informatičkog sistema; b) neovlašećenim uvođenjem, izmenom, brisanjem, prenosom ili prikrivanjem računarski podataka. Za ova krivična dela Direktiva propisuje maksimalnu kaznu zatvora u trajanju od najmanje tri godine. Pored propisanih krivičnopravnih sankcija Direktiva zahteva da države članice propišu strože kazne (maksimalnu kaznu zatvora u trajanju od najmanje pet godina) ako je krivično delo izvršeno u okviru organizovane kriminalne grupe, a prema definiciji Okvirne odluke Saveta o borbi protiv organizovanog kriminaliteta.

Što se tiče oblika krivice, jasno je da se ova krivčna dela mogu izvršiti isključivo sa umišljajem, i to direktnim umišljajem. Ali, pitanje za kažnjavanje za pokušaj je ovde stvar za diskusiju (Jovašević, 2021: 57). Kada će se smatrati da je izvršilac ostao u kažnjivom pokušaju kod krivičnih dela u vezi sa prevarom ili pravljenjem bezgotovinskog instrumenta

plaćanja u nefizičkom obliku? Šta raditi ako izvršilac neovlašćeno pristupi aplikaciji drugog lica za plaćanje ili aktiviranje platnog naloga, ali ne izvrši transakciju jer na računu žrtve nije bilo sredstava. Hoće li on u tom slučaju odgovarati za pokušaj krivičnog dela zloupotrebe bezgotovinskog instrumenta plaćanja u nefizičkom obliku ili će se zadržati na kažnjavanju za neko drugo krivično delo, npr. Neovlašćeni pristup?

U praksi je teško dokazati cilj – umišljajno postupanje, naročito u slučaju ako se krivično delo nije realizovalo. Ali, pokušaj je društveno opasno delo i uvek bi u ovakvim slučajevima trebalo imati u vidu da postoji opasnost ugrožavanja za pravno dobro. Izvršilac je želeo da dođe do protivpravne imovinske koristi, pa treba i da odgovara za put do povrede, bio on pogrešan ili ispravan.

Direktiva preporučuje da se pokušaj inkriminiše kao takav i bude kažnjiv kod skoro svih krivičnih dela a naročito pokušaj prbavljanja nezakonito stečenog, napravljenog ili falsifikovanog bezgotovinskog instrumenta plaćanja koji nije u fizičkom obliku za sebe ili druge s ciljem prevare. Direktiva predviđa i odgovornost pravnih lica za navedena krivična dela, i daje preporuku državama da preduzmu mere za uspostavljanje krivične odgovornosti u skladu sa opštim pravilima o tome.

3. BEZGOTOVINSKI OBLICI PLAĆANJA I MOGUĆE ZLOUPOTREBE LJUDSKIH PRAVA

Neposredno nakon donošenja Direktive 2019/713/EU došlo je do globalne epidemije izazvane virusom SARS-Cov-2 COVID19, koji je svoje posledice ostavio i na bezgotovinska (nefizička) plaćanja u EU. Koristeći se korona merama od početka 2020. povećan je broj učesnika u bezgotovinskim oblicima plaćanja, uz moto da plaćanje karticama ili smartphoneom nije samo brže, nego je i higijenski prihvatljivije. Ovakva preporuka bila je data ne samo u državama EU, već se mogla videti i kao preporuka Narodne banke Srbije.[7] U kontekstu rešenja iz same Direktive, želimo da ukažemo ne samo na povećanje bezgotovinskih oblika plaćanja i zloupotreba, već i na moguće kršenje ljudskih prava u kontekstu ovih krivičnih dela, o čemu je reč i u samim rešenjima iz Direktive.

Tako je prema podacima Centralne banke Nemačke do povećanog obima plaćanja platnim karticama došlo od 2018. godine, a naročito od početka pandemije. U 2021. godini maloprodajni objekti su 56% prometa ostvarili preko bezgotovinskog plaćanja, čime je Nemačka negdje u sredini lestvice. U Luksemburgu, Francuskoj ili Estoniji ljudi češće plaćaju karticom. Na samom vrhu lestvice su skandinavske zemlje. Tamo mnogi hoteli, trgovački centri i drugi uopšte ne žele prihvatiti plaćanje novčanicama. U Švedskoj 82% ljudi u međuvremenu plaća bezgotovinski. U celoj EU se elektronsko plaćanje „reklamira" kao siguran i brz način plaćanja, odnosno kao „higijenska mjera".[8]

[7] https://www.rtv.rs/sr_lat/ekonomija/aktuelno/nbs-savetuje-gradjanima-da-koriste-bezgotovinsko-placanje_1103241.html, [22.10.2022.].

[8] https://www.dw.com/hr/korona-ubrzala-smrt-gotovinskog-pla%C4%87anja/a-56144847, DW 21-7-2021, [22.10.2022.].

Pandemija je pokazala građanima ali i donosiocima odluka koliko je bezgotovinsko plaćanje praktično, pa je Evropska Komisija digitalizaciju i bezgotovinski način plaćanja proglasila vrhovnim prioritetima – odmah nakon zaštite klime.

Ono što Direktiva 2019/713/EU ukazuje u vezi krivičnopravne reakcije na zloupotrebe bezgotovinskih plaćanja može da ima i još jednu dimenziju, koja se tiče oblasti ljudskih prava, i to u sferi zaštite podataka o ličnosti ili prava na slobodu kretanja. Ovo se naročito odnosi na plaćanja uz pomoć smartphonea, odnosno u onim situacijama kada se tokom procesa plaćanja mora na tastaturi upisati i PIN. To je slučaj pre svega kod takozvane NFC-komunikacije. Ta tehnika se koristi uglavnom kod beskontaktnog plaćanja manjih iznosa. Mnoge benzinske stanice ili diskonti su opremljeni takvim uređajima za plaćanje karticama bez kontakta, odnosno NFC-čitačima. A da bi se i mobilni aparati povezali sa uređajem potrebno je instalirati jednu aplikaciju. Koliko je taj način plaćanja u međuvremenu značajan, može se dobro videti u Holandiji. Tamo je NFC-plaćanje popularno, a od 2019 tako se obavlja najveći broj transakcija, više i od gotovinskog plaćanja, odnosno klasičnog plaćanja putem kartice.

To nije potpuno neproblematično, ali ni posebno obrađeno Direktivom, jer mobilni uređaji nisu u potpunosti zaštićeni od napada hakera. Ljudi koji tako kupuju stvari, ujedno i otkrivaju gde su – kupovali. A te podatke o lokaciji kupovine neke aplikacije evaluiraju i pohranjuju, iz bezbednosnih razloga. Kuda sve to vodi? I bez unošenja ličnih podataka na ovaj način se vrši prikupljanje podataka o kretanju lica koje je izvršilo plaćanje, kao i gde se nalazi. Koliko se ovim vrši ugrožavanja prava iz Evropske konvencije o ljudskim pravima?! U SAD-u Google već sada ima pristup velikom broju podataka kreditnih kartica i s njima može ciljano upravljati reklamama za trgovce na licu mesta, može ih analizirati, vršiti ponude vlasnicima računa i skuplje prodavati određene proizvode ili usluge. Ali, ovo bi već bila tema nekog drugog rada, sa drugačijim krivičnopravnim rešenjima koja nas kao izazov tek očekuju.

4. REŠENJA U KRIVIČNOM PRAVU SRBIJE U VEZI SA FALSIFIKOVANJEM I ZLOUPOTREBOM BEZGOTOVINSKIH OBLIKA PLAĆANJA

Analizom pozitivnog krivičnog zakonodavstva u vezi sa falsifikovanjem i zloupotrebom bezgotovinskih instrumenata plaćanja jasno je da je zakonodavac propisao posebno krivično delo protiv privrede vezano za zloupotrebe platnih kartica (član 243. KZ), ali i druga krivična dela koja se mogu podvesti pod krivična dela u vezi sa prevarama i falsifikovanjem bezgotovinskih instrumenta plaćanja iz Direktive. Ta krivična dela podeljena su u različite glave Krivičnog zakonika (dalje u tesktu: KZ). Imajući u vidu objekt krivičnopravne zaštite i cilj ta bi krivična dela mogla da budu u posebnoj glavi krivičnih dela. U ovom radu nećemo posebno izdvajati ni jedno krivično delo a u vezi odredbi Direktive, kako bi to možda bilo kod tradicionalnih naučnih radova napisano, imajući u vidu obim rada, ali i množinu krivičnih dela u našem krivičnom zakoniku, već ćemo dati isključivo opšti osvrt.

Imovina kao objekt zaštite u pogledu tih krivičnih dela dolazi u nematerijalnom obliku. Istovremeno, mogla bi isto tako i da budu u grupi krivičnih dela protiv privrede. U vezi umišljaja u našem krivičnopravnom sistemu postoji nekoliko oblika prevara (u privrednom poslovanju, računarska prevara, subvencijska, izborna...), kao i falsifikovanje (falsifikovanje novca, računarsko, falsifikovanje isprava itd.) Za potrebe ovog rada treba dakle posebno označiti i krivična dela protiv bezbednosti računarskih podataka. Ali ono što razlikuje računarsku prevaru od prevare sa bezgotovinskim instrumentom plaćanja u nefizičkom obliku jeste funkcija plaćanja. Da bi postojalo krivično delo prevare sa bezgotovinskim instrumentom plaćanja, treba doći do funkcije plaćanja ili bar do pokušaja, a kod računarske prevare isti se cilj (sticanje protivpravne imovinske koristi) ostvaruje drugim radnjama izvršenja: unosom, izmenom, brisanjem, oštećenjem itd.

Analizom Glave Direktive u vezi sa krivičnim delima, možemo konstatovati da je naš Krivični zakonik već usklađen sa članom 4- 6 Direktive i da se modaliteti izvršenja krivičnih dela iz Direktive mogu podvesti pod već postojeće inkriminacije u okviru Krivičnog zakonika (Stojanović, 2021).[9] Ali, za razliku od Direktive koja vrlo precizno ovu problematiku obrađuje na jednom mestu, jasno je da se u našem krivičnom zakonodavstvu ona nalazi na različitim mestima i zaštitnim objektima. Posebno treba imati u vidu da se kao izvršioci ovih krivičnih dela pojavljuju i pojedinci, ali i posebno organizovane kriminalne grupe, koje koristeći moderne tehnologije pri izvršenju tih krivičnih dela i ne moraju da pojedinačno znaju jedni za druge, i da vrše radnje koje su kao takve inkriminisane. Pored zatvorskih kazni već predviđenih u našem zakonu, čini se da bi se moglo pronaći prostora i za uvođenje nove mere bezbednosti u vezi sa ovim krivičnim delima, kada je ono izvšreno putem internet, odnosno meru bezbednosti zabrane pristupa internetu ukoli postoji opasnost da bi se novom zloupotrebom intereneta moglo ponovo izvršiti krivično delo.

Dakle, u odnosu na odredbe krivičnog materijalnog prava, standardi utanovljeni Direktivom mogu da se grupišu u navedene tri grupe zaštitnog objekta (krivična dela protiv imovine, krivična dela protiv privrede i protiv računarskih podataka), ali povrede ovih prava u vezi sa bezgotovinskim sredstvima plaćanja i nekim od posledica mogu da se štite i drugim krivičnim delima. Tako bi bilo sa krivičnim delima protiv sloboda i prava čoveka i građanina, gde je krivično delo neovlašćeno prikupljanje ličnih podataka iz čl.146., jer to delo može da bude posledica zloupotrebe bezgotovinskih sredstava plaćanja, kao i kod krivičnih delima protiv pravnog saobraćaja, gde je krivično delo falizfikovanja isprave iz člana 355. i drugo.

Množina krivičnih dela kojima se štite bezgotovinski oblici plaćanja, zahtevaju u odnosu na rešenja u materijalnom krivičnom zakonodavstvu diskusiju o njihovom mogućem prekomponovanju u posebnu glavu u KZ, uz neophodno usklađivanje Zakona o platnim uslugama koji je donet 2018.godine, dakle pre Direktive, gde bi se određene blanketne odredbe trebale svakako nalaziti.

Uvažavajući ipak obim rada, ovde nećemo iznositi analize pojedinih krivičnih dela, već smo samo ukazali na neophodnost pravljenja sistema zaštite kod bezgotovinskih oblika plaćanja (uključujući i platne kartice), gde je KZ samo jedan od delova te zaštite.

[9] Prečišćeni tekst KZ naveden kao deo Komentara sadrži u sebi stanje zakonodavstva sa 1.12.2019.,gde se nalaze krivična dela predviđena Direktivom.

Slično je i sa krivičnom odgovornošću pravnih lica, gde samo možemo da konstatujemo usklađenost Zakona sa odredbama Direktive. Ono što ovde želimo da naglasimo, jeste da što se tiče usklađenosti kaznenih odredbi i standarda iz Direktive za krivičnim pravom Srbije nije neophodno njihovo doslovno preuzimanje, jer u najvećoj meri sankcije za nabrojane zabranjene radnje iz Direktive već postoje sankcije u krivičnom zakoniku.

U odnosu na procesne odredbe Direktive koje se odnose na delotvorne (čitaj efikasne) istrage protiv sve tri grupe krivičnih dela iz nje, a naročito imajući u vidu da ova krivična dela nemaju samo nacionalni, već i prekogranični značaj i posledice, Direktiva opominje da se preduzmu potrebne mere radi što bržeg otkrivanja i procesuiranja ovih krivičnih dela. Činjenica je da je u najvećem reč o elektronskim dokazima, pri čemu su digitalni zapisi izuzetno važni u tom kontekstu, ali i da je sa njima izuzetno jednostavno manipulisti.

Iako sama Direktiva poziva nacionalna zakonodavstva na krivičnopravnu reakciju, upravo transnacionalni oblik izvršenja i posledica krivičnih dela protiv bezgotovinskih sredstava plaćanja ukazuje na prekograničnu situaciju i saradnju.

U navedenom primeru sa tri optužena jasno je da su izvršioci iz više različitih država izvršavali protivpravne radnje: neovlašćeni pristupi aplikacijama bili su u jednoj državi, transfer novca u drugoj, a posledice su nastupale nezavisno od toga na teritoriji potpuno treće države. U takvim situacijama koriste se različiti elektronski dokazi, od IP adrese, istorije pretraživanja, elektronske pošte i drugo.

Stoga bez pravosudne i policijske saradnje ne može biti ni preventivnog ni represivnog rada u cilju pružanja operativne i svake druge podrške. U Srbiji već postje posebne jedinice koje se bave u okviru tužilačke organizacije ili MUP-a borbom protiv visokotehnološkog kriminaliteta, gde bi ulazila i krivična dela gde se zloupotrebljavaju bezgotovinski instrumenti plaćanja.

Da bi imali zadovoljavajuće rezultate, a u okviru stvarne a ne samo deklaratorne implementacije odredbi analizirane Direktive, neopho je da nadležne organizacione jedinice MUP-a i tužilaštva budu opremljeni sa softverskim i hardverskim komponentama i da budu dovoljno edukovani u radu sa digitialnim dokazhima i forenzičkim metodama i procedurama.

Važnost borbe protiv zloupotreba u ovoj oblasti navela nas je da izvršimo uvid i u programe edukacije nosilaca pravosudnih funkcija u cilju potpune implentacije odredbi Direktive, pa smo ostali uskraćeni za odgovor o vrsti i količini znanja koju sudije i tužioci imaju u ovoj oblasti, jer bi obuka trebala da bude permanentna i da obuhvati sve tužioce i sudije koji se bave ovom materijom. Reč je o kontinuiranoj edukaciji, a ne o projektnoj inicijativi, i na sajtu NBS nije pronađena ni jedna edukacija sa pravosuđem u vezi primene ove Direktive.

Ali, kako smo već više puta naveli, Republika Srbija jeste u najvećoj meri uskladila svoje zakonodavstvo sa odredbama Direktive. Odredbe koje bi trebalo poboljšati tiču se dakle eventualnog redefinisanja mesta određenih krivičnih dela u sistematici KZ, uspostavljanja operativnih tela ne samo na nivou policije već i tužilaštava i sudova za sprovođenje delotvornih istraga za ova krivična dela, i poslednje ali ne i najmanje važno, da se obebzedi podrška i pomoć žrtvama ovih krivičnih dela. Jer, to nije samo u odnosu na žrtvu obligacioni odnos između oštećenog i banke, već je i stvar javnog interesa.

ZAKLJUČAK

Ubrzani procesi korišćenja „novih" platnih usluga u poslednje vreme su ipak imali i svoj „bum", koji se povezuje za globalnom epidemijom izazvanom virusom COV19, što je učvrstilo primat bezgotovinskog oblika plaćanja kao osnovnog u plaćanjima i roba i usluga u svim zemljama EU i van nje. Ali, takve transakcije su često praćene negativnim posledicama kroz različite oblike prevara sa platnim karticama. Zloupotrebe bezgotovinskih sredstava plaćanja su u uzlaznoj liniji od trenutka stalnog povećanja izdatih platnih kartica koje su u upotrebi, dakle od 2008. godine. Prevare ovog tipa predstavljaju oblik informatičkog kriminaliteta koji je rezultat tehnološkog razvoja i sve različitijih metoda kojima se služe kriminalne grupe pri njihovom izvršenju, bez obzira na državne granice i jurisdikcije. Kriminalne grupe su se brzo prilagodile i koriste situaciju za različite oblike krivičnih dela zloupotreba sa bezgotovinskim, nefizičkim instrumentima plaćanja.

Europol[10] upozorava da će IT kriminalci pratiti stanje na tržištu i razvoju platnih usluga, kroz uvođenje različitih softvera u cilju internetskih napada. Savremeni oblici krivičnih dela zloupotreba i falsifikovanja bezgotovinskih instrumenata plaćanja događaju se svakodnevno i pogađaju sve sfere društva. Zato je važno da zemlje članice EU-a, ali i zemlje kandidati kao i zemlje koje pripadaju evropskoj pravnoj tradiciji zaista implementiraju u svoja domaća zakonodavstva nove inkriminacije kojima će se realizovati zaštita takvih transakcija.

U odnosu na Srbiju možemo zaključiti da je postojeći krivičnopravni okvir već u skladu sa Direktivom u vezi krivičnih dela koja inkriminiše Direktiva na način da u nedostatku bukvalnih rešenja i inkriminacija za svaku situaciju iz Direktive se koristimo postojećim inkriminacijama (krađa, falsifikovanje isprave, prevara i dr.), čime se ostvaruju radnje pojedinih krivičnih dela iz Direktive. Međutim, u odnosu na zaštitu podataka o ličnosti, neovlašćenom prikupljanju podataka i drugo, što može da bude posledica izvšrenja krivičnih dela u vezi sa bezgotovinskim sredstvima plaćanja, u ovom trenutku još uvek nemamo dovoljnu društvenu reakciju nadležnih institucija.

Implementacija bi se najprvo odnosila na uspostavljanje operativnih tela za prekograničnu saradnju i vođenje delotvornih istraga za ta krivična dela, kao i obezbeđivanje podrške i pomoći žrtvama. Ni jednog trenutka ne smemo izgubiti iz vida prava oštećenog iliti žrtve, i da u konkretnom slučaju nikako ne može biti izgubljeno iz vida, zbog koga se zaista krivični postupak vodi! Usklađenost domaćeg zakonodavstva i odredbi Direktive ne znači samo postojanje inkriminacija u nacionalnom kaznenom zakonodavstvu u celini, već i čitav niz drugih mera i aktivnosti kako bi se one i primenjivale, uz evenutalno uvođenje i nekih novih mera bezbednosti u krivičnom pravu. Pod drugim aktivnostima se pre svega misli na stalnu edukaciju profesionalaca, usvajanje novih znanja i praksi u radu relevantnih činilaca, kao i neophodnu specijalizaciju. Samo bi se na taj način došlo do zadatka definisanog kao stvaranje funkcionalne zajednice digitalnog društva uz adekvatan pravni mehanizam koji bi služio i prevenciji, represiji i zaštiti oštećenih u odnosu na krivična dela prevare, zloupotrebe i falsifikovanja bezgotovinskih instrumenata plaćanja, usklađenih sa evropskim standardima.

[10] V.sajt European Multidisciplinary Platform v.Criminal Threats, https://www.cepol.europa.eu/training-education/european-multidisciplinary-platform-against-criminal-threats, [22.10.2022.].

LITERATURA

1. *Clough, J. (2015) Principles of Cybercrime* 2nd Ed. Cambridge Unviersity Press.
2. Immerwahr, D. (2021) *Opinions, Guest essay - New York Times*, 2 juli 2021.
3. Jovašević, D. (2021) *Krivično pravo*, opšti deo, 5. izmenjeno i dopunjeno izdanje, Beograd: Dosije.
4. Pavlović, Z. (2006) „Krivičnopravna zaštita platnih kartica", XLIII Savetovanje Udruženja za krivično pravo i kriminologiju SCG, Zlatibor-Beograd, u: *Nova rešenja u krivičnom zakonodavstvu i dosadašnja iskustva u njihovoj primeni*, (Bejatović, S. (ur.)), Beograd: Udruženje za krivično pravo i kriminologiju SCG i Intermex, 164-171.
5. Stojanović, Z. (2021) *Komentar Krivičnog zakonika*, 9. izmenjeno i dopunjeno izdanje, Beograd: Službeni glasnik.

Internet izvori

1. https://www.nytimes.com/1988/01/17/books/looking-back-at-looking-backward-we-have-seen-the-future-and-it-didn-t-work.html, [21.10.2022.].
2. https://archive.nytimes.com/www.nytimes.com/books/00/12/24/bookend/bookend.html, [21.10.2022.].
3. https://www.euronews.rs/biznis/biznis-vesti/42178/narodna-banka-srbije-upozorila-gradane-na-prevaru-sa-laznim-dina-karticama-ne-ostavljate-licne-podatke/vest, [2.10.2022.].
4. https://what-europe-does-for-me.eu/, [2.10.2022.].
5. https://www.informacija.rs/Sajber-hronika/SAD-optuzile-clanove-grupe-Carbanak-za-kradju-15-miliona-kreditnih-kartica.html, [22.10.2022.].
6. https://www.europol.europa.eu/media-press/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain, [22.10.2022.].
7. https://www.rtv.rs/sr_lat/ekonomija/aktuelno/nbs-savetuje-gradjanima-da-koriste-bezgotovinsko-placanje_1103241.html, [22.10.2022.].
8. https://www.dw.com/hr/korona-ubrzala-smrt-gotovinskog-pla%C4%87anja/a-56144847 DW 21-7- 2021, [22.10.2022.].
9. https://www.cepol.europa.eu/training-education/european-multidisciplinary-platform-against-criminal-threats, [22.10.2022.].

FALSIFICATION AND ABUSE OF NON-CASH PAYMENT INSTRUMENTS AND EUROPEAN STANDARDS

General social digitization and dynamic lifestyle changes, with the increasing use and spread of "smart" phones, with many different contents they offer, lead to the emergence of new relationships between banks, buyers and sellers, which relate to modern business with payment cards. Payments are made, regardless of whether it is a traditional or online business, and modern banking is constantly searching for the most optimal way of payment with the use of new technological and communication solutions. Payment card transactions are a frequent target for the commission of criminal acts, which is not only a challenge for the legislator to set up a legal framework for protection, but also for detection authorities and jurisprudence. The European standards that are being formulated try to respond to these challenges, which also requires implementation into domestic legislation. Directive 2019/713/EU of the European Parliament and the Council on the fight against fraud and counterfeiting in connection with cashless means of payment precisely provides the basis for the protection of cashless payment instruments, in accordance with the requirements set in connection with payments today and the criminal law reaction in domestic legislation.

KEYWORDS: *payment cards, payment risk, IT crime.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.04

KRIVIČNOPRAVNO SUPROTSTAVLJANJE VISOKOTEHNOLOŠKOM – KOMPJUTERSKOM KRIMINALITETU: SAVREMENI IZAZOVI, DILEME, PERSPEKTIVE

Sadmir Karović*
Marina M. Simović**

Visokotehnološki – kompjuterski kriminalitet po svojoj prirodi i fenomenološkoj rasprostranjenosti predstavlja transnacionalni fenomen koji zavređuje posebnu pažnju i interes naučne i stručne javnosti, prije svega zbog negativnih posljedica, ali i drugih specifičnosti svojstvenih za ovaj kriminalitet. U radu je naglašena uslovljenost i povezanost informacijskih i komunikacijskih tehnologija sa kriminalitetom, kompleksnost definisanja ovog kriminaliteta, zloupotreba interneta, kao i krivičnopravni (materijalni i procesni) aspekt ovih krivičnih djela, te njihova povezanost sa drugim krivičnim djelima. U tom smislu, navedene su i određene specifičnosti i problemi praktične prirode u pogledu blagovremenog, efikasnog i zakonitog djelovanja subjekata, odnosno agencija za sprovođenje zakona na planu blagovremenog otkrivanja i dokazivanja ovih krivičnih djela, sa osvrtom na postojeće otkrivačke i dokazne mogućnosti i nedostatke. S obzirom na ubrzan razvoj informacijskih i komunikacijskih tehnologija, kao i prisutnu fenomenološku raznovrsnost navedenih krivičnih djela, sasvim je realno očekivati i neke nove fenomenološke oblike ispoljavanja u budućnosti, iz čega proizilazi i realna potreba proširenja kataloga ovih krivičnih djela, te propisivanja adekvatnih i srazmjernih zakonskih rješenja procesne prirode na planu prikupljanja dokaza.

KLJUČNE RIJEČI: *visokotehnološki kriminalitet, kompjuterski kriminalitet, internet, krivično djelo, dokazivanje.*

* Vanredni profesor, Pravni fakultet, Univerzitet u Travniku, BiH, zaposlen u Državnoj agenciji za istrage i zaštitu. E-mail: *karovic.s@hotmail.com*

** Sekretar Ombudsmena za djecu Republike Srpske, vanredni profesor, Fakultet pravnih nauka Univerziteta „Apeiron" Banja Luka. E-mail: *vlado_s@blic.net*

1. INFORMACIJSKE I KOMUNIKACIJSKE TEHNOLOGIJE I KRIMINALITET

Razvoj i korištenje informacijskih i komunikacijskih tehnologija možemo posmatrati dvojako, i to kroz prizmu upotrebe koja je usmjerena na društveno korisne svrhe i ciljeve i, s druge strane, kroz prizmu zloupotrebe koja je usmjerena na bržu, jednostavniju i efikasniju operacionalizaciju i implementaciju kriminalnih aktivnosti i ciljeva. Visokotehnološki kriminalitet[1] inkorporira različite oblike zloupotrebe informacijskih i komunikacijskih tehnologija koji su kao takvi usmjereni na operacionalizaciju i implementaciju kriminalnih aktivnosti i ciljeva. Dakle, pored upotrebe informacijskih i komunikacijskih tehnologija, što se smatra značajnim i izuzetno korisnim napretkom i poželjnim progresom nauke i modernog čovjek, odnosno društva, na planu unapređenja ovih tehnologija, paralelno sa tim omogućena je istovremeno i zloupotreba informacijskih i komunikacijskih mogućnosti. Iz navedenog možemo izvesti zaključak da se i postojeći oblici kriminaliteta na određen način „modernizuju", ali se istovremeno obezbjeđuju pretpostavke za pojavu nekih novih fenomenoloških oblika kriminaliteta transnacionalnog karaktera koji zahtijevaju adekvatne krivičnopravne (materijalne i procesne) odgovore, odnosno zakonska rješenja koja omogućavaju blagovremeno, efikasno i zakonito djelovanje subjekata, odnosno agencija za sprovođenje zakona u vezi otkrivanja i dokazivanja krivičnih djela iz oblasti visokotehnološkog kriminaliteta.

Transnacionalna komponenta ovog kriminaliteta je nametnula obavezu i odgovarajuće ili srazmjerno potrebne (re)akcije međunarodne zajednice na planu izrade, usaglašavanja i usvajanja određenih međunarodnopravnih dokumenata koji se neposredno odnose na visokotehnološki kriminalitet. Transnacionalni karakter visokotehnološkog kriminaliteta suštinski znači da ovaj kriminalitet prevazilazi nacionalne geografske granice, tako da izvršioci ovih krivičnih djela, svjesni te činjenice, bez obzira na fizičku, odnosno geografsku udaljenost - veoma jednostavno, brzo i efikasno mogu da dogovaraju, pripremaju i u praktičnom smislu operacionaliziraju, tj. realizuju određene kriminalne aktivnosti.

Pojava, odnosno prisustvo raznih oblika visokotehnološkog kriminaliteta, posebno u zadnje dvije decenije, potvrđuje tezu da se kriminalitet kao složen, prije svega društveni, a onda i pravni fenomen i realitet u društvu - veoma brzo i jednostavno prilagođava na novonastale uslove i okolnosti. U tom smislu, neophodno je apostrofirati da instituacionalni oblici državne reakcije na kriminalitet moraju biti adekvatni, srazmjerni i kompatibilni realnim otkrivačkim, istražnim i dokaznim potrebama, imajući u vidu svakako i prihvaćene, odnosno usvojene međunarodnopravne standarde koji se neposredno odnose na zaštitu ljudskih prava i sloboda svakog pojedinca, a samim tim i na katalog propisanih prava osumnjičenog, odnosno optuženog lica, uključujući i univerzalne garancije u krivičnom postupku. Komparativnim osvrtom, visokotehnološki kriminalitet prepoznajemo i drugim krivičnopravnim nacionalnim sistemima, kako u okruženju i regiji, tako i na međunarodnom nivou. Usvajanjem i stupanjem na snagu

[1] U naučnoj i stručnoj literaturi se, pored pojma visokotehnološki kriminalitet, za ovaj kriminalitet koriste različiti pojmovi kao što su kompjuterski kriminal, sajber kriminal i dr.

krivičnih zakona i zakona o krivičnom postupku[2] u Bosni i Hercegovini na svim nivoima iz 2003. godine, novo krivično (materijalno i procesno) zakonodavstvo je prihvatilo i neka nova zakonska rješenja, a jedna od novina u materijalnom krivičnom pravu jeste i inkriminacija krivičnih djela iz oblasti viskotehnološkog kriminaliteta na entitetskom nivou i u Brčko Distriktu Bosne i Hercegovine.

2. KOMPLEKSNOST DEFINISANJA VISOKOTEHNOLOŠKOG KRIMINALITETA – KOMJUTERSKI KRIMINALITET

Visokotehnološki, kompjuterski ili računarski kriminalitet, kako se često u naučnoj i stručnoj literaturi, ali i opštoj javnosti pojmovno određuje ova (pod)vrsta kriminaliteta, obuhvata određene kriminalne aktivnosti koje se po svojoj prirodi, načinu, sredstvu izvršenja i drugim specifičnostima odnose na zloupotrebu informacionih tehnologija – kompjutera, odnosno računara ili mreže, a u cilju njihove praktične operacionalizacije kriminalnih aktivnosti, odnosno izvršenja određenog krivičnog djela. S obzirom na veoma intenzivan i dinamičan razvoj kompjuterskih tehnologija, veoma je zahtjevno pojmovno odrediti i definisati visokotehnološki kriminalitet.

Pojedinci i kriminalne grupe veoma efikasno koriste digitalnu sferu kao platformu za neke nove modalitete poslovanja, posebno kada se radi o određenim uslugama. Naime, ubrzan razvoj informacionih tehnologija praktično omogućava i pojavu nekih novih fenomenoloških oblika ovog kriminaliteta, tako da je veoma teško definisati ovaj pojam ili konstruisati jednu sveobuhvatnu i opšteprihvatljivu univerzalnu definiciju koja bi obuhvatala sve aspekte ovog kriminaliteta. Prisutne definicije u naučnoj i stručnoj literaturi se uglavnom odnose na određivanje skupa, odnosno kataloga kriminalnih aktivnosti koje inkorporira ovaj kriminalitet. U tom smislu, visokotehnološki kriminal se može definisati kao kriminalna djelatnost koja uključuje informacionu tehnologiju, infrastrukturu, neovlašćen pristup, ilegalno presretanje putem informatičkih uređaja, oštećenje, uništenje, izmjenu ili potiskivanje podataka, uticaj na djelovanje informacionog sistema unošenjem, prenosom, oštećenjem, uništenjem ili izbacivanjem podataka, krađom podataka, prevarom i dr. (Đuro-Degan i dr. 2011: 292-293). Uopšteno govoreći, kompjuterski kriminalitet može da se ispolji korišćenjem, oštećenjem, zloupotrebom, ili bilo kojom drugom manipulacijom dva osnovna segmenta kompjuterskog sistema - hardvera („hardware“) i softvera („software“) (Matijašević & Ignjatijević, 2010: 853).

Sajber kriminal (visokotehnološki kriminal) se generalno shvata kao krivično djelo gde su kompjuteri i mreže glavna meta, koriste se kao sredstva za izvršenje krivičnog djela

[2] Zakon o krivičnom postupku Bosne i Hercegovine (*Službeni glasnik Bosne i Hercegovine*, br. 3/03, 32/03, 36/03, 26/04, 63/04,13/05,48/5,46/06,76/06,29/07,32/07,53/07,76/07,15/08,58/08,12/09,16/09,93/09,72/13 i 65/18); Zakon o krivičnom postupku Federacije Bosne i Hercegovine (*Službene novine Federacije Bosne i Hercegovine*, br. 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 09/09, 12/10, 08/13 i 59/14), Zakon o krivičnom postupku Republike Srpske (*Službeni glasnik Republike Srpske*, br. 53/12, 91/17 i 66/18) i Zakon o krivičnom postupku Brčko Distrikta Bosne i Hercegovine (*Službeni glasnik Brčko Distrikta Bosne i Hercegovine*, br. 10/03, 48/04, 06/05, 12/07, 14/07, 21/07, 27/14 i 3/19).

ili su mjesto gde se vrši krivično djelo[3]. U tom smislu, postavlja se pitanje opravdanosti korištenja naziva kompjuterski kriminal, s obzirom na to da je to samo jedan segment visokotehnološkog kriminaliteta. Katalog kriminalnih aktivnosti u fenomenološkom smislu koje inkorporira ovaj kriminalitet se sa razvojem informacionih tehnologija povećava, tako da je u budućnosti sasvim realno očekivati i neke nove fenomenološke oblike ispoljavanja.

Ta djela ćemo svrstati u nekoliko kategorija: konvencionalni kriminal koji koristi informatička sredstva i sajber prostor kao podršku za nezakonite aktivnosti (trgovina drogom, oružjem, ljudima, ljudskim organima, itd); proizvodnja i širenje štetnog softvera (destruktivni virusi, trojanci, crvi ili adware/spyware programi); sajber piraterija (muzika, filmovi, softver, itd.); sajber prevare (plišing, spufing, spemovanje, krađa identiteta, finansijske prevare, elektronsko pranje novca, utaja poreza, transfer novca, akademske prevare od strane studenata i naučnika, varanje u školi, na fakultetima, na ispitima, nezakonito kockanje, krađe telefonskih usluga, prevarne Internet aukcije, nigerijske prevare, prevare kod ličnog plaćanja, bankarske prevare, prevare putnika, itd.); sajber manipulacija-uhođenje i nepristojne ponude najčešće seksualne prirode (slanje neželjenih slika, tekstova, video materijala, trgovina ljudima, proizvodnja pornografskog materijala, itd.); sajber provale (neovlašćeno upadanje u računare i mreže, otkrivanje lozinki, špijunaža, presretanje podataka, itd.); sajber maltretiranje (zlostavljanje, sramoćenje, šikaniranje, prijetnje, klevete, širenje uvredljivog materijala, lažnih informacija, bombardovanje neželjenom poštom, itd.); sajber terorizam, sajber ratovanje, sajber vandalizam i sajber sabotaža (pokušaj da se ostvare vjerski, politički ili drugi ciljevi širenjem straha ili uništenjem informacione infrastrukture) (Prlja i dr. 2015: 351-352). Navedena fenomenološka raznovrsnost i prostorna rasprostranjenost i neodređenost komplikuje i otežava sveobuhvatno definisanje. Takođe, prilikom definisanja ovog kriminaliteta ne smiju se zanemariti ili ignorisati i njegova povezanost sa drugim oblicima kriminaliteta, s obzirom na to da se sve više zloupotrebljavaju informacione i komunikacione tehnologije kao pogodno sredstvo za operacionalizaciju različitih kriminalnih aktivnosti. Sa razlogom možemo konstatovati da se i kriminalitet istovremeno usavršava, odnosno modernizuje sa veoma izraženim spektrom različitih fenomenoloških oblika ispoljavanja.

3. (ZLO)UPOTREBA INTERNETA U SAVREMENIM USLOVIMA – MOGUĆNOSTI I RIZICI

Informaciono-komunikacione tehnologije imaju veoma važnu, ako ne i najvažniju ulogu u svim oblastima života građana i društva u cjelini. Praktično je nemoguće zamisliti bilo koju oblast ljudskog djelovanja na današnjem stepenu razvoja društva, odnosno modernog čovjeka, bez upotrebe informaciono-komunikacionih tehnologija. Samo se postavlja pitanje za istraživače koje su to dominantne oblasti odnosno u kojima se više ili manje koriste ove tehnologije, s obzirom na realne potrebe. Internet kao savremena

[3] *https://www.dcaf.ch/sites/default/files/publications/documents/CyberPolicyTool%20SERBIAN.pdf.* [1.8.2022.].

tehnologija je sve više zastupljen i njegove efekte možemo posmatrati dvojako, i to kroz prizmu njegove upotrebe u određene društveno-korisne svrhe (npr. upotreba interneta u funkciji obavljanja školskih zadataka, naučna/akademska istraživanja, prodaja, razne vrste usluga i dr.) i, s druge strane, kroz prizmu zloupotrebe u cilju ostvarivanja i realizacije kriminalnih aktivnosti (kompjuterski kriminal, specifični oblici organizovanog kriminala u vezi neovlaštenog prometa opojnom drogom, oružja, trgovine ljudima, zatim terorizam i drugi oblici kriminaliteta, prekomjerna upotreba interneta od strane djece - zavisnost o internetu i dr). Dakle, pored krivičnih djela propisanih krivičnim zakonom, zloupotreba kompjutera i mreža, po svojoj prirodi i fenomenološkim aspektima proizvodi veoma negativne posljedične refleksije i izvan kataloga krivičnih djela koji se isključivo odnose na krivičnopravnu zaštitu kompjuterskih sistema. U tom smislu, zloupotrebu kompjutera i interneta kao savremenog medija moguće je posmatrati kroz prizmu izvršenja raznovrsnih krivičnih djela.

U vezi krivičnih djela iz oblasti trgovine ljudima, internet se zloupotrebljava na razne načine, a posebno za ostvarivanje kontakta i vrbovanje žrtava, te izradu profila za seksualnu eksploataciju i nuđenje seksualnih usluga zainteresovanim licima, ostvarivanje konverzacije i dogovora između posrednika i klijenata u vezi drugih oblika eksploatacije (npr. radna eksploatacija i dr.). Takođe, kada su u pitanju krivična djela iz oblasti zloupotrebe opojnih droga, internet se pokazao pogodnim za ostvarivanje kontakta, nuđenje i kupovinu opojne droge, te dogovora u vezi same operacionalizacije, odnosno konkretnog čina (primo)predaje navedenih sredstava. Identična je situacija kada su u pitanju krivična djela terorizma, gdje se internet zloupotrebljava kao platforma za ostvarivanje komunikacije i vrbovanje potencijalnih žrtava, širenje destruktivnih, radikalnih i ekstremnih ideja i stavova, te promociju anticivilizacijskih vrijednosti. Zloupotreba interneta omogućava da se kreira i uspostavi propagandna platforma za implementaciju i operacionalizaciju kriminalnih aktivnosti koje se posebno odnose na vrbovanja i regrutovanja mladih, kao i mogućnost veoma jednostavnog i efikasnog promovisanja i afirmacije radikalnih ideja koje sadrže elemente ljudske destrukcije (nasilje, agresivnost i dr.) (Karović i Dubačkić, 2018: 213). Naime, internet u današnje vreme služi kao veoma moćno sredstvo za teroriste, kao i za vršenje krivičnih dela, ali, isto tako, i kao sredstvo propagande, širenja nemoralnih sadržaja, raznih nacionalističkih, retrogradnih i drugih društveno i globalno neprihvatljivih ideja i slično, dok, s druge strane, internet (može da) služi i kao sredstvo pronalaska izvršioca krivičnih djela, kao sredstvo suzbijanja kriminaliteta, kao način eliminisanja mogućnosti za izvođenje određenih terorističkih akata i slično (Milašinović i dr. 2012: 33).

Krivična djela iz oblasti zloupotrebe autorskih prava se praktično operacionaliziraju posredstvom kompjutera, odnosno zloupotrebom interneta, a neovlašteno korištenje i razni oblici zloupotrebe intelektualnog vlasništva u zadnje vrijeme sve više zavređuju pažnju naučne i stručne, ali i opšte javnosti, prije svega zbog negativnih, odnosno štetnih posljedica. U savremenim uslovima ne smijemo izostaviti pranje novca kao veoma specifično krivično djelo, a kompjuter se opet pojavljuje kao pogodno sredstvo za operacionalizaciju kriminalnih aktivnosti (npr. vođenje dvostrukog knjigovodstva i dr.). Ovo je kratak osvrt na neka krivična djela koja se dovode u vezu sa zloupotrebom interneta.

Ono što dodatno zabrinjava i usložnjava efikasnu i energičnu borbu subjekata, odnosno agencija za sprovođenje zakona protiv svih oblika visokotehnološkog kriminaliteta jesu novi fenomenološki oblici, odnosno fenomenološka raznovrsnost ispoljavanja ovog kriminaliteta, te njihova povezanost sa specifičnim oblicima organizovanog kriminaliteta. Odnos sa organizovanim kriminalitetom i njegovim transnacionalnim elementima je interesantan i bitan, s obzirom na to da sprega ova dva oblika kriminalnog djelovanja dovodi do još težih posljedica, do još većih problema u otkrivanju i poimanju problema sa kojim se društvena zajednica danas suočava (Matijašević, 2021: 400). Nema sumnje da je pojava interneta predstavljala revolucionaran (pre)okret u vezi unaprjeđenja kvaliteta života građana, kao i bržeg, efikasnijeg i produktivnijeg rada u različitim segmentima, odnosno oblastima ljudskog djelovanja.

Pored pravnog aspekta posmatranja i interesa, upotreba i zloupotreba interneta je sasvim sigurno u fokusu istraživanja brojnih nauka i naučnih disciplina (bezbjednost, psihologija, sociologija, pedagogija, socijalni rad i dr.) koje svaka iz svog naučnog ugla i predmeta istraživanja nastoji da pronađe adekvatne odgovore na krucijalna pitanja koja se odnose na internet kao savremeni medij i njegove efekte na pojedince, posebno mlade. Multidisciplinarnost (zlo)upotrebe interneta uključujući sve raspoložive fenomenološke oblike ispoljavanja zahtijeva i multidiscplinarni pristup istraživanja na planu traganja i pronalaženja adekvatnih i sveobuhvatnih odgovora i rješenja.

Kada je u pitanju internet u domaćinstvima, rezultati istraživanja iz 2019. godine o upotrebi informaciono-komunikacionih tehnologija u domaćinstvima i pojedinačno (IKT-D) u Bosni i Hercegovine, pokazali su sljedeće: domaćinstava imaju pristup internetu: 72,0%, domaćinstava nemaju pristup internetu: 27,3%, domaćinstavo ne zna da li ima pristup internetu: 0,7% (Jovović & Korajčević, 2020: 16). Procenat upotrebe interneta se vremenom povećava, s obzirom na njegovu sve veću dostupnost i niske, odnosno prihvatljive cijene pretplate svim građanima putem sve većeg broja operatera, pa čak i u najudaljenijim ruralnim dijelovima. U urbanim dijelovima mogućnost korištenja interneta je sasvim opravdano i veća, s obzirom na to da brojni poslovni, trgovački centri, ugostiteljsko-turistički objekti, zatim javne institucije i organi i dr., omogućavaju besplatno korištenje, tj. pristup internetu. Sve pogodnosti koje pruža internet prepoznate su i od strane lica sklonih izvršenju krivičnih djela, prije svega kao realna mogućnost operacionalizacije kriminalnih aktivnosti i ciljeva. Mogućnosti različitih oblika komuniciranja, prije svega razmjena različitih informacija i podataka, izvještavanje na velikim fizičkim udaljenostima, odnosno na različitim geografskim tačkama u svijetu - predstavljaju platformu za neke nove oblike kriminaliteta svojstvene za savremeno doba. Internet, koji je po svojoj prirodi ranjiv i nesiguran, usljed ogromnog broja korisnika, otvorenosti i pravne neregulisanosti, postao je poligon, ali i idealno skrovište za kriminalce različitog tipa (Putnik & Gavrić, 2012: 217).

S druge strane, kompleksnost otkrivanja, istraživanja i dokazivanja raznih krivičnih djela iz oblasti visokotehnološkog kriminaliteta i kriminaliteta koji je povezan ili srodan po svojim krivičnopravnim specifičnostima sa ovim kriminalitetom, predstavlja važan faktor u kontekstu učestale zloupotrebe informaciono-komunikacionih

tehnologija u kriminalne svrhe, odnosno izvršenje krivičnih djela. Izvršioci krivičnih djela iz oblasti visokotehnološkog kriminaliteta prepoznaju sve neadekvatnosti primjene zakonske norme s obzirom na to da postojeća zakonska rješenja materijalne i procesne prirode još uvijek nisu adekvatna, srazmjerna i kompatibilna realnim otkrivačkim, istražnim i dokaznim potrebama, te kao takva ostavljaju dovoljno prostora za razne oblike zloupotrebe i izvršenje određenih krivičnih djela.

Uz to, kada je u pitanju upotreba, odnosno zloupotreba interneta, neophodno je posebno naglasiti i razne oblike zloupotrebe gdje su objekt napada maloljetnici, odnosno djeca kao posebna starosona kategorija (dječija pornografija, prostitucija, trgovina ljudima, radna eksploatacija, terorističke aktivnosti i dr.). Maloljetnici, odnosno djeca usljed njihovog prekomjernog korištenja i nekontrolisanog pristupa kompjuteru i internetu od strane roditelja, odnosno staratelja - postaju žrtve. Uprkos svim postojećim preventivno-zaštitnim mehanizmima i upozorenjima, internet je pogodno sredstvo i način za izvršenje određenih krivičnih djela gdje se maloljetnici, odnosno djeca pojavljuju kao žrtve, odnosno oštećena lica.

4. SAJBER PROSTOR KAO PLATFORMA ZA OPERACIONALIZACIJU KRIMINALNIH AKTIVNOSTI – KRIVIČNOPRAVNI ASPEKT

Opšta ili generalna reforma krivičnog zakonodavstva u Bosni i Hercegovini iz 2003. godine obuhvatila je značajne, pa i u određenim segmentima radikalne izmjene krivičnoog materijalnog i procesnog zakonodavstva, s obzirom na to da su prihvaćena neka nova zakonska rješenja materijalne i procesne prirode sa intencijom zakonodavca da se navedenom reformom postignu postavljeni ciljevi. Posmatrajući i analizirajući oblast visokotehnološkog kriminalitet, u kontekstu usvajanja i stupanja na snagu novih zakona materijalne i procesne prirode iz 2003. godine, u oblasti krivičnog materijalnog prava značajno je inkriminisanje kataloga krivičnih djela iz oblasti visokotehnološkog kriminaliteta na nivou entiteta i Distrikta Brčko Bosne i Hercegovine, dok je u oblasti krivičnog procesnog zakonodavstva značajno pomenuti pojmovno određenje, tj. definisanje pojmova visokotehnoškog kriminaliteta. Krivičnim pravom se štiti korišćenje informacione tehnologije u dozvoljene svrhe, odnosno pruža se zaštita samom funkcionisanju informacione tehnologije (Stojanović i dr. 2018: 324).

Analizom odredbi važećih krivičnih zakona u Bosni i Hercegovini na nivou entiteta - Federacije Bosne i Hercegovine i Republike Srpske, te Brčko Distrikta Bosne i Hercegovine, primijećuje se da je krivičnopravna zaštita kompjuterskih sistema sistematizovana i propisana u posebnoj glavi. U glavi XXXII Krivičnog zakona Federacije Bosne i Hercegovine[4] sistematizovana su „Krivična djela protiv sistema elektronske obrade podataka" gdje su propisana sledeća krivičnih djela: Oštećenje računarskih podataka i programa - član 393, Računalno krivotvorenje - član 394, Računarska prevara - član 395, Ometanje rada sistema i mreže elektronske obrade podataka - član 396, Neovlašteni

[4] *Službene novine Federacije BiH*, br. 36/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16 i 75/17.

pristup zaštićenom sistemu i mreži elektronske obrade podataka - član 397 i Računarska sabotaža - član 398. U Krivičnom zakoniku Republike Srpske[5] navedena krivična djela su sistematizovana i propisana u glavi XXXII - „Krivična djela protiv bezbjednosti kompjuterskih podataka". Komparativnom analizom navedena dva zakona primjećujemo da je u Krivičnom zakoniku Republike Srpske propisano i krivično djelo Izrada i unošenja kompjuterskih virusa - član 409, ali, s druge strane, evidentno je da nije propisano krivično djelo Računarsko krivotvorenje. U Krivičnom zakonu Brčko Distrikta Bosne i Hercegovine[6] navedena krivična djela su sistematizovana u glavi XXXII - „Krivična djela protiv sistema elektronske obrade podataka" i propisana sljedeća krivična djela Oštećenje računarskih podataka i programa - član 387, Računarsko krivotvorenje - član 388, Računarska prevara - član 389, Ometanje rada sistema i mreže elektroničke obrade podataka - 390, Neovlašteni pristup zaštićenom sistemu i mreži elektronske obrade podataka - član 391 i Računarska sabotaža - član 392.

S obzirom na to da je država Bosna i Hercegovina usvojila i ratifikovala brojne međunarodnopravne dokumente, postoji i obaveza usaglašavanja i harmonizovanja domaćeg nacionalnog krivičnog zakonodavstva s međunarodnopravnim standardima. Dražave članice Konvencije o visokotehnološkom (kibernetičkom) kriminalu Vijeća Evrope[7] su se obavezale da će u svom nacionalnom krivičnom zakonodavstvu predvidjeti kao posebno krivično djelo svaku djelatnost koja je preduzeta sa umišljajem, a predstavlja bespravno oštećenje, brisanje, kvarenje, mijenjanje ili prikrivanje kompjuterskih podataka (Tomić, 2007: 399). Konvencija o visokotehnološkom (kibernetičkom) kriminalu Vijeća Evrope je prvi međunarodni sporazum, tj. pravni akt, koji reguliše materijalni, procesni i međunarodni pravni okvir za krivična djela koja su izvršena putem računara, računarskih mreža, kao i korištenjem interneta i drugih računarskih mreža međunarodnog ili lokalnog karaktera (Stamenković i dr. 2017: 11). Navedena obaveza se odnosi i na prilagođavanja, odnosno usklađivanja i harmonizovanja s Konvencijom Vijeća Evrope o kibernetičkom kriminalu i njenim Dodatnim protokolom u vezi kažnjavanja djela rasističke i ksenofobične prirode učinjenih putem kompjuterskih sistema (Pleh, 2019: 69-70). Shodno navedenoj obavezi, krivična djela kojima je propisana krivičnopravna zaštita kompjuterskih sistema u Bosni i Hercegovini, po svom sadržaju, moraju biti kompatibilna i usklađena sa pomenutom konvencijom, koja predstavlja međunarodnopravni osnov propisivanja kataloga ovih krivičnih djela u nacionalnom krivičnom zakonodavstvu.

U tom smislu, posebno je važno naglasiti da katalog krivičnih djela kojima je propisana krivičnopravna zaštita komjuterskih sistema, nije propisan i na državnom nivou, tj. u Krivičnom zakonu Bosne i Hercegovine. Nije jasno zbog čega zakonodavac na

[5] *Službeni glasnik Republike Srpske*, br. 64/17, 104/18 i 15/21.

[6] *Službeni glasnik Brčko Distrikta BiH*, br. 19/20 - prečišćeni tekst.

[7] Budimpešta, 23. novembar 2001. godine. U ovoj konvenciji izraz „kompjuterski sistem" označava svaki uređaj ili grupu međusobno spojenih ili povezanih uređaja, od kojih jedna ili više njih na osnovu programa automatski obrađuju podatke. Izraz „kompjuterski podaci" označavaju svako iskazivanje činjenica, informacija ili koncepata u obliku prikladnom za obradu u kompjuterskom sistemu, uključujući i program koji može prouzročiti da kompjuterski sistem izvrši određenu funkciju.

državnom nivou nije sistematizovao i propisao u posebnu glavu krivična djela kompjuterskog kriminala, cijeneći realne, opravdane i svrsishodne kriminalnopolitičke razloge. O mogućim razlozima zbog čega je to tako moglo bi se pretpostavljati, mada bi bilo ispravnije da su radnje koje su propisane Konvencijom i Protokolom, kao krivičnopravne radnje, postale sastavni dio Krivičnog zakona Bosne i Hercegovine zbog specifičnosti krivičnih djela, jer se radi o krivičnim djelima gdje počinilac krivičnog djela može preduzimati radnju, primjera radi, u Federaciji Bosne i Hercegovine, a posljedica istovremeno nastupiti u Federaciji Bosne i Hercegovine, Republici Srpskoj, Brčko Distriktu ili van teritorije Bosne i Hercegovine. Svakako, ovakvo zakonsko rješenje nije isključilo mogućnost da se krivična djela kompjuterskog kriminala krivično gone pred Sudom Bosne i Hercegovine na osnovu člana 7 stav 2 Zakona o Sudu Bosne i Hercegovine[8]. Sud Bosne i Hercegovine je naime nadležan za krivična djela utvrđena zakonima Federacije Bosne i Hercegovine, Republike Srpske i Brčko Distrikta Bosne i Hercegovine kada ta krivična djela: a) ugrožavaju suverenitet, teritorijalni integritet, političku nezavisnost, državnu bezbjednost i međunarodni subjektivitet Bosne i Hercegovine; b) mogu imati ozbiljne reperkusije ili štetne posljedice na privredu Bosne i Hercegovine ili mogu izazvati druge štetne posljedice za Bosnu i Hercegovinu ili izazvati ozbiljnu ekonomsku štetu ili druge štetne posljedice van teritorije datog entiteta ili Brčko Distrikta Bosne i Hercegovine.Međutim, analizom navedene zakonske odredbe primijećujemo da je zakonodavac propisao restriktivne zakonske uslove, odnosno visoko postavljene standarde u kontekstu moguće nadležnosti na državnom nivou, kada su u pitanju ova krivična djela.

Prilikom razmatranja krucijalnih pitanja koja se odnose na blagovremeno, efikasno i zakonito postupanje subjekata, odnosno agencija za sprovođenje zakona u vezi otkrivanja i dokazivanja krivičnih djela iz oblasti visokotehnološko - kompjuterskog kriminaliteta, neophodno je apostrofirati nekoliko bitnih segmenata, odnosno aspekata, i to:

- opšti razvoj informacionih i komunikacionih tehnologija omogućava pojavu nekih novih fenomenoloških oblika ovog kriminaliteta. Fenomenološka raznovrsnost i rasprostranjenost neposredno utiču na blagovremeno, efikasno i zakonito otkrivanje i dokazivanje ovih krivičnih djela;
- neadekvatnost zakonske norme, u skladu sa realnim otkrivačkim i dokaznim potrebama, jedan je od ključnih aspekata u kontekstu razmatranja pitanja neadekvatnosti državne (re)akcije na razne fenomenološke oblike visokotehnološkog kriminaliteta. Kompleksna ustavnopravna struktura države Bosne i Hercegovine neposredno determinira, odnosno određuje nivoe vršenja zakonodavne, sudske i izvršne vlasti. Posebno zabrinjava činjenica da na državnom nivou zakonodavac nije prepoznao realnu i svrsishodnu potrebu inkriminisanja ovih krivičnih djela, te katalog krivičnih djela iz oblasti visokotehnološkog kriminaliteta sistematizovao i propisao u posebnu glavu, na način da materijalne odredbe budu sadržajno prilagođene, harmonizovane i kompatibilne sa Konvencijom Vijeća Evrope o kibernetičkom kriminalu i njenim Dodatnim protokolom u vezi kažnjavanja djela

[8] *Službeni glasnik BiH,* br. 32/07, 49/09, 74/09 i 97/09.

rasističke i ksenofobične prirode učinjenih putem kompjuterskih sistema. Pored toga, u procesnom segmentu, zakonodavac bi morao preispitati postojeća zakonska rješenja procesne prirode, te razmotriti mogućnost propisivanja srazmjerno potrebnih zakonskih rješenja, posebno u dijelu koji se odnosi na prikupljanje dokaza, uvažavajući sve specifičnosti navedenih krivičnih djela;

- izvršioci ovih krivičnih djela su lica koja u pravilu posjeduju posebna znanja i vještine iz oblasti informatike i tehnike što otežava otkrivanje i dokazivanje ovih krivičnih djela. Samouvjereni i sigurni u svoje znanje, teže da još dublje prodru u virtualni svijet - kako bi ostvarili svoje ciljeve (Gligorević, 2014:164);
- geografska rasprostranjenost je jedan o ključnih problema koji se odnosi na kompleksnost otkrivanja, istraživanja i dokazivanja ovih krivičnih djela, te nemogućnost prikupljanja potrebnih dokaza koja se odnose na postojanje obilježja bića konkretnog krivičnog djela. Opštepoznato je da visokotehnološki kriminalitet, po svojoj prirodi, načinu izvršenja, fenomenološkim oblicima ispoljavanja i drugim krivičnopravnim specifičnostima, prevazilazi nacionalne geografske granice. Dakle, geografska, odnosno fizička udaljenost nije prepreka za izvršenje ovih krivičnih djela, zbog čega za ovaj kriminalitet međunarodna zajednica sa razlogom iskazuje poseban interes i pažnju u smislu pronalaženja adekvatnih odgovora i rješenja materijalne i procesne prirode;
- s obzirom na navedenu geografsku komponentu, odnosno međunarodnu ili globalnu dimenziju ovih krivičnih djela (transnacionalnost), veoma je teško u otkrivačkoj fazi identifikovati izvršioca i njegove saučesnike. U oblasti kompjuterskog kriminaliteta „tamna brojka" je vidno prisutna, što ukazuje na to da je priličan broj izvršenih kompjuterskih krivičnih djela ostao neotkriven (Bošković i Jovičić, 2002:444). Određen stepen anonimnosti izvršilaca ovih krivičnih djela i njihovih saizvršilaca je jedan od važnih razloga nemogućnosti otkrivanja i preduzimanja drugih mjera i radnji na planu otrkivanja i dokazivanja krivičnih djela;
- naknadna spoznaja ošetećenog lica da je žrtva izvršenja nekog od krivičnh djela visokotehnoškog kriminala je jedan od bitnih aspekata u vezi blagovremenog otkrivanja postojanja ovih krivičnih djela. Naime, posljedice izvršenja ovih krivičnih djela nisu tako uočljive i prepoznatljive neposredno nakon preduzimanja radnji izvršenja;
- međusobna uslovljenost i povezanost ovog kriminaliteta sa specifičnim oblicima organizovanog kriminaliteta, pranja novca i drugih (srodnih) krivičnih djela, gdje se kompjuter, odnosno mreža pojavljuju kao pogodno sredstvo za operacionalizaciju kriminalnih aktivnosti, potvrđuje negativne, odnosno štetne posljedične refleksije i destruktivnu prirodu;
- dostupnost i rasprostranjenost informacionih i komunikacionih tehnologija svim građanima, uključujući i maloljetnike odnosno djecu. Poseban sigurnosni problem i izazov u savremenim uslovima predstavlja (ne)adekvatna zaštita maloljetnika, odnosno djece od rizičnih sadržaja gdje oni mogu postati objektom napada, odnosno žrtvom (dječija pornografija, prostitucija, trgovina ljudima, terorističke

aktivnosti, ucjene i dr.). Neadekvatan roditeljski nadzor i staranje nad maloljetnicima, odnosno djecom u vezi prekomjernog korištenja kompjutera i interneta, jedan je od ključnih riziko-faktora;

- neadekvatna stručna osposobljenost lica u subjektima i agencijama za sprovođenje zakona iz oblasti visokotehnološkog kriminaliteta (istražitelji u policiji, tužioci i dr. učesnici) na planu otkrivanja i dokazivanja ovih krivičnih djela, te u određenim situacijama i nedovoljan stepen saradnje (policijske i krivične) na međunarodnom nivou koji je uslovljen složenim procedurama u vezi razmjene informacija i podataka, različita procesna zakonska rješenja i dr., utiče na nemogućnost blagovremenog djelovanja i preduzimanja adekvatnih ili odgovarajućih mjera i radnji usmjerenih na otkrivanje i dokazivanje. U tom smislu, neophodno je profilisanje, odnosno specijaliziranost kadrova koji će biti stručno osposobljeni da odgovore na visoko postavljene zahtjeve u pogledu blagovremenog, efikasnog i zakonitog postupanja;
- ubrzan razvoj informacionih i komunikacionih tehnologija koji će u narednom periodu rezultirati i nekim novim otkrićima na ovom polju, najvjerovatnije će istovremeno omogućiti i neke nove fenomenološke oblike koji će prevazilaziti postojeće otkrivačke, istražne i dokazne mogućnosti, resurse i kapacitete subjekata, odnosno agencija za sprovođenje zakona.

ZAKLJUČAK

Opšti razvoj informacionih i komunikacionih tehnologija u posljednje dvije decenije, uticao je na pojavu različitih fenomenoloških oblika visokotehnološkog kriminaliteta kao pošasti savremenog doba. Pored pozitivne i društveno korisne strane navedenog razvoja ovih tehnologija koji značajno doprinosi bržem, jednostavnijem i efikasnijem obavljanju određenih aktivnosti u svim oblastima ljudskog djelovanja, postoji i druga - destruktivna strana koja se odnosi na zloupotrebu navedenih tehnologija u cilju operacionalizacije kriminalnih aktivnosti, odnosno realizacije kriminalnih ciljeva. Reformom krivičnog (materijalnog i procesnog) zakonodavstva iz 2003. godine, koja je prepoznatjiva po brojnim novinama u vezi prihvatanja nekih novih zakonskih rješenja materijalne i procesne prirode, zakonodavac je inkriminisao, odnosno sistematizovao i propisao krivična djela protiv kompjuterskih sistema na entitetskom nivou (Federacija Bosne i Hercegovine i Republike Srpske) i Brčko Distrikta Bosne i Hercegovine, dok na državnom nivou ova krivična djela nisu propisana što predstavlja jedan od nedostataka pomenute reforme. U procesnom smislu, zakonodavac je u katalogu osnovnih pojmova definisao značenje određenih izraza koji se odnose na visokotehnološki kriminalitet (kompjuterski podaci, kompjuterski sistem).

Međutim, zakonodavac prilikom kreiranja i inoviranja budućih novih zakonskih rješenja, mora iskazati poseban interes i pažnju za katalog krivičnih djela iz oblasti visokotehnološkog kriminaliteta, s obzirom na specifičnosti, fenomenološku

rasprostranjenost, ali i posljedice navedenih krivičnih djela. U tom smislu, neophodno je preispitati postojeća zakonska rješenja materijalne i procesne prirode jer su ona neadekvatna, te razmotriti mogućnost proširenja kataloga i propisivanja novih krivičnih djela, ali i određenih zakonskih rješenja procesne prirode, na planu prikupljanja potrebnih dokaza, a u cilju prilagođavanja i harmonizovanja krivičnog materijalnog i procesnog zakonodavstva sa Konvencijom Vijeća Evrope o kibernetičkom kriminalu i njenim Dodatnim protokolom u vezi kažnjavanja djela rasističke i ksenofobične prirode učinjenih putem kompjuterskih sistema.

Ključno procesno pitanje glasi kako na efikasan i zakonit način otkriti i dokazati krivično djelo iz oblasti visokotehnološkog kriminaliteta, uvažavajući sve specifičnosti koje se odnose na otkrivačku i dokaznu komponentu, a posebno aspekt prikupljanja dokaza neophodnih za efikasno vođenje i okončanje krivičnog postupka. Dakle, poseban problem koji zavređuje pažnju naučne i stručne javnosti jeste kompleksnost i teret otkrivanja i dokazivanja krivičnih djela iz oblasti visokotehnološkog kriminaliteta. Stručna osposobljenost i kontinuirana edukacija iz ove specifične i zahtjevne oblasti lica u subjektima, odnosno agencijama za sprovođenje zakona, kojima su zakonom propisana ovlaštenja (policija, tužilaštvo i dr.), jedan je od uslova za efikasnu i energičnu borbu protiv ovog kriminaliteta. Specijaliziranost kadrova u segmentu informatike i tehnike, u odnosu na visokopostavljene zahtjeve, u vezi otkrivanja i dokazivanja ovih krivičnih djela - realna je potreba, cijeneći da su, kako smo već konstatovali, izvršioci ovih krivičnih djela, lica koja posjeduju posebna znanja i vještine.

LITERATURA

1. Bošković, M. Jovičić, D. (2002) *Kriminalistika metodika, prvo izdanje*. Banja Luka: Viša škola unutrašnjih poslova.
2. Degan, V. Đ., Pavišić, B. Beširević V. (2011) *Međunarodno i transnacionalno krivično pravo*. Beograd: Pravni fakultet Univerziteta Union, Službeni glasnik.
3. Gligorević, R. (2014) „Cyber kriminal", *Economics,* broj 2, 179-189.
4. Jovović, D. Korajčević, Š. (2020) *Upotreba informaciono – komunikacionih tehnologija u Bosni i Hercegovini 2019*, tematski bilten T19, Sarajevo: Agencija za statistiku Bosne i Hercegovine.
5. Karović, S. Dubačkić, A. (2019) „Terorizam u savremenom krivičnom pravu sa posebnim osvrtom na zloupotrebu interneta i viktimizaciju mladih", *Zbornik radova Pravnog fakultet Univerziteta u Travniku*, god. IV. br. 7.
6. Matijašević, J. (2012) „Visokotehnološki kriminal u funkciji organizovanog kriminala", *Organizovani kriminal izazov XXI vijeka*, Željko Bjelajac i Mina Zirojević (ur.), Novi Sad: Pravni fakultet za privredu i pravosuđe, 398-419.
7. Matijašević, J. Ignjatijević, S. (2010) „Kompjuterski kriminalitet u rpavnoj teoriji, pojam karakteristike, posljedice", *Zbornik radova*, Infoteh – Jahorina, Vol 9., Ref. E-VI-8, 852-856.

8. Milašinović, R. Mijalković, S. Amidžić, G. (2012) „Bezbednost i internet", Zbornik radova Međunarodna naučnostručna konferencija, *Suzbijanje kriminala i evropske integracije s osvrtom na visokotehnološki kriminal,* Banja Luka: Visoka škola unutrašnjih poslova.
9. Pleh, H. (2019) „Krivičnopravni aspekti zaštite kompjuterskih sistem, analiza stanja i *de lege ferenda* prijedlozi", Kriminalističke teme, Sarajevo, *Zbornik radova*, godina XIX, broj 5, str. 67-84.
10. Prlja, D. Korać, V. Diligenski, A. (2015) „Maloljetnici i sajber kriminal" *Maloljetnici kao učinioci i žrtve krivičnih djela i prekršaja*, Ivana Stevanović (ur.) Beograd: Institut za kriminološka i sociološka istraživanja, priredila Ivana Stevanović, str. 349-364.
11. Putnik, N. Gavrić, N. (2012) „Mjere i strategije zaštite informacionih sistema od visokotehnološkog kriminala" Zbornik radova Međunarodna naučnostručna konferencija*, Suzbijanje kriminala i evropske integracije s osvrtom na visokotehnološki kriminal,* Banja Luka: Visoka škola unutrašnjih poslova, 217-226.
12. Stojanović, Z. Škulić, M. Delibašić, V (2018) *Osnovi krivičnog prava, Krivično materijalno pravo, Knjiga I.* Beograd: Službeni glasnik.
13. Tomić, Z. (2007) *Krivično pravo II, posebni dio.* Sarajevo: Pravni fakultet, Univerzitet u Sarajevu.

Internet izvori

1. Branko Stamenković, Saša Živanović, Bojana Paunović, Ivana Stevanović, tekst prilagodili kontekstu BiH: Elmedin Muratbegović i Haris Halilović, *Vodič za sudije i tužioce na temu visokotehnološkog kriminala i zaštite djece u Bosni i Hercegovini*, Sarajevo: B-H Konzorcijum za zaštitu djece – UNICEF, Save the Children, Međunarodni forum solidarnosti (MFS) Emmaus, dostupno na: *https://nwb.savethechildren. net/sites/nwb.savethechildren.net/files/library/Smjernice%20za%20 sudije%20i%20tuzioce%20WEB%20Latinica.pdf,* [22.12.2021.].
2. Franziska Klopfer, Irina Rizmal, Milan Sekuloski, Tersa Hatzl, Dragan Mladenović, *Uvod u upravljanje sajber bezbjednošću – priručnik za narodne poslanike*, Ženeva: Ženevski centar za demokratsku kontrolu oružanih snaga (DCAF), *https:// www.dcaf.ch/sites/default/files/publications/documents/CyberPolicyTool%20SERBIAN.pdf,* [25.06.2021.].

CRIMINAL OPPOSITION TO HIGH-TECH – COMPUTER CRIME: CONTEMPORARY CHALLENGES, DILEMMAS, PERSPECTIVES

High-tech - computer crime by its nature and phenomenological prevalence is a transnational phenomenon that deserves special attention and interest of the scientific and professional public, primarily due to the negative consequences but also other specifics inherent in this crime. This paper emphasizes the conditionality and connection of information and communication technologies with crime, the complexity of defining this crime, Internet abuse as well as the criminal (material and procedural) aspect of these crimes, and their connection with other crimes. In that sense, certain specifics and problems of practical nature are stated in terms of timely, efficient and legal action of entities or law enforcement agencies in terms of timely detection and proof of these crimes, with reference to existing detection and evidence possibilities and shortcomings. Given the accelerated development of information and communication technologies as well as the present phenomenological diversity of these crimes, it is quite realistic to expect some new phenomenological forms of manifestation in the future, hence the real need to expand the catalog of these crimes and prescribe adequate and proportionate legal solutions, procedural nature in terms of gathering evidence.

KEYWORDS: *High-tech crime, computer crime, internet, technologies.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.05

ZNAČAJ DIGITALIZACIJE U KRIVIČNOM PRAVU

Ivan Duzlevski*

U ovom radu autor ukazuje na značaj digitalizacije srpskog pravosuđa. Ulaskom u treću deceniju XXI veka pitanje digitalizacije, aktuelizovano pandemijom virusa Covid-19, znatno je prevazišlo trenutnu potrebu reorganizacije rada državnih organa, nadležnih ustanova i komunikacije sa građanima, samim tim i njihovo prilagodjavanje novim zdravstvenim i društvenim okolnostima. U sektoru pravosuđa, u kojem se nezavisno od navedenog teži rešavanju velikog broja starih predmeta, većoj efikasnosti i manjoj potrošnji, potreba za digitalizacijom još više je izraženija.

U radu se analizira upotreba postojećih digitalnih formi u krivičnom postupku (digitalni dokazi) i daje kratak prikaz pojedinih uporednopravnih rešenja o digitalizaciji pravosuđa, ukazuje na ciljeve i benefite sprovođenja tog procesa kod nas, uz isticanje važnosti pridržavanja EU standarda na tom putu kako bi se izbegle ili minimizirale potencijalne zloupotrebe i povreda ljudskih prava i sloboda.

KLJUČNE REČI: *digitalizacija pravosudja, digitalni dokazi, modernizacija, ekonomičnost, zaštita ličnosti i ljudska prava*

* Autor je advokat u Advokatskoj kancelariji Moravčević, Vojnović i partneri iz Beograda.

E-mail: *i.duzlevski@schoenherr.rs* • *ivanduzlevski@gmail.com.*

UVOD

Vanredne posledice po život i rad koje je sa sobom donela pandemija virusa Covid-19 pogodile su sve pravosudne sisteme postavljajući pred njih ozbiljne zadatke i izazove kako dalje funkcionisanje prilagoditi novonastalim okolnostima. Za srpsko pravosuđe, ionako od ranije napregnuto u borbi za rešavanje povelikog broja starih predmeta i skraćenje trajanja sudskih postupaka, nova stvarnost dodatno je otežala njegov reformski put ka dostizanju evropskih pravnih standarda.

Nužno i očekivano, kvalitet i efikasnost suđenja doživeli su izvestan pad, izazvan „višom silom" usled koje je veliki broj ročišta i pretresa odložen na neodređeno vreme. Zdravstveno-epidemiološke razloge: minimiziranje ljudskog kontakta i sprečavanje daljeg širenja virusa, pratio je i sveopšti nedostatak odgovarajuće tehničke opreme i uslova (za digitalno fotografisanje, skeniranje, video i audio snimanje) kojim bi se manjak adekvatnog sudećeg prostora mogao nadomestiti tzv. „suđenjima na daljinu", aktuelan od usvajanja zabrane okupljanja više od pet lica u zatvorenom prostoru radi obezbeđenja fizičke distance od dva metra.

Problem organizacije suđenja posebno je bio izražen u krivičnim postupcima. Opšte je poznato da su svi krivični postupci protiv okrivljenih koji su u pritvoru hitni i ne trpe odlaganja (*član 14 stav 2 Zakonika o krivičnom postupku*). U praksi se postavilo pitanje da li lice koje ispunjava uslove za pritvor zbog vanrednih okolnosti pustiti da se brani sa slobode (i time rizikovati da ponovi krivična dela) ili mu suditi u odsustvu, čime bi se zadiralo u ustavno pravo na odbranu (jer npr. nije moguće tehnički sprovesti lice iz pritvorske jedinice, što je takođe bilo često u jeku pandemije), pa se ubrzano tražilo rešenje kako dalje organizovati suđenja i istrage.

1. POJAM DIGITALIZACIJE PRAVOSUĐA

Pod digitalizacijom pravosuđa podrazumeva se na proces pretvaranja analognih podataka iz nekog sudskog ili javnotužilačkog predmeta (materijalnih dokaza i drugih dokumenata, fotografija, tabela, video i audio zapisa) u digitalne podatke koji će se dalje koristiti na brži i jednostavniji način (u vidu nekog kompjuterskog programa, npr. u „pdf" ili „mp4" formatu). Zanimljivo da se u engleskom jeziku pravi razlika između ovog procesa (*digitisation*) i faze koja ga sledi –u kojoj se pomoću digitalne tehnologije vrši procena digitalnih podataka kako bi se donela bolja poslovna odluka ili novi poslovni model (*digitalisation*).

Digitalizacija pravosuđa je od strane naše pravosudne i čitave društvene zajednice prihvaćen i poželjan proces koji već traje duži niz godina. On se promenljivim tempom aktivno odvija uporedo sa digitalizacijom pojedinih drugih sektora u našem društvu. Izlišno je u 21. veku govoriti o potrebi i prednostima generalne društvene modernizacije, a koja obuhvata i informatički transfer podataka koje koristi naše pravosuđe u digitalni oblik.

Vlada Republike Srbije usvojila je Strategiju razvoja digitalnih veština u Republici Srbiji za period od 2020. do 2024. godine, kao nacionalni strateški program kojim se na celovit način uređuje razvoj digitalnih veština stanovništva. Strategija odražava kontinuitet i naslanja se na Digitalnu agendu za Srbiju koju čine Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine i Strategija razvoja elektronskih komunikacija u Republici Srbiji od 2010. do 2020. godine. Važno je spomenuti da u Srbiji od 2017. godine postoji i deluje telo nadležno za poslove digitalizacije - Kancelarija za informacione tehnologije i elektronsku upravu. Kancelarija obavlja stručne poslove koji se odnose na: razvoj i funkcionisanje sistema elektronske uprave, učešće u uspostavljanju i vođenju informacionih sistema u kojima organi državne uprave i imaoci javnih ovlašćenja vode podatke u registrima od značaja za pružanje usluga elektronske uprave, zatim povezivanje podataka iz registara u nadležnosti drugih državnih organ, pripremu podataka za razvoj sistema veštačke inteligencije i obradu od strane državnih organa i organizacija i privrede, uz sprovođenje mera zaštite podataka o ličnosti, naročito pseudonimizacije i anonimizacije itd.

Kod upotrebe digitalnih podataka i digitalne tehnike u procesu dokazivanja nema takvog saglasja. O dokaznoj snazi digitalnih podataka u krivici se sa nepromenjenom žestinom i dalje vode rasprave, u smislu da li je dokaz i način njegovog pribavljanja zakonit ili ne. Sa stanovišta zaštite pravičnosti i nepristrasnosti suđenja, najspornija je upotreba novih digitalnih tehnologija u samom procesu suđenja, putem video-linka i bez fizičkog prisustva okrivljenog ili njegovog advokata pred sudom, kao rešenje tzv. „pravosuđa na daljinu".

2. DIGITALIZACIJA U ZEMLJAMA EVROPSKE UNIJE

Digitalizaciju pravosuđa u državama Evropske unije (EU) odlikuju komponente međunarodne pravne saradnje i otklanjanje prepreka koje donosi različitost pravnih sistema u EU. U okviru toga, poslednjih godina EU je preduzela korake za modernizaciju informacionih sistema koje koriste službenici za sprovođenje zakona u odgovarajućim državama članicama kako bi se bolje omogućila prekogranična saradnja u krivičnim predmetima. Konkretno, organi za sprovođenje zakona EU, uključujući *Europol*, *eu-LISA* i *Frontek*, opremljeni su najsavremenijim digitalnim (ICT) alatima za prikupljanje i razmenu informacija i mogu da razmenjuju i obrađuju operativne podatke u dobro osmišljenom, šifrovanom i potpuno automatizovanom postupku.

Osim toga, usluge koje pruža zajednički informacioni sistem za prenos i razmenu podataka e-CODEX (e-Justice Communication via Online Data Exchange) omogućava sigurnu komunikaciju između država članica u oblasti pravosuđa. Šira vizija e-CODEX je da svaki građanin ili pravni stručnjak u EU može elektronski komunicirati sa bilo kojim pravnim autoritetom, uključujući komunikaciju pravnih organa međusobno. Sistem e-CODEX se trenutno primenjuje za evropske istražne i platne naloge, postupke za sporove male vrednosti, međusobno priznavanje novčanih kazni i zatvorske kazne. Planirano je da se primena sistema e-CODEX proširi i na razmenu elektronskih krivičnih dokaza između pravosudnih organa (Carrera, Mitsilegas, Stefan, 2021: 47).

3. DIGITALIZACIJA PRAVA U PRIVATNOM SEKTORU

Zanimljivo je našu temu sagledati iz dva, na prvi pogled slična, ugla. Dok pod digitalizacijom pravosuđa podrazumevamo deo šireg reformskog društvenog procesa modernizacije našeg pravnog sistema u celini i poboljšanja javnih usluga čiji su konzumenti svi građani, digitalizacija prava u privatnom sektoru tema je za sebe. Ona je pre svega usmerena na potrebe advokature i subjekata privrednog poslovanja u Srbiji. Prvi, kao pravni zastupnici građana pred organima javne vlasti, nužno će biti zainteresovani da se u najranijoj fazi uključe u proces digitalizacije pravosuđa i da tehnološki i idejno u svom svakodnevnom radu pariraju novim rešenjima koje ćemo nadamo se uskoro videti u našim sudovima. U zamišljenoj percepciji budućnosti našeg pravosuđa možemo da očekujemo pretežnu korespodenciju pravosudnih organa, advokata i građana na digitalnoj osnovi. Privredni sektor, pod kojim ovde mislimo na pravnike i pravne službe u privredi, prepostavljamo imaće svoje prioritete i neće biti u tolikoj meri zainteresovan za digitalizaciju pravosuđa. Jedan aspekt digitalizacije u privredi predstavlja ostvarenje digitalne komunikacije između privrednih društava i države (daleko šireg kruga državnih subjekata od pravosuđa), a drugi aspekt ostvarenje digitalne komunikacije između privrednih društava i različitih subjekata od značaja za poslovanje privrednih društava: vlasnika, poverilaca, zaposlenih, potrošača itd. (Vujisić, 2019) Po prirodi stvari, tu moramo da izuzmemo naše privredne sudove koji rešavaju o privrednim sporovima i koji su oduvek u fokusu svih privrednih subjekata.

Razmatrajući uticaj digitalizacije na privatni sektor ipak možemo da uočimo da on neće biti ravnomeran na sve pravne oblasti. Pojedina istraživanja sprovedena u zemljama EU već su ukazala da se prema stepenu i obimu posledica koje će pogoditi pravnike u nejavnom sektoru posebno izdvajaju oni koji rade u oblastima zaštite podataka o ličnosti, poštovanja i zaštite ljudskih prava i IT bezbednosti. Nešto manji uticaj se očekuje na oblasti ugovornog prava, deliktnog prava i prava intelektualne svojine, a znatno manji na pravo konkurencije, poresko pravo, radno pravo i opšte civilno pravo (BDI: 2015).

Ako sagledamo postojeću regulativu u EU, videćemo da se insistira na zaštiti podataka o ličnosti (GDPR) i da se u tome posebno vodi računa o "ranjivosti" ove zaštite prilikom opšteg naleta digitalizacije (Fondacija SHARE: 2017). Kao posebno važna predstojeća pitanja o kojima će razmatrati države-članice izdvajaju se zaštita podataka o zaposlenima, primena digitalizacije energetske tranzicije i usvajanje zakona o e-zdravstvu.

4. CILJEVI DIGITALIZACIJE PRAVOSUĐA

Neizbežni proces digitalizacije srpskog pravosuđa bi trebalo da ostvari nekoliko ciljeva:

1) *progresija učinkovitosti pravosuđa u celini.* Elektronsko vođenje krivičnih predmeta i pribegavanje video-konferencijama pod propisanim uslovima u našim sudovima i javnim tužilaštvima sa sobom će doneti značajno ubrzanje krivičnih istraga,

suđenja i drugih radnji koji spadaju u krug poslova pravosuđa. Ako se digitalizacija bude uskladila sa modernizacijom drugih državnih sektora sa kojima pravosuđe po prirodi stvari sarađuje i na koje se oslanja (policija, inspekcijski organi, poreska, carina, javni beležnici, katastar nepokretnosti) možemo očekivati značajno bolje rezultate u rasvetljavanju i progonu krivičnih dela i njihovih učinilaca;

2) *veća ekonomičnost krivičnih postupaka.* Osim veće efikasnosti sistema, brža razmena dokaza, podataka i informacija između pravosudnih organa doneće i manju potrebu za trošenjem materijalnih i personalnih resursa države - manji broj dokaznih i operativnih radnji, istražnih ročišta, sudskih pretresa i sednica koje je potrebno sprovesti, time i nosilaca pravosudnih funkcija, stručnih lica i ustanova, prateće administracije i drugog državnog osoblja, sudnica, papira i drugog materijala koji prati svaki krivični postupak. Zamislimo samo benefit od uštede vremena, energije i novca koji se potroše pri kopiranju spisa samo jednog predmeta koji se predaju strankama ili šalju drugom pravosudnom organu uz zahtev za pravnu pomoć. Bilo bi zanimljivo sprovesti istraživanje o broju odloženih suđenja u Srbiji usled tehničkih nemogućnosti zatvorskih uprava da izvrše sprovod pritvorenika do sudnice ili o visini isplaćenih putnih troškova učesnicima u krivičnom postupku;

3) *brža komunikacija pravosudnih organa.* Novi komunikacioni alat bi trebalo da bude tako programiran da korisnicima omogući razmenu velikih količina informacija, poruka i dokaza na jednostavan način i u kratkom roku. Ovo posebno dobija na značaju na polju prekogranične saradnje pravosudnih organa u zajedničkim istragama ili kod zamolnica za međunarodnu pravnu pomoć;

4) *lakši pristup spisima predmeta.* Osim lakšeg rukovođenja predmetima i brže međusobne komunikacije učesnika, u redizajniranom elektronskom sistemu rukovođenja predmetima u sudu i javnom tužilaštvu jednim klikom moći će da se strankama i advokatima (ako imaju pravni interes podrazumeva se) omogući pristup spisima predmeta. Na taj način će se osigurati ne samo da sistem pravilno funkcioniše, nego i da odgovara potrebama svojih korisnika, što je i korak bliže standardima jednakosti oružja i pravičnosti sistema u krivici. U skladu sa Uredbom o kancelarijskom poslovanju organa državne uprave (*Službeni glasnik RS*, br. 21/20 i 32/21) koja počinje da se primenjuje 1. februara 2022. godine u toku je razvoj softverskog rešenja "Pisarnica" koje će biti jedinstveno na nivou cele države i biće na raspolaganju, kako svim državnim organima, tako i jedinicama lokalne samouprave (Pisarnica: 2022). Videćemo da li će primena ove ili slične aplikacije obuhvatiti i srpsko pravosuđe;

5) *preventivni karakter digitalizacije u sprečavanju kriminaliteta.* U našoj pravnoj doktrini postoje shvatanja koja osim navedenih prednosti ukazuju da digitalizacija doprinosi i suzbijanju kriminaliteta. Naime, uobičajene preventivne metode više nisu dovoljne, zbog čega bi trebalo razmisliti o mogućnostima korišćenja modernijih metoda. Preventivni uticaj digitalizacije video bi se tako u digitalizaciji identiteta i potpisa građana i predstavnika pravnih lica, digitalizaciji sredstava plaćanja - tzv. digitalna imovina, upotreba savremenih računara i mobilnih aplikacija (Dimovski, 2021);

6) na posletku i ništa manje značajno je da se jedino upotrebom tehničkih sredstava za audio i video snimanje (ili makar samo audio) u krivičnom postupku može obezbediti puna primena normi važećeg Zakonika o krivičnom postupku. To se u fazi istrage (čak i pre donošenja naredbe iz člana 298. o njenom sprovođenju) odnosi najviše na potrebu za snimanjem saslušanja osumnjičenog, čime se ujedno osnažuje zakonitost same dokazne radnje i jačaju garancije za fer suđenje otklanjanjem mogućnosti da se silom ili prinudom vrši pritisak na okrivljenog.

5. POŠTOVANJE EU STANDARDA U OBLASTI DIGITALIZACIJE

Iskustva pravosudnih sistema sa područja EU koji su u velikoj meri digitalizovani ukazuju nam da se u tom procesu posebno moraju poštovati osnovna prava i slobode čoveka i građanina: pravo na privatnost, bezbednost podataka i komunikacije, zaštita ličnosti, pravo na odbranu i pravičnost suđenja. Digitalizacija, s toga, predstavlja veliki izazov za sektor pravosuđa. Važno je permanentno pratiti njen tok i pažljivo strateški planirati faze njenog sprovođenja u praksi.

Od svih navedenih izazova čini se da je segment *data protection-a* najveći u ovom procesu. Krivični postupci, sami za sebe i po prirodi stvari, su osetljivi iz ugla zaštite ličnih podataka i osnovnih prava i sloboda pojedinca. Ubrzanje krivičnih postupaka nikada ne sme ići na uštrb poštovanja osnovnih principa krivičnog prava, utkanih u naš Ustav i zakon – pre svih pretpostavke nevinosti, principa neposrednosti (osobito u odnosu na okrivljene koji su uhapšeni ili su u pritvoru), prava na delotvornu odbranu (i neposrednu) i na kraju zaštite privatnosti i osetljivih podataka iz predmeta. Uporedo sa digitalizacijom i prebacivanjem velikog broja podataka o ličnosti iz analogne u digitalnu formu sve češće se pojavljuju ozbiljni slučajevi zloupotreba ličnih podataka i narušavanja prava na privatnost pojedinaca. Zbog toga je danas trend u svetu da se obezbedi što efikasnija pravna zaštita ovih vrednosti, kako na međunarodnom tako i na nacionalnom nivou. Garant takve zaštite na tlu EU danas je Evropski sud za ljudska prava koji efikasno sankcioniše sve povrede Evropske konvencije o ljudskim pravima i slobodama. Zaštita je dodatno unapređena usvajanjem Opšte uredbe o zaštiti fizičkih lica u odnosu na obradu podataka o ličnosti i slobodnom kretanju takvih podataka iz 2016 godine (GDPR), sa početkom primene od 2018. godine (Prlja, 2021).

U tom kontekstu napominjemo da je u Republici Srbiji neovlašćeno prikupljanje ličnih podataka propisano čak i kao krivično delo (član 146. Krivičnog zakonika). Krivično će odgovarati onaj ko podatke o ličnosti koji se prikupljaju, obrađuju i koriste na osnovu zakona neovlašćeno pribavi, saopšti drugom ili upotrebi u svrhu za koju nisu namenjeni, kao i onaj ko protivno zakonu prikuplja podatke o ličnosti građana ili tako prikupljene podatke koristi. Zaprećena je novčana kazna ili zatvor do jedne godine, osim ako delo učini službeno lice u vršenju službe kada mu preti zatvor do tri godine.

Na putu ka predstojećoj digitalnoj reformi našeg sudstva valjalo bi se držati određenih standarda koji su druge države dostigle u ovoj oblasti:

Prvo, razmena digitalnih podataka između sudija, tužilaca, advokata, administrativnog osoblja i pravosudnih organa između sebe (na nacionalnom ili prekograničnom nivou) mora se odvijati kroz jedan ***bezbedan komunikacioni kanal***. Svako ilegalno „upadanje" u sistem ugrozilo bi privatnost učesnika postupka, bezbednost i snagu dokaza i normalno odvijanje krivičnog postupka. Zbog toga će biti neophodno da pristup sistemu i način korišćenja podataka kontinuirano obezbeđuju posebne IT službe u sudovima i tužilaštvima.

S druge strane, povećanje brzine razmene informacija između nadležnih javnih organa ***ne sme da postane nedostatak za advokate odbrane***, niti da podriva efikasnost dostupnih pravnih lekova za pojedince, uključujući mogućnost da se ospori relevantnost, tačnost ili zakonitost dokaza prikupljenih u drugoj državi. Naprotiv, digitalizovani spisi predmeta naspram papirnih dosijea trebalo bi da svojom praktičnošću značajno olakšaju svakodnevni rad advokata odbrane. Umesto glomaznih spisa u torbi, ponesite prenosni računar i nosače memorije.

Treće, bitan uslov primene bol koje mere digitalizacije pravosudnih sistema jeste da upotreba digitalnih tehnologija i sredstava elektronske komunikacije ne ugrožava procesna prava učesnika u sudskom postupku: pravo na saslušanje, pravo na jednakost procesnih sredstava, pravo na kontradiktoran postupak, pravo na žalbu, pravo na javnost (Soković, 2021: 244-245). Među tim pravima najugroženije bi bilo ***pravo okrivljenog da bude fizički prisutan na svom prvom saslušanju pred sudijom (tužiocem)***, a koja opasnost se nikako ne sme *a priori* zanemariti. Pravo na usmeno saslušanje i po potrebi fizičko prisustvo u sudnici je zagarantovano i međunarodnim pravom i pravom EU (Carrera, Mitsilegas, Stefan, 2021: 40), tako da se pribegavanje video-konferencijskoj vezi ne može se smatrati valjanom alternativom u takvim okolnostima. Ako se to ne može izbeći (npr. zbog specifičnosti slučaja ili razloga poput pandemije), daljinskom saslušanju pritvorenika moguće je pristupiti samo izuzetno i pod uslovom da se obezbedi slobodna i poverljiva komunikacija okrivljenog sa njegovim advokatom i time obezbedilo puno poštovanje prava na pravično suđenje.

6. DIGITALNI DOKAZI

Postupak digitalizacije u krivičnom pravosuđu, i pored međusobnog preplitanja, ne bi trebalo mešati sa postupkom pribavljanja, čuvanja i korišćenja digitalnih dokaza u krivičnom postupku. Digitalni dokazi mogu biti bilo koja vrsta digitalnog fajla (datoteke) koji potiče iz elektronskog izvora. Ovo uključuje e-poštu, SMS (tekstualne poruke), viber prepisku i komunikacija preko sličnih aplikacija, objave na društvenim mrežama, elektronske finansijske transakcije, audio i video zapisi. Oni se mogu naći na bilo kom serveru ili uređaju koji čuva podatke, uključujući prenosive tehnologije (USB memorije, mobilni telefoni, kućne konzole za video igre, moderni satovi i dr.). U našoj sudskoj praksi oni su još uvek retka pojava naspram materijalnih dokaza klasičnog tipa koji predstavljaju dokaze koje možemo videti i dodirnuti (privremeno oduzete stvari, isprave itd.) i na kojima sudovi najčešće zasnivaj usvoje odluke.

Ova vrsta dokaza se u postupku može prikupiti i izvesti različitim dokaznim radnjama koje poznaje naš Zakonik o krivičnom postupku. Tako je, na primer, na osnovu naredbe suda izvršen pretres stana i drugih prostorija okrivljenog (primenom odredbe člana 152 Zakonika), kojom prilikom je pronađen i uz potvrdu ovlašćenih službenih lica privremeno oduzet hard (član 147 st. 3) disk računara na kojem je pohranjen kompromitujući materijal, nakon čega je po nalogu javnog tužioca isti zapisnički popisan i obezbeđen (zapečaćen i stavljen u depozit). Po predlogu javnog tužioca, sud je odredio pretresanje uređaja od strane stručnog lica (član 152 stav 3) kako bi se kompletna elektronska sadržina učinila vidljivom za sud i stranke. Na taj način sud može gledanjem, slušanjem ili uvidom u njenu sadržinu izvesti dokazivanje ispravom u elektronskom obliku (član 138). Ako je i pored toga za utvrđivanje ili ocenu određenih činjenica u vezi digitalnog materijala neophodno stručno znanje može se odrediti informatičko veštačenje (član 113) kako bi sudski veštak odgovorio na konkretan zadatak veštačenja (npr. da li uvidom u sadržinu hard diska može da se vidi da je okrivljeni komunicirao sa određenim osobama, o čemu, kada, na koji način, koliko često i sl.).

Danas je aktuelno i pitanje domašaja digitilne forenzike, posebne naučne discipline. Digitalni forenzičari, posebno obučena stručna lica danas aktivno učestvuju u otkrivanju krivičnih dela tako što je uz njihovu pomoć moguće oporaviti i analizirati podatke iz elektronskih uređaja koji su izbrisani (ne i trajno uništeni). Ponekad je to jedini ili odlučni način prikupljanja tragova i dokaza izvršenja najtežih krivičnih dela.

ZAKLJUČAK

Dosadašnje iskustvo tehnološko naprednijih zemalja pokazalo je da digitalizacija u bilo kom društvenom sektoru dugoročno donosi velike uštede u državnom budžetu. Potvrda tome je i digitalizacija koju je naša Vlada započela u pojedinim oblastima (digitalizacija uprave, arhivske građe i sl.). Opravdano se očekuje da će svaki uloženi dinar u digitalizaciju pravosuđa danas, sutra uštedeti dva. Stvaranje uslova za digitalno krivično pravosuđe, po ugledu na model koji postoji u Savetu EU (*digital criminal justice - DCJ*), omogućio bi široj pravosudnoj zajednici da brzo i efikasno komunicira i razmenjuje kritične informacije i dokaze tokom čitavog postupaka.

Ekonomičnost postupka ipak nije najvažnije načelo krivičnog procesnog prava. U primeni krivičnih propisa primarno je poštovanje sloboda i prava okrivljenog lica, a njihovo ograničavanje dozvoljeno samo izuzetno i kada to zakon propisuje kao nužno. S toga, primenu tehnologija u krivičnim postupcima, poput alata za video konferencije i suđenje na daljinu trebalo bi koristiti oprezno, na jedan nediskriminatoran, vremenski ograničen, dokazano neophodan i proporcionalan način koji će odražavati sve karakteristike pojedinačnog slučaja.

U tom svetlu, u skorijoj budućnosti bilo bi poželjno osmisliti strategiju modernizacije postojećeg sistema evidentiranja i upravljanja u krivičnim predmetima (sudski LIBRA i tužilački SAPO programi) i usvajanja novih digitalnih alatki. Prvi poželjan

korak ka tom cilju bio bi stvaranje stručne radne grupe, sastavljene od relevantnih predstavnika pravne struke, sa zadatkom da utvrde uslove i prioritete za potpuni prelazak na platformu *e-pravosudja,* sa akcentom na zaštitu građana od bilo kakve pravne nesigurnosti. Pre usvajanja odgovarajućih zakonodavnih instrumenata kojim bi se regulisala relevantna pitanja, u okviru ministarstva nadležnog za pravosuđe i najviših sudskih i tužilačkih pravosudnih tela potrebno je najpre osmisliti strategiju razvoja digitalizacije pravosuđa u celini i po sektorima, kao i u celini i po određenim fazama. Bilo bi poželjno da proces razmatranja i odlučivanja na ovom putu bude obogaćen transparentnim konsultacijama sa profesurom, strukovnim udruženjima i nevladinim sektorom, najpre u vidu organizacije javnih debata na zadatu temu.

Rezultat takvog postupanja bila bi, s toga, zakonodavna inicijativa za digitalizaciju srpskog pravosuđa i njegova harmonizacija sa postojećim sistemima EU. Svesni smo da to ipak nije krajnji cilj i poslednji zadatak nadležnih. Neophodno je već u najranijim fazama osmisliti od strane koga, na koji način i u kojim rokovima će se usvojena zakonska rešenja i sprovesti u praksi. Povrh svega, potrebno je predvideti i posebno telo koje će biti zaduženo za nadzor i evaluaciju čitavog postupka digitalizacije. Da zaključimo, za digitalizaciju prava neophodno je pravo o digitalizaciji (Oster: 2021).

Digitalizacija krivičnog prava i našeg pravosuđa logičan je i nužan korak ka razvoju našeg društva i modernom i efikasnom srpskom pravosuđu koje je spremno da odgovori na izazove digitalnog doba u XXI veku.

LITERATURA

1. Carrera, S., Mitsilegas,V., Stefan, M. (2021) *Criminal Justice, Fundamental Rights and the Rule of Law in the Digital Age*, Brussels: Centre for European Policy Studies, https://www.ceps.eu/wp-content/uploads/2021/05/Criminal-Justice-Fundamental- Rights-and-the-Rule-of-law-in-the-Digital-Age.pdf [28. 11. 2022].
2. Dimovski, D. (2021) „Prevencija kriminaliteta putem digitalizacije", Niš: *Zbornik radova Pravnog fakulteta u Nišu,* vol. 60, br. 91, 227 – 242.
3. Oster, J. (2021) „Code is code and law is law—the law of digitalization and the digitalization of law", *International Journal of Law and Information Technology*, Volume 29, Issue 2, 101-117, https://doi.org/10.1093/ijlit/eaab004 [28. 11. 2022].
4. Prlja, D. (2021) „Digitalizacija i zaštita podataka", *U: Zborniku radova sa Međunarodne naučne konferencije Pravo i digitalizacija,* (G. Obradović, M. Dimitrijević (ur)), Niš: Pravni fakultet Univerziteta u Nišu, http://www.prafak.ni.ac.rs/files/centar_pub/zbornika-sazetaka-pravo-i-digitalizacija-april-2021.pdf [28. 11. 2022].
5. Soković, S. (2021) „Postavljanje EU standarda digitalne transformacije pravosuđa sa posebnim osvrtom na krivično pravosuđe", *Zbornik radova Usklađivanje pravnog sistema Srbije sa standardima EU*, (Snežana Soković (ur.)), Kragujevac: Pravni fakultet Univerziteta u Kragujevcu, 239 – 253.
7. Vujisić, D. (2019) „Digitalizacija kompanijskog prava", *Pravo i privreda,* 57(4-6), 144-153.

Pravni izvori

1. GDPR (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
2. Krivični zakonik, *Službeni glasnik RS,* br. 85/2005, 88/2005-ispr., 107/2005-ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019.
3. Ustav Republike Srbije, *Službeni glasnik RS,* br. 98/2006 i 115/2021.
4. Zakonik o krivičnom postupku, *Službeni glasnik RS*, br. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14, 35/19, 27/21, 62/21.
5. Zakon o zaštiti podataka o ličnosti, *Službeni glasnik RS*, br. 87/2018.

Internet izvori

1. BDI (2015) Industrie 4.0 - Legal challenges of digitalisation, BDI, Federation of German Industries, https://www.noerr.com/~/media/Noerr/PressAndPublications/Brochures/studien/Legal-challenges-of%20digitalisation-Industrie-40.pdfFondacija [28. 11. 2022].
2. Pisarnica (2022) Kancelarija za informacione tehnologije i elektronsku upravu Republike Srbije, https://www.ite.gov.rs/tekst/sr/6063/pisarnica.php [28. 11. 2022].
3. Razvoj digitalnih veština i kompetencija: Brzi pregled stanja 13 modela digitalne pismenosti, Studije medija, inovacije i tehnologije, Univerzitet Brije, Belgija, https://www.nb.rs/view_file.php?_id=5610 [28. 11. 2022].
4. SHARE (2017) SHARE@WORK 2016 – Monitoring digitalnih prava i sloboda u Srbiji, https://labs.rs/Documents/Monitoring_digitalnih_prava_i_sloboda_izvestajza_2016_srb.pdf [28. 11. 2022].

THE IMPORTANCE OF DIGITALIZATION OF THE SERBIAN JUDICIARY

In this paper author points to the importance of digitalization of the Serbian judiciary. With the entry into the third decade of the 21st century, the issue of digitalization, actualized by the Covid-19 pandemic, has significantly exceeded the current need to reorganize the work of state bodies, competent institutions and communication with citizens, and thus adapt them to new health and social circumstances. In the sector of the judiciary, which independently seeks to solve a large number of old cases, greater efficiency and lower consumption, the need for digitalization is even more pronounced.

The paper analyzes the use of existing digital forms in criminal proceedings (digital evidence) and gives a brief overview of certain comparative legal decisions on the digitalization of the judiciary, points out the goals and benefits of implementing this process in our country, while emphasizing the importance of adhering to EU standards on this path in order to avoid or minimize potential abuses and violations of human rights and freedoms.

KEYWORDS: *digitalization of judiciary, digital evidence, modernization, economy, personal protection and human rights*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.06

DIGITALIZACIJA PRAVOSUĐA U REPUBLICI SRBIJI
– primena u praksi i izazovi –

Jelena Samuilov*

Proces digitalizacije je je postao sastavni deo svakog aspekta društvenog života, i sledstveno tome i pravosuđa. Navedeni proces je brz i mora se držati korak sa njim, što vrlo često zahteva značajna finansijska sredstva, kao i dodatno obrazovanje. U pravosuđu kao sastavnom delu društvenog života, digitalizacija je takođe neophodna jer podrzumeva efikasnije pravosuđe, bržu komunikaciju, i smanjenje troškova, ali taj proces ne ide jednakom brzinom u pravosuđu država članica EU i u Republici Srbiji. Proces digitalizacije pravosuđa u Republici Srbiji je započet odavno, ali se vrlo sporo razvija. Razlozi za to su brojni. Iako postoji zakonska regulativa koja podrazumeva digitalni pristup radu, zakonska rešenja su načelna i nedovoljna i ostavljaju mnogo prostora za nedoumice ili onemogućavaju upotrebu digitalnih sredstava u potpunosti, ali utiču i na postupak dokazivanja. Nadalje se kao prepreka primeni u digiltalizaciji pojavljuje neodostatak dovoljno dobre tehničke opreme, ili opreme uopšte, neodvoljno razvijeni i pouzdani programi, isključenje internet mreže, nepostojanje adekvatnih platformi kojima bi bili povezani svi relevantni državni organi za razmenu informacija, tako da je primena digitalizacije u krivičnim postupcima vrlo sužena i svodi se na izradu akata (koji se opet štampaju i dostavljaju drugim organima u papirnom obliku), korišćenje elektronske pošte, formiranje i ažuriranje zvaničnih sajtova tužilaštava i sudova, pristup evidencijama MUP-a i pojedinih državnih organa i tek u ponekim tužilaštvima upotreba SAPO programa, kao elektronske evidencije predmeta. Posebno su prisutni problemi zbog nedovoljno razvijene digitalizacije bili izraženi za vreme pandemije virusa COVID 19, kada pravosuđe Srbije nije bilo ni tehnički ni organizaciono spremno da sprovede postupke. Dok se pravosuđe u Srbiji susreće sa mnogim izazovima u pogledu digitalizacije, u državama članicama Evropske unije proces digitalizacije je u mnogome odmakao jer je pandemija virusa COVID 19 pokazala da je digitalizacija u pravosuđu neophodna, ali je takođe pokazala kakvi su neodstaci u digitalizaciji, te se sada preduzimaju koraci kako bi se postojeća dostignuća unapredila ili iznašla bolja rešenja, posebno iz razloga što pravosuđe EU odlikuje međunarodna pravna saradnja i različiti nacionalni pravni sistemi. Pored već postojećih platformi od kojih su najrazvijeni i najveše kroišćeni E-uprava i e-CODEX koji se koristi za istražne naloge, sprove male vrednosti, platne naloge između država članica, radi se na poboljšanju platformi u krivičnom pravosuđu, posebno u okviru Eurojust-a, Europola i sličnim sastavima i u tom pogledu je

* Zamenik osnovnog javnog tužioca u Pančevu. E-mail: *jsamuilov@pa.os.jt.rs* • *jsamuilov@gmail.com*

napravljen paket mera. Kako bi pravosuđe u Srbiji postalo efikasnije primena digitalizacije se mora unaprediti. To bi podrazumevalo veliku finansijsku podršku i to kako u vezi nabavke adekvatne i kvalitetne tehničke opreme, tako i u organizaciji i izmeni zakonodavstva. Korist od tog ubrzanog procesa bi bili značajna, doprinela bi boljoj organizizaciji i efikasnosti pravosuđa, ali i smnajneju troškova postupka.

KLJUČNE REČI: *digitalizacija pravosuđa, krivični postupak, tehnička opremljenost, primena u praksi.*

UVOD

Digitalizacija i razvoj tehnologija su poslednjih godina postali nezamenljiv deo svakodnevnog života od obavljanja svakodnevnih poslovnih delatnosti do slobodnog vremena i zabave. Digitalna tehnologija se neprestano i ubrzano razvija. U takvim okolnostima se nije moguće uvek i na adekvatan način snaći imajući u vidu ne samo brzinu dostignuća, već i mogućnosti da se inovacije prihvate. No, kao i svaki drugi segment života i digitalizaciju moramo prihvatiti i ići u korak sa njom. Kao i kod svih drugih sfera savremenog života i digitalizacija ima svojih benefita, koje treba iskoristiti maksimalno, kao što su brzina komunkacije, ušteda vremena u razmeni podataka, smanjenje troškova, ali u isto vreme, izbeći, u najvećoj meri, njene nedostatke, posebno one koji se tiču osnovnih ljudskih prava, koja su zagarantovana svim najvažnijim pravnim aktima država, ali i poveljama UN, kao i u povelji EU o osnovnim ljudskim pravima. Samim tim je primena novih tehnologija praćena mnogim izazovima.

Posebno je pandemija bolesti COVID-19 otvorila pitanje digitalizacije kao važno u svakodnevnom životu. U samom početku pandemije, kada su u svim državama sveta kontakti među ljudima bili ograničeni, primena novih tehnologija i digitalizacija su ublažile posledice zahtevanog postupanja u životima ljudi, poslovi su mogli koliko toliko neometano da se obavljaju, kontakti su se održavali putem ekrana, pa su posledice „zatvaranja" bile na taj način ublažene, ali kako je pandemija dobijala na vremenu i kako je vreme odmicalo postali su uočljivi problemi primene digitalizacije, pre svega se otvorilo pitanje opremljenosti svih da pristupe digitalnom svetu, problem finansijske podrške, pa i problemi sa poštovanjem osnovnih ljudskih prava.

Kako je pravosuđe jedan od stubova svake države, neizostavna sfera svakodnevnog života, to primena novih tehnologija, kao i digitalizacija nije mogla zaobići ni pravosuđe. Imajući u vidu da su pravosudni sistemi država različiti, da imaju različita pravila kao i različitu opremljenost i spremnost za primenu novih tehnologija, to se postavilo i pitanje primene digitalizacije i novih tehnologija kako u nacionalnim zakonodavstvima, tako i u međudržavnoj saradnji, dok se u isto vreme, posebno u toku pandemije virusa COVID – 19 javila i te kako velika potreba za upotrebom novih tehnologija u pravosuđu.

1. DIGITALIZACIJA PRAVOSUĐA U SRBIJI

1.1. Zakonske mogućnosti u krivičnom pravu i postupanju tužilaštva

Zakonik o krivičnom postupku u pogledu primene digitalnih sredstava posebno dozvoljava upotrebu novih digitalnih tehnilogija u nekim segmetima, Naime, u čl.242 stav 3 koji se odnosi na dostavljanje, se navodi da se dostavljanje može vršiti i na oglasnoj tabli ili internet stranici organa postupka, ali uz saglasnost lica kome se dostavljanje ima izvršiti i preko punomoćnika za prijem pismena, putem poštanskog faha ili elektronske pošte. Dostavljanje se smatra izvršenim protekom od osam dana od isticanja pismena na

oglasnoj tabli ili internet stranici organa postupka, odnosno prijema potvrde da je predato punomoćniku za prijema pismena, poštanskom fahu, odnosno dostavljeno elektronskim putem. Nadalje, Zakonik o krivičnom postupku u čl. 245 stav 2 i 3 pod posebnim načinom dostavljanja dozvoljava da, ako organ postupka smatra da će obaveštenje biti primljeno, učesnik u postupku, a ako postoji opasnost od odlaganja izuzetno i okrivljeni, se može obavestiti telegramom ili telefonom o pozivu na glavni pretres ili drugom pozivu ili o odluci o odlaganju glavnog pretresa ili drugoj radnji, a o dostavljanju ili obaveštenju izvršenom u skladu sa ovim članom organ postupka će sastaviti službenu belešku. Zastupljenost digitalizacije je načelno proklamovan i u čl. 230 Zakonika o krivičnom postupku u kome se navodi da je moguće podneti elektronski podnesak odnosno da pismeni podnesak može biti sastavljen i u obliku elektronskog dokumenta koji je snadbeven elektronskim potpisom podnosioca, te je navedeno da se ovakav podnesak podnosi organu postupka putem elektronske pošte, a organ postupka mora bez odlaganja podnosiocu da potvrdi elektronskim putem prijem podneska, dok o elektronskom podnesku organ postupka sastavlja službenu belešku.[1]

Poseban osvrt treba dati i rešenju upotrebe modernih sredstava digitalizacije u postupku dokazivanja. Zakonik o krivičnom postupku kao posebne dokazne radnje između ostalih predviđa tajni nadzor komunikacije, tajno praćenje i snimanje, kao i računarsko pretraživanje podataka, s tim da upotrebu ovih posebnih dokaznih radnji vezuje za posebno određena krivična dela propisana čl. 162 ZKP-a, i u tom pogledu predviđa korišćenje telefona, drugih tehničkih sredstava, računara, kao i elektronske adrese osumnjičenih.

Osim Zakonika u krivičnom postupku digitalizacija je predviđena i u Pravilniku o upravi u javnim tužilaštvima gde se u odeljku XIII „Upotreba informaciono- komunikacionih tehnologija u radu javnih tužilašava" u čl. 86-89 predviđa da se u javnim tužilaštvima po pravilu u radu koriste informaciono komunikacione tehnologije za obradu teksta, vođenje evidencija, obradu i prikupljanje statističkih podataka za elektronsku razmenu podataka, računovodstvene poslove, kao i za praćenje propisa, sudske prakse i javnotužilačke prakse. Nadalje se predviđa vođenje elektronskog upisnika i pomoćnih knjiga, kao i razmena podataka sa drugim pravosudnim organima u okviru pravosudnog informacionog sistema Republike Srbije, kao i korišćenjem informaciono - komunikacionoh tehnologija, vršenje razmene podataka sa drugim državnim organima vodeći pri tom računa o zaštiti o tajnosti podtaka. Za ovo Pravilnik o upravi u javnim tužilaštvima predviđa postojanje integralnog informacionog sisitema koji predstavlja jedinstvenu i internu računarsko –komunikacionu mrežu tužilaštava u Srbiji i obuhvata obavljanje poslova iz nadležnosti javnog tužilaštava elektronskim putem, a radi ujednačavanja postupanja i unapređenja rada.[2]

[1] Zakonik o krivičnom postupku (*Službeni glasnik RS,* br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - Odluka US RS i 62/2021 – Odluka US RS).

[2] Pravilnik o upravi u javnim tužilaštvima (*Službeni glasnik RS,* br. 110/2009,87/2010,5/2012,54/2017,14 /2018 i 57/2019).

1.2. Primena u praksi

Poznato je da se pravosuđe u Srbiji od ranije bori u rešavanju velikog broja "starih" predmeta, da se vrlo često pokazuje kao neefikasno i sporo. Doprinos tome svakako leži i u činjenici da se u postupcima pred sudovima i tužilaštvima u Republici Srbiji još uvek postoji kontinuirana upotreba papirnatih spisa, odnosno većina komunikacije se odvija u papirnatom obliku, što dovodi do oslabljene efikasnosti u komunikaciji, posebno između različitih organa, i to u pogledu brzine komunikacije, pouzdanosti i troškova, a ne manje značajno je i pitanje zaštite životne sredine.

Trenutno se najviše prednosti digitalizacije u pravosuđu Srbiji koriste prilikom izrade sudskih i tužilačkih akata, jer su računari u potpunosti zamenili nekada prisutne mehaničke mašine, kao i prilikom čuvanja navedenih akata. Nadalje, značajna je primena digitalne mreže prilikom preuzimanja podataka sa internih mreža (npr. preuzimanje izrađenih akata sa mreže daktilobiroa ili razmena podataka ili akata između zamenika ili sudija). Takođe je u krivičnom postupku značajna i mogućnost pristupa evidencijama MUP-a, kao i državne uprave kroz Pravosudni informacionii sistem kojem imaju pristup ovlašćena lica iz tužilaštava ili suda, što u mnogome olakšava i ubrzava rad u krivičnim postupcima jer se više ne mora čekati na izdavanje pismnih dokumenata koje izdaju navedeni organi, a koji su se neretko čekali i više od jednog meseca.

U primeni je korišćenje elektronske pošte u vidu komunikacije sa drugim državnim organima kao i strankama u smislu dostavljanja različitih dokumenata, obaveznih uputstava, javnotužilačke prakse, pa i u pogledu pozivanja stranaka.

Organizovane su internet stranice svih ili većine tužilaštava i sudova u Republici Srbiji koji su vidljivi preko svih pretraživača i na kojima su istaknuti podaci vezani za rad tužilaštava ili sudova, od organizacione strukture, akata na osnovu kojih se radi ili koje se donose, informatora o radu, servisnih informacija o radu organa, aktuelnosti i saopštenja za javnost.

Nadalje je u okviru Ministarstva pravde pokrenut portal koji se odnosi na mogućnost da se putem interneta prate tokovi predmeta u osnovnim i višim sudovima i to svim zainteresovanim stranama, a koji podaci su preuzeti iz sistem LIBRA, sitema koj se odnosi na rad sudova.

Osim sistema LIBRA, koji se od 2010. godine koristi u sudovima, i koji predstavlja elektornski upisnik i odnosi se na tokove predmeta , u okviru kojih je svaki podnesak skeniran i prikazan u elektoronskom obliku, u tužilaštvima i to samo pojedinim je u upoptrebi program SAPO, koji takođe treba da predstavlja elektornski upisnik, ali obuhvata i kretanje spisa između pisarnice, daktilobiroa i obrađivača, podrazumeva da se u svakom trenutku može znati gde se predmet nalazi i da se ceo postupak izrade akata u tužilaštvu obavlja elektronski, kao i da više ne postoje upisnici koji se vode ručno.

1.3. Problemi u javnotužilačkoj praksi

Digitalizacija se, sa svom svojom brzinom u razvoju, nametnula kao neophodnost i kao poželjan proces ali koji traje duži niz godina. Ovo sve iz razloga što se proces digitalizacije suočava sa mnogim problemima u našem sistemu. Na prvom mestu treba

pomenuti finansijsku potporu koja u našem sistemu vrlo često izostaje, a koja se ogleda u tome da nedostaje dovoljno dobra tehnička oprema i uslovi, pri čemu se ovde misli na dobre i kvalitetne računare, štampače, dovoljan broj skenera, ali i posebno one opreme koji bi služili za digitalno fotografisanje, skeniranje, video i audio snimanje. Sa druge strane se javlja i problem obučenosti kadrova za korišćenje tehničke opreme i učešće u digitalizaciji uopšte, još uvek imamo izvršioce koji znaju da rade samo u WORD Office formatu, koji ne poznaju druge operativne sisiteme i platforme, niti načine na koji način da upotrebom digitalizacije odnosno njenih benefita unaprede svoj rad.

Problemi sa digitalizacijom u pravosuđu u Republici Srbiji su posebno pokazali kao stvarni i čini se dodatno uvećali kada je u martu 2020. godine proglašeno vanredno stanje usled pandemije izazvane virusom COVID -19. Ono sve što je pandemija i sledstveno vanredno stanje postavilo kao zahteve pred celo čovečanstvo a to su minimiziranje ljudskih kontakata u cilju sprečavanja širenja virusa, u pravosuđu u Srbiji je izazavalo probleme, prvenstveno, jer nije bilo tehnički opremljeno za takav pristup radu, kao ni organizaciono, jer je trebalo oragnizovati „suđenje na daljinu", posebno u krivičnim postupcima, odnosno u postupcima protiv okrivljenih koji su u pritvoru , a koji postupci su hitni i ne trpe odlaganja, a osumnjičenog nije bilo moguće sprovesti iz pritvorske jedinice, kao i u drugim postupcima koji su u to vreme označeni kao postupci koji ne trpe odlaganje (nasilje u porodici, postupci gde su oštećeni maloletna lica ili deca). Dodatno otežavajuća okolnost je bila i ta što je navedena suđenja trebalo oragnizovati, a da se pri tome ne krše osnovna prava okrivljenih u postupku, zagarantovanih našim Ustavom i zakonom, pre svih pretposatvke nevinosti, principa neposrednosti, prava na delotvornu i neposrednu odbranu, zaštite privatnosti i osetljivih podataka iz predmeta[3].

Na isti način se postavlja pitanje sprovođenja suđenja putem video-linka u momentima kad neposredno ispitivanje ili saslušanje nije moguće. Benefit ovakvog korišćenja digitalizacije je nesumnjiva, posebno jer bi se na taj način smanjili troškovi postupka, jer se između ostalog smanjuje potreba za sve skupljim prevozom, te bi se ubrzao postupak, jer se vrlo često dešava da se postupak ne završava u optimalnom roku obzirom da je upravo nemogućnost učesnika u postupku da prisustvuju postupku u zakazno vreme, bilo zbog toga što nemaju novac za prevoz ili zbog toga što su u poslednje vreme sve češće na radu u inostarnstvu, postupci se odlažu na duže vreme. Osim što vrlo često ne postoji tehnička oprema, adekvatna video i audio oprema, kao ni dovoljno drugih mogućnosti za takvu organizaciju, ovde se kao osnovni problem postavlja pitanje poštovanja osnovnih ljudskih prava i prava okrivljenih zagarantovanih Ustavom i procesnim zakonima. Ovakva mogućnost organizovanja suđenja je prvenstveno uslovljena izmenama zakonodavstva koje bi osiguralo uzajmno poverenje, operativnost, sigurnost i poštovanje osnovnih prava učesnika u postupka, posebno okrivljenih u krivičnim postupcima, a to je pravo na pravično suđenje, pravo na odbranu, pravo učestvovanja u suđenju, pravo na komunikaciju sa advokatom(braniocem), pravo postavljanja pitanja svedocima i pravo osporavnja dokaza. Benefiti

[3] Ustav Republike Srbija(*Službeni glasnik RS,* br.98/2006 i 115/2021), Zakonik o krivičnom postupku, (*Službeni glasnik RS*, br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – Odluka US RS i 62/2021 - Odluka US RS).

video suđenja, odnosno korišćenja video linkova za suđenje bi bili brojni, ali takvu primenu osim tehničke mora pratititi i zakonska podrška i izmena.

Primena digitlanih i audio vizuelnih sredstava bi bila nezamenljiva i prilikom vršenja uviđaja. Uviđaj je posebno važna dokazna radnja kod procesuiranja krivičnih dela prilikom obezbeđivanja dokaza u mnogim krivičnim delima, posebno u oblasti saobraćaja, krivičnih dela protiv životne sredine, opšte sigurnosti i drugih. Tužilac, kao organ koji rukovodi uviđajem mora da ima stručna znanja i neophodnu tehničku opremu kako bi mogao izvesti ovu radnju efikasno i obezbediti dokaze. Imajući u vidu prirodu nekih krivičnih dela tužioci retko imaju stručna znanja, sa druge strane, čak i kada raspolaže dovoljno dobrim stručnim znanjem, nemaju uopšte na raspolaganju tehičku opremu, a vrlo često tu opremu nemaju ni policijski službenici, kao ni eventaulno prisutni inspektori iz određenih oblasti. Neizostavno bi u uviđajima bila potrebna upotreba dronova, uređaja za posebne vrste snimanja, otkrivanja tragova i dokaza ispod zemlje, u vodi i slično.

U praktičnom pogledu digitalizacija potpuno izostaje u radu i zastupanju na sudu. Naime, mnogo bi praktičnije, ali i povezano sa manjim troškovima, bilo da svaki tužilac ili sudija ima svoj računar, ili tablet koji može da nosi sa sobom na suđenje, u kome su u digitalnom obliku predmeti koji se zastupaju na sudu, da se svaki akt predaje organu elektronski, što bi značilo da više nema papirantih spisa koji znaju da teže i po nekoliko kilograma, koje tužilac nosi u rukama u sud ili sudija drži na glavnom pretresu ili ročištu. Ovo bi sa svoje strane zahtevalo izvesnu finansijsku potporu kao i adekvatnu obuku zaposlenih u pravosuđu, kao i veća ulaganja u interne mreže, ali bi na duži rok sasvim sigurno donprinelo smanjenju troškova postupka, kao i zaštiti životne sredine. Ovo podrazumeva da bi i drugi učesnici u postupku (veštaci, stručni savetnici i drugi) mogli dostavljati dokumenatciju i podneske isključivo u elektronskom obliku.

Upotreba SAPO programa od strane tužilaca je ograničena samo na nekoliko tužilaštava u Republici Srbiji, jer iako su svi tužioci bili u obavezi da tokom 2021. godine prođu obuku, primena ovog programa još uvek, čitavu godinu dana posle obuke, uopšte nije zaživela. Brojni nedostaci ovog programa su uočeni još tokom obuke (npr. izuzetno mali prozor u donjem desnom uglu ekrana koji prikazuje tužilački akt, jedva čitljiv i gotovo nevidljiv), izuzetno kompilikovan način prenosa dokumenta, mnogo „koraka" da se dokument pošalje između različitih organizacionih delova tužilaštava, što se sve pokazalo kao problem i u primeni ovog programa u tužilaštvima koji ih koriste, te vrlo česta blokada programa jer je verovatno zahtevan i prevelik za mreže koje su postavljene u tužilaštvima upravo za upotrebu ovog programa. Navedene mreže su se pokazale kao nedovoljno pouzdane i prilikom preuzimanja dokumenata između organizacionih jedinica tužilaštava i tamo gde je SAPO u upotrebi na način da vrlo često pada mreža, da „koči" upotreba programa, da nije moguće uvek preuzeti neki dokument i slično. U pogledu mreže koja je postavljena za upotrebu SAPO programa, kao preventiva za zaštitu mreže, ograničen je spoljni internet, što je trebalo svakako uraditi zbog zaštite podataka, ali je trebalo bolje preispitati koji će sajtovi ostati otvoreni, jer je nekada potrebno u radu koristiti i isključene sajtove (npr. Google mape) kako bi se lakše shvatilo gde se nešto desilo, koja je konfiguracija terena zbog prikupljanja dokaza i slično, posebno ako

prilikom uviđaja nije korišćen dron, koji se po pravilu ne koristi jer ni ne postoji, a i pitanje njegove upotrebe nije do kraja zakonom definisano.

Ovo otvara još jedan problem upotrebe digitalizacije u praksi pravosuđa u Srbiji a to je upotreba digitalnih sredstava u postupku dokazivanja, posebno u krivičnim postupcima. Kao što je napred rečeno Zakonik o krivičnom postupku isto dozvoljava ali u pogledu strogo određenih krivičnih dela, dok se u pogledu drugih krivičnih dela, koja nisu određena ZKP-om, usled vrlo intezivne digitalizacije i mogućnosti elektronskih sredstava, mogu koristiti ova sredstva za prikupljanje dokaza, ali ne postoji jedinstven stav prakse o dozvoljenosti ovako pribavljenih dokaza, a to nije jasno definisano ni u samom Zakoniku o krivičnom postupku. Najčešći primer jeste korišćenje kamera za video nadzor koji se koriste u gradu na javnim mestima, u prodavnicama, školama ili drugim institucijama, kao i snimci koji su načinjeni mobilnim telefonima fizičkih lica. U praksi u pogledu upotrebe tako prikupljenih dokaza još uvek nema saglasnosti da li se radi o dozvoljeno ili nedozvoljeno pribavljenim dokazima.

U pogledu pozivanja, kao i podnošenja elektronskih podnesaka, iako ih Zakonik o krivičnom postupku u potpunosti poznaje i propisuje način na koje se sporovode, ipak ograničava njihovu upotrebu i to od pozivanja samo ako je opasnost od odlaganja u pitanju, dok i za pozivanje i za podnošenje elektronskog podneska zahteva sastavljanje službene beleške u papirnatom obliku koji se stavlja u predmet. Mogućnost prikupljanja dokaza putem digitalnih sredstava i njegovo bolje regulisanje u zakonskim rešenjima bi svakako bilo povezano sa lakšim i bržim dokazivanjem i većim brojem uspešno rešenih predmeta. I sam Pravilnik o upravi u javnim tužilaštvima predviđa da će se, ukoliko se upisnici i pomoćne knjige vode u elektronskoj formi, na kraju svakog radnog dana odštampati uneti podaci i čuvati na način predviđen za čuvanje upisnika.[4]

Već je bilo reči o problemima vezanim za video konferencije odnosno za suđenje putem video linka i ograničenja vezana za taj način rada, ali ne samo u toj primeni, kao veliki problem se javlja i u svim drugim oblastima digitalizacije i njene primene u praksi, problem nedostatka tehničke opreme. Oprema kojom raspolaže pravosuđe u Srbiji u sudovima i tužilaštvima redovne nadležnosti je često vrlo zastarela i dotrajala, ne podržava obim rada u pravosuđu, mreže ne dozvoljavaju nesmetan rad, ne postoji jedinstven elektronski način vođenja predmeta i praćenja njihovih tokova, ograničena je upotreba interneta i time dostupnost velikom broju neophodnih informacija.

U novijim vremenima se takođe povećava broj krivičnih dela učinjenih putem interneta i društvenih mreža. Osim tužilaštva za visoko tehnološki kriminal, druga tužilaštava ne poseduju ni opremu ni dovoljno obučenih izvršilaca da postupaju u ovim predmetima, a kada se sa druge strane uzme u obzir činjenica da posebno odeljnje tužilaštva kao i organ policije koji postupaju u oblasti visoko tehnološkog kriminala postupaju samo u pogledu krivičnih dela koja su određena Zakonom o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala[5], a da je izvršenje i drugih krivičnih dela, koja nisu obu-

[4] Pravilnik o upravi u javnim tužilaštvima (*Službeni glasnik RS*, br. 110/2009, 87/2010, 5/2012, 54/2017, 14/2018 i 57/2019).

[5] Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala (*Službeni glasnik RS*, br. 61/2005,104/2009).

hvaćena ovim Zakonom u ekspanziji, sasvim sigurno se javlja potreba da i tužilaštva, a i sudovi opšte nadležnosti imaju svu adekvatnu opremu i obučene izvršioce, kako bi ova druga krivična dela mogla biti uopšte ili lakše dokazana.

Zbog svih problema sa kojima se digitalizacija u Srbiji susreće, iako je načelno, nophodna njena primena je za sada vrlo ograničena.

2. PRIMENA DIGITALIZACIJE U PRAVOSUĐU U DRŽAVAMA ČLANICAMA EVROPSKE UNIJE

2.1. Izazovi u dogitalizaciji pravosuđa EU i rešavanje problema

Digitalizacija u pravosudnim sistemima država članicama Evropske unije je takođe pred velikim izazovima, imajući u vidu da digitalizaciju u ovim državama odlikuje međunarodna pravna saradnja i otklanjanje prepreka usled različitih pravnih sistema država članica. Posebno je taj problem bio izražen u pandemiji COVID- 19 koja je pokazala potrebu država članica za delotvornijim pravosuđem, te su države članice pokrenule niz inicijativa u pogledu digitalizacije pravosuđa. Pandemija je podstakla potrebu da EU ubrza nacionalne reforme za digitalizaciju rešavanja predmeta, razmene informacija i dokumenata sa strankama i advokatima, te svima omogući kontinuiran i jednostavan pristup pravosuđu, a kako je to definisano i Izveštaju o vladavini prava za 2020. godinu.[6] Ovu potrebu su prepoznali i Savet Evrope u Evropski Parlament i doneto je niz zaključaka koji vode tome da se u EU ubrza digitalizacija pravosuđa. Iako je urađeno dosta u tom pogledu ipak je prepoznata potreba da se dodatno ojačaju i kapaciteti pravosuđa i na nacionalnim i na evropskom nivou u pogledu digitalizacije pravosuđa. Imajući u vidu da je Evropska komisija, radeći na Izveštaju o digitalizaciji pravosuđa utvrdila da postoje brojni izazovi koji se stavljaju pred države članice u procesu digitalizacije pravosuđa, kao što su, između ostalog, nemogućnost jednakog pristupa elektronskom prvaosuđu, a u kontekstu krivičnog prava, žrtve mogu pristupiti elektronskom spisu samo u sedam država članica, a okrivljeni u devet, da se dokazi mogu podneti isključivo u digitalnom obliku u krivičnim postupcima u 13 država članica, da je i dalje kontinuirana upotreba papirnatih spisa, ali da se u postojećem zakonodavstvu EU ne propisuju mehanizmi ni detaljni aranžmani za digitalne prenose podatka i informacija, što značajno otežava i usporava komunikaciju između pravosudnih organa država članica.[7]

Paket instrumenata koji je od strane ove Komisje predložen za digitalizaciju pravosuđa se može svrstati u četiri tačke :1. Finasijska podrška državama članicama, kako bi se iskoristio potencijal za stvaranje dugoročnog učinka; 2. Zakonodavne inicjative, kako bi se utvrdili zahtevi za digitalizaciju u cilju boljeg unapređenja i boljeg pristupa pravosuđu; 3. Informatički alati, koji se mogu nadograditi i koristiti u svim državama članicama, s tim da

[6] Izveštaj o vladavini prava za 2020. godinu –Stanje vladavine prava u Evropskoj uniji (COM(2020)580 final) i Komunikacija komisije Evropskom parlamentu, vijeću, Evropskom gospodarskom i socijalnom odboru i odobru regija, https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX:5202DC0710, [19.09.2022.].

[7] *Ibidem.*

se njihovom upotrebom moraju obezbediti privatnost, zaštita podataka i transparentnost; i 4. Unapređenje nacionalnih instrumenata za koordinaciju i praćenje kojima bi se između ostalog obezbedila i razmena iskustava i primera dobre prakse. Ovaj paket instrumenata obuhvata obavezujuće i neobavezujuće mere. Obavezna digitalizacija je potrebna u području postupaka prekogranične saradnje kako bi se omogućila delotvorna i brza prekogranična saradnja, dok drugi alati nisu obavezujući i ukuljčuju mogućnost za razmenu informacija i primera dobre prakse. Sve mere koje se odnose na digitalizaciju pravosuđa moraju da se sprovode uz potpuno poštovanje osnovnih prava, kao što su pravo na zaštitu ličnih podataka, na pošteno suđenje i na delotvoran pravni lek, te načela propocionalnosti i supsdijarnosti, te se u parničnim psotupcima mora osigurati jednakost procesnih sredstava.[8]

2.2.Primena digitalizacije u pravosuđu država članica EU-informatički alati

U pogledu novih informatičkih alata posebno se javila potreba razjasniti da li je potrebno i u kojoj meri koristiti određene aplikacije „veštačke inteligencije". U istraživanju Evropske komisije je utvrđeno da pravosudna tela sve više koriste ove aplikacije, te da su od posebnog značaja u području pravosuđa anonimizacija sudskih odluka, pretvaranje govora u tekst i transkripcija, mašinsko prevođenje, *chatboti* kojima se podupire pristup pravosuđu i robotska automatizacija procesa (automatizacija postupka kao što su organizacija, planiranje i upravljanje objektima, određivanje prioriteta, kategorizacija i raspodela dokumenata i zadataka upotrebom robotskog programa).[9] Postoje različiti stavovi u pogledu primene aplikacija „veštačke inteligencije" u pravosuđu država članica, jer iako su prednosti njihove upotrebe jasne, postoje i znatni rizici za povezani sa njihovom upotrebom u pogledu poštovanja osnovnih ljudskih prava. U tom pravcu je pokrenuto javno savetovanje i na osnovu svih predloga koje su tokom javnog savetovanja dali evropske i nacionalne advokatske komore, pravni stručnjaci i članovi akademske zajednice, kao i članovi civilnog društva, radiće se na poboljšanju ovih aplikacija zasnovanih na veštačkoj inteligenciji kako bi se ista unapredila i izbegli za sad prepoznati rizici.

U okviru država članica EU se već može koristiti alatima za javno informisanje kao što su EUR-Lex[10] i evropski portal E-pravosuđe.[11] E-pravosuđe omoćuva pristup informacijama o pravosuđu i glavni je izvor pravnih i praktičnih informacija u domenu pravosuđa u EU za širu javnost. Njime se omogućuje i pristup međusobno povezanim registrima između ostalim i poslovnih registara (BRIS), koji omogućuje pristup poslovnim registrima i informacijama o više od 20 miliona društava sa ograničenom odgovornošću u Evropi.[12]

U pogledu primene portala E-pravosuđe značajno je što je to jedinstveno mesto za pristup uslugama (tzv. "one-stop shop") u području pravosuđa. Ovo se odnosi na

[8] *Ibidem.*

[9] *Ibidem.*

[10] https://eur-lex.europa.eu, [19.09.2022.].

[11] https://e-justice.europa.eu, [19.09.2022.].

[12] Komunikacija komisije Evropskom parlamentu, vijeću, Evropskom gospodarskom i socijalnom odboru i odobru regija.

to što ovaj portal trenutno omogućava pojedincima da pomoću interneta pokreću prekogranične sporove male vrednosti ili platne naloge u skladu sa merodavnim sekundarnim zakonodavstvom EU.[13] U pogledu sporova male vrednosti pokretanje ovih sporova putem portala e-pravosuđe moguće je za sporove čija vrednost ne prelazi iznos od 2000 Eura. Primenjuje se među svim državama članicama osim Danske. To je pismeni postupak, osim u slučajevima kada sud smatra da je potrebna usmena rasprava. Njime se utvrđuju rokovi za stranke i sud kako bi se ubrzao postupak, a primenjuje se na materijalne i nematerijalne sporove. Sudska odluka koja je dobijena u ovom postupku uglavnom se automatski priznaje i izvršava u drugoj državi članici[14].

Osim pristupa sastavu povezanih poslovnih registara, direktivama EU se uvode i novi zahtevi u pogledu digitalizacije poslovnih registara i tu se razvijaju pilot projekti zemljišnih knjiga (LRI), sastava povezivanja registara stvarnog vlasništva (BORIS), pristupa sudskoj praksi nacionalnih sudova u mašinski čitljivom obliku, kao što je sudski identifikator sudske prakse (ECLI) koji je jedinstven identifikator sa istim prepoznatljivim formatom za sve države članice i sudove u EU.[15]

Takođe se preporučuje upotreba video konferencija, jer se upotrebom video konferencija u sudskim postupcima, ako je to dopušteno nacionalnim zakonodavstvima, smanjuje potreba za skupim putovanjima te se može olakšati postupak. Iako je na nivou nacionalnih pravosudnih sistema država članica upotreba video konferncija znatno u upotrebi, kao prioritet se preporučuje upotreba video konferencija u prekograničnim postupcima. Pri upotrebi video konferncija se ne bi trebalo kršiti pravo na pošteno suđenje, ni pravo na efikasnu i delotvornu odbranu, kao što su pravo učestvovanja u suđenju, pravo na poverljivu komunikaciju sa advokatom, pravo postavljanja pitanja svedocima i pravo osporavanja dokaza.[16]

Alat za najsigurniju prekograničnu saradnju u građanskim, trgovačkim i krivičnim stvarima je informacioni sistem za prenos i razmenu podatka e-CODEX. Uspostava ovog sistema predstavlja zlatni standard za sigurnu digitalnu komunikaciju u prekograničnim sudskim postupcima i prestavlja glavni alat za uspostavljanje međuoperativne, sigurne i decentralizovane komunikacijske mreže među nacionalnim informacionim sistemima u prekoraničnim građanskim i krivičnim postupcima. Radi se o softverskom paketu kojim se omogućuje povezivanje nacionalnih sistema čime se korisnicima kao što su pravosudna tela, pravni stručnjaci, građani omogućuje brzo i sigurno slanje i primanje dokumenata, pravnih obrazaca, dokaza i drugih informacija.[17] Sistem e-CODEX se koristi za sad za evropske istražne i platne naloge, postupke za sporove male vredno-

[13] Handbook European law relating to access to justice, https://echr.coe.int/document/handbook_ access_justice_eng.pdf, [19.09.2022.] i Uredba EZ br.861/2007 Evropskog parlamenta i Veća o uvođenju evropskog postupka za sporove male vrednosti od 11.07.2007.godine. čl. 5 st.1.

[14] Handbook European law relating to access to justice.

[15] Komunikacija komisije Evropskom parlamentu, vijeću, Evropskom gospodarskom i socijalnom odboru i Odboru regija.

[16] *Ibidem.*

[17] *Ibidem.*

sti, međusobno priznavanje novčanih kazni i zatvorske kazne. e-CODEX se već upotrebljava u sastavu digitalne razmene dokaza (eEDES) i određenim pilot projektima kao što su razmena evropskih istražnih naloga i zahteva za uzajamnu pravnu pomoć u krivičnim postupcima; dobrovoljna razmena zahteva u okviru postupaka za evropski platni nalog i postupka sporova male vrednosti; sistem iSupport--eletronski sastav vođenja predmeta i siguran komunikacijski sastav za prekograničnu naplatu obaveza izdržavanja. Sistemom e-CODEX upravlja konzorcijum država članica i drugih organizacija.[18]. Ova platforma je oblikovana tako da poboljša učinkovitost i brzinu postojećih postupaka saradnje uz istovremeno osiguravanje sigurnosti razmena i omogućavanje provere autentičnosti i celovitosti poslatih dokaza.[19]

Posebna se pažnja posvećuje digitalnom krivičnom pravosuđu i u okviru toga uočena je od strane Evropske komisije potreba za modernizacijom digitalnih alata za pravosudnu saradnju i razmenu informacija u krivičnim postupcima u celoj EU. Mere koje se preporučuju za dalje unapređenje digitalnih alata u krivičnom postupku su potreba za modernizacijom Eurojustov-im sastavom vođenja predmeta, kao i modernizacijom veze" podudaranje/nema podudaranja" među Eurojustov-im,Europolovim i EPPO –im sastavima vođenja predmeta. Pristup „pododaranje/nema podudaranja" je minimalan pristup podacima kojim se otkrivaju ograničena količina znanja i ličnih podatka. Stranci koja podnosi zahtev omogućava se da proveri postoje li relevantne informacije o fizičkoj osobi, drugom subjektu ili predmetu u informacijskom sastavu druge strane, a da druga strana ne mora da objavi više pojedinosti od odgovora: "da, pododuranje podatka postoji" ili "ne, nema podudranja u našoj evidenciji". Planirana modernizacija će omogućiti ovim organizacijama da su u svakom trenutku te organizacije informisane o svim vezama između istraga ili krivičnih gonjenja na kojima rade, u skladu sa svojim posebnim mandatima. To bi im omogućilo da vide da li postoje podudaranje između informacija koje oni poseduju i informacija drugih agencija i tela EU. Osim navedenog u pogledu modernizacije digitalizacije u krivičnom pravosuđu pojavila se potreba za razmenu informacija u vezi sa krivičnim delima terorizma, kao i pogledu Eurojustov-og registra za borbu protiv terorizma, te bi trebalo prilagoditi i prekogranične digitalne razmene velikih datoteka kako bi razmena bila sigurnija[20].

U okviru Evropske unije obećavajuća praksa u primeni i napretku digitalizacije je i Interaktivni vodič namenjen građanima Ujedinjenog kraljevstva Velike Britanije koji bi im pomogao u izricanju presude koji se zove „Vi presudite". Taj alat olakšava pristup pravosuđu tako što građane upoznaje sa sudskim postupcima izvan same sudnice.[21]

Jednako se vodi računa o dostupnosti svim grupama i građanima u pristupu pravosuđu prilikom digitalizacije. Tu se posebno vodi računa o osetljivim grupama, ljudi

[18] *Ibidem.*

[19] *Ibidem.*

[20] Komunikacija komisije Evropskom parlamentu, vijeću, Evropskom gospodarskom i socijalnom odboru i odobru regija.

[21] Handbook European law relating to access to justice, 181 i 182; FRA (2012): Fundamental rights:challenges and achievements in 2011- FRA Annual report, 207.

sa invaliditetom, kao i licima koji nemaju potrebna tehnička sredstva ili digitalne veštine kao što su deca ili starije osobe. U tom smislu treba unaprediti digitalizaciju pravosuđa, ali i omogućiti svaki drugi vid upotrebe elektornskih sredstava, posebno ako su obimni predmeti u pitanju. To garantuje i Evropski sud za ljudska prava koji je u predmetu Lawyer Partners a.s protiv Slovačke zauzeo upravo takav stav. Naime, u ovom predmetu podnosilac pritužbe, privatna kopmanija sa ograničenom odgovornošću je htela pokrenuti više od 70.000,00 građanskih parnica za naplatu duga. Zbog velikog broja tužbi, kompanija ih je snimila na DVD i poslala sudu zajedno sa pismenim obrazloženjem. Sud je odbio da ih registruje kao tužbe zato što mu nedostaje potrebna oprema. Žalba Ustvanom sudu je odbijena jer je podnesena van zakonom propisanog roka od dva meseca. Evropski sud za ljudska prava je napomenuo da bi, u štampanom obliku, tužbe ove komapnije i proprtani dokumeti imali više od 40 miliona stranica. U tim se okonostima odluka kompanije o sredstvu podnošenja tužbi nije mogla smatari neprimerenom. Domaći zakon je omogućavao elektronsko podnošenje tužbi, te je odbijanje suda da registruje te tužbe je predstavljalo nesrazmerno ograničenje podnosiočevog prava na pristup sudu.[22]

3. NAPREDAK DIGITALIZACIJE U PRAVOSUĐU REPUBLIKE SRBIJE

3.1. Predlozi za budućnost

U pravosuđu u Srbiji digitalizacija je u ograničenom obimu već duži vremenski u toku. To jeste neophodan, ali istovremeno veoma spor proces. Digitalizacija u pravosuđu u Srbiji se suočava sa nekim „početničkim" poteškoćama, kao što su nedostatak opreme ili adekvatnih softverskih programa, dok se, kako smo videli, u EU sada već koriste aplikacije „veštačke inteligencije". Stoga pravosuđe Srbije, kao deo evropskog pravosudnog sisitema, i sasvim sigurno interaktivno povezano sa pravosuđima drugih Evropskih zemalja, mora učiniti mnogo toga da poboljša digitalizaciju, kako bi funkcionisalo, prvenstveno na nacionalnom nivou, ali i na međunarodnoj razini. Jednostavno, zahtev stvarnosti je da pravosuđe „drži korak" u digitalizaciji sa evropskim standardima i bude još bolje, kako bi se doprinelo efikasnosti pravosuđa, čije poboljšanje je neophodno.

Da bi se unapredio postupak digitalizacije pravosuđa mora se poći od ciljeva koji se žele postići. Ono što bi trebalo da se postigne na prvom mestu je poboljšanje efikasnosti pravosuđa. To se može, uz pomoć digitalizacije, postići na razne načine. Neophodno bi bilo da se uspostave elektronsko vođenje krivičnih predmeta, u koje bi ovlašćena lica mogla, u svakom trenutku, imati uvid gde se nalaze i šta se u spisma pojedinog predmeta nalazi. Osim toga, potrebno bi elektronski uvezati sudove, a posebno tužilaštva sa drugim državnim organizacijama sa kojima sarađuju (policija, inspekcijski organi, poreski

[22] ESLJP Laweyr Partners a.s protiv Slovačke br.54252/07,3274/08,3377/08,3505/08,3526/08,3741/08,3786/08,3807/083824/08,15055/08,29548/08,29551/08, 29552/08,2955/08, 29557/08 od 16.06.2009. i Handbook European law relating to access to justice, https://echr.coe.int/document/handbook_access_justice_eng.pdf, [19.09.2022.].

organi, javni beležnici i dr.), što podrazumeva da i ovi organi imamju unapređene digitalne sisteme i evidencije. Na ovaj način bi se u mnogome ubrzao postupak, jer sadašnji PIS sistem u mnogome ubrzava postupak, ali nije još uvek dovršen, ne može se pristupiti podacima svih državnih organa sa kojima se sarađuje. Digitalizacijom bi trebalo da se postigne i veća ekonomičnost postupka. Ovo bi se postiglo elektronskom razmenom podataka i dokaza, što bi smanjilo troškove vezane za materijal kao što je papir, troškovi poštanskog saobraćaja, ali bi se na ovaj način rada smanjio i broj ročišta, sudskih pretresa, samim tim i manje putnih troškova, ali i manje izvršilaca koji su sada neophodni. Ostvarila bi se brža komunikacija, ali bi trebalo digitalizacijom omogućiti lakši pristup strankama spisima predmeta i pravosuđu uopšte. Iz prakse EU se može videti, a svakako primeniti i u našem pravosuđu, da je poželjno postojanje jednog sigurnog portala koji bi bio glavni izvor pravnih i praktičnih informacija u domenu pravosuđa za širu javnost.

Ništa manje značajna bi bila promena u zakonodavstvu Republike Srbije. Procesni zakoni bi trebalo da se menjaju na način da prihvate digitalizaciju sa svim njenim mogućnostima, bilo da se radi o postupku dokazivanja, razmene podatka, dostavljanja akata ili samog suđenja. Ne može biti prihvatljivo štampanje elektronskih upisnika nakon svakog radnog dana, kao što sad predviđa Pravilnik o upravi u javnim tužilaštvima[23], ili sačinjavanje službenih beležaka za svaki akt preduzet elektronskim putem. Time se ne postiže nijedan cilj digitalizacije, već se, naprotiv uvećavaju troškovi i usložnjava posao što će uticati na umanjenje ekonomičnosti i efikasnosti. Osim toga, trebalo bi da se digitalizacija kreće u pravcu sve veće upotrebe video konferencija, odnosno suđenja putem video linka, uz obezbeđivanje sve tehničke i logističke podrške kako bi ovakav način suđenja bio u skladu sa garantovanim osnovnim pravima stranaka u postupku. Ovaj proces je težak i ne toliko brz, jer je potrebno naći pravu ravnotežu između potrebe modernizacije zakonodavstva sa jedne strane i posledično veće ekonomičnosti postupka i poštovanja prava na pošteno suđenje kao i prava na odbranu, učestvovanje na suđenju, pravo na ospravanje dokaza i druga, ali i usklađenosti sa zakonodavnom regulativom EU u ovom pogledu.

Sav napredak digitalizacije u pravosuđu podrazumeva pre svega finansijsku podršku. Bez te podrške sve ostaje u domenu ideje. To bi značilo da digitalizacija u pravosuđu ne može da napreduje ukoliko se ne otklone sadašnji porblemi vezani za tehničku opremu i manjkavosti internih mreža, nedovoljno korišćenja interneta, kao i nedovoljno razvijene i sigurne portale koji su u upotrebi ili ograničenoj upotrebi. Digitalizacija je brz proces i napredak se dešava u kratkim vremenskim periodima iz kojih razloga taj proces mora da se prati što efikasnije, ali bez finansijske podrške teško da se može govoriti o napretku.

[23] Pravilnik o upravi u javnim tužilaštvima (*Službeni glasnik RS*, br. 110/2009,87/2010,5/2012,54/2017,14/2018 i 57/2019).

ZAKLJUČAK

Digitalizacija je sa svim svojim dostignćima umnogome promenila savremeni život. Danas ne možemo da zamislimo svakodnevni život bez digitalizacije, često se pitajući kako je sve ranije funkcionisalo bez nje. Tako se digitalizacija pokazala kao neophodnost i u pravosuđu, koje više ne bi moglo ni najmanje funkcionisati na način kako je pre radilo. Iako je proces digitalizacije odavno započeo u našem pravosuđu, on još uvek na početku i nije dao sve učinkovite rezultate koji bi se moglo očekivati, obzirom na proteklo vreme kao dostignuća koja je digitalizacija do sada postigla u svetu. Razlozi zbog čega je stanje u pravosuđu Srbije u pogledu digitalizacaije još uvek u nekoj vrsti početnog stanja, i to onaj deo koji se odnosi na praktično postupanje, je pre svega u tome što izostaje značajna i ozbiljna finansijska podrška u tom smeru. Značajna ulaganja u digitalizaciju, pre svega savremenu i sveobuhvatnu opremu, pravljenje dobrih i sigurnih softverskih programa, otvaranja novih platformi, sigurnu elektronsku komunikaciju između državnih organa, za ekonomiju kakva je u Srbiji sigurno predstavlja veliko opterećenje, ali benefiti koji se digitalizacijom postižu donose značajne uštede u državnom budžetu i to na srednji rok, što je pokazala digitalizacija u zemljama koje su tehnološki naprednije od naše. Benefiti od digitalizacije su svakako bili vidljivi tokom pandemije virusa COVID-19, kada nije bilo poželjno ostavrivati međusobne kontakte, jer je upravo digitalizacija pomogla u mnogim poslovima. Ulaganjem u digitalizaciju pravosuđa u Srbiji bi se napravilo modreno i efikasno provosuđe spremno da odgovori na sadašnje izazove, kao i izazove koji će se javiti u budućnosti.

IZVORI

Pravni akti

1. Ustav Republike Srbije (*Službeni glasnik RS,* br. 98/2006 i 115/2021).
2. Zakonik o krivičnom postupku (*Službeni glasnik RS*, br. 72/2011,101/2011, 121/2012,32/2013, 45/2013,55/2014,35/2019,27/2021- Odluka US i 62/2021-Odluka US).
3. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala (*Službeni glasnik RS*, br. 61/2005,104/2009).
4. Pravilnik o upravi u javnim tužilaštvima (*Službeni glasnik RS*, br. 110/2009, 87/2010, 5/2012, 54/2017, 14/2018, 57/2019).

Međunarodni izvori

1. Izveštaj o vladavini prava za 2020. godinu - Stanje vladavine prava u Evropskoj uniji (COM(2020)580 final).
2. Komunikacija Evropske komisije Evropskom parlamentu, Veću, Evropskom gospodarskom i socijalnom odboru i odboru regija (SWD(2020) 510 final) - https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX:52020DC0710, [19.09.2022.].
3. Uredba EZ br.861/2007 Evropskog parlamenta i Veća od 11.07.2007. godine o uvođenju evropskog postupka za sporove male vrednosti, SL 2007 L 199.
4. FRA (2012): Fundamental rights:challenges and achievements in 2011- FRA Annual report.

Internet izvori

1. https://eur-lex.europa.eu, [19.09.2022.].
2. https://e-justice.europa.eu, [19.09.2022.].
3. Handbook on European law relating to access to justice -https://echr.coe.int/document/handbook_access_justice_eng.pdf, [19.09.2022.].

Sudske odluke

1. ESLJP Laweyr Partners a.s protiv Slovačke, br. 54252/07,3274/08,3377/08,3505/08,3526/08,3741/08,3786/08,3807/083824/08,15055/08,29548/08,29551/08, 29552/08,2955/08, 29557/08 od 16.06.2009.

DIGITALIZATION OF JUDICIARY IN THE REPUBLIC OF SERBIA
- Application in Practice and Challenges –

The digitalization process has become an integral part of every aspect of social life, and consequently of the judiciary. The digitalization process is fast and must be kept up with, which very often requires significant financial resources, as well as additional education. In justice as an integral part of social life, digitalization is also necessary because it implies more efficient justice, faster communication, and cost reduction, but this process does not proceed at the same speed in the justice system of EU member states and in the Republic of Serbia. The process of digitalization of the judiciary in the Republic of Serbia started a long time ago, but it is developing very slowly. There are many reasons for that. Although there is a legal regulation that implies a digital approach to work, the legal solutions are principled and insufficient and leave a lot of possibilities for doubts or prevent the use of digital means completely, but they also affect the proof procedure. Furthermore, the lack of technical equipment, reluctantly developed and reliable programs, the disconnection of the Internet, the lack of adequate platforms to connect all relevant state authorities for the exchange of information appear as obstacles to the application of digitalization, so that the application of digitalization in criminal procedures are very narrow and reduced to the preparation of acts (which are again printed and delivered to other authorities in paper form), use of e-mail, establishment and updating of official websites of prosecutor's offices and courts, access to the records of the Ministry of Interior and individual state bodies, and only in some prosecutor's offices the use of the SAPO program, as an electronic case record. In particular, the problems due to insufficiently developed digitalization were expressed during the COVID 19 virus pandemic, when the judiciary of Serbia was neither technically nor organizationally ready to carry out procedures. While the judiciary in Serbia faces many challenges in terms of digitalization, in the member states of the European Union the digitalization process has advanced in many ways, especially because the pandemic of the COVID 19 virus has shown that digitalization in the judiciary is necessary, but it has also shown the shortcomings of digitalization, and steps are now being taken to improve the existing achievements or find better solutions, especially which is very demanding because the EU judiciary is characterized by international legal cooperation and different national legal systems. In addition to the already existing platforms, the most developed and the most customized of which are E-Government and e-CODEX, which is used for investigative orders, small value cases, payment orders between member states, work is being done to improve platforms in criminal justice, especially within Eurojust, Europol and similar formations and in this regard a package of measures was created.

However, digitalization is an unstoppable process and if the judiciary in Serbia has to become more efficient, more work must be done on digitalization. This would imply great financial support for digitalization, both in the procurement of adequate and high-quality technical equipment, as well as in organization, and also changes in legislation. The benefits from that accelerated process would be great, and would range from better organization and efficiency of the judiciary to a significant reduction in the currently significant costs of the procedure.

KEYWORDS: *digitalization of justice, criminal procedure, technical equipment, application in practice.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.07

DIGITALNI DOKAZI: ŠTA DONOSI DRUGI DODATNI PROTOKOL UZ BUDIMPEŠTANSKU KONVENCIJU?

Arben Murtezić*

Proces prikupljanja dokaza u krivičnom postupku svakim danom postaje sve složeniji. Sve veći broj predmeta na različite načine prelazi granice jedne jurisdikcije a dokazi se sve češće nalaze u digitalnoj formi, te se često dokazi nalaze pod kontrolom globalnih telekomunkacionih kompanija. Pomenuta važnost digitalnih dokaza je prepoznata još prije dvije decenije prilikom donošenja Budimpeštanske konvencije 2001. godine. U ovom dokumentu je u fokusu, naravno kompjuterski kriminal ali u domenu digitalnih dokaza je tretirana i saradnju u borbi protiv konvencionalnog kriminala.

Ne treba posebno naglašavati koliko je ovo pitanje u protekle dvije decenije dobilo na značaju, te se broj i potreba za ovakvim dokazima multiplicirala. Uporedo s tim, javili su se novi izazovi te porasla svijest da tradicionalni načini međunarodne saradnje nisu dovoljni i da je veća efikasnost u prikupljanju i korištenju neophodna. Upravo navedeno je rezultiralo donošenjem Drugog protokola koji je otvoren za potpisivanje u maju ove, 2022. godine. Obzirom na aktulenost i opisani značaj materije te razumljivu oskudnost stručne i akademske literature, ovaj rad bi mogao da posluži kao polazna osnova za iniciranje šireg i dubljeg istraživanja svih teorijskih i praktičnih aspekata ovog dokumenta od kojeg se u budućnosti mnogo očekuje.

U uvodnim dijelovima se sažeto podsjeća na definiciju, pravne i tehničke karakteristike digitalnih dokaza te predmet i suštinske odredbe Konvenencije posebno u ovom segementu. Centralni dio rada predstavlja evoluacija Drugog protokola u cilju sagledavanja najznačajnijih novina koje donosi.

KLJUČNE RIJEČI: *digitalni dokazi; međunarodna saradnja; Budimpeštanska konvencija; Drugi protokol.*

* Doktor pravnih nauka, direktor Centra za edukaciju sudija i tužilaca FBiH, Sarajevo, Bosna i Hercegovina. Email: *arben.murtezic@cest.gov.ba*

UVOD

Uprkos nacionalnim i međunarodnim mehanizmima, istina je da upotreba kompjutera i interneta u kriminalne svrhe raste. Jednostavno kao što građani globalno i svakodnevno koriste *online* servise, uključujući e-mail, društvene mreže, usluge rezervacije hotela ili aviona ili usluge plaćanja, tako i kriminalci koriste ove prednosti globalizacije i informatizacije. Tako se sve više krivičnih djela događa na mreži uz pomoć komunikacijskih mreža, a ta djela proizvode digitalne dokaze koji ostaju pohranjeni u brojnim zemljama i to često nepoznatim ili neidentifikovanim zemljama. Iako je zbog toga shavtanje da je globalna saradnja i ujednačavanje zakonskih propisa postala *conditio sine qua non* uspješne borbe protiv kriminala (Sijerčić-Čolić i Halilović, 2020) ne može se reći da je informacionu globalizaciju pratila globalizacija u krivičnopravnom postupku. Naime, djelovanje organa za provođenje zakona je u velikom dijelu još uvijek ograničeno političkim i geografskim granicama njihove države. Odnosno, ako u svojim istragama moraju da pribave dokaze u drugim zemljama, po pravilu, da bi nastavili svoju istragu, moraju poštovati suverenitet tih drugih zemalja i stoga moraju da podnose zahtjev za međunarodnu pomoć (Verdelho, 2019). Kada se tome doda karakteristična formalnost krivičnog postupka koja se naročito ogleda u principima prihvatljivosti dokaza te tehnički izazovi adekvatnog korištenja digitalnih dokaza, jasno je koliko je situacija u tom pogledu složena. Najaktuelniji pokušaj da se ovi problemi globalno prevaziđu je donošenje *Drugog dodatnog protokola uz Budimpeštansku konvenciju (ETS 185)* (u daljem tekstu "Drugi protokol") koji je otvoren za potpisivanje u maju 2022. godine. U ovom tekstu se prije svega podsjeća na osnovne karakteristike, definicije i principe korištenja digitalnih dokaza zatim podsjeća na najvažnije dijelove Budimpeštanske konvencije. Centralni dio rada je fokusiran na Drugi protokol i novine koje donosi. Obzirom na razumljiv nedostatak literature vezan za ovaj potpuno nov dokument radi se prvenstveno o primarnom istraživanju kroz analizu samog teksta i zvaničnih obrazloženja ovog protokola. Ovaj rad bi trebao imati i društveni značaj kroz poticaj nadležnim da potpišu i ratificiraju, te izvrše potrebne pripreme za ratifikaciju.

1. DEFINICIJA, KARAKTERISTIKE I OSNOVNI PRINIPI KORIŠĆENJA DIGITALNIH DOKAZA

1.1. Definicija digitalnih dokaza

Vjerovatno najčešće korištena definicija digitalnih dokaza u akademskoj i stručnoj literaturi potiče iz 2012. godine i sadržana je u dokumentu Međunarodne organizacije za standarde. Prema Smjernicama za identifikaciju, pribavljanje i čuvanje digitalnih dokaza (ISO, 2012), digitalni dokazi su informacije ili podaci, koji se čuvaju ili prenose u binarnom obliku, a na koje se može osloniti kao na dokaz. Interesantno je, kada se radi o Konvenciji, iako su digitalni dokazi jedna od centralnih tema, ni osnovni tekst ni specijalizovani, Drugi protokol o kome će kasnije biti riječi, ne sadrže posebnu definiciju

digitalnih dokaza već se posredno može zaključiti da je digitalni dokaz potencijalno i praktično svaki kompjuterski podatak. Naime, definicija kompjuterskih podataka se takođe zasniva na ISO definiciji te se pod kompjuterskim podacima označava svako predstavljanje činjenica i informacija u formi prilagođenoj za kompjutersku obradu, ubrajajući tu i programe koji su takve prirode da kompjuterski sistem vrši svoju funkciju. Ova prilagođenost direktnoj kompjuterskoj obradi je osnovna karakteristika podataka u ovoj. Prema zvaničnom obrazloženju kompjuterski podaci koji se automatski obrađuju, osim što mogu biti meta nekog od krivičnih djela definisanih ovom konvencijom, mogu bit i predmet primjene jedne od istražnih mjera definisanih ovom konvencijom.

1.2. Priroda digitalnih dokaza

Digitalni dokazi su po svojoj tehničkoj prirodi kompleksni jer su u isto vrijeme izuzetno osjetljivi ali i trajni i izdržljivi. Njihov sadržaj i lokacija mogu se relativno lako i brzo mijenjati, međutim ako su pravilno sačuvani, mogu pružiti kritične dokazne informacije na neupitan i nepobitan način. Štaviše, uništavanje digitalnih dokaza zahtijeva dosljedan napor i obično praktičan pristup fizičkom mediju koji ih sadrži, budući da informacioni sistemi koji prenose podatke imaju mehanizme osiguranja (Karagiannis & Vergidis, 2021). Uništavanje digitalnih dokaza nije jednostavno i često zahtijeva fizički pristup komjuteru, serveru, disku ili sličnom prijenosnom mediju. Pored toga isti digitalni podaci se često mogu naći na dva ili više odvojenih mjesta što je nekad dio tehničkog procesa. Recimo, elektronska pošta se može naći i na kompjuteru sa kojeg se šalje, ali i na kompjuteru koji prima te posrednim serverima. Dalje, podaci se često kopiraju i odvojeno u svrhu osiguranja i ovaj postupak je često automatizovan. Tolerancija grešaka je koncept koji je posebno važan za infrastrukturu za skladištenje podataka i odnosi se na sposobnost računarskog sistema ili podsistema za skladištenje da trpi kvarove u komponentama hardvera ili softverskih dijelova, a da ipak nastavi da funkcioniše bez prekida usluge i, što je najvažnije, bez gubitka podataka ili ugrožavanja bezbednosti.

1.3. Principi korištenja

Prema uglednom Institutu SANS za obuku i certifikaciju o informacionoj bezbjednosti, prilikom prikupljanja i čuvanja digitalnih dokaza mora se poštovati pet pravila, a svako pravilo odgovara svojstvu koje dokaz mora imati da bi se smatrao validnim i relevantnim.

Prihvatljivost - Digitalni dokazi moraju biti prikupljeni kroz zakonski dozvoljenu proceduru, tako da mogu biti prihvaćeni pred sudom. Nepoštivanje ovog pravila je jednako neprikupljanju dokaza samo što cijena može biti znatno veća i plaćena kroz neuspješno procesuiranje predmeta u čije je različite faze nekada godinama uključeno desetine ljudi.

Autentičnost - Ako dokaze ne možete pozitivno povezati s krivičnim djelom, ne možete ih iskoristiti za bilo što. Morate biti u mogućnosti pokazati da se dokazi odnose na konkretno djelo na relevantan način.

Kompletnost dokaza - Nije dovoljno prikupiti dokaze koji samo pokazuju jednu perspektivu događaja. Ne samo da trebate prikupiti dokaze koji mogu dokazati osumnjičenog, već i dokaze koji bi mogli dokazati njegovu nevinost. Digitalni dokazi moraju biti u mogućnosti da otkriju svaki aspekt incidenta koji se istražuje, čime funkcionišu i okrivljujuće i oslobađajuće. Na primjer, ako možete pokazati da je napadač bio logovan u sistem u vrijeme izvršenja djela, također morate pokazati ko je još bio prijavljen i zašto mislite da taj drugi to nije učinio. To se zove oslobađajući dokaz i važan je dio dokazivanja slučaja.

Pouzdanost procedure prikupljanja i analize ne smiju dovesti u pitanje autentičnost i istinitost dokaza. Digitalni dokazi moraju biti prikupljeni i analizirani na način koji potvrđuje autentičnost i istinitost dokaza. Primjenjivi postupak mora stvoriti jedinstvenost i singularnost koja taj određeni dokaz čini morfološki i tehnološki prepoznatljivim i različitim od bilo kojeg drugog sličnog digitalnog objekta.

Uvjerljivost - Dokazi koje iznosite trebaju biti jasno razumljivi i vjerodostojni. Nema smisla predstavljati binarni prikaz procesne memorije ako sudsko vijeće ne zna šta to znači. Slično tome, ako ih predstavite u formatiranoj, ljudima razumljivoj verziji, morate biti u mogućnosti da pokažete odnos prema originalnom binarnom sistemu, inače nema načina da zna da li ste lažirali.

2. BUDIMPEŠTANSKA KONVENCIJA: KRATKO PODSJEĆANJE

Konvencija o Kompjuterskom kriminalu (ETS br. 185) Vijeća Evrope, otvorena je za potpisivanje u Budimpešti 23. novembra 2001. godine. Od tada do danas je postala, bez konkurencije, globalno najznačajniji međunarodni dokument u borbi protiv kompjuterskog kriminala. Ovo ne samo zbog broja zemalja koje su je potpisale, a to nisu samo članice Vijeća Evrope, već primjera radi i Sjedinjene Američke Države i Japan, nego i zbog uticaja na nacionalana zakonodavstva širom svijeta.

Budimpeštanksa konvencija reguliše posebno primjenjive metode djelovanja državnih organa u istragama vezanim za visokotehnološki kriminal, kao i minimalne standarde zaštite od zloupotrebe velikih ovlasti koje državni organi stiču u cilju efikasne borbe. visokotehnološki kriminal. Zato je Budimpeštanska konvencija, koja prilagođava „klasične“ procesne mjere u uslovima digitalne ere (Kostić & Petrović, 2021), od velikog značaja za praktičan rad specijalnih policijskih jedinica i tužilaštava za visokotehnološki kriminal, posebno ako se ima u vidu da se u digitalnoj eri mjesto gdje nastupa posljedica i mjesto izvršenja nalazi na velikoj udaljenosti od mjesta gdje se počinitelj nalazi, često na teritoriji druge zemlje. Prema odredbama CETS 185, ugovorne strane su dužne da usvoje zakonske i druge mjere u cilju efikasnog vođenja istraga i krivičnog postupka, kako za krivična djela koja se mogu smatrati kompjuterskim zločinima, tako i za druga krivična djela koja se mogu izvršiti putem kompjuterskog sistema. Ove mjere se odnose i na prikupljanje dokaza protiv izvršilaca u elektronskoj formi, što je regulisano drugim, procesnim dijelom Budimpeštanske konvencije. Naime, članovi 16–21 propisuju

procesne mjere koje omogućavaju hitno čuvanje kompjuterskih podataka, čuvanje i djelomično pohranjivanje podataka o prometu, pretrazi i zapljeni pohranjenih podataka, prikupljanje podataka i podataka o prometu u realnom vremenu, kao i presretanje podataka o sadržaju komunikacije.

Relativno brzo nakon što je osnovni tekst otvoren za potpisivanje, 2003. godine, Konvencija je dopunjena dodatnim protokolom koji se odnosi na kriminalizaciju djela rasističke i ksenofobične prirode počinjenih putem kompjuterskih sistema (ETS br. 189, u daljem tekstu „Prvi protokol"). Na Drugi dodatni protokol, koji je tema narednog poglavlja, se čekalo znatno duže te je usvojen na dvadesetu godišnjicu Konvencije, što je od strane Vijeća Evrope na različite načine, kroz svečane manifestacije i izjave podcrtano kao važna simbolika.

Naime, jasno je da je informaciona i komunikaciona tehnologija u posljednjih 20 godina evoluirala i transformisala globalno društvo na teško zamislive i predvidljive načine. Međutim, od tada je takođe došlo do značajnog povećanja eksploatacije tehnologije u kriminalne svrhe. Gotovo da postoji opšti konsenzus da je kompjuterski kriminal ozbiljna prijetnja ljudskim pravima, vladavini zakona i funkcionisanju demokratskih društava. Prijetnje koje predstavlja Kompjuterski kriminal su brojne, uključujući seksualno nasilje nad djecom na internetu i druga krivična djela protiv dostojanstva i integriteta pojedinaca. Zatim krađu i zloupotrebu ličnih podataka koji utiču na privatni život pojedinaca. Poseban problem je gore spomenuto širenje rasističkih i ksenofobnih materijala i govora mržnje a sa ovim su povezani i drugi napadi na demokratske institucije kao što je miješanje u izborni proces te napadi na kritičnu infrastrukturu ili zloupotrebu tehnologije u terorističke svrhe. Pandemija Covid-19 je donijela nove izazove te porast kriminala povezanog sa pandemijom, uključujući napade na bolnice i medicinske ustanove koje razvijaju vakcine protiv virusa; zloupotreba naziva domena za promoviranje lažnih vakcina, tretmana i lijekova. Pored toga, ne treba posebno naglašavati koliko je život koji se zbog različitih restrikcia dodatno preselio u digitalnu sferu donio otvorio mogućnosti za zloupotrebe.

Uprkos svemu, Konvencija je u mnogome izdržala test vremena i velikih promjena, prije svega zato što su koncepti koje sadrži tehnološki neutralni te se odredbe koje se odnose na materijalno krivično pravo, pa mnogome i na praktične aspekte saradnje mogu primijeniti i na postojeće i na buduće tehnologije. Ovo zbog toga što ključna pitanja kojima se Konvencija bavi ne samo da u posljednje dvije decenije nisu izgubila na aktuelnosti već su i dobila na značaju. U tom smislu, kratko se treba podsjetiti da je Konvencija prvenstveno usmjerena na usklađivanje krivičnog materijalnog prava i povezanih propisa za djela koja se u užem ili širem smislu podvode pod kompjuterski kriminal. Zatim, Konvencija promoviše potrebu za prilagođavanjem domaćeg krivičnog procesnog zakonodavstva na način neophodan za istragu i gonjenje takvih krivičnih djela, kao i drugih krivičnih djela počinjenih putem kompjuterskog sistema. Na kraju, ono što je za ovaj rad posebno značajno, insistira se na adekvatnim rješenjima vezanim za upotrebu elektronskih dokaza uopšteno i uspostavljanje brzog i efikasnog režima međunarodne saradnje.

3. DRUGI DODATNI PROTOKOL O DIGITALNIM DOKAZIMA

Kako je navedeno u preambuli, ovaj Protokol ima za cilj dalje jačanje saradnje u vezi s kompjuterskim kriminalom ali i sposobnosti pravosuđa i agencija za sprovođenje zakona da prikupljaju dokaze u elektronskom obliku o krivičnom djelima u svrhu konkretnih krivičnih istraga kao i uspostavu dodatnih alata koji se odnose na efikasniju međunarodnu pomoć i druge oblike saradnje nadležnih organa. Ovo uključuje, između ostalog, saradnju u hitnim slučajevima kada postoji značajan i neposredan rizik po život ili sigurnost bilo kojeg fizičkog ili pravnog lica i direktnu saradnju između nadležnih organa i pružalaca usluga i drugih subjekata koji posjeduju ili kontrolišu relevantne informacije.

Nomotehnički i sadržajno, ovaj protokol je podijeljen u četiri poglavlja: Opšte odredbe; Mjere za poboljšanu saradnju; Uslovi i zaštitne mjere i Završne odredbe.

Opšte odredbe, očekivano, se odnose na svrhu i djelokrug ovog Protokola. Tako je naglašeno da se odredbe protokola odnose na krivične istrage ili postupke, ne samo u vezi sa kompjuterskim kriminalom, već i za svako krivično djelo koje uključuje dokaze u elektronskom obliku koji se također obično nazivaju „elektronski dokazi" ili „digitalni dokazi". Isto tako, kao što je uobičajeno za opšte odredbe, ovo poglavlje sadrži definicije ključnih pojmova ali definicije pojmova Konvencije primjenjive na ovaj Protokol. Kao što je rečeno, definicije ključnih pojmova su uobičajeni dio mnogih domaćih i međunarodnih propisa. Međutim, ovo u domenu kmpjuterskog kriminala ima posebnu težinu.

Naime, korištenje i razvoj informacionih i komunikacionih tehnologija je rezultirao pojavom čitavog niza, novih i često teško prevodivih termina, obzirom da je engleski neka vrsta zvaničnog ili univerzalnog jezika u ovoj oblasti. Međutim ni za one kojima je ovaj jezik maternji jezik ili ga odlično poznaju situacija nije uvijek jednostavna jer se stalno uvode novi termini kojima se označavaju pojave i različite riječi dobijaju novo značenje, a pri tome često ni lingvistički, pravni ili tehnički stručnjaci nemaju ključni uticaj.

Navedeno često utiče na efikasnost procedura kod zahtjeva za međunarodnu pomoć i druge oblike saradnje. Imjući to u vidu, dodata je i odredba o „jeziku" kako bi se omogućio pragmatičniji pristup u ovom pogledu.

Drugo poglavlje Poglavlje sadrži osnovne, suštinske, odredbe ovog Protokola, koji opisuju različite metode saradnje koje bi kroz ratifikaciju i razvoj prakse trebali biti dostupni u budućnosti. Suštinski, za svaku vrstu saradnje, pored opštih važe i posebni principi te je ovo poglavlje adekvatno i podijeljeno na više dijelova. Naravno, u prvom dijelu su opšti principi primjenjivi na sve oblike saradnje u ovom poglavlju. Drugi dio je posvećen postupcima koji unapređuju direktnu saradnju sa pružaocima usluga i entiteta u drugim zemljama. Treći dio sadrži principe primjenjive na postupke koji unapređuju međunarodnu saradnju između nadležnih organa za otkrivanje pohranjenih kompjuterskih podataka. Četvrti dio se odnosi na procedure za hitnu međunarodnu pomoć. Na kraju su principi vezani za procedure koje se odnose na međunarodnu saradnju u nedostatku drugih primjenjivih međunarodnih sporazuma.

Treće poglavlje predviđa uslove i mjere zaštite. Oni zahtijevaju da strane primjenjuju uslove i zaštitne mjere slične članu 15. Konvencije i na ovlaštenja i procedure ovog Protokola. Ovo poglavlje kroz detaljan skup mjera zaštite za zaštitu ličnih podataka odražava izuzetnu važnost koja se pripisuje pitanju zaštite ličnih podataka u digitalnom prostoru i koje na određeni način stoji kao suprostavljeno interesu za brzim i efikasnim prikupljanjem digitalnih dokaza.

Završne odredbe sadržane u Poglavlju IV su svakako slične standardnim završnim odredbama drugih konvencija Vijeća Evrope te na sličan način regulišu pitanja procedure, potpisivanja izjava, rezervi ili ukazuju koje odredbe Konvencije su primjenjive i na ovaj Protokol. Međutim, određene specifičnosti su sadržane u članovima koje se "Učinci ovog protokola", član 17. o "Saveznoj klauzuli" i član 23. o "Konsultacijama stranaka i ocjeni implementacije" i razlikuju se u različitom stepenu od analognih odredbi Konvencije. Ovim posljednjim članom ne samo da se primjenjuje član 46. Konvencije, već također predviđa da će strane periodično ocjenjivati efektivnu upotrebu i implementaciju odredaba ovog protokola.

Za nas je posebno interesantna "savezna" ili "federalna" klauzula iz člana 17. Naime, iako ovaj Protokol tretira međunarodnu saradnju, a ne domaće mjere, ocijenjeno je da su odredbe koje se odnose na unutrašnje odnose u složenim državama potrebne u ovom Protokolu. Ovo zbog toga što većina mjera ovog Protokola ne djeluje na isti način kao tradicionalna međunarodna pravna pomoć jer pruža niz mjera saradnje koje su efikasnije od tradicionalne međusobne pomoći i koje ne zahtijevaju nužno uključenje centralne vlade. Konkretno, ovaj Protokol uvodi mogućnost da nadležni organi jedne države mogu tražiti saradnju direktno od privatnih kompanija u drugoj državi. Ove mjere zahtijevaju određene proceduralne korake kod kojih u složenim državama centralna vlada može imati poteškoća u zahtijevanju od nadležnih organa konstitutivnih država ili teritorijalnih entiteta da ih poštuju. Moguće je da, taj centalni organ nema nadležnosti prema tom dobavljaču i da bi uspostavljanje ovakvog mehanizma zahtijevalo proširenje centralnih nadležnosti. Drugim riječima, protokol sadrži zahtjeve za poduzimanjem zakonodavnih ili drugih mjera koje savezna država možda neće moći zahtijevati od svojih konstitutivnih država ili drugih sličnih teritorijalnih entiteta da ih donesu. U tom smislu, recimo, ovaj Protokol sadrži detaljne odredbe o zaštiti podataka, kakve Konvencija ne sadrži i potpisivanjem bi se država obavezala na prilagođavanje u tom smislu.

Osnovi razlog za uvođenje ove klauzule je da se omogući potpisivanje Sjedinjenim Američkim Državama u kojima većina globalnih operatera i ima sjedište, te se zbog toga čini da su ključne u provedbi. S tim uvezi, poznato je da u SAD, u skladu sa ustavom i osnovnim principima federalizma, konstitutivne države donose vlastite krivične i krivičnoprocesne zakone (odvojeno od saveznih zakona); osnivaju svoje sudove, tužioce i policiju; i istražuju i procesuiraju državna krivična djela. Državni nadležni organi su nezavisni i nisu podređeni saveznim vlastima.

Dakle, ako vlasti konstitutivne države ili sličnog teritorijalnog entiteta zatraže oblike saradnje predviđene ovim Protokolom, može se dogoditi da primjenjuju različite procesne zakone i zakone o privatnosti od onih koje primjenjuju centralni državni

organi. Zatim da ne odgovaraju centralnoj vladi u smislu organizacione hijerarhije ili centralna vlada nema zakonsku moć da upravlja njihovim radnjama. U takvim situacijama moglo bi postojati samo garancija da će konstitutivna država ili sličan teritorijalni entitet ispuniti zahtjeve ovog Protokola – one koji se odnose na traženje informacija ili dokaza, kao i one koji se odnose na naknadno postupanje s takvim informacijama ili dokazima ako ih sam primjenjuje, ili ako su njegovi organi tražili saradnju preko, ili uz učešće organa centralne vlade, koji bi se pobrinuli za njihovo ispunjenje.

Bez obzira što je, kako je navedeno, ova klauzula ovdje prvenstveno zbog SAD kao apsolutnog lidera u svijetu digitalnih komunikacija na čijoj teritoriji velika većina najmoćnijih kompanija ima sjedište te od čijeg pristupanja uveliko zavisi uspjeh Protokola ona je bitna i za druge složene države pa je ovdje opširnije predstavljena.

ZAKLJUČAK

Međunaradna saradnja nema alternative ukoliko se želi uspjeh pred svakodnevnim izazovima koje predstavlja korištenje tehnologije i informacionih sistema u kriminalane svrhe. Brzina kojom se razvijaju pojavni oblici te konkretne radnje izvršenja krivičnih djela u digitalnom svijetu daleko prevazilaze tempo postupanja notorno konzervativnih a često, i u najrazvijenijim zemljama, tromih pravosudnih sistema. Pokušaj da se procedure pojednostave i ubrzaju sigurno ne smije ići na račun poštivanja zakonitosti i zaštite ljudskih prava. Iz gore predočenog teksta se čini da Drugi protokol predviđa adekvatan balans između ovih ciljeva i teško je kroz samo tumačenje teksta pronaći dijelove koji zaslužuju posebnu kritiku. Međutim, kao i kod svakog opšteg pravnog akta, međunarodnog ili nacionalnog, ocjena uspješnosti i svrsishodnosti će uslijediti kroz praksu i za tako nešto će trebati godine.

Ono što već sada možemo reći jeste da se radi o najvažnijem dokumentu u izuzetno značajnoj oblasti i sasvim je izvjesno da će taj primat zadržati prilično dug period. Potpisivanje i ratificiranje ce mogu bez rezervi preporučiti, a istraživanju različitih aspekata praktične primjene treba posvetiti veliku pažnju. Naročiti trud treba uložiti u stručnu i profesionalnu edukaciju ne samo nosilaca pravosudnih funkcija i pripadnika različitih agencija za sprovođenje zakona, već i odgovarajućih službi telekomunikacionih konpanija i državnih institucija nadležnih za ovaj sektor. Iskustvo i razvijeni mehanizmi koje Vijeće Evrope ima za praćenje i podršku u primjeni Konvencije će sigurno biti dragocjeno u slučaju Drugog protokola, te ih svakako treba adekvatno iskoristiti.

LITERATURA

1. Braid, M. Collecting Electronic Evidence After a System Compromise, Global Information Assurance Certification Paper for SANS Institute. Available online: https://www.giac.org/paper/gsec/659/collecting-electronic-evidence-system-compromise/101519, [20.8.2021.].
2. Council of Europe, Convention on Cybercrime (CETS No 185), Budapest, November 23, 2001. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documen- tId=0900001680081561. [20.8.2021.].
3. Council of Europe (2001), *Explanatory Report to the Convention on Cybercrime.*
4. International Organization of Standardization (2012), *Information Technology – Security Techniques – Guidelines for Identification, Col- lection, Acquisition and Preservation of Digital Evidence*, ISO/IEC 27037:2012 Standard, Geneva, Switzerland.
5. Karagiannis, C., & Vergidis, K. (2021) „Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal". *Information*, *12*(5), 181.
6. Kostić, J. & Petrović, N. M. (2021). „Digital evidence and criminal law cooperation in the digital age", *Archibald Reiss Days*, 11, 43-54.
7. Sijerčić-Čolić, H. & Halilović, H. (2021) „Digitalni dokazi in sodobni kazenski postopek". *Zbornik 1. konferenca prava informacijske varnosti*. GV Založba.
8. Verdelho, P. (2019) „Obtaining digital evidence in the global world". *UNIO–EU Law Journal*, *5*(2), 136-145.

DIGITAL EVIDENCE: WHAT DOES THE SECOND ADDITIONAL PROTOCOL TO THE BUDAPEST CONVENTION BRING?

The process of collecting evidence in criminal proceedings is becoming more and more complex every day. An increasing number of cases crosses the borders of one jurisdiction in various ways, and evidence is increasingly found in digital form. Therefore, the evidence is often under the control of global telecommunications companies. The aforementioned importance of digital evidence was recognized even two decades ago when the Budapest Convention was adopted in 2001. In this document, the focus is, of course, on computer crime, but in the domain of digital evidence, cooperation in the fight against conventional crime is also tackled.

There is no need to emphasize how important this issue has become in the past two decades, and the number and need for such evidence has multiplied. At the same time, new challenges arose and awareness grew that traditional methods of international cooperation are not enough so the greater efficiency in collection and use digital evidence is necessary. The aforementioned resulted in the adoption of the Second Protocol, which is open for signing in May of this year, 2022. Considering the actuality and described importance of the matter and the understandable paucity of professional and academic literature, this work could serve as one of the starting points for initiating a wider and deeper research into all theoretical and practical aspects of this document, from which much is expected in the future.

In the introductory parts, the definition, legal and technical characteristics of digital evidence ar briefly described, as well as essential provisions of the Budapest Convention in the relevant segment. The central part of the work is the evaluation of the Second protocol in order to present the most significant novelties it brings.

KEYWORDS: *digital evidence, international cooperation, Budapest Convention, The Second Protocol.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.08

UPOTREBA DOKAZA PRIKUPLJENIH DRONOVIMA U KRIMINALISTIČKIM ISTRAŽIVANJIMA

Adnan Duraković*
Miodrag N. Simović**
Sabina Duraković***

Dronovi imaju sve veću ulogu u kriminalističkim istraživanjima, prije svega u provođenju uviđaja, ali i u drugim kriminalističkim radnjama, naročito pretraživanju lica mjesta nakon što je događaj završen ili u nadzoru još aktivnog događaja. Organ koji provodi uviđaj, a to je prije svega policija, mora brzo i vidljivo osigurati lice mjesta, kao i sve predmete i tragove na njemu. Pretraživanje, snimanje i dokumentovanje, prikupljanje i analiza tragova mora biti obavljeno bez narušavanja lica mjesta i kontaminacije. Ulazak osoblja u ovo područje nosi rizik i zahtijeva vrijeme, osoblje i kompleksne aktivnosti.

Zapljena drona i njegova forenzička analiza su osnov za prikupljanje dokaza. Pored dronova, pametni telefoni igraju ključnu ulogu u ovom procesu jer su oni osnov za komunikaciju telefon – dron, za određivanje statusa leta, kao i sve produkte u vidu fotografija i videa. Sve to treba da rasvijetli ulogu korisnika, odnosno vlasnika drona - ukoliko je neko drugi uzurpirao tu komunikaciju i preuzeo upravljanje dronom.

Dijelovi drona imaju jedinstvene oznake, a analiza fizičkih komponenti provodi se u sklopu forenzike fizičkih dijelova, kao i podaci nastali u toku leta koji se analiziraju u sklopu digitalne forenzike. Sve to će omogućiti prikaz leta drona. S druge strane, adekvatna zaštita od ilegalne upotrebe dronova, kao i istrage vezane za njih, podrazumijevaju praćenje trendova. Posebno je važno da se djelovanje dronovima razlikuje značajno u periodu mira, krize i rata.

Borba protiv zloupotrebe dronova uključuje upotrebu svih dostupnih načina i sredstava, kao i iskorištavanje slabosti koje imaju dronovi generalno i pojedine vrste dronova. Prije svega, onemogućavanje djelovanja dronova se odnosi na bespilotnu letjelicu, prije nego na ostale komponente sistema kao što su daljinska kontrola, komunikacija i personal koji upravlja letjelicom.

KLJUČNE RIJEČI: *dron, uviđaj, vještačenje, istraga.*

* Doktor pravnih nauka, redovni profesor Pravnog fakulteta Univerzitet u Zenici.
E-mail: *dadnan07@gmail.com*

** Doktor pravnih nauka, potpredsjednik Ustavnog suda Bosne i Hercegovine, redovni profesor Pravnog fakulteta Univerziteta u Bihaću i redovni član Akademije nauka i umjetnosti Bosne i Hercegovine.
E-mail: *miodrag.simovic@ustavnisud.ba*

*** Magistar, viši asistent na Ekonomskom fakultetu Univerziteta u Sarajevu.
E-mail: *sabina.durakovic@efsa.unsa.ba*

UVOD

Uviđajna ekipa na mjestu izvršenja krivičnog djela, pored rutinskih koraka koje preduzima, često nailazi na specifične situacije i zahtjeve koje mora riješiti zbog specifičnosti lica mjesta i načina izvršenja djela ili tragova i dokaza koje treba pronaći, izazvati, fiksirati i izuzeti. Svaki uviđaj ograničen je sposobnošću da se organizacijski i tehnički osigura lice mjesta, da se dokazi zaštite od kontaminacije i uništenja, kao i da se obezbijedi sljedivost dokaza. Kontaminacija, uništavanje ili odnošenje dokaza dešava se ljudskim i životinjskim aktivnostima, kao i djelovanjem vremenskih pojava. Brz pristup licu mjesta, kao i brzo bilježenje i fiksiranje svih tragova i promjena je ključan za daljnja forenzička i kriminalistička istraživanja, kao i za sudski postupak (Robinson, 2010; Park, Kim, Seok, 2016: 147–149). Uporedo sa provođenjem svih faza uviđaja (informacijska, statička, dinamička, kontrolna) jeste stalna procjena sigurnosti osoblja i lica mjesta, a provodi se i misaona rekonstrukcija događaja. Srž dokumentovanja unutar uviđaja je fotografisanje i snimanje, uz upotrebu novih tehnologija (Mekala, Baig, 2019: 172–189).

Upotreba dronova je izazov i potreba novih okolnosti (Andrejević, 2016: 21–43; Sciancalepore *et. al*., 2019: 67–72). Oni se pojavljuju i kao sredstvo za izvršenje krivičnih djela ili su posljedice njihove upotrebe zahtijevale provođenje uviđaja, vještačenja ili drugih radnji (Clark *et. al*. 2017: S3–S14; Ahn, 2020: 557–561).

Dronovi su dio novih okruženja u kojima se odvija život (zajedno sa mobilnim telefonima i tabletima), uz pohranjivanje podataka „u oblacima" i upotrebu raznih hardverskih i softverskih rješenja za činjenje i rješavanje krivičnih djela (Crotty, 2014: 219-265; Lee, La, Kim, 2018: 1131–1133). U tom smislu, dronovi su predmet forenzičkih ispitivanja, ali i sami su predmet antiforenzičkih mjera koje su usmjerene na uništavanje podataka ili onemogućavanja pristupa podacima od strane službi za provođenje zakona (Boštjan, 2016: 7-25).

1. KORISNOST DRONOVA

Bespilotne letjelice, bez obzira na to kojih veličina, modela i načina rada (npr. sa fiksnim krilima ili rotorima), mogu se koristiti za beskonačno mnogo zadataka i samo mašta limitira njihovu upotrebu (Hummel *et. al*., 2019; *Rydén et. al*., 2019: 1–6). Pored industrijski rađenih bespilotnih letjelica, brojni hobisti prave i orginalne vlastite kreacije (Rao *et. al*., 2016: 83–90). Njihova korisnost definisana je *cost- benefit* analizom[1], i to je nešto što podržava njihovu upotrebu u odnosu na klasične avione i helikoptere (Sandbrook, 2015: 636–647; Završnik, 2016: 243– 266). Primjenjuju se najčešće za snimanje određenog prostora, nekada i sa prenosom slike uživo, za snimanje scena sa različitim

[1] **Cost-benefit analiza** (CBA) ili analiza troškova i koristi ili kako se ponekad zove benefit-cost analiza kvantifikuje i dodaje novčane vrijednosti svim efektima i utroščima vezanim za realizaciju projekta ili planiranje investicija, na osnovu čega se vrši proračun neto dobiti datog subjekta. Faktički, vrši se procjena slabosti i snaga svih ponuđenih alternativa na osnovu čega se bira opcija koja ostvaruje najveću dobit (benefit), a najmanje troškova realizacije (cost).

senzorima i detekciju promjena u sredini (npr. kod ekoloških incidenata), kod praćenja požara i poplava, u građevinarstvu za inspekcije objekata i postrojenja, za razne hobiste i filmske aktivnosti, za snimanje mjesta nesreće i pretraživanje određenih prostora i potragu za predmetima, leševima, ljudima i vozilima (Jeong, Bito, Tentzeris, 2017: 1–4; Viswanathan, Baig, 2020: 29–41).

Dometi, kao i nosivost dronova, cijenovni raspon, broj osoblja koje je potrebno za održavanje i korištenje - teme su o kojima su napisani brojni radovi. Ti parametri su od značaja za temu ovog rada u smislu da li letjelica djeluje van optičke vidljivosti operatera i koliko dalek ima radijus leta, koliko opreme i sofisticiranosti opreme nosi, koliko dugo ostaje u vazduhu, na kojoj visini leti, doba dana ili noći, na koji način se ostvaruje komunikacija sa letjelicom, da li su to radio-talasi, *wifi*, preko mobilnog uređaja, bazne stanice na zemlji ili preko satelita (Mishra, Dedhia, Wavhal, 2015: 1-2).

Za kriminalističko-forenzičke potrebe, kao i za poslove generalnog ili specijalnog nadzora i prikupljanje obavještajno interesantnih podataka o aktivnostima mali dronovi su (zbog cijena i koristi) veoma pogodni (Renduchintala *et. al.* 2017: 91–96; Renduchintala *et. al*., 2019: 52–72; Sharma *et. al*., 2019: 824-827; Yousef, Iqbal, 2019: 1–3). Pogled iz vazduha, upotreba vještačke inteligencije za interpretiranje rezultata nadzora, kao i upotreba raznih senzora - omogućava djelovanje u realnom vremenu ili uz naknadnu interpretaciju prikupljenjog materijala pomoću odgovarajućih algoritama (Yousef *et. al*., 2020: 66–71).

Za uviđaj dronovi omogućuju u ranoj fazi procjenu lica mjesta događaja, brz pregled lica mjesta, foto, video i grafičko snimanje mjesta, identifikovanje predmeta i njhovih lokacija, dodjeljivanje bar kodova svakom pojedinačnom predmetu ili tragu, automatsko vođenje dnevnika o svemu navedenom u formi datuma, sata, GPS lokacije i 3D prikaz (Bouafif, Kamoun, Iqbal, 2020: 35–57). Sve to je kod letjelica koje se nose u prtljažniku automobila cjenovno nisko u poređenju sa letom helikopterom ili sa velikim bespilotnim letjeliocama koje koristi vojska za strateška snimanja.

Operater na zemlji definiše prostornu zonu koju će letjelica obraditi - bilo da koristi manuelni ili automatski rad. Fotografije sa odgovorajućim kamerama su takvog kvaliteta da u uvećanju daju prikaz detaljnosti - kao da se gleda u stvarnosti snimljeni objekat.

Prednost dronova, u odnosu na dosadašnje sredstva i tehnike, jeste da oni imaju programabilne funkcije, malih su dimenzija tako da se lako mogu transportovati u prtljažniku vozila, da im je cijena prihvatljiva, da su posebno od značaja u početnoj informativno-orijentacijskoj fazi uviđaja, ali i kod forenzičke obrade lica mjesta, naročito kada se radi o nepristupačnim lokacijama gdje postoji opasnosti za istraživače (npr. zmije otrovnice, minirana područja i sl.). Sve te poslove operateri dronova mogu obaviti za relativno kratko vrijeme u odnosu na klasične metode, mogu forenzičarima dostavljati potrebne alate ili transportovati predmete do laboratorija na brz način, čime se skraćuju preliminarna ili finalna vještačenja (Barton, Azhar, 2017: 91–96). U stanju su da daju bar kodove za dokaze i da održavaju lanac nadzora nad dokazima (bez kontaminacije).

2. OSNOVNE KARAKTERISTIKE DRONOVA

Pošto je riječ o upotrebi ili zloupotrebi dronova, odnosno njihovoj upotrebi za kriminalistička i forenzička istraživanja ili su oni sami predmet forenzičkih i kriminalističkih istraživanja - potrebno je nešto reći o njima.

Dron se sastoji od fizičkog dijela, odnosno same letjelice, kontrolne stanice (daljinski upravljač *radio kontroller* koja omogućuje veze za prenos podataka i podršku za naknadnu obradu podataka, softverske ili digitalne komponente koju čine operativni sistemi najčešće isti oni koje koriste mobiteli, tableti, uređaji za čuvanje medija, fotografija i video zapisa, bilo da su integrisani u sam dron ili su odvojivi), datoteke, *firmware*[2] i ROM (Read-Only Memory)[3]. Zahvaljujući svojoj hardverskoj i softverskoj konfiguraciji, dronovi su korisni za mjerenja, fotografisanja, pronalaske predmeta prilikom uviđaja i naknadne rekonstrukcije. Koriste metode fotogrametrije[4] za stvaranje tačnog prikaza mjesta izvršenja krivičnog djela, zajedno s udaljenostima dokaza, i to na komplikovanim ili nepristupačnim mjestima zločina (Bhoopesh *et al*, 2019: 824-827).

Za mnoge situacije su pogodne različite tehnike osvjetljenja, uz korištenje UV zraka[5] i infracrvenih zraka[6]. U kriminalističkoj praksi primjene, poput gledanja udaljene zone lica mjesta, hvatanje iz vazduha perspektive, fotografisanje mjesta događaja i s više karakteriziranih tačaka, snimanje i mapiranje mjesta zločina - od izuzetne su važnosti kako u ranoj fazi uviđaja, tako i u analizi nakon uviđaja. Mapiranje mjesta zločina može se postići korištenjem softvera npr. autodesk[7], revit softver[8] (za arhitektonski dizajn, MEP[9], strukturni dizajn i konstrukciju) itd. (Bhoopesh, *et al*, 2019: 824-827).

[2] Firmware je softver koji je ugrađen u dio hardvera. Jednostavno, to je „softver za hardver" (*https://www.lifewire.com/what-is-firmware-2625881*).

[3] Memorija samo za čitanje ili ROM je vrsta pohrane na računaru koja sadrži trajne podatke koji se, normalno, mogu samo čitati.

[4] Fotogrametrija je tehnika mjerenja pomoću koje se iz fotografskih snimaka izvodi oblik, veličina i položaj snimljenog predmeta.

[5] Ultraljubičasto zračenje (skraćeno UV prema engl. *ultraviolet*) obuhvata elektromagnetno zračenje sa talasnim dužinama manjim od vidljivog zračenja, ali većim od onih koje imaju meki X-zraci. Dijeli se na blisko (380-200 nm, NUV), daleko ili vakuumsko (200-10 nm, skraćenica FUV ili VUV) i ekstremno (1-31 nm, skraćenica EUV ili XUV) ultraljubičasto zračenje. *https://hr.wikipedia.org/wiki/Ultraljubičasto_zračenje.*

[6] Infracrveno zračenje ili infracrvena svjetlost (lat. *infra*: ispod; kratica IR od eng. *infrared*) je elektromagnetsko zračenje valnih duljina približno između 0,8 μm i nekoliko stotina mikrometara. Otkrio ga je 1800. F. W. Herschel, zapazivši da u spektru sunčeva zračenja, dobijenom s pomoću optičke prizme, najvišu temperaturu pokazuje područje koje se nastavlja na crveni dio vidljivog spektra. Za ljudsko oko to je zračenje nevidljivo, ali se može osjetiti na koži kao osjećaj topline. *https://hr.wikipedia.org/wiki/Infracrve no_zračenje.*

[7] Autodesk, Inc. je američka multinacionalna softverska korporacija koja proizvodi softverske proizvode i usluge za arhitekturu, inženjering, građevinarstvo, proizvodnju, medije, obrazovanje i zabavnu industriju. Autodesk ima svoje mjesto u San Franciscu, Kalifornija i kancelarije širom svijeta.

[8] Revit softver pomaže arhitekturi, inženjerstvu i građevinarstvu (AEC) da stvore visokokvalitetni objekat i infrastrukturu.

[9] Mechanical, electrical and plumbing - mehanički, električni i vodovodni (MEP) odnosi se na ove aspekte projektinga i gradnje zgrada.

Ako je opremljen odgovarajućim tehnikama osvjetljenja (UV i IR), dron može tražiti nevidljive tragove kao što su latentni otisci prstiju, otisci obuće, isprani tragovi krvnih mrlja itd., a može ih lako fotografisati, bez ugrožavanje integriteta dokaza. Može mjeriti toksine u vazduhu, pratiti požare, poplave, pronalaziti tijela u svim fazama raspadanja, dijelova tijela kao što su lobanje, dijelovi odjeće i predmeta.

Od vrste i broja senzora - zavisi veličina i cijena dronova i senzora. U vezi s tim, zavisi i upotreba u zemaljskim stanicama podataka za prenos uživo ili nakon slijetanja drona i skidanje podataka softeverskih programa i algoritama. Moguće je pravilno očitavanje, tumačenje, mapiranje i prikaz tih podataka u odgovarajućem obliku. Mogu se koristiti laseri i 3D kamere, koji su, zajedno sa GPS sistemom i zapisima koje stvar dron - detaljni izvor informacija i vjerodostojna interpretacije onoga što je pronađeno

3. ORGANIZACIJSKA FAZA UVIĐAJA

Organizacijska faza uviđaja pretpostavlja da postoji opremljen i obučen organ, odnosno osoblje koje je operativno sposobno da provede odgovarajuće aktivnosti (Kao *et. al*., 2019: 1890-1899). Upotreba dronova kod uviđaja različitih krivičnih djela ili pak za policijske aktivnosti podrazumijeva: krizno i preventivno djelovanje i *post delicti* djelovanje i pretpostavlja da postoje obučeni operateri (*Zubair et al*., 2022: *1-17;* Bouafif *et al*. 2018: 1–6). Operateri se brinu o sigurnom letu letjelica, učinkovitom prikupljanju dokaza, ali i o pripremi leta koji im prethodi. Priprema leta sastoji se od primanja informacija, analize i izvršenja naloga.

Planiranje misije letenja je bitna faza s obzirom na to da mali dronovi (za razliku od letjelica koje su velike) najčešće na licu mjesta ne stvaraju promjene, mogu izbjeći prepreke i letjeti tamo gdje velike letjelice ne mogu (Yanmaz *et. al*., 2017: 79–91). Međutim, operateri moraju znati osnove aeronautike, propise o plovidbi (uključujući blizine vazdušnih luka), ruta letenja, visine leta, nadzor nad dronom i vremenske prilike, uz poznavanje forenzičkih postupake kako bi pretraživanja i registrovanja dronom bila adekvatna za sudski postupak.

Nadzor prometa, praćenje osumnjičenog, nadzor mase, otkrivanje krivičnih djela u realnom vremenu, pomoć u istragama mjesta događaja, pomoć prilikom lišenja slobode, generisanje informacije za taktiku timova u situacijama oružanog sukoba, za brzu isporuku opreme i medicinskih potrepština, snimanje područja za obavještajne zadatke itd. - mogu se koristiti u svakoj fazi kriminalističke istrage i od raznih agencije za provedbu zakona. Koristan su instrument u obavještajnom radu i za posebne istražne radnje (tajne radnje, korištenje prislušnih i sličnih uređaja), za sigurno nadziranje i ubacivanjem prislušnih uređaja unutar prostora ili lokacija.

4. REVERZIBILNO KORIŠTENJA BESPILOTNIH LETJELICA

Reverzibilno korištenja bespilotnih letjelica podrazumijeva da one i same postaju oruđe ili čak meta zločina, što je predmet kriminalističkih istraživanja (Goodman, 2013). Mogu se koristiti od strane kriminalaca zbog pokretljivost i mogućnosti da prevaziđu zemaljske prepreke čime su pogodni za prenos zabranjene robe u zatvore ili preko granica ili unutar određenih područja, letove u zonama zabrane letenja, za sudar i izazivanje nesreća sa velikim letjelicama, za ugrožavanje VIP osoba, te za snimanja pojedinaca ili objekata. Dronovi različitih tipova, veličina i snaga motora mogu nositi terete - od eksploziva, oružja i droge, a težina tereta utiče na performanse leta i potrošnju energije. Svaka od ovih situacija zahtijeva kriminalisitičko istraživanje, uz upotrebu forenzičklih tehnika pod uslovom da je sam dron, teret ili kontroler dostupan.

Dronovi koju su komercijalno sredstvo za prenos roba ili za obavljanje određenih zadaća - sami mogu biti predmet otmice kroz uzurpaciju kontrole nad samim dronom ili prenosom podataka sa njega. Nesreće najčešće nastaju usljed gubitka veze sa dronom, a da on nema automatski, odnosno programiran način rada i slijetanja.

5. FORENZIČKO ISPITIVANJE DRONOVA

Forenzička ispitivanja dronova su usmjerena na ispitivanje hardvera, odnosno tijela drona, serijskih brojeva, motora, propelera, baterija, tereta i senzora, softvera i sadržaja koje je dron generisao u obliku datoteka, GPS podataka (Al-Room *et. al*., 2021:1–25; Iqbal *et. al.,* 2019: 1–6). Cilj je da se identifikuje dron ako je registrovan, njegov vlasnik ili osoba koja je uzurpirala dron, da bi se nedvosmisleno utvrdio način upotrebe drona (npr. nagib drona i kamere i smjer leta ukazuju da li je na toj lokaciji samo prelijetao ili snimao) i potrošnja baterija, uz procjenu da li je dron nosio teret i koje težine - ako nije nađen (Lan, Lee, 2022: 291–296). Od značaja su grafički prikazi, uz rekonstrukciju putanje leta, sa značajnim tačkama polijetanja i slijetanja.

Za pristup podacima potrebni su portovi na dronu, kartice i pristup podacima (bez ili sa mjerama kojima se neutrališu antiforenzičke mjere onoga ko je koristio dron). Na samom dronu mogu biti instalirani softveri koji onemogućavaju pristup podacima bez lozinke ili brišu podatke nakon nekog vremena ili daljinski aktiviraju brisanje podataka. Više tehnologija je u igri s obzirom na način kako se dronovi zaustavljaju u letu, bilo fizičkim ili elektronskim mjerama.

Pametni telefoni igraju važnu ulogu u procesu upravljanja dronovima. Oni imaju dvije svrhe u interakciji telefon-dron, gdje se korisnici mogu prebacivati između ručnih i automatskih/autonomnih načina upravljanja. Dronovi preko pametnih telefona šalju svjetlosne naredbe, podatke o statusu drona, slike i video putem wifi komunikacijskih kanala. Pametni telefon može izdati skup unaprijed definisanih naredbi koje mijenjaju rad rotora drona - za promjenu položaja drona u ručnom načinu rada. Alternativno, algoritmi za obradu i strojno učenje mogu se realizovati na pametnom telefonu klijenta, te generisati naredbe koje dron

vraćaju u autonomne načine letenja. Za veće udaljenosti - za prenos podataka između dronova i pametnih telefona se koristi radio komunikacijski kanal od 2,4 GHz.

Odašiljač i kontroler prijemnika spojeni su na pametni telefon putem USB kabela montiranog na prijemniku drona, dok se autonomna navigacija drona može postići na temelju proračuna leta i obrade temeljene vizije leta koja se realizuje na pametnom telefonu. Lažni agent može koristiti lažnu adresu e-pošte i prijaviti se u mobilnu pametnu aplikaciju drona i sakriti svoj identitet dok dron leti i počiniti neke krivične radnje kao što je „povreda vazdušnog prostora" ili provođenje nezakonitih aktivnosti kao što je fotografisanje strateških ili osjetljivih lokacija kod onih letjelica koje imaju malo ili nikakve sigurnosne kontrole za sprječavanje ugrožavanja uređaja (Baig *et al*. 2022).

U slučaju da je dron upleten u kriminalne aktivnosti, njegovo oduzimanje i naknadna analiza u laboratoriju za digitalno forenzičko istraživanje - ključni je dio postupka prikupljanja i analize dokaza. Izazovi povezani s forenzikom drona uključuju dekompoziciju drona i dijelova koji se nalaze rasuti unaokolo, što zahtijeva skupljanje materijala i njegovo povezivanje. Oni digitalni forenzički alati koji su upotrebljivi na određenim dronovima i komponentama - neće moći biti upotrijebljeni na drugim tipovima dronova i drugim komponentama, tako da je za potpun forenzički postupka potrebno mnoštvo softvera i hardvera. Uz to, pojedini dronovi nemaju određenih portova i moguć je samo bežičan prenos slika, pa i to predstavlja ozbiljan problem.

Pristup podacima sa drona može biti onemogućen jer su forenzičari blokirani nemogućnošću pristupa usljed mehanizama zaštite koje je instalirao ili sam proizvođač ili je to učinjeno naknadno manipulacijom visokotehnološki edukovanog vlasnika ili korisnika. Ako je vlasnik i identifikovan, on sam možda neće biti voljan da omogući pristup podacima, čak i pod prijetnjom zakonske kazne. Osim toga, dronovi imaju višestruke datoteke i neke od njih mogu biti čitljive a neke ne, usljed nepostojanja odgovarajućih alata i softvera za skidanje podataka i njhovo čitanje.

Flash i RAM memorija mogu izgubiti podatke nakon pada, ako se baterija drona isprazni. Podaci mogu biti i enkriptirani[10], što otežava ili onemogućuje očitanje. Poznato je takođe da komponente drona imaju različite identifikacijske brojeve. Takve informacije mogu sadržavati serijske brojeve drona (dodijelio ih proizvođač), njegovih propelera, motora, kamera i ugrađeni GPS uređaj. Zavisno od vrste drona, takve informacije mogu, ali i ne moraju biti dostupne za istražitelja, ali ako su dostupne - korisno je utvrditi vezu između drona i njegovog potencijalnog korisnika (Baig *et al*., 2022).

[10] Enkripcija (engleski: *encryption*) ili šifriranje je kodiranje poruke, tj. postupak pretvaranja originala (čistog teksta) u nečitljiv oblik. Tako enkriptiran tekst ima engleski termin *ciphertext*. To je proces u kriptografiji kojim se vrši izmjena podataka tako da se poruka, odnosno informacije, učine nečitljivim za osobe koje ne posjeduju određeno znanje (ključ). Ovaj pojam se najviše koristi u računarstvu, gdje se određeni podaci enkriptuju i najčešće tako zaštićeni šalju putem e-maila. Nadalje, postupak dekodiranja poruke, tj. vraćanja poruke iz njenog enkriptiranog oblika u originalni (čisti tekst) oblik naziva se dekripcija. Vrlo važan termin u kriptografiji je ključ. Ključ ima veliku ulogu u enkripciji i dekripciji poruke.
Enkripcija (engleski: *encryption*) ili šifriranje je proces u kriptografiji kojim se vrši izmjena podataka tako da se poruka, odnosno informacije, učine nečitljivim za osobe koje ne posjeduju određeno znanje (ključ). Ovaj pojam se najviše koristi u računarstvu, gdje se određeni podaci enkriptuju i najčešće tako zaštićeni šalju putem e-maila.

Tokom samog leta dron u svojim datotekama bilježi podatke koji su generisani tokom leta, a kada se skinu sa drona - moguće je rekonstruisati različite aspekte kretanja i operacija drona, kao što su: vremenske odrednice, trajanje leta, brzina, snaga, skretanje, nagib, kotrljanje i visina. Ako su podaci čitljivi, moguć je i grafički prikaz leta drona što sliku čini preglednom i daje jasne okvire za zaključke o prirodi leta i aktivnostima. Forenzika dronova je ukratko usmjerena na preuzimanje i korištenje podataka o mrežnom prometu između drona i kontrolera, preuzimanje zapisnika iz dnevnika koje automatski vodi dron u odgovarajućim datotekama, analizu sistema datoteka i skidanje i pregledavanje produkata kao što su fotografije i video snimci.

Hardverska forenzika, kao i kod svakog uviđaja, uključuje pregled drona i njegovog tereta (npr. eksploziv, droga, oružje koje je instalirano na njemu), te obradu drona - da bi se skinuli otisci pristiju sa njega i komponenti kao što su baterije kamera. Zatim, vrši se analiza tehničkih karakteristika drona: vrsta drona, opis nosivosti, maksimala udaljenost i vrijeme i visina leta, radna frekvencija, vrsta veze između drona i kontrolera, putanja leta, moguće tačke polijetanja i dovođenje u vezu drona sa osobom i mobilnim telefonom ili kontrolerom. Sve to je vrlo složeno s obzirom na to da postoji veliki broj dronova i da njihov hardver i softver nije isti, kao i količina i vrsta podataka koje oni generiraju i čuvaju.

Ukratko, rad je fokusiran na vraćanje svih podataka drona na siguran način, i to tako da se oni mogu nedvosmisleno povezati s podacima na nečijem mobitelu. Neki od alata usvojenih za forenzičku istragu uključivali su 2D i 3D rendgenske uređaje, DataCon, CSVView[11], EnCase/FTK Imager[12] i Compact Forensic Imaging Device[13] (CFID). Preuzimanje hardvera uključuje pažljivo rastavljanje matične ploče drona i flash memorijskog čipa. Ako je model drona poznat kroz registraciju njegovog korisnika, lakše je prepoznati pravu tehničku tablicu sa podacima za referencu koja zauzvrat pomaže u razumijevanju usvojene tehnike pohrane podataka. Mogu se koristiti i rendgenske aparati za traganje strujnih krugova i pinova (tačaka u čipu), te za čitanje podataka - ako nisu bili dostupni za čitanje direktno s memorijskog čipa (preko čitača čipa).

Sažetak bi bio da forenzički ispravne i održive stavke podataka uključuju mapu crne kutije (informacije o letu), mapu sistema (informacije o operativnom sistemu i procesu), nadogradnju mape (informacije o firmveru), datoteku dnevnika (pojedinosti o sistemu, disku i procesu), FTP datoteku (naredbe, vrijeme početka i podaci za prijavu), serijski broj ploče i kamera i serijski broj senzora. Enkripcija podataka opterećuje forenzičare i istražni proces i proces će se stoga morati oslanjati na one podatke koji su izdvojeni u formatu otvorenog teksta. Podaci se mogu prikupljati putem USB i wifi veze, pristupne tačke koju uspostavlja dron tokom pokretanja. Daljinski upravljač se također može koristiti za prikupljanje podataka o putanji leta.

[11] CSView je jednostavan preglednik koji odmah prikazuje početak datoteke sa podacima tako da nema čekanja na velike fajlove za očitavanje.

[12] Digitalna platforma za istragu sa dugom evidencijom kriminalnih aktivnosti, Faucal Tool Kit.

[13] CFID je dizajniran za vojno, obavještajno i policijsko osoblje za jednostavno, prenosno i neupadljivo snimanje, kloniranje, kopiranje i brisanje podataka iz prenosnih medija kao što su USB i SD kartice.

Slike i videozapisi pohranjeni su u unutrašnjoj flash memoriji uređaja i mogu se preuzeti putem FTP-a (*File Transfer Protocol*). GPS koordinate uključene su samo kada su bile dostupne tokom leta. Uz to, vrši se analiza različitih tehnika za pronalaženje slike i podataka o snimanju videa iz drona. Korištene su kako bežične veze FTP, Telnet i žičane veze putem USB priključka ili serijskog (UART[14]) priključka. Serijska (UART) veza je donijela prednost u pogledu količine dostupnih podataka, odnosno medija datoteke, kao i datoteke sistema bespilotne letjelice i podatake sa drona. Koriste se različiti operativni sistemi - kako oni licencirani, tako i *open source* (Baig *et al*. 2022).

6. OTKRIVANJE I DOKUMENTOVANJE ZEMALJSKIH TAJNIH GROBNICA I POVRŠINSKIH OSTATAKA LJUDI

Otkrivanje i dokumentovanje zemaljskih tajnih grobnica i površinskih ostataka ljudi su, isto tako, područje u kojem se koriste bespilotne letjelice i senzori, kao i automatski algoritmi obrade. To je problem složenog odlučivanja u uslovima neizvjesnosti koji zahtijeva identifikacija i inteligentno zaključivanje o direktnim dokazima o ljudskim ostacima i njihovoj okolini. Kao takav, to je koliko inženjerski i geoprostorni, toliko i antropološki problem (Bryce *et al*, 2018).

Cilj je pretraživanja uopšteno "odabrati detekciju i strategiju otkrivanja koja maksimizira snimljene podatke i fizičke dokaze pronađene na mjestu događaja, dok minimizira izmjene mjesta događaja i dokaza", izbjegavajući nepotrebne destruktivne tehnike ili vremensko trošenje na pretraživanje i manje destruktivne tehnike koje štede vrijeme, a jednako su učinkovite (Abate *et al*, 2019: 95-107). Međutim, tačna detekcija ljudskih ostataka često je teška jer mnogo faktora (velika geografska područja koja treba pokriti, vegetativne prepreke, neravan teren i razne opasnosti) mogu rezultirati ugrožavanjem života službenika (Wescott, 2018: 327-342).

Prvo, mnogi senzori montirani na UAV - *unmanned aerial vehicle*[15] (npr. toplinski, radarski) otkrivaju dokaz izvan dometa ljudskog vida. Senzori se mogu kategorisirati u (a) pasivne ili aktivne (posljednji emituje signal) i (b) površinske ili penetrirajuće (potonji omogućuje snimanje slike skrivenih objekata, npr. u zemlji). Njihovi podaci mogu biti obrađeni računarima, analizirani od strane stručnjaka ili neka kombinacija to dvoje. Treće, bespilotne letjelice imaju potencijal za pružanje troškovno i vremenski učinkovitog načina dobijanja visoke rezolucije (spektralne i prostorne).

Senzori su po svojoj prirodi inženjerski zadaci, a traganje i spašavanje je način na koji oni koji koriste letjelice znaju šta mogu dobiti od tih senzora (pod ograničenjima kao što su visina leta, sunčeva svjetlost i doba dana kada se snimanje vrši, vrijeme koje stoji na raspolaganju, uz poštovanje sigurnosnih protokola letenja). Potraga za ljudskim

[14] Univerzalni asinhroni prijemnik i predajnik - UART (Universal Asynchronous Receiver and Transmitter) je digitalno kolo za serijski prenos paralelnih podataka. UART se sastoji iz predajnika i prijemnika. Predajnik funkcioniše kao konvertor podataka iz paralelnog u serijski, a prijemnik kao konvertor iz serijskog u paralelni oblik; *es.elfak.ni.ac.rs/pld/Materijal/UART.pdf.*

[15] Vazduhoplov bez posade.

ostacima putem bespilotnih letjelica uključuje obradu prostora, uz korištenje određenih spektara koje imaju senzori, sa razumijevanjem faza raspadanja ljudskog tijela i posljedica koje, pri tome, nastaju na samom tijelu i okolini. Na očitavanje utiče protok vremena od smrti, stadij raspadanja tijela, vrsta tla i vegetacije, temperatura okoline, doba dana, odnosno sat u kojem se obavlja let, cjelovitost tijela ili njegova uznemirenost od strane lešinara, razbacanost ljudskih ostataka, postojanje i dubina groba, broj osoba u grobnici i sl. (Bryce, *et al*., 2018: 45-61).

U ranijim forenzičkim istraživanjim grobova i grobnica utvrđeno je da se promjene dešavaju na samom tijelu, u promjeni sastava tla, u toplinskom spektru, u fizičkom uznemirenju vegetacije, kao i promjeni boje vegetacije u UV spektru usljed procesa koji nastaju raspadanjem ljudskih tijela. Forenzičko - antropološko istraživanje se kao izvor oslanjalo na tri senzora: termovizijska kamera[16], hiperspektralna kamera[17] i crveno-zeleno-plavi (RGB) fotoaparat. Ovi senzori su raspoređeni na tri bespilotne letjelice s više rotora.

Koriste se metode poput normalizovane razlike vegetacijskog indeksa, iskorištavaju se spektralne i dvodimenzionalne prostorne informacije, SfM, lidar[18], stereo-vid[19] i sl. Može se koristiti izrada trodimenzionalnog modela okoline, a postoje algoritmi za šumarstvo, za biljke/list segmentaciju u poljoprivredi i za detekciju i mjerenje ugljika[20] u travnjacima što je po prirodi stvari složeno i nepredvidljivo tokom mjerenja. Otkriveno je da toplinska detekcija ljudskih ostataka bila je najveća kada su ambijentalne temperature bile između 10 i 35°C. Osim toga, isušena koža i ostala tkiva apsorbuju sunčevo zračenje različito od okolnog terena, emitujući više topline. Pilot istraživanje u Centru forenzičke antropologije u državi Teksas (*The Forensic Anthropology Center at Texas State - FACTS*) je pokazalo da površinska temperatura kože može biti 5-10°C veća od okolnog tla za više od 30 dana (Bryce *et al*, 2018).

Vidljiv spektar i blisko infracrvenom području korišćeni su za otkrivanje krvi, odnosno kože u forenzičkom kontekstu. Pri tome su korišćena tijela i za praćenje ljudi prema odjeći i otkrivanje specifičnih materijala (npr. krv, koža). Softverski algoritmi za otkrivanje ljudi i vozila u daljinskom očitavanju - pokazuju od 90 do 100% stope tačnosti.

Međutim, sve ovo nije bez nedostataka. Prvo, kombinacija prostornih, spektralnih i vremenskih podataka često se pretvara u veliki problem, sa ogromnim brojem podataka i njihovom obradom. To zauzvrat može ograničiti vrijeme leta i pokrivenost.

[16] Termovizijska dijagnostika se koristi u vojnoj i medicinskoj industriji i bezbjednosnim sistemima. Ove kamere omogućavaju da ljudsko oko sagleda ono što ne može da vidi. Svako tijelo emituje određenu količinu energije koja može da se registruje kamerom za termoviziju.

[17] Hiper - spektralna slikovna dijagnostika detektuje promjene u svjetlosti koje reflektiraju tlo i biljke ispod kojih se nalaze tijela u raspadanju.

[18] Lidar je metoda za određivanje raspona (varijabilna udaljenost), ciljajući objekat ili površinu laserom i mjereći vrijeme - da bi se reflektovano svjetlo vratilo na prijemnik.

[19] Trodimenzionalnost vida ili stereo-vid je sposobnost čula vida da predmete detektuje u tri dimenzije, dakle i po dubini. Stereo vid je najviši nivo binokularnog vida. Prvi nivo je istovremeno gledanje sa oba oka (simultana percepcija), drugi je spajanje slika iz oba oka u jednu (fuzija slika) i treći nivo je stereo vid. Stereo vid se određuje posebnim testovima (titmus test).

[20] Ugljenik, ugljik ili karbon (C, lat. *carboneum*), nemetal je IVa grupe.

Uobičajena praksa je da se bend talasa za snimanje odabire na nekoliko bendova (od stotina) za korištenje. Uz to, algoritmi smanjuju stotine opsega podataka u drastično manje, s ciljem osigurati da su obrasci i dalje prisutni u smanjenom prostoru.

Drugo, povećana dimenzionalnost (prostorna, spektralna i vremenska) ima negativan uticaj na obrade signala i algoritme. Upitno je i precizno pozicioniranje. Vrlo velika preciznost je potrebna za dokumentaciju, a možda i otkrivanje. Nadalje, većina sistema ne može obraditi podatke u stvarnom vremenu, a konstrukcija slike i analitika se mora raditi *offline* (Bryce *et al*, 2018: 45-61). Osim toga, uticaj imaju i atmosferske korekcije (vodena para, ugljen dioksid, kiseonik, uticaj sjena koje stvara sunce, što utiče na spektar koji se koristi itd.). Pored toga, efikasnost limitiraju maksimalna nadmorska visina leta, kao i da letjelica mora uvijek biti u vidnom polju.

7. BESPILOTNE LETJELICE U HITNIM SLUČAJEVIMA POPLAVA

U radu ćemo dati i prikaz studija za procjenu koje bespilotne letjelice mogu biti od koristi u pripremi i odgovoru na hitne slučajeve poplava i razvijanja smjernica za njihovo raspoređivanje prije, tokom i nakon poplave. Naime, analogno poplavama, upotreba bespilotnih letjelica na istom modelu može se primijeniti za odgovor u postupanju policije na krizne situacije (Salmoral *et. al*., 2020: 2-21). Umanjenje efekata poplava uključuje upozoravanje i informisanje prije i tokom događaja, evakuaciju prije poplava, spašavanje ljudi i organizovanje odgovora, s ciljem zaštite ljudskih života, ublažavanja patnje i ponovnog uspostavljanja poremećenih usluga (npr. voda, struja, prevoz). Unutar ovog okvira i na temelju dokumentovanih protokola zapovijedanja i kontrole, odluke se donose na najnižem prikladnom novou, uz koordinaciju na najvišem potrebnom novou. Hitne službe zahtijevaju i upoređuju različite informacija: od snimaka iz vazduha - do pojedinačnih izvještaja svjedoka u podršci donošenja odluka (Lucieer, Jong, De Turner, 2013: 97-116).

Prije, tokom i nakon događaja potrebne su različite informacije. Na primjer, tokom poplave lokalne informacije su u stvarnom vremenu ili gotovo u stvarnom vremenu o broju ljudi, zgrada i druge infrastrukture koje su u opasnosti. Pored toga, snimke iz vazduha nakon događaja mogu pružiti vitalne i detaljne informacije radi procjene područja. Međutim, takvo gledanje dovelo je do *ad hoc* i oportunističkog korištenja bespilotnih letjelica - umjesto strateške procjene kako ih najbolje koristiti i za koju svrhu prije.

Razne vrste misija u hitnim reakcijama na poplave (uključujući stratešku svijest o situaciji, inspekcije, pretragu terena, traženje vode, procjena štete i svjesnost o taktičkoj situaciji), s naznakom podataka (npr. slike, video-zapisi i ortomozaici[21]), generisani u letovima, još uvijek nisu usvojili sigurne preporuke koji produkti i kakve kvalitete su potrebni u svakoj pojedinoj fazi djelovanja - od pripreme i reakcije na krizni događaj do oporavka. Matrica analize može biti dizajnirana i korištena kao pomoć zahtjevima hitnog odgovora na poplave, zavisno od vrste i prirode poplava (Ward *et al*. 2015: 712–715).

[21] Orthomosaic je fotografija koja je sačinjena od nekoliko fotografija (mosaic) i uvijek nudi gornji pogled (orthogonal).

To će se postići kroz sljedeća četiri sveobuhvatna cilja: (1) mapirati trenutne uloge postojećih organizacija uključenih u odgovor na hitne slučajeve; (2) identifikovati postojeće aplikacije bespilotnih letjelica (unutar komponenti sistema upravljanja rizikom od poplava); (3) odrediti zahtjeve specifične za za upotrebu dronova koji pomažu u upravljanju rizikom od poplava i aktivnostima i (4) razviti prilagodljivi i prenosivi okvir matrične analize koji zatim može koristiti kao temelj za smjernice za učinkovitu primjenu bespilotnih letjelica za upravljanje rizikom i djelovanjem prije, tokom i nakon poplave (Salmoral, 2020). Cilj je da se izaberu najbolje komponente upravljanja, koje bi uključivale upozoravanje na poplave, praćenje poplava i procjenu rizika od poplava, identifikaciju puta evakuacije, procjena štete i spašavanje.

Sve navedeno je potrebno kako bi se dronovi ili bespilotne letjelice mogle prostorno rasporediti i ispravno podesiti konfiguracije plana leta, a na koje utiču povezani fakori. Tri glavna identifikovana faktora povezana su sa vrstom sliva, odnosno porijeklom i vrstom poplava: veličina, vrsta izvora poplave i faza poplavnog događaja. Veličina sliva utiče na količinu prikupljenih podataka i vrste bespilotnih letjelica koje su potrebne za pružanje prostorne pokrivenosti. Odgovori na prethodna pitanje utvrđuju vrijeme dostupno za postavljanje bespilotne letjelice i korištenje određenih aplikacija i tehnologija za datu situaciju.

Odgovor na poplavu sliva određen je na temelju vremena između početka padavina i mogućnosti plavljenja. Na temelju klimatskih i slivnih uslova - odgovor na poplave smatra se „sporim" kada se poplave češće javljaju više od osam sati nakon kiše, „srednje" kada se poplava dogodi između tri i osam sati i „brzo" kada se početak poplave događa za manje od tri sata.

Matrica faza u kojoj će se bespilotna letjelica koristiti jeste: „prije događaja", „tokom događaja" i „nakon događaja" (Salmoral, 2020). „Prije događaja" odnosi se na aktivnosti kao što su modeliranje poplava, izgradnja sredstava za smanjenje rizika od poplava i planiranje odgovora na definisanu veličinu poplave. „Tokom događaja" počinje čim se izda prvo upozorenje na poplavu, dok se „nakon događaja" odnosi na oporavak i fazu čišćenja - kada se voda povukla i nije u objektima ili urbanoj infrastrukturi. Aplikacije koje dronovi mogu da imaju usmjereni su na mjerenje dubine poplave i brzinu protoka vode, geometriju poplave, određivanje kota, evakuacijskih ruta, identifikovanje ljudi koji trebaju spašavanje, izvore poplava i smatraju se ključnim za donošenje odluka tokom poplave. Ključno pitanje je tačnost ovih podataka i vrijeme potrebno za obradu podataka - kako bi se dobile jasne slike za donošenje odluka.

Sirovi proizvodi bespilotnih letjelica uključuju video visoke rezolucije (HD), infracrveno snimanje, Crveno-zeleno-plavu (RGB) sliku[22], RGB video, RGB video streaming i termalnu sliku. Ukupno je identifikovano 14 ishoda naknadne obrade (Salmoral, 2020: 7)

[22] RGB je kratica za engleski pojam "Red (crvena) Green (zelena) Blue (plava)". RGB je aditivni model boja kod kojeg se zbrajanjem osnovih boja dobija bijela boja. Jedna boja se opisuje kroz tri vrijednosti: dio crvene, dio zelene i dio plave boje. Svaki dio boje varira između 0% i 100%. Prostor RGB-boja se šematizira u obliku kocke. *https://hr.wikipedia.org/wiki/RGB.*

ZAKLJUČAK

Zahvaljujući svojoj hardverskoj i softverskoj konfiguraciji, dronovi su korisni za mjerenje, fotografisanje, pronalaske predmeta prilikom uviđaja i naknadnu rekonstrukciju. Koriste se različite tehnike osvjetljenja npr. UV i infracrveni zraci što im otvara brojne mogućnosti. U kriminalističkoj praksi gledanja udaljene zone lica mjesta i fotografisanje mjesta događaja, s više karakteriziranih tačaka i iz vazduha - temelj je kvalitetne pripreme za uviđaj i samog provođenja uviđaja.

Dronovi u realnom vremenu prate požare, poplave, pronalaze tijela u svim fazama raspadanja i dijelove tijela. Od vrste i broja senzora - zavisi veličina i cijena dronova i senzora. U vezi s tim, u zemaljskim stanicama ili nakon prenosa uživo ili nakon slijetanja drona i skidanja podataka - softeverski programi i algoritmi omogućuju pravilno očitavanje, tumačenje, mapiranje i prikaz tih podataka u odgovarajućem obliku. Mogu se koristiti laseri i 3D kamere, koji su zajedno sa GPS sistemom i zapisima koje stvar dron, detaljni izvor informacija i vjerodostojna interpretacije onoga što je pronađeno.

Prednost dronova u odnosu na dosadašnje sredstva i tehnike je da imaju progamabilne funkcije, malih su dimenzija i cijena im je prihvatljiva. Od posebnog su značaja u početnoj informativno - orijentacijskoj fazi uviđaja, ali i kod forenzičke obrade lica mjesta, naročito kada se radi o nepristupačnim lokacijama.

Zbog pokretljivost i mogućnosti da prevaziđu zemaljske prepreke, dronovi su pogodni za prenos zabranjene robe, letove u zonama zabrane letenja, za sudar i izazivanje nesreća sa velikim letjelicama, za ugrožavanje VIP osoba i za snimanja iz vazduha pojedinaca ili objekata. Dronovi različitih tipova, veličina i snaga motora mogu nositi terete - od eksploziva, oružja i droge, a težina tereta utiče na performanse leta i potrošnju energije. Svaka od ovih situacija zahtijeva kriminalističko istraživanje, uz upotrebu forenzičklih tehnika.

Pametni telefon može izdati skup unaprijed definisanih naredbi koje mijenjaju pozicije i manevre drona u ručnom ili autonomnom načinu rada. Autonomna navigacija drona može se postići na temelju proračuna leta i obrade temeljene vizije leta koja se realizuje na pametnom telefonu. Ispituje se i hardver drona u forenzičkim ispitivanjima, a fokus je identifikacija vlasnika drona preko brojeva drona i baterije, kamere, motora, tereta i lokacije polijetanja, odnosno preko daljinskog upravljača ili mobitela koji je dostupan.

Digitalni forenzički alati koji su upotrebljivi na određenim dronovima i komponentama neće moći biti upotrijebljeni na drugim tipovima dronova i drugim komponentama. Pored toga, pojedini dronovi nemaju određenih portova i moguć je samo bežičan prenos slika, pa i to predstavlja ozbiljan problem. Takođe, pristup podacima sa drona može biti onemogućen jer su forenzičari blokirani nemogućnošću pristupa usljed mehanizama zaštite koje je instalirao ili sam proizvođač ili je to učinjeno naknadno manipulacijom visokotehnološki edukovanog vlasnika ili korisnika.

Pojavljuje se niz problema i od korištenja dronova za tačnu detekcija ljudskih ostataka. Potraga za ljudskim ostacima putem bespilotnih letjelica uključuje obradu prostora, uz korištenje određenih spektara koje imaju senzori. Naposlijetku, upotreba ovih letjelica na modelu poplava može se primijeniti za odgovor u postupanje policije na krizne situacije.

LITERATURA

1. Abate, D., Sturdy, Colls, C., Moyssi, N., Karsili, D., Faka, M., Anilir, A., Manolis, S. (2019) „Optimizing search strategies in mass grave location through the combination of digital technologies", *Forensic Sci Int Synerg*, 3, 1, 95-107; *doi: 10.1016/j.fsisyn.2019.05.002. eCollection 2019.*
2. Ahn, H. (2020) *Deep learning based anomaly detection for a vehicle in swarm drone system*. In: Proceedings of the 2020 International Conference on Unmanned Aircraft Systems (ICUAS), Athens, Greece, 1–4 September 2020, 557–561.
3. Al-Room, K., Iqbal, F., Baker, T., Shah, B., Yankson, B., MacDermott, A., Hung, P.C. (2021) „Drone Forensics: A Case Study of Digital Forensic Investigations Conducted on Common Drone Models", *Int. J. Digit. Crime Forensics (IJDCF)*, 13, 1–25 [CrossRef].
4. Andrejević, M. (2016) *Theorizing drones and droning theory*. In A. Završnik (Ed.), Drones and Unmanned Aerial Systems (21–43), Cham: Springer International Publishing.
5. Barton, T.E.A., Azhar, M.H.B. (2017) *Forensic analysis of popular UAV systems*. In: Proceedings of the 2017 Seventh International Conference on Emerging Security Technologies (EST), Canterbury, UK, 6–8 September 2017, 91–96.
6. Bhoopesh, K.S., Geetanjali, C., Ved P.M. (2019) *Comparitive Analysis and Implication of UAV and Al in Forensic Investigations*, IEEE, doi: 10.1109/AICAI.2019.8701407; *https://www.researchgate.net/publication/332758621_Comparitive_Analysis_and_Implicatio n_of_UAV_and_AI_in_Forensic_Investigations.*
7. Boštjan, S. (2016) *Drones in (slovene) criminal investigation*, Faculty of Criminal Justice and Security, Ljubljana, Slovenia, pp. 7-25; *https:// hrčak.srce.hr/file/268980.*
8. Bouafif, H., Kamoun, F., Iqbal, F., Marrington, A. (2018) *Drone forensics: Challenges and new insights*. In: Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018, 1–6.
9. Bryce, M, Derek, T. Anderson, Daniel, J. Wescott, R.M, Melissa, F. A. (2018) „Survey and Insights into Unmanned Aerial Vehicle-Based Detection and Documentation of Clandestine Graves and Human Remains Article in Human Biology", *Hum Biol*, pp. 45-61; *https://www.researchgate.net/publication/326586150.*
10. Bouafif, H., Kamoun, F., Iqbal, F. (2020) „Towards a better understanding of drone forensics: A case study of parrot AR drone 2.0.", *Int. J. Digit. Crime Forensics (IJDCF)* 2020, 12, 35–57. [CrossRef].
11. Clark, D.R., Meffert, C., Baggili, I., Breitinger, F. (2017) „DROP (DRone Open source Parser) your drone: Forensic analysis of the DJI Phantom III", *Digit. Investig.*, 22, S3–S14. [CrossRef].
12. Crotty, S. (2014) „The aerial dragnet: A drone-ing need for fourth amendment change", *Valparaiso University Law Review*, 49(1), 219– 265.

13. Drone Technology Uses and Applications for Commercial, Industrial and Military Drones in 2021 and the Future. 2021. Available online: *https://www.businessinsider.com/dro ne-technology-uses-applications*.
14. Drones Add a New Dimension to Crime Scene Investigations. [online]. Available: *https://www.huffingtonpost.com/projourno/drones-add-a-new-dimensio_b_6033392.html.*
15. Flynt, J. *How Much Weight Can a Drone Carry*? Available online: *https://3dinsider.com/drone-payload/.*
16. Flynt, J., *Best Heavy Lift Drones-Large Drones. That Have High Lift Capacity.* Available online: *https://www.dronethusiast. com/heavy-lift-drones/.*
17. Goodman, M. (2013) „Criminals and terrorists can fly drones too", *Time*, Retrieved from *http://ideas.time.com/2013/01/31/criminalsand-terrorists-can-fly-drones-too/.*
18. *Helicopter Versus Drones: The cost of the war on rhinos* [online]. Available: *http://www.cnn.com/2013/10/16/world/africa/helicopters-versus-drones-rhino/index.html?iref=allsearch.*
19. Hummel, K.A., Pollak, M., Krahofer, J. (2019). *A distributed architecture for human-drone teaming: Timing challenges and interaction opportunities*, Sensors, 19, [CrossRef] [PubMed].
20. Iqbal, F., Alam, S., Kazim, A., MacDermott, Á. (2019) *Drone forensics: A case study on DJI phantom 4*. In Proceedings of the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 3–7 November 2019, 1–6.
21. Jeong, S., Bito, J., Tentzeris, M.M. (2017) *Design of a novel wireless power system using machine learning techniques for drone applications*. In Proceedings of the 2017 IEEE Wireless Power Transfer Conference (WPTC), Taipei, Taiwan, 10–12 May 2017, 1–4.
22. Kao, D.Y., Chen, M.C., Wu, W.Y., Lin, J.S., Chen, C.H., Tsai, F. (2019). „Drone forensic investigation: DJI spark drone as a case study", *Procedia Comput. Sci.,* 159, 1890–1899. [CrossRef].
23. Lan, J.K.W., Lee, F.K.W. (2022) *Drone Forensics: A Case Study on DJI Mavic Air 2*. In Proceedings of the 2022 24th International Conference on Advanced Communication Technology (ICACT), Seoul, Korea, 13–16 February 2022, 291–296.
24. Lee, D., La, W.G., Kim, H. (2018) *Drone detection and identification system using artificial intelligence*. In Proceedings of the 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 17–19 October 2018, 1131–1133.
25. Lucieer, A., Jong, S.M., De. Turner, D. (2013) "Mapping landslide displacements using Structure from Motion (SfM) and image correlation of multitemporal UAV photography Mapping landslide displacements using Structure from Motion (SfM) and image correlation of multitemporal UAV photography", *Prog. Phys. Geogr.*, 38, 97-116.
26. Mekala, S.H., Baig, Z. (2019*) Digital Forensics for Drone Data - Intelligent Clustering Using Self Organising Maps*. In Future Network Systems and Security. In Robin Doss,

S., Piramuthu, W.Z, 0001, editors, Future Network Systems and Security - 5th International Conference, FNSS 2019, Melbourne, VIC, Australia, November 27-29, 2019, Proceedings, Volume 1113 of Communications in Computer and Information Science, 172-189, Springer, 2019.

27. Park, J., Kim, Y., Seok, J. (2016) *Prediction of information propagation in a drone network by using machine learning.* In Proceedings of the 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea, 19–21 October 2016, 147–149.
28. *Police to Use Spy Drones on Criminals*. [Online]. Available: *http://www. theaustralian. com.au/news/sa-police-to-useunmanned-drones-to-spy-on criminals/ story-e6frg6n6-1226671865697.*
29. *Police crime investigations now use drones*. Drone Makers, UK. [online]. Available: *https://www.independent.co.uk/lifestyle/gadgets-and-tech/news/uk-police-drones-24-hour-unitinve stigate-crimes-missing-person-search-cases-cornwalldevon-forces-a7639641.html.*
30. Rao, B., Gopi, A. G., Maione, R. (2016) „The societal impact of commercial drones", Technology in Society, 45, 83–90.
31. Renduchintala, A.L.S., Albehadili, A., Javaid, A.Y. (2017*). Drone forensics: Digital flight log examination framework for micro drones*. In Proceedings of the 2017 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 14–16 December 2017, 91–96.
32. Renduchintala, A., Jahan, F., Khanna, R., Javaid, A.Y. (2019) „A comprehensive micro unmanned aerial vehicle (UAV/Drone) forensic framework", *Digit. Investig.* 2019, 30, 52–72. [CrossRef].
33. Robinson, E. (2010) *Crime Scene Photography, Second Edition*, Elsevier Academic Press, Burlington.
34. Rydén, H., Redhwan, S.B., Lin, X. (2019) *Rogue drone detection: A machine learning approach*. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakesh, Morocco, 15–18 April 2019, 1–6.
35. Salmoral, G., Rivas, C., Monica, M., Manoranjan, B., David, M., Prathyush, P., Leinster, P. (2020) „Guidelines for the Use of Unmanned Aerial Systems in Flood Emergency Response", *Water*, 2, Water, 2-21; *doi:10.3390/w12020521.*
36. Sandbrook, C. (2015) „The social implications of using drones for biodiversity conservation", „Ambio", 44(S4), 636–647.
37. Sciancalepore, S., Ibrahim, O.A., Oligeri, G., Di Pietro, R. (2019) *Detecting Drones Status via Encrypted Traffic Analysis*. In Proceedings of the ACM Workshop on Wireless Security and Machine Learning (WiseML 2019), Miami, FL, USA, 15–17 May 2019; Association for Computing Machinery: New York, NY, USA, 2019, 67–72. doi: [CrossRef].
38. Sciancalepore, S., Ibrahim, O.A., Oligeri, G., Di Pietro, R. (2020) „PiNcH: An effective, efficient, and robust solution to drone detection via network traffic analysis", *Comput. Netw.,* 2020, 168, 107044. [CrossRef].

39. Sharma, B. K., Chandra, G., Mishra, V.P. (2019) „Comparitive Analysis and Implication of UAV and AI in Forensic Investigations", *Amity International Conference on Artificial Intelligence (AICAI)*, 824-827.
40. Viswanathan, S., Baig, Z. (2020) *Digital Forensics for Drones: A Study of Tools and Techniques*. In: International Conference on Applications and Techniques in Information Security; Springer: Berlin/Heidelberg, Germany, 29–41.
41. Ward, P.J., Jongman, B., Salamon, P., Simpson, A., Bates, P., De Groeve, T., Muis, S., De Perez, E.C, Rudari, R., Trigg, M.A. *et al.* (2015)„Usefulness and limitations of global flood risk models", *Nat. Clim. Chang.,* 5, 712–715.
42. Wescott, D.J. (2018) „Recent advances in forensic anthropology: decomposition research", *Forensic Sci Res,* 13, 3(4), 327-342; *doi: 10.1080/20961790.2018.1488571. eCollection2018. PMI D:30788450.*
43. Yanmaz, E., Quaritsch, M., Yahyanejad, S., Rinner, B., Hellwagner, H., Bettstetter, C. (2017). *Communication and coordination for drone networks*. In Ad hoc Networks; Springer: Berlin/Heidelberg, Germany, 79–91.
44. Yousef, M., Iqbal, F. (2019) *Drone forensics: A case study on a DJI Mavic Air*. In: Proceedings of the 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 3–7 November 2019, 1–3.
45. Yousef, M., Iqbal, F., Hussain, M. (2020) *Drone forensics: A detailed analysis of emerging DJI models*. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020, 66–71.
46. Završnik, A. (2016) „Drones, resistance and countersurveillance". In A. Završnik (Ed.), *Drones and Unmanned Aerial Systems* (243–266). Cham: Springer International Publishing.
47. Zubair, B., Majid, A.K., Nazeeruddin, M., Ghassen B.B. (2022) „Drone Forensics and Machine Learning: Sustaining the Investigation Process", *Sustainability, vol. 14, 1-17; https://doi.org/10.3390/su14084861.*

THE USE OF EVIDENCE COLLECTED BY THE DRONES IN CRIMINAL INVESTIGATIONS

Drones have an increasing role in criminal investigation, primarily in conducting investigations, but also in other criminal investigation activities, especially searching the scene after the event is over or monitoring event that is still active. The body conducting the investigation, which is first and foremost the police, must quickly and visibly secure the scene as well as all objects and traces on it. Search, recording and documentation, collection and analysis from the site must be performed without harassment and contamination. The entry of staff into the area carries risk and requires time, staff and complex activities.

The seizure of the drone, as well as basic and forensic analysis of the drone and its contents is the basis for gathering evidence. In addition to drones, smartphones play a key role in this process because they are the basis for telephone - drone communication, and can be crucial for determining the status in flight, and lead to all products of drone activity - in the form of photos and videos. All this should shed light on the role of the user or owner of the drone if someone else has misused that communication and taken control over of the drone. Parts of the drone have unique markings and the analysis of physical components is carried out as part of the forensics of physical parts, as well as data generated during the flight that are analyzed as part of digital forensics. All this will enable the drone flight to be shown.

On the other hand, adequate development of protection against illegal use of drones as well as investigations related to them implies monitoring and following the trends in this area. What is especially important to point out is that drone operations differ significantly in times of peace, crisis and war.

The fight against the misuse of drones includes the use of all available means and methods, as well as the exploitation of all the weaknesses that drones in general and certain types of drones have. First of all, drone deactivation refers to the focus on the drone itself rather than on other components of the system such as remote control, communication and personnel operating the aircraft.

KEYWORDS: *drone, investigation, expertise, investigation.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.09

THE RETENTION OF TRAFFIC AND LOCATION ELECTRONIC COMMUNICATIONS DATA IN THE EUROPEAN UNION FOR THE PURPOSE OF CRIMINAL PROCEEDINGS

Ana Krnić Kulušić*

The retention of traffic and location electronic communications data remained to be one of the most debatable topics in the European Union regardless of its advantages in investigating and processing crimes. The regime introduced by the Data Retention Directive in 2006 has attracted the interest of both experts and the public. While some emphasized the importance of protecting national security, others focused on it being a gross invasion of citizens' privacy. The broad debate ended with the declaration of the Data Retention Directive invalid by the Court of Justice of the European Union. With this ruling, the court did not rule out the possibility of retaining data for the purpose of fighting against serious crime but found that the same is allowed only with appropriate safeguards. The subsequent Court's decisions however shed more light on the issue. After the Data Retention Directive has been revoked, the data retention domain remained regulated by the 2002 ePrivacy Directive. In parallel, the European Commission began proposing a new ePrivacy Regulation which should be aligned with the current state of play in the field of privacy and electronic communications. However, the process for adopting it turned out to be lengthy and still not completed. The most recent Court decision in the Dwyer case confirmed that the EU law precluded the general and indiscriminate retention of traffic and location data relating to electronic communications for the purposes of combating serious crime while giving more clarifications on data retention possibilities. This paper analyses the current regulatory framework in the field of data retention and relevant case law.

KEYWORDS: *retention of traffic and location electronic communication data, EU, criminal proceedings.*

* Mag. iur. univ. spec. elect. comm, Head of Regulatory Affairs and Data Protection, Iskon Internet Inc. Zagreb, Croatia. E-mail: *ana.krnic.kulusic@iskon.hr*

INTRODUCTION

The growth and development of the electronic communications market made the retention of telecommunications data (i.e., data in electronic communications) one of the most debatable topics in the European Union. The discussion on it being based on the delicate balance between safeguarding national safety and guaranteeing the protection of human rights and fundamental freedoms.

Terrorist attacks in the United States of America and Europe prompted the Member States of the European Union and the European legislator to introduce the obligation to collect and retain data in electronic communications to fight terrorism and serious crimes more effectively. As a result, a specific regulation was adopted in 2006, in the form of a directive, which set the framework for the data retention regime.

Even though it is indisputable among experts and the public that the retention of data in electronic communications is a useful and effective tool for the prevention, detection, investigation and prosecution of criminal offenses, the question of encroaching on the fundamental rights and freedoms of individuals arose soon. Primarily the rights to privacy, the protection of personal data and the right to freedom of expression guaranteed by the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights.

These issues were initially raised at the level of individual Member States and soon after before the Court of the European Union. As a result of one of the judgments of the Court, the 2006 directive regulating the field of data retention was declared invalid. In the following years, several judgements paved the way for a data retention regime in the European Union and an initiative for a new regulation in the field of privacy and electronic communications was instigated. However, the adoption process turned out to be lengthy and still unfinished.

This paper analyzes the developments and current state in the field of traffic and location data retention in electronic communications in the European Union for the purpose of criminal proceedings.

1. DEFINITION OF TRAFFIC AND LOCATION DATA

The Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter: Directive on Privacy and Electronic Communications or ePrivacy Directive) defines "traffic data" as any data processed for the purpose of the conveyance of a communication on an electronic communications network or the billing thereof.[1] According to it, traffic data may imply data referring to the routing, duration, time or volume of a communication, the protocol used, the location of the terminal equipment of the sender or recipient, to the network on

[1] Article 2.

which the communication originates or terminates, to the beginning, end or duration of a connection.[2]

In practice, traffic data reveals the contacts an individual has had by means of electronic communications, the exact time of these contacts and their duration. Location data disclose the area of electronic communications origination and termination associated with a piece of particular terminal equipment. To put it simply, location data reveals the place where a person resides and for how long.

According to the European Commission, traffic and location data do not serve simply as evidence but also as a first step in finding more substantial information through the identification of further elements such as a device, a person, or the location of a crime.[3]

Traffic and location data must not be mistaken for the content of transmitted electronic communications and the lawful interception thereof which are regulated separately.

According to ETSI, a European Standards Organization[4], lawful Interception (LI) is a security process in which a service provider or network operator collects and provides law enforcement officials with intercepted communications of private individuals or organizations[5]. Lawful interception implementation is regulated by the European Council Resolution from 1995 which allows for LI to prevent crime, including fraud and terrorism.[6]

This paper does not examine over-the-top service providers (OTTs) in light of data retention as no EU or national legal framework is currently imposing a general data retention obligation on them for law enforcement purposes.

2. THE DATA RETENTION DIRECTIVE

The Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (hereinafter: the Data Retention Directive) entered into force on May 3, 2006, with a deadline for transposition into national legislation until September 15, 2007.

The adoption of the Data Retention Directive followed as a direct response of the legislation of the European Union (hereinafter: EU) to terrorist attacks in the United States of America, Great Britain, and Spain. Namely, states affected by terrorism stressed the

[2] Recital 15.

[3] European Commision, Study on the Retention of Electronic Communications Non-Content Data for Law Enforcement Purposes, 2020, 120, [25.8.2022.].

[4] ETSI is a standards body dealing with telecommunications, broadcasting and other electronic communications networks and services. More details are available at www.etsi.org, [25.8.2022.].

[5] See the following webpage: https://www.etsi.org/technologies/lawful-interception#:~:text=Introduction,of%20private%20individuals%20or%20organizations, [3.9.2022.].

[6] Council Resolution of 17 January 1995 on the lawful interception of telecommunications, available at the following webpage: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:C:1996:329:TOC, [25.8.2022.].

importance of retaining data in electronic communications in the fight against terrorism and other serious forms of crime. As a result of these specific circumstances, at the time of the adoption of the directive in question, the European legislator focused on security issues, while the protection of privacy (at least temporarily) was put on the back burner.

The main goal of the Data Retention Directive was to harmonize the legislation of the EU Member States on the issue of data retention in electronic communications. According to the Directive, Member States are obliged to store identification, traffic, and location data of users of electronic communications services for at least six and at most 24 months, where the storage does not refer to the content of the communication itself.

The procedure and conditions for accessing stored data are left to national legislation in accordance with the principles of necessity and proportionality. The Directive also specifies the obligations of providers of electronic communication services and public communication networks (hereinafter: operators) to ensure that retained data is available to competent authorities to ensure its availability for the purpose of investigation, detection, and prosecution of serious criminal offences.

Leaving no one indifferent, right from the very beginning, the Data Retention Directive has attracted the interest of experts as well as the public. While some emphasized the importance of protecting national security, others focused on it being a gross invasion of citizens' privacy.

The controversy of the adopted text was soon proved by the impediments in its transposition into national legislation in some of the Member States. Specifically, the Constitutional Courts of Romania and Germany have repealed certain provisions of the national laws transposing the Data Retention Directive.

2.1. Declaration of the Data Retention Directive Invalid – CJEU Judgment in the Digital Rights Ireland case

The Data Retention Directive was repealed by the judgment of the Court of Justice of the EU (hereinafter: Court or CJEU) in the joined cases C-293/12 *Digital Rights Ireland* and C-594/12 *Government of the Province of Carinthia et al.*[7]

Case C-293/12 concerns a dispute brought by Digital Rights Ireland regarding the legality of national legislative and administrative measures relating to the retention of electronic communications data. The request from case C-594/12 refers to the claims of the Government of the province of Carinthia and others regarding the compatibility of the law transposing the Data Retention Directive into Austrian law with the federal constitutional law.

The Court ruled that, by requiring the retention of the data and by allowing the competent national authorities to access them, the Directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection

[7] Available at the following webpage: https://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN, [20.8.2022.].

of personal data. Furthermore, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the persons concerned a feeling that their private lives are the subject of constant surveillance.

Following the abovesaid, the Court reasoned that the fight against serious crime is indeed of primary importance for public security, but that such a goal cannot by itself justify that the measures provided for in the Directive are considered necessary. Indiscriminate retention of data and of those persons for whom there is no indication of a connection with serious criminal offenses (practically the entire EU population is monitored), the general absence of restrictions that would limit the collection, retention and access to data, the absence of criteria for the irreversible destruction of data and the absence of a ban on export data from the EU are key arguments from the judgment.

With this ruling, the court did not rule out the possibility of retaining data for the purpose of fighting serious crime but found that the same is allowed only with appropriate safeguards.

The Directive was repealed with an *ex tunc* effect and expired on 8 April 2014, bringing the European legislator back to the beginning under this initiative. However, at the same time, a significant legal gap arose and the inconsistency of Member States' national legislations with the EU law. The same directive that was repealed was already transposed to Member States' national legislations and applied there.

3. THE EU LEGISLATIVE FRAMEWORK AFTER THE DATA RETENTION DIRECTIVE

After the repeal of the Data Retention Directive, CJEU found that Article 15, paragraph 1 of the ePrivacy Directive is applicable to data retention measures in the national legislations of the Member States.

The provision in question stipulates that the Member States may adopt legal measures to limit the scope of rights and obligations when such limitation represents a necessary, appropriate and proportionate measure within a democratic society with the aim of protecting national security, defense, public safety and with the aim of prevention, investigation, detection and prosecution criminal acts, i.e. unauthorized use of the electronic communication system. In addition, it is specified that the Member States may adopt legal measures that enable the retention of data for a limited period. At the same time, additional obligations in the form of internal protocols and procedures for the purpose of security protection are imposed on operators.

The Data Retention Directive was preceded by the ePrivacy Directive, which applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks.[8] As already mentioned above, personal data regulated by this Directive and processed by operators are traffic, location, and content of the communication.

[8] Article 3.

4. JUDGMENT OF THE CJEU IN THE TELE2 SVERIGE/WATSON JOINED CASES

After the repeal of the Data Retention Directive, the CJEU, in its judgment in the combined cases C-203/15 *Tele2 Sverige* and C-698/15 *Watson et al.*[9], dated December 21, 2016, set several detailed requirements that national legislations must meet for the data retention to be considered compliant with EU law.

The first case relates to the dispute between Tele2 Sverige and the Swedish Post and Telecommunications Supervisory Authority concerning an order sent by the regulator to Tele2 Sverige to retain data on the location of its subscribers and registered users. The second case is related to the dispute between Tom Watson, Peter Brice and Geoffrey Lewis, and the Home Office of the United Kingdom of Great Britain and Northern Ireland on the compatibility of national data retention legislation with EU law.

In both cases, the key question is the same, namely whether national legislation, when it comes to data retention, is harmonized with EU law. When deciding on that issue, the Court made the following conclusions.

i. Traffic and location data are equally sensitive information with regard to the right to respect for private life, as is the content of communications itself. The Court pointed out that these data can enable the making of very precise conclusions about the private life of the persons whose data have been retained (e.g. daily habits, places of permanent or temporary residence, daily or other movements, activities performed, social relations and social environments visited by these persons).

ii. The measure of retention of traffic and location data was assessed as a serious interference with fundamental rights that can only be justified in the case of the fight serious criminal offenses. Even the fight against serious criminal offenses cannot justify the "general and indiscriminate" retention of all data. However, the court clearly reasons that targeted retention is allowed for the purpose of fighting serious crimes, but under the condition that it is limited to "strictly necessary" (when it comes to the categories of data that should be retained, the intended means of communication, persons, and duration). Consequently, the Court orders that national regulations must be based on objective criteria for granting access to data of subscribers or registered users. In principle, access can only be granted to the data of persons who are suspected of intending to commit or have committed a serious crime or have participated in the commission of a crime. Exceptionally, in the case of terrorist activities, access to the data of other persons can be granted when it is objectively possible to conclude that the data in the specific case can make a real contribution.

iii. Access to retained data, except in justified emergency cases, must be previously approved by a court or an independent administrative body. A reasoned request must be submitted to a court or an independent administrative body.

[9] Available at the following webpage: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=-CELEX%3A62015CA0203, [25.8.2022.].

iv. The persons whose data has been accessed must be informed about it as soon as such notification becomes possible, i.e., as soon as it stops jeopardizing the investigation, and so that individuals can exercise their legal rights. Otherwise, users of electronic communications could justifiably believe that their private life is subject to permanent surveillance.

v. Retained data must be effectively protected, remain within the EU, and ultimately be irretrievably destroyed. Operators must be ordered to ensure adequate technical and organizational measures and must guarantee a particularly high level of protection and security.

5. JUDGMENT OF THE CJEU IN THE MINISTERIO FISCAL CASE

The *Ministerio Fiscal* case[10] was initiated before the CJEU by the Spanish Attorney General's Office following a domestic court decision denying the police access to retained personal data. Namely, the police submitted a request that the operators be ordered to provide the phone numbers activated on the stolen device as well as the personal data of the users of those phone numbers. The request was rejected with the explanation that the delivery of retained data is possible only in the case of serious crimes, which in this case, violent theft is not.

The CJEU decided that law enforcement authorities may access personal data retained by operators in cases related to criminal offences that are not particularly serious. Provided that that access does not constitute a serious violation of privacy.

The court ruled that the access of state authorities to the identity data of SIM card holders activated on a stolen mobile phone constitutes an infringement of their fundamental rights from Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Such violation, however, is not so serious that this approach should be approved only when it comes to the fight against serious crime.

The court reasons that the violation that is not serious can be justified with the aim of preventing, investigating, detecting and prosecuting criminal offenses in general (not only serious ones). According to the Court, the violation, in this case, is not serious, since the police are looking for basic information about the identity of persons, on the basis of which it is not possible to draw precise conclusions about their private life.

The reasoning from this judgment leads to the conclusion that the CJEU in the *Tele2 Sverige/Watson* judgment was primarily motivated by the volume and nature of the data that should have been available to the authorities without selection and special controls.

[10] Available at the following webpage: https://curia.europa.eu/juris/document/document.jsf?docid=206332&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=252986, [25.8.2022.].

6. JUDGMENTS IN PRIVACY INTERNATIONAL CASE, AND JOINED CASES LA QUADRATURE DU NET AND OTHERS, FRENCH DATA NETWORK AND OTHERS, AND ORDRE DES BARREAUX FRANCOPHONES ET GERMANOPHONE AND OTHERS

On 6 October 2020, the CJEU passed two landmark decisions confirming that EU law precludes national legislation requiring electronic communications services providers to carry out the general and indiscriminate transmission or retention of traffic and location data for the purpose of combating crime in general or of safeguarding national security. The respective judgements were rendered in case C-623/17, *Privacy International*, and in joined cases C-511/18, *La Quadrature du Net and Others*, C-512/18, *French Data Network and Others*, and C-520/18, *Ordre des Barreaux Francophones et Germanophone and Others*. [11]

CJEU took a stand, in situations where a Member State is facing a serious threat to national security which proves to be genuine and present or foreseeable, such State may derogate from the obligation to ensure the confidentiality of data relating to electronic communications by requiring, by way of legislative measures, the general and indiscriminate retention of this data for a period which is limited in time to what is strictly necessary but which may be extended if the threat persists.[12] Relating to combating serious crime and preventing serious threats to public security, a Member State may provide for the targeted retention of this data and its expedited retention. Such interference with fundamental rights must be accompanied by effective safeguards and be reviewed by a court or by an independent administrative authority. The Member State may carry out general and indiscriminate retention of IP addresses assigned to the source of an Internet connection for a period that is strictly necessary and carry out a general and indiscriminate retention of data relating to the civil identity of users of electronic communication services. In the latter, the duration of the retention is not limited specifically.

7. E PRIVACY REGULATION

As part of the Digital Single Market initiative, the European Commission published in January 2017 the first proposal for a new ePrivacy Regulation that should replace the ePrivacy Directive. According to the initial plans, the ePrivacy Regulation was supposed to enter into force together with the General Data Protection Regulation[13]

[11] Available at the following webpages: https://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=509867, [25.8.2022.].

https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=511900, [25.8.2022.].

[12] Judgement in Joined Cases 511/18, 512/18 and 520/18 La Quadrature du Net and Others [2020], paras 168 and 177.

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such

(hereinafter: GDPR), but that turned out to be too ambitious. The legislative procedure is still ongoing, with no clear end date.

Unlike the ePrivacy Directive, the regulation of the same name should be harmonized with the current rules of the GDPR. Its main goal is to regulate the protection of data privacy in electronic communications, and in relation to the GDPR, it is conceived as a *lex specialis* as it covers a specific, narrow area. Although it is a regulation (and no longer a directive), the possibility of applying additional mechanisms by the Member States is foreseen for the purpose of its more effective application and interpretation.

One of the key reasons for the adoption of the new regulation is the development of new technologies, i.e. the development of the electronic communications market. Numerous services are neither foreseen nor covered by the currently valid directive (adopted in 2002, and last amended in 2009) because they simply did not exist at the time, or their application was not so wide. This primarily goes for emerging OTT services that provide instant messaging features.

The latest proposal of the ePrivacy Regulation[14] does not include specific provisions in terms of data retention. It preserves the fundamental nature of Article 15 of the ePrivacy Directive and aligns it with Article 23 of the GDPR which enables the Member States to restrict the rights and obligations provided by the GDPR to benefit national security, defense, etc. I.e., Member States are free to impose national targeted data retention measures as long as they are in line with the EU law, including the case law of the CJEU on the interpretation of the ePrivacy Directive and the Charter of Fundamental Rights.

8. RECENT DEVELOPMENTS IN DATA RETENTION – THE DWYER CASE

Judgment in Case C-140/20[15] *Commissioner of An Garda Síochána and Others* is the most recent considerable development in the data retention domain in the EU. Namely, in March 2015 Graham Dwyer was sentenced to life imprisonment for the murder of a woman. One of the key pieces of evidence, that the Irish competent court based its decision on, was metadata collected from Mr Dwyer's mobile phone. Mr Dwyer was caught and sentenced after police followed his activities through texts and phone data. There were no witnesses or physical evidence.

In his appeal before the Irish Court of Appeal Mr Dwyer challenged the first instance ruling for having incorrectly admitted as evidence traffic and location data relating to mobile telephone calls. To be able to contest the admissibility of the respective evidence, Mr Dwyer brought civil proceedings before the High Court in Ireland contesting

data, and repealing Directive 95/46/EC [25.8.2022.].

[14] ePrivacy Regulation proposal and othe related documents are available at the following webpage: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications [12.9. 2022.].

[15] Available at the following web page: https://curia.europa.eu/juris/document/document.jsf?text=&docid=257242&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=50280, [28.8.2022.].

the validity of provisions of an Irish law of 2011 which governed the retention of data and access to that data. Supposedly, the act violated the rights granted to him by EU law. As the High Court upheld Mr Dwyer's submission, Ireland appealed against it to the Supreme Court. The Supreme Court asked for clarification from the CJEU in relation to the retention of traffic and location electronic communications data for the purposes of combating serious crime and the necessary safeguards for accessing them. Another question posed by the Supreme Court was related to the scope and temporal effect of a possible declaration of invalidity that it may be obliged to make since the 2011 Act was adopted to transpose the Data Retention Directive which was declared invalid by the CJEU.

CJEU ruled that the EU law precluded the general and indiscriminate retention of traffic and location data relating to electronic communications for the purposes of combating serious crime. It furthermore ruled that the national court may not impose a temporal limitation on the effects of a declaration of invalidity of a national law that provides for such retention. However, the admissibility of evidence obtained by means of such retention is, in accordance with the principle of procedural autonomy of the Member States, subject to compliance, *inter alia*, with the principles of equivalence and effectiveness. Meaning that the CJEU decision may not be applied only to future cases and that it applies retrospectively, benefiting the cases like the one related to Graham Dwyer in Ireland. The CJEU furthermore stated that general and indiscriminate retention of data is only lawful in cases of national security.

However, CJEU repeated its earlier case law that EU law does not preclude legislation that provides, for the purposes of combating serious crime and preventing serious threats to public safety, for the targeted retention of traffic and location data which is limited to categories of persons or geographic locations, the general and indiscriminate retention of IP addresses assigned to the source of an internet connection, the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems, and the expedited retention (quick freeze) of traffic and location data in the possession of service providers. These four measures are not precluded by EU law provided that they ensure, with clear and precise rules, that the retention of data is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

In the aftermath, the ruling of the CJEU is obligatory for the Irish Supreme Court in the Dwyer case and could have an impact on criminal convictions elsewhere in the EU, as well. Mr Dwyer may use the Supreme Court's ruling in his appeal, which is currently before the Court of Appeal, to argue that evidence obtained from telecommunications data should not have been allowed to enter into evidence. However, regardless of the CJEU decision, the Irish court is still free to decide on the admissibility of evidence in line with the national criminal procedure rules. Mr Dwyer's appeal has been fixed for early December 2022.

CONCLUSION

Eight years after the repeal of the Data Retention Directive and several groundbreaking CJEU judgments later, the European legislator has not yet addressed the domain of data retention in electronic communications comprehensively. The lengthy adoption process of the new ePrivacy Regulation demonstrates the sensitivity of the topic and how difficult it is to strike the sensitive balance between the right to privacy and individual and national safety. Additionally, the OTT players are still not included in data retention regulations which proves how the market moves much quicker than the legislation. This should change, at least temporarily, with the new ePrivacy Regulation.

CJEU played the most important role in ensuring the right to privacy and by its case law contributed to establishing the rules for data retention. The rules developed over the years as new cases were presented to Court. The Court never denied the importance and the benefits of traffic and location data retention but decided that this powerful tool needs to be restricted to protect the right to privacy.

The ramifications of the CJEU judgements are far-reaching and relate to many criminal proceedings as is the situation in the Dwyer case. However, a lot of the weight is put on national legislation and national courts which will be interesting to follow in the upcoming period.

REFERENCES

1. Dragicevic, D., Gumzej, N. (2013). *Obvezno zadržavanje podataka i privatnost*, Zbornik Pravnog fakulteta u Zagrebu, 64, (1) 39-80.
2. Court of Justice of the European Union Judgement in Joined Cases C-293/12 *Digital Rights Ireland Ltd*, and C-594/12 *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others*, https://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN, [25.8.2022.].
3. Court of Justice of the European Union Judgement in Joined Cases C-203/15 *Tele2 Sverige* and C-698/15 *Watson et al.*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CA0203, [25.8.2022.].
4. Court of Justice of the European Union Judgement in Case C-207/16 *Ministerio Fiscal*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CA0203, [25.8.2022.].
5. Court of Justice of the European Union Judgement in Case C-623/17 *Privacy International*, https://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=509867, [25.8.2022.].
6. Court of Justice of the European Union Judgement in Joined Cases C-511/18 *La Quadrature du Net and others*, C-512/18 *French Data Network and others*, and C-520/18 *Ordre des barreaux francophones et germanophone and others*, https://

curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=511900, [25.8.2022.].
7. Court of Justice of the European Union Judgment in Case C-140/20 *Commissioner of An Garda Síochána and others*, https://curia.europa.eu/juris/document/document.jsf?text=&docid=257242&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=50280, [28.8.2022.].
8. Czerniak, D. (2021) "Collection of location data in criminal proceedings - European (the EU and Strasbourg) standards", *Revista Brasileira de Direito Processual Penal*, Vol. 7, No. 1.
9. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications).
10. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive).
11. www.etsi.org, [10.11.2022.].
12. European Commission, Digital Single Market, https://ec.europa.eu/priorities/digital-single-market_en, [10.11.2022.].
13. European Commission, Shaping Europe's digital future, https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation, [1.9.2022.].
14. European Commission, Study on the retention of electronic communications non-content data for law enforcement purposes, 2020, https://op.europa.eu/en/publication-detail/-/publication/081c7f15-39d3-11eb-b27b-01aa75ed71a1, [1.9.2022.].
15. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

ČUVANJE PODATAKA O SAOBRAĆAJU I LOKACIJI ELEKTRONSKIH KOMUNIKACIJA U EVROPSKOJ UNIJI ZA POTREBE KRIVIČNOG POSTUPKA

Zadržavanje podataka o saobraćaju i lokacijskim elektronskim komunikacijama i dalje je jedna od najspornijih tema na nivou Evropske unije, bez obzira na njene prednosti u istrazi i procesuiranju zločina. Režim koji je uveden Direktivom o zadržavanju podataka 2006. godine privukao je interesovanje kako stručnjaka, tako i javnosti. Dok su jedni isticali važnost zaštite nacionalne bezbednosti, drugi su se fokusirali na to da je to ozbiljan atak na privatnost građana. Široka debata završena je proglašenjem Direktive o zadržavanju podataka nevažećom od strane Suda Evropske unije. Ovom presudom sud nije isključio mogućnost zaržavanja podataka u svrhu borbe protiv teškog kriminala, ali je utvrdio da je to dozvoljeno samo uz primenu odgovarajućih mera zaštite. Međutim, kasnije odluke suda bacile su više svetla na ovo pitanje. Nakon što je Direktiva o zadržavanju podataka opozvana, domen zadržavanja podataka je ostao regulisan Direktivom o e-privatnosti iz 2002. godine. Paralelno, Evropska komisija je predložila novu Uredbu o e-privatnosti koja bi trebalo da bude usklađena sa trenutnim stanjem u oblasti zaštite privatnosti i elektronskih komunikacija. Međutim, ispostavilo se da je process njenog usvajanja dugotrajan i još uvek nije završen. Najnovija odluka Suda u slučaju Dvier potvrdila je da zakon EU onemogućava opšte i neselektivno zadržavanje podataka o saobraćaju i lokaciji koji se odnose na elektronske komunikacije u svrhu borbe protiv teškog kriminala, uz davanje dodatnih pojašnjenja o mogućnosti zadržavanja podataka.

KLJUČNE REČI: *zadržavanje saobraćajnih i lokacijskih elektornskih komunikacionih podataka, EU, krivični postupak.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.10

DIGITAL EVIDENCE AND PROTECTION OF PERSONAL DATA: SOCIOLOGICAL AND LAW ASPECT*

Ana Vuković**

In the era of digitalization, which began in a rudimentary form since the first photograph appeared, the privacy of the individual was transformed from a right to a social privilege. By switching to digitalization of data, instead of memory and written forms, individuals have accepted the change of the right to privacy as one of the basic freedoms in the corpus of human rights. The author points out that in the process of digitalization the change of public / private axis in the use and protection of personal data at the individual level leads to an imaginary sense of universal control through the real consequence of loss of privacy. Sociological and legal aspect of the paper will include an analysis of the process and relationship among digital evidence and protection of personal data. In the conclusion of the paper the author will give an overview of consequences of the use of digital evidence on the right to privacy.

KEYWORDS: *digital evidence, right to privacy, public-private relationship, freedom, control.*

* This paper was written as part of the 2022 Research Program of the Institute of Social Sciences with the support of the Ministry of Education, Science and Technological Development of the Republic of Serbia.

** Ph.D, Research Associate, Institute of Social Sciences, Belgrade, Serbia.

E-mail: *annvukovic@yahoo.com*

1. PROTECTION OF THE RIGHT TO PRIVACY BETWEEN INDIVIDUAL AND SOCIAL: SEPARATION OR MUTUALITY

Violation of the right to privacy is a violation of a person's dignity and in close connection with the evaluation of a human being and understanding of a person as a member of society. The right to privacy is an individual right that should be independent from both the community (in the wider sense society) and the state. However, with the introduction of new technologies, the use of computers, personal mobile phones and the Internet, this right has undergone transformation and disintegration. The transformation is reflected in the fact that it has become part of digital evidence, and by changing the socially desirable pattern of attitudes towards privacy in the context of personal (personal data) protection. Namely, an individual who does not have a collective awareness of the value of each of his personal data, as well as the personal data of another person, may have the opportunity to transform his right and the right to privacy of another person.

Disintegration implies that the right to privacy has suddenly become ubiquitous and everyone's, so that the memory of one act is subject to countless reproductions through everyone's memory in digital form. So, let's say, instead of a few pictures from a social gathering, we have a lot of pictures of everyone present in digital form, which can quickly be spread and become part of the digital archive of other people. Instead of enjoying a moment to remember, the individual separates himself from the mutual vision of the former collective social consciousness and transforms his privacy into a public act, where he exists only if he is present online (Vuković, 2021).

In this way, personal data is multiplied, which can then be found most often on Facebook, Twitter, Instagram and other personal profiles, and, in fact, the common profile of everyone who is on the picture from the previous example. The reason for the accumulation of digital evidence in the form of personal data is depersonalized social relations (internet sociability as a new form of closeness), but the cause can also be narcissism, that is, an individual's obsession with the desire for power through the creation of a parallel social (virtual) reality of an omnipresent self instead of an autonomous personality (Vuković, 2022: 39-41).

In modern conditions, the ideology of family life experienced the abdication of authority and the reshaping of ego. Due to the disintegration of parental authority, there has been a shift from a society in which the dominant values of the superego (values of self-mastery) are in the direction of the glorification of a society in which the values of the id (values of self-indulgence) are recognized. In a milder form, this trend prepares a young person for a way of life in a permissive society oriented to pleasure and consumption (Lasch, 1986: 202).

Speaking about the concept of networked individualism, other authors believe that "the family certainly changes, but it seems that its guardian or rooting role does not change as radically as its structure changes. And other traditional sources of security such as nation, religion or community are also losing their rooting potential much more

slowly than individualization theorists predicted" (Petrović, 2013: 63). "And where traditional institutions lose their importance or disappear carried by the wave of changes in ideas, values or objective conditions of life, new, adapted to the turbulent society, forms of social communication and association arise (*Ibid*. 63)."

Our social capital is represented by the social networks we enter during our lives, in which our private and other social (public) roles are intertwined. In research on whether social capital can be virtual in the sense of whether the Internet plays a key role in the production of social capital, it was observed that "virtual social capital represents one version of network capital", but "it cannot exist without the technology of the Internet, (…) without people, who can (have access) and know (have the necessary skills to use it), as well as without the cyberspace that is created through the Internet (Petrović, 2013: 235).

The basic idea that keeps people in submission (discipline) when it comes to the use of digital forms is the idea that we can no longer live without the Internet and modern technology. According to Foucault, the main means of discipline are space and time, which if used productively form surveillance, where power is invisible, but constantly present (Foucault 1997 according to Antonić, 2021: 236-237). Ways of disciplining when it comes to space are achieved "1. by fencing space (…); 2. by target division of space (…); 3. by functional redistribution of space, i.e. by creating useful space for a specific purpose; 4. by sorting people into appropriate compartments (for example, the class is divided into groups according to success)". Discipline where time is used as a tool involves five moves: "1. dividing time into as clear as possible (and shorter segments); 2. purposeful classification of segments (like a school schedule); 3. linking certain actions to certain segments (dividing actions and placing them in segments); 4. by making different series of actions, arranging them from the simplest to the most complex; 5. By dividing and ranking, that is, by hierarchizing the series of actions, so that each series ends with some threshold)" (*Ibid*. 236).

Does this structuring of time and space for the purpose of disciplining remind you of invisible disciplining in virtual space? Similar principles and rules of new desirable patterns of social behaviour can be observed on the Internet. Every action when sending an email or typing a message on an Android phone, Internet chat rooms as a fence of space for certain social groups and topics, with partitions and subtopics that are discussed virtually, etc.

2. DIGITAL EVIDENCE: INFORMATION ON PERSONALITY

Computers and evidence that can be obtained from the Internet consist of a huge amount of data and information in electronic (digital) form. Our pictures, instant messages, emails, digital transactions, mobile phone clouds, private internet histories, all of these can be used as digital evidence, even though it is private. The common man is often not familiar with the potential ways of archiving digital traces of their activities that may contain personal data and other types of data.

In our legal literature, personal data can be divided based on the degree of confidentiality into "ordinary" personal data and "sensitive" personal data, which are also called "special category" of personal data. The degree of confidentiality is related to the importance that information has for a person. "Ordinary" personal data carry ordinary information about a person, while "sensitive" personal data carry particularly important information about the personal identity of a person. Violation of sensitive personal data, as a rule, produces a more significant consequence for a person than the violation of ordinary personal data. According to this division, sensitive personal data enjoys a higher degree of legal protection than other types of personal data. The group of sensitive personal data includes data on religious and philosophical beliefs, racial and ethnic origin, genetic data, biometric data, data on a person's sexual life and sexual orientation, and data on health status. Other personal data belong to the group of 'ordinary' personal data" (Andonović, Prlja, 2020: 21-2).

In the contemporary world, digitalization represents dehumanization and a form of specific social control, a general surveillance that an individual cannot monitor and control, and cannot be completely absent from (Vuković, 2021: 45). Today, conformism is in the form of "passive acceptance of surveillance technologies" as the price for technical progress, and manifests the weakness of the individual and loss of identity through internalized supervision in consumer society (Subotić, 2011: 265).

Therefore, digital evidence is a link between private and public, it is private to the extent that others cannot access the data, however, with the process of universal digitization of various personal data, this data is at too high risk of becoming public. Therefore, it is debatable whether it is sustainable to divide into less and more sensitive personal data, when they are in digital form. Discussions about the problematic nature of the biometric citizen identification system began in Serbia in 2006, when "the most powerful media houses in Serbia generally affirmed surveillance systems and censored the activities of privacy fighters." (...) For greater control over some population" (Subotić, 2011: 6). The newspaper articles talked about whether and why the chipping of identity cards represents a form of threat to the right to privacy. At the same time, most members of the general population were not informed about what personal data would be on the chip and who would be allowed to read the chip.

Given that the majority of the population of Serbia consists of elderly people who are either not or minimally digitally literate, this meant that they would adapt to the state's decision on the necessity of introducing electronic chipped ID cards. This population is also the one that uses the computer and the Internet less often, but because of this, it is the most vulnerable if it has to do all its obligations, for example paying household bills, exclusively online in the near future.

In the Serbian Criminal Code, Article 146, the unauthorized collection of personal data is regulated: 1) whoever acquires personal data that is collected, processed and used on the basis of the law without authorization, communicates it to another or uses it for a purpose for which it was not intended, will be punished by a fine or imprisonment for up to one year. 2) The penalty from paragraph 1 of this article shall also be imposed

on anyone who collects personal data of citizens against the law or uses such collected data. 3) If the offense referred to in paragraph 1 of this article is committed by an official in the performance of his duties, he shall be punished by imprisonment for up to three years.

Also, the Serbian Criminal Code, among other things, regulates the violation of the right to privacy through violation of privacy of letter and other mail (article 142): "whoever without authorization opens another's letter, telegram or other closed correspondence or consignment or (…) without authorization withholds, destroys or delivers to another person somebody else's letter, telegram or other mail or who violates the privacy of electronic mail will be punished with fine or imprisonment up to two years". And, another article for example, whoever without authorization makes a photographic, film, video or other recording of another thereby significantly violating his personal life or who delivers such recording to a third party or otherwise enables him to familiarize himself with contents thereof, shall be punished with a fine or imprisonment up to one year" (article 144).

The Council of Europe Convention on Cybercrime was signed in Budapest in 2001, to combat the abuse of high technology. Among other things, this convention regulates "group of alleged acts constitutes crimes against computers and computer systems in the strict sense. The Convention has named this group as: Criminal offenses against the confidentiality, integrity and availability of computer data and systems". National Assembly o Republic of Serbia ratified both documents in 2009 and "by ratifying the Convention and Additional Protocol there should essentially have been innovated all laws that directly or indirectly regulated the area of information and communication technologies, and particularly the laws governing criminal-legal protection of these areas" (Zirojević, 2015: 1-2). The European Union's General Data Protection Regulation (GDPR) was adopted in 2016 (replacing the old legal framework from 1995), and implementation began in 2018 (SHARE, 2018).

3. THE POWER OF ONLINE STIGMATIZATION

One of the most well-known definitions of power is the one given by Weber: "power is the prospect of carrying out one's will within a social relationship despite resistance, regardless of what these prospects are based on (Weber, 1976: 37)". In a social relationship, the possession of power, according to Weber, gives us the possibility to impose our own will on the behaviour of others (ibid., 46). This term best describes the individual's desire to impose his will, through the virtual presence of his views and opinions, that is, personal data or data about others.

The shaping of private, and in fact public, opinion on social networks has led to an individual sense of power in the individual. Therefore, the desire for power and wider social recognition, among many people (more or less alienated), has enabled the availability of digital evidence of attitudes and memories. The power in potency and forms

of its possible abuse have complexly marked the floating belonging to the Internet community, and opened wide the door for the private to intertwine with the public, mostly to the detriment of the right to privacy.

Another classic of sociological theory, Parsons defined four forms of influence (persuasion, incentive, obligation activation and coercion), of which only obligation activation represents power, because "power rests on reminding person B that he has undertaken some obligation, that calling (...) to her duties, it is an appeal to her conscience, to the common system of values from which this and that obligation arises" (Antonić, 2021: 133). Internet archives of personal data have the power of potential stigma because they have an unlimited shelf life. Especially when setting up archives about some data that was created in the past.

In the Criminal Code, there is the possibility of deletion from the records after the judgment has expired, the "Internet Code" has its own rules, and data on it, even when they are deleted, for example, can appear on another Internet site. Because personal information is practically any information that can be linked to a specific person. An example of an individual violation of the right to privacy can be a man who was punished a long time ago, and released, but that information remained in the digital archive of an article on the Internet.

An example of the collective threat to the right to privacy in our country is the leaking of information of almost all adult citizens in 2013, when the personal data: first name, last name, middle name, social security number and status of citizens in the records of holders of the right to free shares is more than five million citizens of Serbia who applied for free shares in 2008 and about 4,000 financial documents that were in the database of the Privatization Agency were compromised. In the meantime, the agency was shut down, and the case became statute-barred before the competent authorities (*Ibid.* 2018: 28).

The right to erasure - 'right to be forgotten' is particularly interesting. The exercise of this right can be requested by an individual if "the data is no longer necessary for the purposes for which it was collected, the consent, which was the basis for the processing, has been withdrawn, an objection to the processing has been filed; the data has been processed illegally; the deletion is in accordance with the legal obligation of the operator, the data was collected from the child in connection with the offer of information society services". If the organization has publicly published the subject data, it should inform other organizations that process it, "so that all links to the data or copies are deleted", however, there are also exceptions to this right "when there is an overriding public interest and the organization does not have to act upon request (including freedom of speech, archiving, scientific and statistical purposes, exercise or defence against legal claims)" (SHARE, 2018).

However, experience suggests that an online story can follow some individual years after an event in which they participated took place. The potential abuse of trust in social relations and violation of human dignity even in cases where it is proven that it was not done or that it was falsified remains recorded as an online stigma in the virtual

space. What we can also notice is that the legal regulation, as well as the broader education of individuals in terms of personal data protection and its use as digital evidence, lags behind the amount of personal data that has been left in cyberspace for years. In that sense, "the information society has already shown itself to be a society that brings with it a wide range of unintended side effects, the most important of which can be expressed in terms such as fragmentation, the splitting of time into smaller and smaller parts, and the consequent loss of internal connectivity", in which "the following moment lives parasitically from this moment" (Eriksen, 2003).

CONCLUSION

Considering the changes brought about by digitalization in the modern world, the extension of the definition of the right to privacy has been changed, without the consent of the individual, or more often with unexplained consequences about possible abuses. Although the law cannot legislate all possible legal consequences of the use of personal data, legal regulation has been delayed throughout the world, as it has allowed a few individuals to collect personal data, as well as to set up data archives without the prior consent of the person. Even when there may have been consent, individuals who are digitally illiterate, as well as those who are on average, were not aware of where, when and how they could leave personal data, and especially how they could partially protect it. The social constitution of the numerical abundance of data as an imperative for social progress, instead of organizing complex collective experiences in more direct communication, called into question the connection of generations that were socialized in different social periods, and forced to live in parallel online and offline worlds.

The speed of the flow of personal data and the forms of its circulation leave the potential for the "tyranny of the moment" in one click on the Internet and social networks, and the presence of the personal on the Internet in image and text has become a matter of new social status and prestige that may or may not be rooted in reality. While in classical liberal society the principle was valid: vices are private and virtues are public, in post-capitalist society there is an inversion of public moral principles, so that now there is an insistence on public promotion of human privacy, its control and legal protection. Meandering structures of the personal (private) once existed in the memories of individuals, now they are more often archived on the Internet as a public good.

REFERENCES

1. Andonović, S., Prlja D. (2020) *Osnovi prava zaštite podataka o ličnosti* [*Basics of Personal Data Protection Rights*], Beograd: Institut za uporedno pravo.
2. Antonić, S. (2021) *Moć i poslušnost* [*Power and Obedience*]. Beograd: Srpska književna zadruga.
3. Eriksen, H. T. (2003) *Tiranija trenutka: brzo i sporo vreme u informacionom društvu* [Tyranny of the Moment: Fast and Slow Time in the Information Age], Beograd: Biblioteka XX vek.
4. Krivični zakonik (*Službeni glasnik Republike Srbije*, broj 85/2005, 88/2005 - ispr., 107/2005 - ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019) ["*The Official gazette of RS*"]. Available at: https://www.paragraf.rs/propisi/krivicni-zakonik-2019.html.
5. Lasch, Ch. (1986) *Narcistička kultura* [The Culture of Narcissism]. Zagreb: Naprijed.
6. Petrović, D. (2013) *Društvenost u doba interneta* [*Sociability in the age of the* Internet]. Novi Sad: Akademska knjiga.
7. SHARE (2018) *Vodič kroz GDPR i zaštitu podataka o ličnosti - moji podaci, moja pra*va [*Guide to GDPR and personal data protection - my data, my rights*] Share Fondacija. Available at: https://www.sharefoundation.info/wp-content/uploads/Podaci-u-doba-interneta-Final.pdf.
8. Subotić, O. (2011) *Informaciono kontrolisano društvo* [*Informationally Controlled Society*]. Beograd: Bernar.
9. Veber, M. (1976) *Privreda i društvo* [*Economy and Society*]. Beograd: Prosveta.
10. Vuković, A. (2021) "Responsibility in the Protection of Personal Data and Prevention of Abuse and Crime". In: *Institutions and Prevention of Financial Crime*, (Kostić, J., Stevanović, A., Matić Bošković, M. (eds.)). Beograd: Institut za uporedno pravo, Institut za kriminološka i sociološka istraživanja, 39-48.
11. Vuković, A. (2022) "Kriza uloge porodice i obrazovanja i nasilno ponašanje dece" ["Crisis of the Role of Family and Education and Children's Violent Behaviour"]. In: *Violence and Children*, Zirojević, M. (ed.). Beograd: Institut za uporedno pravo.
12. Zirojević, M. (2015) "Computer related Crime – the Decision of the Council of Europe", *PRAVO – teorija i praksa*, bro*j* 4–6*,* 1-15.

DIGITALNI DOKAZ I ZAŠTITA LIČNIH PODATAKA: SOCIOLOŠKOPRAVNI ASPEKT

U eri digitalizacije, koja je u rudimentarnom obliku počela još od kada se pojavila prva fotografija, privatnost pojedinca se transformisala iz prava u društvenu privilegiju. Prelaskom na digitalizaciju podataka, umesto sećanja i pisanih formi, pojedinci su prihvatili i promenu prava na privatnost kao jednu od osnovnih sloboda u korpusu ljudskih prava. U radu autor ukazuje da u procesu digitalizacije promena ose javno/privatno u korišćenju i zaštiti ličnih podataka na nivou pojedinca dovodi do imaginarnog osećaja sveopšte kontrole kroz realnu posledicu gubitka privatnosti. Sociološkopravni aspekt rada obuhvata analizu procesa i odnosa digitalnog dokazivanja i zaštite ličnih podataka. U zaključku rada autor daje osvrt na posledice upotrebe digitalnih dokaza na pravo na privatnost.

KLJUČNE REČI: *digitalni dokaz, pravo na privatnost, odnos javno i privatno, sloboda, kontrola.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.11

DIGITALIZATION OF THE TRIAL – AN AUSTRIAN PERSPECTIVE

Julia Innerhofer*

The progress of digitalization does not stop at the criminal procedure. This concerns the preliminary investigations, the main proceedings as well as the appellate proceedings and therefore all three stages of the trial. The use of digital tools in the main proceedings is of utmost interest since this phase is construed as the center of the criminal proceedings. In Austria, there are different forms and extents of digitalization, which concern either recordings of the proceedings or the use of live links within the proceedings. When one thinks about these cases, issues regarding fundamental principles of the criminal procedure arise. What can be considered progress must therefore also be viewed critically.

KEYWORDS: *digitalization, criminal procedure, trial, Austria*

* Univ.-Ass. Mag. The University of Vienna, Institute for Criminal law and Criminology.
E-mail: *julia.innerhofer@univie.ac.at*

1. RECORDINGS

1.1. Recordings for publicness and media coverage

In earlier days, when one wanted to know about the happenings of a main proceeding, he or she had to either attend the trial in the courtroom or read about it later in the newspapers. Nowadays, it is technically possible to record the whole trial or to transmit a livestream of it. A trial may even be broadcasted to another (court)room in order to guarantee publicness in large-scale proceedings,[1] since the principle of oral and public proceedings have to be respected. Section 12 and 228 (1) Code of Criminal Procedure (CCP), article 90 (1) Federal Constitution, article 6 European Convention on Human Rights (ECHR) and article 47 EU Charter of Fundamental Rights (EU Charter) demand a certain publicness for a criminal trial.

In contrast, this form of transmission is explicitly not allowed for the purpose of media coverage. Section 228 (4) CCP as well as section 22 Media Act specifically prohibit these kinds of recordings or transmissions for television or radio. There are various reasons why the press freedom is limited in this way. The most important one is the protection of personality although the possible disturbance of the external order in the courtroom and the potential interference with the establishment of the truth also play a role (Mann: 2015: 24). Most reasons concern the same underlying issue. The accused and the witnesses should focus on the trial itself and not on the media since this could lead to them not being completely open or putting on a show, which would both hinder effective criminal proceedings. In the light of the above, it is questionable how written live tickers are to be judged. They are not included in the list of forbidden practices and therefore allowed. Nevertheless, some of the reservations concerning video transmissions – and additional ones – are also relevant for live tickers (Thiele, 2016: 130, Lutschounig, 2017: 849).

1.2. Recordings for documentation and transcription

On-site proceedings may also be recorded for another reason since it might be very useful for the court to record the proceedings for further documentation and transcription. Optional audiovisual recordings for that purpose are regulated in section 271a CCP. This provision stipulates that if such a recording is made, it must cover the entire main proceedings. If the recording is only started later, it must then run to the end (Mann: 2015: 3). For the sake of completeness, however, a recording of the whole trial is recommendable. Clearly, the breaks or interruptions with any consultations between the defendants and their defence counsels may not be recorded, because these events are not part of the main proceedings and should stay confidential (Birklbauer: 2020: 293).

The recordings may even replace other forms of protocols to a certain extent. When audiovisual recordings are being used, only the most important information specified in section 271a (1) (1)-(3) CCP has to be written down additionally. After the proceedings,

[1] Mann, D. in *Fuchs/Ratz*, WK StPO § 228 Rz 8.

both sources are used to compile a transcript.[2] The recording is then not deleted but instead added as an attachment to the file.

This is also relevant as section 271a (2) CCP gives the participants of the proceedings a right to demand to replay any recordings or to transfer them on an electronic data storage device in a commonly used file format. The presiding judge may decide on the method of making available, because both alternatives are considered to be legally equivalent (Mann, 2015: 10f).

According to the legislative materials, section 271a CCP was intended to point the way to the future of recording, which was reasoned with the increased security of the documentation, the improved availability for all parties involved as well as the thereby made possible – to a large extent – dispensability of the written transcription.[3] However, even if audiovisual recordings are increasingly becoming more prominent, they are still not the standard. Section 271a (1) CCP stipulates that if the presiding judge considers this to be useful, the transcription of the proceedings may, within the means and equipment available to the courts, be supported by using technical means for audio and video recordings. Therefore, it depends on whether the presiding judge considers it expedient and whether the necessary equipment is available, which varies throughout Austria.[4] In any case, there is no subjective right to such a recording (Murschetz: 2013: 217). However, the obligatory audiovisual recording of the main proceedings is demanded repeatedly because it naturally serves better traceability and review (Sautner: 2019: 210).

Audiovisual recordings seem rather unproblematic in respect to the fundamental principles of the proceedings since the proceedings still take place within the courtroom and without the use of live links. The recording even helps with assessing the evidence since the statements may be evaluated by taking facial expressions and gestures into consideration, which is only possible if attention is paid to a good camera perspective. Moreover, it is important to respect the prohibition to record conversations between the defendant and the defence cousel during breaks in order to not affect the right of defence – which is set out in section 7 CCP, article 6 ECHR and article 47 EU Charter – by listening in on their conversations.

1.3. Presentation of previous recordings

Recordings can even be used for evidentiary purposes in the trial. Here, recordings from the preliminary investigations – specifically previous statements from the defendant or witnesses – may be shown under certain circumstances.

---

[2] In some cases, pursuant to section 271a (3) CCP, the protocol is not needed and the audiovisual recording – together with the information as stated in section 271a (1) (1-3) CCP – suffices.

[3] ErläutRV 679 BlgNR 22. GP 10.

[4] According to *Birklbauer*, Technische Unterstützung bei der Protokollführung in der Hauptverhandlung: Anwendungsbereich und Grenzen, JSt 2022, 128 (134) Austrian courts are not yet fully equipped with audiovisual recording systems. While the Regional Court of Vienna as well as the whole district of the Higher Regional Court of Vienna seem to be well equipped, the situation is completely different for the district of the Higher Regional Court of Innsbruck as there is apparently no court with such an equipment.

If the defendant deviates from his or her earlier statement or refuses to give answers, the presiding judge may – in accordance with section 245 (1) CCP – either read out in whole or in part the transcript of the earlier testimony or present technical recordings of the questioning of the accused. However, it is not admissible to show earlier statements made by the now defendant in his or her capacity as a witness, because that would contradict the *nemo-tenetur* principle (Kirchbacher, 2009: 60).

Section 252 (1) CCP regulates a similar form of indirect taking of evidence by means of the presentation of previous recordings. It enumerates specific reasons why earlier statements of witnesses and co-accused may be shown in the main proceedings. According to the provision, it is allowed if the persons questioned have since died, if their whereabouts are not known or if their personal appearance could not be effected because of their age, illness, their stay in a distant location or because of other significant reasons. Moreover, the possibility of presenting an earlier statement may be used if the persons questioned deviate in relevant points from their prior testimony or if witnesses rightfully refuse to give testimony and the prosecution authority and the defendant had the opportunity to participate in the questioning by the court. It is also permitted if a witness, not authorized to do so, or a co-accused refuses to give testimony and lastly if the prosecution authority and the defendant agree on it.

The use of previous recordings instead of just transcripts or protocols does not seem to conflict strongly with fundamental principles of the procedure. Due to the principle of immediacy, which is set out in section 13 CCP, evidence should generally be taken and heard during the main proceedings. This also helps the defendant to exercise his or her right to a fair hearing as regulated in section 6 CCP. However, if there are certain obstacles to that due to the unavailability of certain witnesses, it is still better to view audiovisual recordings than to just read out statements as it enhances a more effective assessment of evidence.

2. LIVE LINKS

2.1. Virtual statements

While the above-mentioned possibilities focus on-site proceedings with the use of recordings, the Austrian law also allows some options of live links. This offers the possibility of communication in real time with people outside of the courtroom. There are several reasons why this can become a necessity in a trial and the CCP therefore regulates different forms of it (Sautner, 2019: 210).

Pursuant to section 250 (3) CCP, some witnesses have to be questioned audiovisually and separate for their own protection or for other purposes to establish the truth. This includes victims under section 65 (1) (a) CCP, victims under section 66a CCP, other witnesses who meet the criteria listed in section 66a CCP and persons who are asked to make a statement in proceedings against a relative (Sautner, 2019: 210). The mentioned

victims and witnesses have in common that they have special protection needs due to their age, their psychological and health conditions as well the type and specific circumstances of the criminal offence. The list enumerates for example victims who are minors or victims whose sexual integrity and self-determination might have been violated. To protect them, they should be questioned without being in the same room as the defendant.[5] In practice, the presiding judge usually questions the victim or witness in an adjoining room, which is transmitted into the courtroom. This way, the other parties to the proceedings are able to hear the answers and may later ask their questions through the judge (Kirchbacher, 250). The main goal of this partially virtual form of questioning is to prevent secondary victimization (Sautner, 2019: 210). It is interesting that this method of interrogation, which is common in Austria, is not permitted in Germany because there the judge must be present in the courtroom at all times (Brodowski, 2022: 336).

Section 247a (1) CCP stipulates that witnesses who, because of their age, illness, frailty or who for other relevant reasons, are incapable of appearing before the court, may be questioned by using technical measures for audio and video transmission. Since the provision mentions other relevant reasons for being incapable of appearing, it is questionable what is included. One possible application example may be found with people who are indispensable from home for a long period because they have to take care of a seriously ill relative (Hinterhofer, 2000: 234). Another valid reason may be any acute danger to the witness (Kirchbacher, 4). In case the prosecution authority and the defence counsel agree or apply jointly, it is furthermore permitted to question someone through audiovisual transmission if the habitual residence of the witness is outside the judicial district for which the court has jurisdiction. Here, the virtual statement may be given from the seat of the court in whose judicial district the witness is present. Something rather similar is prescribed in section 247a (2) CCP for witnesses who are unable or unwilling to appear before the court because they are abroad. Such witnesses may also be questioned through a live link if the competent authority in that country renders legal assistance. The regulation within section 247a CCP is in addition and an alternative to section 252 (1) CCP, which means that the court may decide what form of audiovisual statement it deems suitable and sufficient in the trial (Kirchbacher, 9). The regulation just described, however, offers a better possibility of taking into evidence than the before mentioned provision because live interaction has several advantages over a recording.[6] Through a virtual statement via live link, it is possible to speak to the victim during the main proceedings, which gives the parties to the proceedings the opportunity to question the witness directly and to better assess their answers. In the same way, the witnesses also get the chance to amend or clarify their statement.

[5] While this form of questioning is a legal necessity for minor victims of sexual offences, all other victims and witnesses who fall under the mentioned category only have to be questioned that way if a request is made concerning this matter, see section 165 (4) CCP.

[6] See also *Sautner*, JBl 2019, 210 (212) who finds the discretion inconsistent because there is – in contrast – indeed a ranking between a statement in presence and a virtual statement. Therefore, it would only be logical if there were a similar ranking between a virtual statement and a recording.

Before 2020, it was unthinkable to question the accused virtually through means of audiovisual equipment in the main proceedings. However, the COVID-19 pandemic changed that drastically. Lockdowns and contact restrictions led to an overall increased digitalization, which also includes the judiciary and the trial (Sautner, 2022: 330). Section 239 was amended[7] by adding a new reference in the provision, through which defendants in custody may now participate via audiovisual transmission in the event of a pandemic or if it appears necessary for the prevention and control of notifiable diseases under the Epidemics Act 1950 in accordance with a regulation of the Federal Minister of Justice. Such a regulation was first issued on 16.3.2020,[8] replaced by a new regulation on 25.3.2020,[9] amended twice[10] and put out of force as of 31.5.2022 (Sautner, 2022: 330). Nevertheless, this does not mean that such a regulation cannot be implemented again. The amendment in the CCP is set for an indefinite period of time and in case the COVID-19 situation makes it necessary, the Minister of Justice is hence authorized to issue a new one. Concerning the application of the regulation, a related decree of the Minister of Justice from 22.4.2020 had to be respected. It was stipulated that the principle of proportionality must be kept in mind and that video participation should therefore be limited to cases in which it is not possible otherwise. In contrast, if there are sufficient protective measures, the defendant should rather be present in person. According to the decree, this applies even more to procedures with lay judges. If, however, an audiovisual participation cannot be avoided, it must be possible to follow the trial from both ends of the transmission. While the defendant must be able to listen to the proceeding, to ask questions and to speak with his or her defence counsel, the parties to the proceedings within the courtroom should be able to see the video transmission and to ask questions themselves.[11] These principles will have to be observed again if a new regulation brings back this form of questioning in the main proceedings.

Virtual statements pose relevant threats to the fundamental principles of the criminal procedure, in particular the principle of publicness, the principle of orality, the principle of immediacy, the principle of fair hearing, the right of defence and the independent evaluation of evidence. The compliance with the principle of publicness could be guaranteed by making sure the public in the courtroom is able to hear and – even better – to also see the virtual statement. Since the virtual statements are given via live links, they should not affect the principles of immediacy and orality. Although they are delivered from outside of the courtroom, the judge is able to hear, see and assess them immediately. However, the effective independent evaluation of evidence may be limited due to the inferior evidential value of audiovisual participation in comparison to a traditional proceeding. Technical settings and problems, reduced concentration, different behavior

[7] BGBl I 2020/14.

[8] BGBl II 2020/99.

[9] BGBl II 2020/113.

[10] BGBl II 2020/114 and BGBl II 2020/243.

[11] See *BMJ*, Erlass vom 22.4.2020 über die praktische Handhabung des erweiterten Anwendungsbereichs der Durchführung von Videokonferenzen, GZ 2020-0.254.712.

of witnesses or the defendant than within the courtroom and a reduced assessability have to be kept in mind (Oberlaber & Schmollmüller, 2022: 340). By knowing the potential risk factors, it is possible to mitigate them. Another principle that might be affected is the one concerning fair hearing. If witnesses give their statements virtually it must therefore be ensured that the defendant – or rather his or her defence counsel – is able to question the witness like he or she would be sitting in the courtroom. However, audiovisual questioning enables witness questioning in some cases where it would not have been possible otherwise and must therefore also be viewed positively. Fair hearing is specifically problematic if the person participating virtually is the defendant. It is essential for him or her to efficiently take part in the proceedings (Sautner, 2022: 330). The European Court of Human Rights (ECtHR) has ruled that virtual partaking of the defendant can be in accordance with the rights set out in article 6 ECHR.[12] In fact, it depends on the concrete realization and it is necessary that the defendant gets the possibility to express himself/herself, to be heard and to ask questions. Moreover, it is important to ensure confidential communication between the defendant and the defence counsel. This also leads to another crucial principle – the right of defence. In this regard, it is particularly relevant where the defence counsel sits – in the courtroom or next to the defendant. If he or she sits in the courtroom, he may be able to follow the proceedings better. However, communication with the defendant is more limited. Therefore, in case of doubt, it is probably advisable to place the defence counsel next to the defendant (Sautner, 2022: 330; Oberlaber & *Schmollmüller*, 2022: 340).

2.2. Virtual trials

The above-mentioned possibilities demonstrate that virtual statements are nowadays often part of the main proceedings and as such thoroughly regulated in the CCP. Contrary, it is not permitted to hold an entirely virtual criminal trial, where all parties to the proceedings participate from different locations and only speak to one another via Zoom or a similar platform. While not even the COVID-19 pandemic introduced this option for criminal proceedings, it may, however, be used in civil and administrative trials.

Before the pandemic, civil proceedings were also very much focused on on-site proceedings with punctual virtual witness statements (Leupold, 2021: 339). Lockdowns and contact restrictions led to a drastic digital expansion. Due to that, a new law – 1. COVID-19-JuBG[13] – was enacted, which regulates different accompanying measures in the judiciary. Section 3 of this act states, inter alia, that the court – in its own discretion – may conduct oral proceedings without the personal presence of the parties or their representatives using appropriate technical means of communication for audiovisual transmission. For most proceedings it is necessary that the parties agree to it, while some may be virtually conducted without a specific consent (Scholz-Berger & Schumann: 2020: 469). In practice, such virtual proceedings are conducted with the presiding judge sitting

[12] See ECtHR *Sakhnovskiy v Russia* App n. 21272/03 [2 November 2010].

[13] BGBl I 2020/16 as amended by BGBl I 2022/72.

in the courtroom or his or her office, while the parties participate via the chosen platform. To enable the public to partake in the proceedings, the judge has to call out the court proceeding and give the people a chance to follow it from the same or another room. The provision is currently limited in time until 31.12.2022 and it will be interesting to see whether virtual proceedings will continue to be part of the civil jurisdiction in the future. A current draft legislation proposes to implement the virtual trial in the Code of Civil Procedure and therefore even for the time after the pandemic.[14]

Digitalization is also further advanced in administrative proceedings. While audiovisual statements had been used before the pandemic, it nevertheless expanded the range of application (Wimmer: 2021: 347). The newly introduced COVID-19-VwBG[15] allows the competent authority or court to hold oral proceedings without the personal presence of the parties or their representatives by using appropriate technical means of communication for audiovisual transmission.[16] According to the relevant provisions, the parties do not need to consent to the virtual trial but they have to be given a chance to participate. Same as the corresponding civil clause, the law is currently limited in time until 31.12.2022 but may also be prolonged.

Although criminal proceedings differ from civil and administrative ones and the personal impression is of much more relevance, it may be possible that the provisions of civil and administrative law have a model effect on criminal trials in the (distant) future. It goes without saying that such hypothetic virtual criminal proceedings would have to be regulated thoroughly. Moreover, due to the special nature of the proceedings – which differs vastly from the other mentioned ones – and the important evaluation of evidence in the main proceedings, it would rightly be the exception rather than the rule.

Concerning the potential risks regarding the fundamental principles of the proceedings, virtual trials have to be viewed even more critically than virtual statements. Nevertheless, reference can be made to the above-mentioned problems for the most part. It would therefore be crucial to safeguard the principles of publicness,[17] of orality, of immediacy, of fair hearing, the right of defence and the independent evaluation of evidence.

CONCLUSION

Digitization offers many opportunities for audiovisual feeding-in or participation. In many cases, this facilitates procedures or makes them possible in the first place. There is often a saving in time and money. In addition, testimony is enabled that would not be possible in a pure presence setting due to illness, care obligations or for protection reasons. In the pandemic, the variety of uses was particularly evident and it could be put

[14] 138/ME 27. GP Mat 8 f.

[15] BGBl I 2020/16 as amended by BGBl I 2022/85.

[16] See sections 3 and 6 of the mentioned act.

[17] For example by transmitting the virtually held trial into an open courtroom, which would be in accordance with section 228 (4) CCP and section 22 Media Act.

to good use in the post-pandemic period as well. However, virtual statements or virtual trials should also be viewed critically with regard to the fundamental principles of the proceedings. Therefore, care must always be taken to ensure ideal realization while respecting all procedural safeguards. Furthermore, it must always be considered what the available alternative is. While a hearing in presence is usually the best solution, virtual participation is the second best and as such it must not be underestimated.

REFERENCES

1. Birklbauer, A. (2020) „Die Zulässsigkeit von Ton- und Bildaufnahmen einer Hauptverhandlung im Spannungsfeld zwischen Erforderlichkeit und Fairness", *Journal für Strafrecht,* Issue 4, 293-300.
2. Brodowski, D. (2022) „Audiovisuelle Vernehmungen und Verhandlungen in Deutschland", *Journal für Strafrecht,* Issue 4, 336-339, https://doi.org/10.33196/jst202204033601.
3. Clemens, T. (2016) „Tweets aus dem Gerichtssaal", In: *Der Einsatz von "textbasierten Internetdiensten" für die Live-Berichterstattung aus Gerichtsverhandlungen,* Vereinigung d. ö. Richter.
4. Hinterhofer, H. (2000) „Videovernehmungen und deren Verwertbarkeit im österreichischen Strafprozess – Überlegungen de lege lata et ferenda", Österreichische Richterzeitung, 234-246.
5. Kirchbacher **in** Fuchs/Ratz, WK StPO § 247 (Stand 1.6.2015, rdb.at), Manz.
6. Kirchbacher/Sadoghi in Fuchs/Ratz (Hrsg), Wiener Kommentar zur Strafprozessordnung (Stand 01.04.2020, rdb.at), § 245, Manz.
7. Köpf, J., Birklbauer, A. (2022), Technische Uterstützung bei der Protokollführung in der Hauptverhandlung: Anwendungsbereich und Grenzen, *Journal für Strafrecht,* Issue w, 128-134, https://doi.org/10.33196/jst202202012801.
8. Mannek, D. (2017) In: WK StPO § 228 *Fuchs/Ratz*, (Stand 8.9.2017, rdb.at).
9. Murschetz, V. (2013) Videodokumentation – österreichische und internationale Perspektive, AnwBl, Manz.
10. Leupold, P. (2021) Öffentlichkeit im Zivilprozess – Verfahrensgrundsätze und Rechtsentwicklung im Lichte der Krise, *Journal für Rechtspolitik*, Issue 4, 339-355. https://doi.org/10.33196/jrp202104033901.
11. Lutschounig, M. (2017) *Medienöffentlichkeit im (Zivil-)Prozess - droht ein "gläserner" Gerichtssaal?,* Manz.
12. Oberlaber, J., Schmollmüller, L. (2022), "Videoverhandlungen bzw -vernehmungen im Spannungsverhältnis zu den Prozessgrundsätzen", *Journal für Strafrecht,* Issue 4, 340-247, https://doi.org/10.33196/jst202204034001.
13. Sautner, L. (2019) *Videotechnologie im Strafverfahren: Kommunikation, Dokumentation und Reproduktion, Juristische Blätter,* Issue 4, 210-224, https://doi.org/10.33196/jbl201904021001.

14. Sautner, L. (2022) „Vernehmung und Verhandlung via Videokonferenz im österreichischen Strafprozess", Journal für Strafrecht, Issue 4, 330-335. https://doi.org/10.33196/jst202204033001.
15. Scholz-Berger, F., Schumann, J. (2020) *Die Videokonferenz als Krisenlösung für das Zivilverfahren*, Manz.
16. Wimmer, A. (2021), „Audiovisuelle Öffentlichkeit verwaltungsgerichtlicher Verhandlungen?", Zeitschrift der Verwaltungsgerichtsbarkeit, Issue 5, 347-353. https://doi.org/10.33196/zvg202105034701.

Other sources

1. ECtHR *Sakhnovskiy v Russia* App n. 21272/03 [2 November 2010].
2. ErläutRV 679 BlgNR 22. GP 10.
3. Erlass vom 22.4.2020 über die praktische Handhabung des erweiterten Anwendungsbereichs der Durchführung von Videokonferenzen, GZ 2020-0.254.712. Available at: https://www.rakwien.at/userfiles/file/Kopfpapier_Erlass.pdf.

DIGITALIZACIJA SUĐENJA – AUSTRIJSKA PERSPEKTIVA

Digitalizacija je prisutna u svim fazama krivičnog postupka: istrazi, glavnom pretresu i žalbenom postupku. Upotreba digitalnih alata je od posebnog značaja za glavni pretres, jer se ova faza smatra središtem krivičnog postupka. U Austriji su prisutni različiti oblici digitalizacije u krivičnom postupku. Ona se manifestuje npr. kroz snimanje postupka ili korišćenja linkova neposredno u toku postupka. U vezi sa tim postavlja se pitanje postupanja u skladu sa osnovnim principima krivičnog postupka. Stoga, iako se digitalizacija smatra napretkom, ona se ne može posmatrati nekritički.

KLJUČNE REČI: *digitalizacija, krivični postupak, suđenje, Austrija.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.12

SPORAZUMNO PRIZNANJE KRIVICE U DIGITALNOM OKRUŽENJU

Nataša Mrvić Petrović*

U radu se ispituju karakteristike sporazumnog pregovaranja u krivičnim stvarima (pregovaranje o priznanju krivice). Upotreba tehnologije vođene podacima promoviše revolucionarne promene u oblasti krivičnog pravosuđa, koje je već izazvala strategija novog menadžerizma. Na primerima iz običajnog i kontinentalnog zakonodavstva autor ukazuje na drugačiju praksu pregovaranja o priznanju krivice. Na osnovu analize inostranih primera i sagledavajući pregled razvoja e-uprave i e-pravosuđa u Srbiji od 2018. godine, autor zaključuje da bi posebno bilo moguće unaprediti efikasnost prekršajnog postupka.

KLJUČNE REČI: *sporazum o priznanju krivice, strategija novog menadžerstva, prekršajni postupak, e-pravsuđe, digitalno okruženje.*

* Doktor pravnih nauka, naučni savetnik Instituta za uporedno pravo, Beograd.
ORCID 0000.0003.0424-0610
E-mail: *nmrvic@iup.rs*

UVOD

Od sedamdesetih godina XX veka u anglo-američkim zemljama, a kasnije i u Evropi restrukturira se javni sektor pod uticajima strategije novog upravljanja (*New managerialism*). Reč je već svugde u zapadnom svetu prihvaćenoj dogmi da rad javnih službi treba organizovati po modelu sličnom poslovnom upravljanju. Prihvatanje navedenog koncepta nije teklo uvek bez protivrečnosti, niti se odvijalo u različitim sredinama u isto vreme i sa istim intenzitetom. Najveća razlika postoji između anglo-američkih država i zemalja kontinentalne Evrope. Ipak u svim sredinama postepeno dolazi do zaokreta u organizaciji rada policije i krivičnog pravosuđa koja se saobražava, umesto ciljevima vladavine prava i pravde – tim „staromodnim" profesionalnim vrednostima – zahtevima da rad službi bude efikasan, efektivan i ekonomičan prema pravilu ASAP („as Soon as Possible") (Salet & Terpstra, 2020: 827-828). Pod uticajem takvog pristupa iz anglo-saksonskog pravnog sistema, uz „blagoslov" iz Preporuke Saveta Evrope (87)18 o pojednostavljenju krivične pravde, i u zakonodavstvima kontinenalno pravnog tipa su preuzeti mehanizmi usmereni na pojednostavljenje i ubrzanje krivičnog postupka, poput uslovnog odbacivanja krivične prijave po oportunitetu javnog tužioca, sporazumnog priznanja krivice i poravnanja (medijacije) u krivičnim stvarima (Mrvić Petrović, 2010: 113). Tako je i u Republici Srbiji Zakonikom o krivičnom postupku 2011. godine, posle neuspelog pokušaja iz 2009. godine, dopušteno sporazumevanje javnog tužilaštva i odbrane o vrsti i visini sankcije koja će osumnjičenom biti izrečena bez obzira za koje je krivično delo prema njemu bila podneta krivična prijava ili pokrenuta istraga, a 2013. je institut sporazumevanja o prekršaju regulisan i u odredbama Zakona o prekršajima (ZP). Štaviše Zakonom o izmenama i dopunama ZP (2016) ukinuti su raniji kriterijumi po kojima je sud prilikom odobravanja sporazuma vodio računa da sporazum nije protivan razlozima pravičnosti i da ne postoji očigledna neravnoteža između dogovorene sankcije i težine izvršenog prekršaja. Pored toga je čl. 337 st 6 Zakona o bezbednosti saobraćaja na putevima (2009) predviđeno, suprotno odredbama istog zakona i ZP-a kao sistemskog zakona, sledeće: „Ako su ispunjeni uslovi za zaključenje sporazuma o priznanju prekršaja, prilikom zaključenja sporazuma moguće je u zavisnosti od zakonom propisane dužine trajanja zaštitne mere, sporazumeti se da zaštitna mera (zabrana upravljanja motornim vozilom) ne bude izrečena, odnosno bude izrečena učiniocu prekršaja u trajanju kraćem od propisanog u stavu 1. ovog člana". Kako se vidi sporazumno priznanje krivice, kod nas preimenovano u priznanje krivičnog dela ili prekršaja dopušteno je prema našim zakonima bez izuzetka za bilo koje krivično delo ili prekršaj, čak i u pogledu zakonom propisane obavezne zaštitne mere, iako je *ratio legis* njene obaveznosti vezan za karakter i težinu propisanog prekršaja. Sve što je pomenuto svedoči o tome da su se, što se tiče zakonodavca, brzo stekli uslovi da se institut sporazumevanja o kaznenom delu[1] (tzv. procesna nagodba ili pogodba) prihvati bez ikakvog ograničenja u kaznenoj praksi.

Cilj sporazumnog priznanja krivice koje se postiže kroz neformalno pregovaranje o optužbi i kazni jeste izbegavanje suđenja. Otuda praksa sporazumnog priznanja

[1] Izraz kazneno delo jednako se odnosi na krivično delo i prekršaj, dok se pod kaznenim postupkom podrazumeva i krivični i prekršajni postupak.

krivice predstavlja otklon od adversijalnog krivičnog postupka. Institut nije svojstven ni prekršajnom postupku – u našem pravnom sistemu su državni organi kao ovlašćeni podnosioci zahteva za pokretanje prekršajnog postupka po odredbama posebnih zakona dužni da nadziru primenu zakona u praksi i da, reagujući na nezakonitosti *ex offo* podnose zahteve za pokretanje prekršajnog postupku ili krivične prijave. Zato ovlašćenje da sklapaju procesne nagodbe u slučajevima u kojima po zakonu moraju da iniciraju prekršajne postupke protivreči njihovim osnovnim nadležnostima.

Učestala primena sporazumnog priznanja krivice u praksi svedoči o uveliko prisutnim promenama u organizaciji rada kaznenog pravosuđa, kojima se teži ka ubrzanju i efikasnosti procedure uz zaobilaženje garantija javnog suđenja i zaštite ljudskih prava u sudskom procesu. Ne treba previše podsećati da je ideja o zakonitom i poštenom sudskom postupku imanentna demokratskom uređenju i kao takva još uvek ideološki neprevaziđena, a praksa svekolikog sporazumevanja o krivici nije saglasna tom konceptu.

Jasno je da tehnološki napredak, dostupnost jeftinih elektronskih uređaja i olakšana razmena informacija putem interneta dodatno doprinose ubrzanju rada nadležnih državnih organa i sudova. Otuda primena digitalne tehnologije može da pospeši promene u krivičnom pravosuđu nastale pod uticajima strategije tzv. novog upravljanja. Postavlja se pitanje da li se na taj način otkrivaju ili prikrivaju nedostaci menadžerskog pristupa kaznenoj pravdi. Kako u radu ograničenog obima nije bilo moguće odgovoriti na postavljeno pitanje ukazano je na izazove po osnovna prava i slobode građana koje sobom nosi neformalno sporazumevanje o priznanju krivice i na inostranu praksu u kojoj *on-line* sporazumno priznanje krivice već postaje stvarnost, sa ciljem da posluže kritičkom preispitivanju domaćeg zakonodavstva i prakse.

1. NEDOSTACI I PREDNOSTI SPORAZUMNOG PRIZNANJA KRIVICE PREMA PRIMERIMA IZ STRANIH ZAKONODAVSTAVA

Tehnološki napredak svakako doprinosi i menjanju obima, fenomenologije i strukture kriminaliteta, budući da se promenilo okruženje u kome se vrše kaznena dela, među kojima su sve češće zastupljena ona koja su pojedinim obeležjima (vremenom, načinom, sredstvom, radnjom ili mestom izvršenja) povezana sa upotrebom računara, računarskih mreža, programa ili podataka, pa i virtuelnog novca. Upotrebom elektronskih uređaja u sklopu digitalne forenzike danas postaje relativno jednostavno brzo identifikovati učinioca, zato što je moguće u vrlo kratkom vremenu uz pomoć računara sakupiti, pregledati, uporediti i proveriti na hiljade različitih podataka koji mogu da se odnose na mogućeg učinioca, lokaciju i određeni događaj. Korišćenje digitalnih i interaktivnih video zapisa, podataka iz elektronskih evidencija i pretraživanje digitalno zabeleženih snimaka sa javnih mesta, fotografija i informacija koje se šire društvenim mrežama omogućava relativno lako otkrivanje učinioca kažnjivog dela ili identifikovanje nosioca bilo koje aktivnosti u nadziravanom prostoru. Policijske aktivnosti odvijaju se bez direktnog, ličnog kontakta i usmene komunikacije i međusobno i u odnosu na

osumnjičene, jer se komunikacija odvija preko kompjutera i razmenom kompjuterskih formata – umesto pozornika na ulicama („birokratije na uličnom nivou") policijski službenici danas predstavljaju „birokratiju na nivou ekrana", budući da sve važne informacije prikupljaju na taj način (Salet & Terpstra, 2020: 840).

Dok, s jedne strane, zahvaljujući digitalnoj forenzici postaje lako otkriti ko je učinilac, dotle je zbog sve učestalijeg propisivanja kaznenih dela (*mala prohibita*) sve teže isključivo prema pravnim obeležjima razgraničiti kažnjiva od dopuštenih ponašanja i tumačenjem ih pravilno pravno kvalifikovati. Razlog je taj što se razlika između dozvoljenog i zabranjenog ponašanja sve češće temelji na subjektivnom odnosu učinioca prema preduzetoj radnji (*mens rea*) – umesto ranije prakse da se dispozicije kaznenih dela jednostavno definišu danas preovlađuju zakonski opisi krivičnih dela čije je konstitutivno obeležje izazivanje posledice u vidu ugrožavanja te treba dokazati da je učinilac, preduzimajući radnju, mogao da ima svest o posledici koju će izazvati, što je naročito sporno kada su u pitanju prekršaji ili kazneni delikti iz oblasti ekologije, finansijskog ili korporacijskog kriminaliteta sa elementima korupcije (Regina Rauxloh 2011: 311; isto i u 2012: 104). Stoga je razumljivo da praksa nalazi načina da prevaziđe teškoće dokazivanja da se u radnjama učinioca stiču sva obeležja bića takvih krivičnih dela.

Suprotstavljene potrebe da se brzom reakcijom nadležnih organa spreči nedopušteno ponašanje i da se kroz postupke sudova svih instanci temeljno proveri osnovanost optužbe u pojedinačnom slučaju (pri tome u okviru rokova zastarelosti i bez povrede prava na pravično suđenje) razrešavaju se kompromisno sporazumnim priznanjem krivice[2], bilo da se institut primenjuje kao deo običajnog ili zakonski regulisanog prava. To je najbolji primer rutine u kojoj upravljački imperativi dobijaju prioritet u odnosu na osnovnu svrhu krivičnog postupka da se u zakonito sprovedenom postupku nezavisne sudske vlasti utvrdi da li je izvršeno krivično delo, ko ga je izvršio i da se krivcu izrekne zakonita i pravična kazna ili druga sankcija radi zaštite društva od kriminaliteta.

Kao nasleđe liberalno birokratskog modela sudskog parničnog postupka sporazumno priznanje krivice se u *common law*-u vrlo često primenjuje i u krivičnim stvarima. Uporedno-pravni pregled zakonodavstava Sjedinjenih Američkih Država (SAD), Kanade, Velike Britanije, Australije i Novog Zelanda pokazuje da prisutne razlike,[3] ne dovode u pitanje učestalu primenu instituta u praksi, naročito u odnosu na lakša kaznena dela, koja većinom odgovaraju prekršajima u našem pravnom sistemu.

[2] Za potrebe ovog rada pod procesnom nagodbom ili sporazumnim priznanjem krivice (u nas krivičnog dela ili prekršaja budući da krivičnog dela nema bez krivice, a da se za prekršaje odgovara i iz nehata) razume se „pismena saglasnost volja okrivljenog i javnog tužioca, čiji je glavni predmet određivanje sankcije koja će okrivljenom biti izrečena i bez održavanja glavnog pretresa, u zamenu za njegovo priznanje krivice" (Bajović, 2015:187).

[3] Sporazum tužilaštva i okrivljenog o priznanju izvršenja dela i krivice radi blažeg kažnjavanja drugačije se naziva u raznim zemljama (*plea bargaining* u SAD, *plea negotiations* u Australiji, *resolution discussions* u Kanadi, *sentence indication* na Novom Zelandu), negde se primenjuje kao neformalni deo tužilačke prakse (Australija, Engleska i Vels, SAD, pri čemu u Engleskoj ne može da postoji sigurnost da će sud odobriti zaključeni sporazum, dok u SAD u zanemarljivom procentu sudovi odbijaju sporazum), a u drugim zakonodavstvima (Kanada, Novi Zeland) sporazum o krivici regulisan je statutima kao faza koja prethodi suđenju i može ga isključiti (Brook *et al*. 2016: 1153-1162).

Najrazvijenija je praksa sporazumnog priznanja krivice u SAD. Institut je dinamičke prirode i stalno se razvija kroz učestalu primenu. Prema prosečnim podacima za savezne i ostale sudove, 95% slučajeva završava se na taj način (Duncan, 2022: 394), tj. na svake dve sekunde tokom radnog vremena neki kazneni slučaj okonča se procesnim „cenjkanjem" (Subramanian *et al.* 2020: 1). Stoga Turner (2021: 975) ističe da je praktični značaj sporazumevanja o krivici toliki da bi se krivično pravosuđe moglo smatrati delom sistema procesnih nagodbi, suprotno uobičajenoj tvrdnji da procesne nagodbe predstavljaju temelj kaznenog pravosuđa. Konkretnije, 2016. godine sporazumno priznanje krivice primenjeno je u 13,2 miliona kaznenih postupaka (u 99,6% slučajeva lakših kaznenih dela) zato što osumnjičeni racionalno odlučuje da prihvati sporazum kako ne bi bio izložen visokim troškovima suđenja, dok, s druge strane, sasvim u skladu sa ciljevima tzv. upravljačke pravde, sud u skladu sa sporazumom uobičajeno određuje probaciju, kojom odlaže suđenje dok ne prođe period proveravanja (Subramanian *et al.* 2020: 16). Sporazum prethodi izjašnjavaju optuženog o krivici pred sudom, pri čemu on može prihvatiti krivicu, izjasniti se da ne osporava navode optužbe (lat. *nolo contendere*) ili da nije kriv. Od 1970. godine, prema praksi Vrhovnog suda SAD u slučaju tzv. Alfordovog priznanja (slučaj *North Carolina v. Alford*) validnim se smatra sporazumno priznanje koji zaključi okrivljeni iako se izjasnio da nije kriv, ali dopušta da bi dokazi tužilaštva verovatno rezultirali osuđujućom presudom ako bi mu se sudilo (Findley *et al.* 2022: 538).

Kako je u isključivoj nadležnosti tužilaštva, postupak pogađanja je neformalan, osim što postoje interne smernice za primenu u praksi. Odvija se daleko od očiju javnosti. Temelji se na ideološkom pristupu da, po analogiji sa poravnanjem u ugovornom privatnom pravu, obe strane imaju „uzajamnih koristi" od procesne nagodbe. Uslov punovažnosti sporazuma, baš kao i u parnici, jeste da postoji saglasnost volja i da su stranke ravnopravne. Međutim, okrivljeni i tužilaštvo nisu u jednakoj procesnoj poziciji niti raspolažu jednakim moćima kao što je to slučaj u parnici. Stoga je postupak sporazumevanja u krivičnim stvarima kontroverzan jer navodi nevine optužene da priznaju krivicu, zamagljuje istinite činjenice, dovodi do preterano blagih osuda i omogućava različito postupanje u sličnim slučajevima.

Posebno zabrinjava nedostatak transparentnosti, zato što se pregovara privatno i neslužbeno, žrtve i javnost nisu prisutni, a često ni okrivljeni, ponude o priznanju krivice nisu dokumentovane, a konačni sporazumi nisu uvek u pisanom obliku, niti se unose u sudski zapisnik, dok je sudsko preispitivanje tih sporazuma obično površno – kako sud ne može da otkrije kakvi su ustupci obećani, sadržaj sporazuma je zaštićen od spoljne sudske kontrole (Turner, 2021: 975). Sud, koji inače ne učestvuje u postupku procesnog pogađanja, nego za sporazum saznaje na javnom ročištu prilikom izjašnjavanja optuženog o krivici, obično kontroliše samo smer i proces nagodbe, a ne i njen stvaran sadržaj. Pri tome uobičajeno prihvata sporazum, iako ima procesne mogućnosti da ga odbije ili da odloži izjašnjavanje do dostavljanja izveštaja odeljenja za određivanje sankcija. To znači da tužilaštva raspolažu velikom diskrecijom u pogledu sklapanja sporazuma, iako u novije vreme (u periodu od 2010. do 2017.) kroz presude Vrhovnog suda SAD dolazi do izražaja tendencija da se utiče na poštovanje procesnih prava okrivljenih na delotvoran pravni

savet tokom postupka sporazumevanja o krivici i na uvažavanje prava na zabranu samooptuživanja, koga se okrivljeni izričito moraju odreći, inače bi se mogla osporiti ustavnost osude (Subramanian *et al*. 2020: 9). Tako su sudovi proširili pravo pozivanja na VI amandman (pravo optuženog na javno suđenje) i na I amandman (pravo na javni pristup) na niz vansudskih postupaka, uključujući tu i sporazumno priznanje krivice (Turner, 2021: 985).

Učestala praksa sporazumnog priznanja krivice kritikuje se zato što nosi opasnost op povrede ustavom garantovanih prava građana, a svakako anulira i osnovna procesna načela pretpostavke nevinosti i *in dubio pro reo*. Stručnjaci konstatuju da je dovoljno da optuženi tokom pregovaranja dâ najosnovnije podatke o učinjenom kaznenom delu ili da potvrdi već formulisan odgovor i da sumarno obrazloži delo koje priznaje, pri čemu ne može da sazna da li i kojim dokazima protiv njih raspolaže optužba, niti sud, prilikom odobravanja sporazuma, ispituje da li optuženi shvata pravne posledice svog priznanja, što bi trebalo da sud čini shodno propisanim obavezama i standardima prihvaćenim u praksi (Subramanian *et al*. 2020: 8). Prema standardima izgrađenim u sudskoj praksi faktički (vansudski) karakter nagodbe razlog je što tužilaštvo nije dužno da u postupku pregovaranja saopšti odbrani dokaze kojima raspolaže a koji idu u prilog optuženom – što bi moralo učiniti da je došlo do suđenja. Kako o takvim informacijama odbrana nema načina da stekne saznanje, postoji neravnoteža procesnih stranaka koja može da ima nepovoljnih posledica po ostvarivanje prava okrivljenog (kao civilizacijsku tekovinu), s jedne strane, dok, s druge strane, kako ističe Meredith Duncan (2022: 395), podstiče nepoverenje javnosti u rad krivičnog pravosuđa. Pomenuto zapažanje potvrđuju rezultati istraživanja. Prema istraživanju iz 2018. godine ne može se isključiti značajan broj lažnih priznanja nevinih osoba, jer je od 166 ispitanih advokata njih 148 navelo da su bili uključeni u barem jedan slučaj u kome je njihov klijent odlučio da prizna krivicu iako se izjasnio da je nevin, pri čemu se to naročito odnosilo na mlade sa mentalnim poteškoćama (Subramanian *et al*. 2020: 44, 45). I nedavno istraživanje naknadnih oslobađajućih sudskih presuda za teška krivična dela za period od 2010-2020. godine pokazalo je da okolnost što jedino tužilaštvo zna za raspoložive dokaze tokom postupka pregovaranja daje priliku tužilaštvu da manipuliše pregovaranjem tako što optužene „hvata u zamku" nudeći im toliko povoljne uslove za priznanje krivice koje bi prihvatila čak i nevina lica, iako je očigledno da su dokazi optužbe toliko „tanki" da slučaj nikako ne bi mogao biti dobijen na sudu (Findley, 2022: 601). Pri tome se u uslovima izrazitih društvenih i ekonomskih nejednakosti ne može isključiti faktički nepovoljniji položaj žena, mladih, Afroamerikanaca, Latinoamerikanaca, kojima se nude stroži sporazumi nego belcima, kao i osoba sa duševnim poremećajima i mentalnim poteškoćama koje su sklonije lažnom samoprijavljivanju (Subramanian *et al*., 2020: 26; Turner, 2021: 993; Roach prema Findley *et al*. 2022: 537).

Rezimirajući razloge zbog kojih se u SAD pokazuje spornim postupak sporazumnog priznanja krivice Duncan (2022: 396) navodi: nejaku zaštitu ustavnih prava građana, proceduralne odredbe koje narušavaju procesnu ravnotežu stranaka i loša očekivanja od tehnološkog napretka. Već je i ranijih godina preporučivano da se procesna nagodba dozvoli samo u odnosu na određene vrste kaznenih dela, da se i diskreciona ovlašćenja tužilaštva u vezi pogodbe ograniče, kao i da se omogući ravnopravniji položaj

sudija i advokata tokom procesne pogodbe (Devers, 2011: 3-4). Uslov za to jeste da se obezbedi transparentnost postupka neformalnog pregovaranja oko sporazuma o priznanju krivice. Kako to ostvariti danas kada je tehnološki napredak pojačao jaz između položaja tužilaštva i odbrane u fazi pregovaranja zato što odbrana restriktivno može da pristupi dokazima kojima raspolaže tužilaštvo? Pomenuta neravnoteža doprinosi nepouzdanosti osuda kao i slabom kvalitetu usluga odbrane. Da institut procesne nagodbe ne bi više koristio tužilaštvu nego odbrani trebalo bi omogućiti osumnjičenom da, pre nego što se izjasni o krivici, ostvari digitalizovani pristup svim ne-povlašćenim informacijama koje se odnose na njegov slučaj, a kojima raspolaže država (Duncan, 2022: 408-409). Kao moguće rešenje Jenia Turner predlaže da bi valjalo pojačati sudsku kontrolu uslova pod kojima optuženi priznaje izvršenje kaznenog dela, pri čemu će dostavljene ponude biti pohranjene u federalnoj bazi podataka koja će biti dostupna kako tužilaštvu, tako i sudijama i braniocima; stranke bi mogle pretraživati podatke u skladu sa svojim potrebama, što je posebno značajno u slučaju kada optuženi odbije sporazum, kada se nastavlja sa suđenjem za krivično delo (Turner, 2021: 977, 1022). Elektronske baze podataka o sporazumnim priznanjima još su važnije zato što su ponude tužilaštva u većini država neformalne (ne zahteva se da ih tužilaštvo uputi u pisanoj formi), nego se usmeno daju ili ostaju u internoj dokumentaciji tužilaštva, ako su bile razmenjene e-poštom sa braniocem (Turner, 2021: 978-979).

U svrhe deljenja podataka između tužilaca, odbrane, kasnije i suda mogli bi se iskoristiti programi za upravljanje predmetima u tužilaštvu koji omogućavaju vođenje predmeta i skladištenje digitalnih dokaza (Turner, 2021: 1009). Oni bi posle obrade prijave mogli biti prebačeni u digitalnu datoteku i jednim pritiskom na taster mogla bi biti ponuda preneta odbrani, softver bi mogao generisati sporazume automatskim popunjavanjem obrasca sa tačnim podacima o predmetu u skladu sa već postojećom praksom da advokati odbrane dobijaju povratno obaveštenje e-poštom kad god elektronski unesu neki podnesak ili datoteku na odgovarajuću adresu. Novina bi bila samo u tome što bi sada mogli učitati ponudu za sporazumevno priznanje krivice. Digitalne platforme preko kojih se evidentiraju izvršeni unosi mogle bi generisati podatke o zaključenim sporazumima i na taj način dopustiti analizu donetih odluka i trendova u procesnim nagodbama o priznanju krivice, pod uslovom da se tako konfigurišu da korisnicima dopuste pretraživanje ponuda datih u sličnim slučajevima, čime bi se podstaklo ujednačenje prakse i revizija tužilačkih odluka, da se ne spominje značajno ubrzanje obrade predmeta u tužilaštvima (Turner, 2021: 1000-1001). Pomenuti predlog ima osnovu u jednom prethodnom radu Turner u kome je navodila dobra iskustva iz građanskog procesnog prava iz 2006. godine u pogledu dostupnosti e-podataka obema strankama i o ovlašćenjima suda ako pregovaranje ne uspe, smatrajući da se *mutatis mutandis* ista rešenja mogu iskoristiti i u krivičnom postupku (Turner, 2019: 280-282). Radikalniji je predlog Duncan (2022: 401-404) koja smatra da bi jedino digitalizacija po sistemu otvorenih fajlova, suprotno restriktivnom pristupu u pravima određenih država, omogućila da se unapredi sada nepovoljan položaj branilaca i okrivljenih u fazama pregovaranja pre formalnog početka krivičnog postupka, ilustrujući navedeno slučajem Alvarez iz Teksasa

koji je uticao na promenu modela restriktivnog pristupa informacijama. Stoga se Duncan zalaže za digitalizaciju sistema otvorenih datoteka, koje bi, osim nadležnim organima, bile dostupne i optuženom i braniocu čime bi bilo omogućeno pružanje pravnih usluga pre nego što dođe do izjašnjavanja o krivici, na osnovu uvida u podatke i dokaze kojima raspolažu policija i tužilaštvo (Duncan, 2022: 438).

U Velikoj Britaniji se neformalno postignutim sporazumnim priznanjem krivice okončava čak 90% predmeta magistratskih sudova (Thomas, 1978: 171), ali institut u praksi redovno nadležnih viših sudova nema velikog značaja kao u SAD budući da u tim postupcima sudovi zadržavaju svoje diskreciono pravo da odlučuju o kaznama. Međutim, u martu 2009. Glavni državni tužilac doneo je smernice za rad tužilaca u vezi optužbi za teške i složene prevare, kako bi se u tim slučajevima iskoristile prednosti sporazuma o priznanju krivice, zato što je to ekonomičniji postupak, manje stresan za žrtve i svedoke (HCJC, 2009: 20). Po tom osnovu je *Serious Fraud Office* (SFO) 2009. prvi počeo da primenjuje u Engleskoj i Velsu regulisane procedure koje su vodile formalnom sporazumnom priznanju krivice u slučajevima finansijskih prevara i korupcije u privredi. Sporazum se postiže u propisanoj proceduri, pri čemu se zapisnički konstatuje tok pregovaranja, a sporazum zajednički sastavljaju tužilac i okrivljeni i upućuju ga sudu. Prema opštim načelima tužilac mora delovati „otvoreno, pošteno i u interesu pravde", pri čemu se pod pravdom podrazumeva da sporazum treba da odgovara težini krivičnog dela i da omogući žrtvama, sudu i javnosti da imaju poverenja u ishod sporazuma (Alge, 2013: 4). Iako se čini da je sporazumevanje u interesu pravde, u suštini sporazumno priznanje krivice u slučajevima teških prevara služi da se u skladu sa idejom upravljanja rizikom zločina krivični slučaj okonča bez suđenja i van očiju javnosti, uz izbegavanje stigmatizacije koju nosi javno suđenje, kako bi se sačuvala društvena pozicija, karijera, poslovanje i poslovni ugled učinioca iz kruga „belih okovratnika" ili privrednog subjekta „prevelikog za zatvor" („to big to jail") (Alge, 2013: 6; King & Lord, 2018: 14-15). S druge strane, jednako kao i u SAD, tužilaštvo u postupku vansudskog pregovaranja nije dužno da učini dostupnim odbrani dokaze kojima raspolaže. Otuda se opravdano javlja pitanje da li korišćenje digitalne tehnologije kojom se prikriva izvor dokaza i identitet svedoka onemogućava prava odbrane shodno adversijalnom sistemu i primenu čl. 4 britanskog ZKP-a kojim je proklamovano procesno načelo zabrane samookrivljavanja u korist okrivljenog (Cambell *et al.* 2019: 289).

U sistemu kontinentalnog prava sporazumno priznanje krivice nije bilo zakonom prihvaćeno sve dok tradicionalni inkvizitorno-akuzatorni model krivičnih postupak nije zamenjen adversijalnim po ugledu na *common law*. Time se otvorilo pitanje odnosa između proklamovanih načela krivičnog postupka i prakse sporazumevanja koja tim načelima protivreči, iako je zakonom predviđena. Na primer, u nemačkom pravu je 2009. izmenama Zakonika o krivičnom postupku regulisano sporazumevanje javnog tužioca i odbrane uz odobrenje suda, kao jedan vid ubrzanja i pojednostavljenja krivičnog postupka.[4] Opisujući ta rešenja Rauxloh (2011: 321) ističe značaj snimanja toka pre-

[4] Opisujući raniji normativni okvir u Nemačkoj Rouxloh (2020) poistovećuje sa sporazumnim priznanjem krivice uslovno odbacivanje krivične prijave po načelu oportuniteta javnog tužioca, a slično postupaju

govora i krajnjeg dogovora (čak i u situaciji kada sporazum nije postignut) čime je omogućena transparentnost tog postupka i mogućnost sudske revizije. Pa ipak se postavlja pitanje da li je takvo postupanje spojivo sa osnovnim vrednostima nemačkog krivičnopravnog sistema, posebno zato što paralelno teče uz formalni sudski postupak (Rauxloh, 2011: 326). Slično se primećuje i u drugim zakonodavstvima, na primer, istočno nordijskim[5]. U njihovim pravima prihvaćen je tradicionalni germanski koncept krivičnog dela tj. činjenično stanje (ono što jeste – *sein*) podvodi se pod apstraktni zakonski opis krivičnog dela (ono što treba da bude - *sollen*), pri čemu postupak sporazumnog priznanja nije u skladu ni sa takvim konceptom, niti sa strukturom postupka, jer menja tradicionalni procesni položaj i procesnu ulogu stranaka koji počinju da se tretiraju kao klijenti (Erno, 2021: 260). Pored toga okrivljeni po pravilu nema informacije dovoljne da donese kvalitetnu odluku, nedostaje mu uvid u postojeću praksu, kao laik ne zna kako se odvija krivični postupak niti može ostvariti pristup datotekama tužilaštva (ne zna kojim dokazima protiv njega ono raspolaže i ne može proceniti dokaznu snagu činjenica čak i kada bi znao koje su) tako da u svemu okrivljeni zavisi od vlastitih i procena svog branioca, a posebno je štetno što je iz takvih postupaka isključena javnost koju bi javno tužilaštvo trebalo da zastupa, kao i žrtva (Rauxloh, 2011: 327).

Sva kritika sporazumnog priznanja krivice zasniva se na tome da primena instituta omogućava kažnjavanje bez suđenja na osnovu „kvazi-sudskih" ovlašćenja tužilaštva. Međutim, akademski razlozi kojima se osporava etičnost pregovaranja o krivičnom delu i krivici i neusklađenost sa procesnim načelima, potisnuti su danas sasvim u drugi plan zbog praktičnih prednosti pomenutog vida „menadžerske pravde". Tako se ističu prednosti instituta koji daje autonomiju okrivljenom da se složi sa predlozima tužilaštva (Erno, 2021: 264-265), dok Rauxloh (2011: 301) ocenjuje da procesna nagodba pomaže i stabilizuje krivičnopravni sistem, rasterećujući ga od brojnih bagatelnih slučajeva i čineći ga efikasnim.

Prednosti sporazumnog priznanja krivice za ubrzanje rada sudova naročito su prepoznate posle iskustva sa pandemijom virusa kovid 19, koja je uticala na prolongiranje sudskih sporova. Zato se i u Indoneziji upravo priprema procesni zakon kojim se, pod nadzorom i uz odobrenje suda, dopušta sporazum o priznanju krivice između javnog tužilaštva i osumnjičenim. S obzirom na učestalu praksu iznuđivanja priznanja okrivljenog tokom policijskog ispitivanja (Heravan & Sihotang, 2021, p. 137, 144), u Nacrtu zakona se predviđa da će sud proveriti i dobrovoljnost datog priznanja (Heravan & Sihotang, 2021, 148). Transparentnost i pouzdanost postupka pregovaranja mogla bi se postići primenom blokčejn tehnologije, za šta se zalažu Sinaga & Bolifaar (2020, 119). Reč je o tome da navedena tehnologija omogućava da se svi podaci, podnesci, pritužbe i slično koje šalje korisnik automatski generišu i koriste kao osnov za odluku nadležnog

Heravan i Sihotang (2021) opisujući ustanovu *transgressio* u pravima Francuske i Holandije. Međutim, valjalo bi ih razlikovati zbog ishoda i (izvesne) uloge suda pri sporazumnom priznanju krivice, budući da ostali pomenuti alternativni postupci imaju isključivu funkciju neintervencije: izbegavanja pokretanja krivičnog postupka ili obustave pre krivične osude na osnovu diskrecije tužilaštva (Mrvić Petrović, 2010: 111).

[5] U Finskoj je sporazumevanje o krivici uvedeno u krivični postupak 2015. godine, dok se u Švedskoj primenjuje kroz pilot programe od 2021. samo u odnosu na krunske svedoke (svedoke-saradnike) čijim je svedočenjem potrebno obezbediti osudu okrivljenog (Erno, 2021: 257, 259).

organa, pri čemu su trajno zapisani. Time se obezbeđuje pouzdanost sistema koji se prvenstveno koristi za naplatu potraživanja, a u ovom slučaju ta prednost omogućava transparentnost i sigurnost u postupku pregovaranja. Zanimljiva ideja, međutim, nije prihvatljiva u evropskom i našem pravu, budući da Opšta uredba EU o zaštiti podataka za sve građane EU i Evropskog ekonomskog prostora (EEA) (General Data Protection Regulation – GDPR) i Zakon Republike Srbije o zaštiti podataka o ličnosti iz 2018. kojim je, shodno Sporazumu o stabilizaciji i pridruživanju sa EU, Republika Srbija uskladila nacionalno zakonodavstvo u oblasti zaštite podataka sa pravnim aktima EU ne dopuštaju trajno čuvanje podataka o ličnosti.

2. MOBILNE APLIKACIJE RADI SAMOPRIJAVLJIVANJA

Mobilne aplikacije (računarski programi) kojima je moguće prijaviti se preko mobilnog uređaja radi postizanja sporazumnog priznanja krivice danas su realnost u *common law* sistemu. Postoji nekoliko primera razvijenih aplikacija takve vrste. U Ujedinjenom Kraljevstvu elektronski sistem Kraljevskog tužilaštva (*Crown Prosecution Service*) omogućava uspostavljanje neposredne saradnje policije i tužilaštva. Takođe, u sistem su uključeni magistratski sudovi. Sudija na taj način dobija mogućnost da neposredno sazna podatke iz elektronske krivične prijave kao i da se upozna sa drugim dokumentima policije i tužilaštva, s tim što su nadležni inspektorati u ranijem izveštaju ukazali na izvesne teškoće prilikom korišćenja elektronskog sistema budući da, prema alineji 1.36 iz izveštaja inspektora, sistem nije uvek besprekorno funkcionisao te je slanje e-pošte iz kancelarije u kancelariju bilo neophodno ili nije bilo moguće ograničiti uvid na tačno određene podatke, tako da je sudija mogao da sazna i druge koji su mogli da utiču na ishod sudskog odlučivanja (HMCPSI and HMIl, 2016: 7). Posle uspeha usluge samoprijavljivanja za izvršenje kaznenog dela putem e-pošte, britanska vlada je od 2014. godine omogućila elektronsku uslugu „Izjasni se" (Make a Plea, 2022) osobama optuženim za kazneno delo ili ovlašćenim predstavnicima optuženog pravnog lica. Prema podacima sa zvaničnog sajta engleske vlade od 2015. do 2017. broj korisnika ove aplikacije uvećan je za osam puta (Make a Plea, 2022).[6] Aplikacija se koristi preko programa zajedničke platforme za sudove i tužilaštva (HMCTS). U uputstvu se ističe da korisnik aplikaciji pristupa na osnovu prethodnog obaveštenja policije pozivom na svoj jedinstveni broj (URN), uz navođenje drugih podataka (broja vozačke dozvole, broja nacionalnog osiguranja, pojedinosti o prihodima i rashodima, na primer, za stanarinu,

[6] Podaci se odnose na pilot projekat prijava saobraćajnih prekršaja u oblasti Mančestera gde je od 11. februara 2015. godine ostvarena mogućnost da se okrivljeni telefonom prijavljuju za procesnu pogodbu (bilo je 500 korisnika koji su trebalo da budu sudski saslušani do sredine aprila te godine). Potom je organizovana usluga preko pozivnog centra za usluge policije (organizovanog u smislu podrške korisnicima odgovorima na prijave i zahteve, u ovom slučaju za sklapanje procesnog poravnanja). Prve godine bilo je primljeno 72 poziva (14% od nekadašnjih 500) od kojih 37 samo od korisnika koji su podnosili zahteve za sporazumno priznanje krivice. Platforma se u međuvremenu tehnološki unapređuje, a dostupna je radnim danima od 9 do 17 časova i može da se redirektuje na nacionalni centar (Data in Government, 2022).

hipoteku, održavanje domaćinstva i komunalne usluge itd.). Osoba koja želi da aplicira upućuje se na Službu za sudove i tribunale NjKV ako ima pitanja vezano za svoj slučaj ili radi pomoći u popunjavanju upitnika o priznanju krivice *online*. Kako se vidi, angažovanje stručnog punomoćnika nije neophodno, mada je moguće. Na blogu Data in Government (2022), jedan od kreatora tog proizvoda svedoči da je podružnica MOJ Digital Services u Mančesteru osnovana aprila 2014. kako bi se smanjio broj nepotrebnih poseta sudu radi davanja izjava o priznanju krivice. Reč je o magistratskom sudu, a „proizvod ispunjava definisane potrebe korisnika i može se primeniti širom zemlje" (Data in government, 2022). Dizajner ističe da je proizvod nastao na osnovu sagledavanja potreba obavljenim intervjuima sa mogućim korisnicima (optuženim, pravnim zastupnicima, sudijama), kao i prema toku sudskog postupka i podacima iz sudskog spisa. Cilj je da se zaobiđe „papirologija", tj. razvijen je obrazac koji objašnjava korisnicima kako da se *online* izjasne, pogledaju izjavu koju su poslali sudu (o čemu primaju potvrdu e-poštom), a zatim treba da sačekaju da ih sud obavesti o rezultatu elektronske prijave i o tome šta treba dalje da učine. Obezbeđen je razvoj programa kroz učestalo korišćenje aplikacije uz sudelovanje specijalista iz policije Mančestera i iz magistratskih sudova u Mančesteru i Salfordu. Reč je većinom o prekršajima u oblasti javnog saobraćaja, npr. za neplaćanje karte u prevozu u vozilima javnog saobraćaja ili u železničkom prevozu.

Na sličan način funkcioniše i aplikacija „Kompjutersko izjašnjenje o krivici" (Plead guilty from computer, 2022) kojom je moguće dati izjavu o krivici u predmetima Magistratskog suda države Viktorija (Australija) preko Pravosudnog centra. Na sajtu se objašnjava da se na ovaj način odlučuje u hiljadama jednostavnih predmeta (oko 25% iz nadležnosti prekršajnih sudova), najčešće za prekršaje u saobraćaju i javnom prevozu, u kojima se uobičajeno izriču novčane kazne, te da se na taj način štedi vreme i troškovi dolaska građana na sud, a i sudski troškovi. Izjašnjenje o krivici posredstvom mreže predstavlja se kao nova digitalna usluga za građane za određene vrste lakših kaznenih dela, a temelji se na zakonskoj mogućnosti pismenog izjašnjavanja o krivici (NJC Magistrat's Court of Victoria, 2022). Slična usluga pod nazivom „Izjašnjavanje o krivici na daljinu" omogućena je od 2021. godine preko jedinstvene platforme u postupcima za saobraćajne prekršaje koje vode magistratski sudovi australijske države Kvinslend (Quinsland Courts, 2022). Potrebno je da korisnik podnese elektronsku prijavu preko platforme u određenom roku (najkasnije dva dana pre termina za sudskoj izjašnjavanje) sudu ili javnom tužilaštvu, posle čega dobija uzvratnu informaciju da li je prihvaćeno njegovo izjašnjenje ili ne. Uz pozitivnu odluku suda dostavlja se okrivljenom platni nalog koji je dužan da plati. U suprotnom, sud će zakazati ročište za izjašnjenje o krivici. Izričito je na sajtu isključena mogućnost naknadnog izjašnjavanja o krivici, kao i bilo kakvih sporazumnih predloga okrivljenog koji se odnose na odluku nadležnog organa o oduzimanju vozačke dozvole, a koja obavezno sledi u slučaju vožnje u alkoholisanom stanju, bez vozačke dozvole ili sa nevažećom dozvolom (Quinsland Courts, 2022).

Treći primer je iz SAD, gde je u sklopu *Court Technology Project*-a, razvijen program koji omogućava korisniku da se *online* izjasni o krivici (Plea Online, 2022). Na pomenutom sajtu se ističu prednosti takvog izjašnjavanja u odnosu na slanje popunjenog pisanog

obrasca elektronskom poštom, pa se kaže da je reč o brzom digitalnom procesu, koji omogućava da se sačuvaju svi važni elementi datog procesa i da ga ubrzaju, kao i da je ovakvo izjašnjavanje pogodno za osobe koje su žive daleko od sedišta suda, fizički su sprečene da prisustvuju suđenju ili su odsutne (u zatvoru). Omogućena je privatna i bezbedna komunikacija sa sudom, kako bi osoba preuzela odgovornost za svoju situaciju. Korisnik posredstvom aplikacije može da se izjasni na jedan od tri načina: 1) da je kriv i prihvati ponudu javnog tužioca o kažnjavanju, 2) da ne osporava optužbu, ali da objasni slučaj i navede olakšavajuće okolnosti ili 3) da nije kriv, pri čemu je dužan da pošalje elektronsku dokumentaciju kojom potkrepljuje svoje tvrdnje (fotografije, skenirani dokumenti) koju dostavlja sudu na razmatranje. Ako ne dostavi dopunsku dokumentaciju, smatraće se da se odrekao prava na pisanu odbranu. Sud će svoju odluku korisniku dostaviti elektronskim putem. Prema podacima sa sajta (Plea Online, 2022), prednost korišćenja aplikacije je u tome što se predmeti, uobičajeno saobraćajnih prekršaja, rešavaju danima, a ne mesecima, pri čemu sud odlučuje da li neko može da se izjasni o krivici *online* ili ne. Komunikacija se obavlja preko *Matterhorn* veb platforme dizajnirane kako bi sudovima omogućila da rešavaju brojne prekršajne predmete, sporove, donose naloge i slične odluke i to *online*.[7] Da bi koristili usluge sudovi se priključuju na pomenutu platformu, baš kao i ostali korisnici.

Ono što posebno pada u oči, u svakom od navedenih primera reklamira se elektronska „usluga" koja spada u domen rada policije ili krivičnog pravosuđa a korisnicima se nudi na sličan način kao da se radi o povoljnosti koju dobijate kao potrošač ili, u najboljem slučaju, kao korisnik e-uprave. Digitalizacija usluge ima i izvesnih prednosti u *common law* sistemu u uslovima neformalnog sporazumevanja zato što su obezbeđeni dokazi o komunikaciji sa sudom ili tužilaštvom koja se odvija posredstvom platformi koje mogu pristupiti i državni organi i građani. Drugo što čini mogućom primenu aplikacije, za razliku od kontinentalnog prava, jeste što je moguće predvideti koji bi nivo niže kazne okrivljeni mogao da očekuje, zato što su rasponi propisanih novčanih kazni manji a njihova visina se u konkretnom slučaju određuje primenom aktuarskog računa prema objavljenim tablicama.

ZAKLJUČAK

Postupak sporazumnog priznanja krivice jedan je od primera kako se kazneno pravo restrukturira iz mehanizma zaštite građana od kriminaliteta u fleksibilan mehanizam (selektivne) državne intervencije na pojedini kazneni delikt. Takav instrument sasvim odgovara savremenoj težnji da se postigne efikasno upravljanje rizikom zločina. Učestaloj praksi sporazumevanja doprinela je i promena funkcije kaznenog prava – ne postoji potreba da se otkrije i dokaže prestup već da se utvrdi povezanost određenog ponašanja sa kaznenom odgovornosti učinioca, pri čemu u mnogim situacijama nije više jasno gde ona počinje, ali uprkos tome treba obezbediti da krivična pravda

[7] Prema podacima sa promotivnog sajta Online Dispute Resolution Outcomes (2022: 1) platforma se može koristiti u različitim slučajevima: vezano za karte u prevozu i naplate parkinga, oduzete dozvole, u sitnim i porodičnim sporovima pa i za izjave krivice.

bude dostižna. Istovremeno, zbog korišćenja novih tehnologija, svedoci smo nastanka post-moderne sudske kulture koja se zasniva na drugačijem načinu komuniciranja i interakcije između organa krivičnog pravosuđa i stranaka (pa i drugih učesnika u postupku). Da bi prednosti novih tehnologija bile iskorišćene na prihvatljiv način, bilo bi potrebno obezbediti ravnopravnost stranaka u dostupnosti elektronskim informacijama i transparentnost postupka sporazumnog priznanja krivice, a možda bi, u nekim slučajevima, trebalo u javnom interesu zakonom ograničiti primenu instituta procesne nagodbe. U drugim slučajevima, pod uslovima da je postupak sporazumevanja zakonom regulisan, ako je tok pregovaranja zapisnički fiksiran ili sniman, bez rizika od povrede prava optuženog na odbranu, institut zaista može doprineti ubrzanju krivične pravde, makar ona imala karakteristike „kvazi-sudske", zbog naglašene uloge i velikih diskrecija javnog tužioca u postupku postizanja sporazuma.

S obzirom na navedena strana iskustva u korišćenju aplikacija za priznavanje krivice u vezi saobraćajnih prestupa i način na koji je institut sporazumnog priznanja krivičnog dela ili prekršaja regulisan u našem pravu treba očekivati da će vrlo brzo biti omogućeno *online* podnošenje zahteva za osporavanje prekršajnog naloga ili za sporazumno priznanje prekršaja. Tome na ruku ide okolnost da je od 2016. godine već moguće dostavljanje prekršajnog naloga okrivljenom elektronskim putem, pa bi bilo celishodno omogućiti mu da na isti način komunicira sa podnosiocem naloga i sa sudom u slučaju kada osporava prekršajni nalog. Prema stranim primerima moguće je založiti se za mogućnost da se okrivljeni na taj način može koristiti pravom na pisanu odbranu ili da može predložiti sporazumno priznanje prekršaja. Da postoje opravdani razlozi i tehničke mogućnosti da se u tom pravcu razmišlja potvrđuju okolnosti da su od 2018. godine već preduzeti koraci radi kreiranja platforme e-sud (sa ciljem da se omogući podnošenje e-zahteva za upravni sud), kao i to da je pandemija kovida 19 pospešila aktuelnost projekta o jedinstvenoj platformi radi suđenja na daljinu.

Slična platforma mogla bi da povezuje prekršajne sudove u Srbiji, a preko njih i nadležne državne organe – podnosioce zahteva za pokretanje prekršajnog postupka koji pregovaraju sa optuženim o sporazumnom priznanju prekršaja. Na taj način bilo bi moguće obezbediti kontrolu tog postupka, koji se sada odvija daleko od očiju javnosti i ujednačenu primenu instituta u praksi. Trebalo bi dobro razmisliti na koji način će se omogućiti da ostanu zabeleženi podaci o postupku i sadržini pregovaranja, budući da zbog našeg zakona neće biti moguće iskoristiti prednosti blokčejn tehnologije, koje su već prepoznate u izradi tzv. pametnih ugovora i decentralizovanih aplikacija kojima su omogućene različite funkcije (na primer, identifikacija korisnika i sistem potpisa i slično), uz garancije da decentralizovani registar ne može biti promenjen.

Navedeni primeri, većinom iz *common law* zakonodavstava, svedoče kako se „kaznena pravda" raspršuje – ne samo po nosiocu funkcije, koji ne mora isključivo da bude sud, nego i po sadržaju (vrsti i visini kazne ili mere, broju optužbi, pravnoj kvalifikaciji dela itd.) pa i po tome što se iz sudnica gde mora da caruje „živa reč" učesnika preseljava u kabinete i „proviruje" iz ekrana računara. Važno je da je dostižna i brza, mada možda nepotpuna – samo da se ne pretvori u svoju suprotnost.

LITERATURA

1. Alge, D. (2013) „Negotiated Plea Agreements in Cases of Serious and Complex Fraud in England and Wales: A New Conceptualisation of Plea Bargaining?“, *European Journal of Current Legal Issues* – Web JCLI, 19(1), https://core.ac.uk/download/pdf/46598062.pdf [28. 7. 2022].
2. Bajović, V. (2015) „Odmeravanje kazne i sporazum o priznanju krivičnog dela“, *Nauka, bezbednost, policija*, 20(2): 179-193.
3. Brook, C.A., Fiannaca, B., Harvey, D., Marcus, P., McEwan, J. & Pomerance, R. (2016) „A Comparative Look at Plea Bargaining in Australia, Canada, England, New Zealand, and the United States“, *William & Mary Law Review*, 57/4): 1147-1224, https://scholarship.law.wm.edu/ wmlr/vol57/iss4/4 [28. 7. 2022].
4. Cambell, L., Ashworth, A. & Redmayne, M. (2019) *The Criminal Process*. Oxford: University Press.
5. Devers, L. (2011) *Plea and Charge Bargaining, Research Summary*, Washington: Bureau of Justice Assistance, U.S. Departmant of Justice, January 24, 2011. https:// bja.ojp.gov › PleaBargainingResearchSummary [28. 7. 2022].
6. Duncan, M.J. (2022) „Digital Ecosystem of Accountability“, *American Criminal Law Review* 59(2), 393-438.
7. Ervo, L. (2021) „Plea Bargaining Changing Nordic Criminal Procedure: Sweden and Finland as Examples“, In: L. Ervo, A. Letto-Vanamo & A. Nylund (eds.), *Rethinking Nordic Courts, Ius Gentium: Comparative Perspectives on Law and Justice* 90. Cham: Springer, 255-269. https://doi.org/10.1007/978-3-030-74851-7_14 [15. 7. 2022].
8. Findley, K.A., Angulo Amaya, C., Hatch, G. & Smith, J. (2022) „Plea Bargaining in the Shadow of a Retrial: Bargaining Away Innocence“, *Winsconsin Law Review*, 3: 533-612, https://wlr.law.wisc.edu/wp-content/uploads/sites/1263/2022/05/14-Findley-Camera-Ready.pdf [28. 7. 2022].
9. Heravan, W.N. & Sihotang N. (2021) „Adoption of the Plea Bargaining Concept to Improve Judicial Efficiency During the Covid-19 Outbreak“, *Law Research Review Quarterly* 7(2), 135-152. https://doi.org/10.15294/lrrq.v7i2.46174 [15. 7. 2022].
10. King, C. & Lord, N. (2018) *Negotiated Justice and Corporated Crime: The Legitimacy of Civil Recovery Order and Deferred Prosecution Agreements*, Cham: Springer-Palgrave.
11. Mrvić Petrović, N. (2010) *Alternativne krivične sankcije i postupci*, Beograd: Medija centar Odbrana.
12. Rauxloh, R. E. (2011) „Formalization of Plea Bargaining in Germany: Will the New Legislation Be Able to Square the Circle?“, *Fordham International Law Journal* 34(2), 296-331.
13. Rauxloh, R. (2012). *Plea Bargaining in National and International Law: a comparative study*. London-New York: Routledge.

14. Salet, R. & Terpstra, J. (2020) „Criminal justice as a production line: ASAP and the managerialization of criminal justice in the Netherlands", *European Journal of Criminology* 17(6): 826-844. https://doi.org/10.1177/1477370819828332 [17. 7. 2022].
15. Sinaga, H.D.P. & Bolifaar, A.H. (2020) „Blockchain Adoption for Plea Bargaining of Corporate Crime in Indonesia" *ICBCT' Proceedings of the 2020 The 2nd International Conference on Blockchain Techology*, March 2020, Hawwai. New York: ICBCT, 115-119. https://doi.org/10.1145/3390566.3391680 [15. 7. 2022].
16. Subramanian, R., Digard, L. Washington, M. & Sorage, S. (2020) *In the Shadows: A Review of Research on Plea Bargaining*. Washington: Vera Institute of Justice & Safety + Justice Challenge.
17. Thomas, P.A. (1978) „Plea Bargaining in England", *Journal of Criminal Law and Criminology*, 69(2): 170-178, https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=6067&context=jclc [28. 7. 2022].
18. Turner, J.I. (2019) „Managing Digital Discovery in Criminal Cases", *Journal of Criminal Law and Criminology,* 109(2): 237-312. https://scholarlycommons.law.northwestern.edu/jclc/vol109/iss2/3 [15. 7. 2022].
19. Turner, J.I. (2021) „Transparency in Plea Bargaining", *Notre Dame Law Review,* 96(3), 973-1023.

Pravni izvori

1. GDPR (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), *OJ* L 119, 4.5.2016, p. 1–88.
2. Zakonik o krivičnom postupku, *Službeni glasnik RS*, br. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14, 35/19, 27/21, 62/21.
3. Zakon o bezbednosti saobraćaja na putevima, *Službeni glasnik RS*, br. 41/09, 53/10, 101/11, 32/13- odluka US, 55/15 – dr. zakon, 9/16 – odluka US, 24/18, 41/18 – dr. zakon, 87/18, 23/19, 128/20 – dr. zakon.
4. Zakon o prekršajima, *Službeni glasnik RS*, br. 65/13, 13/16, 98/16, 98/19, 91/19, 91/19-dr. zakon.
5. Zakon o zaštiti podataka o ličnosti, *Službeni glasnik RS*, br. 87/2018.

Internet izvori

1. Her Majesty's Crown Prosecution Service Inspectorate (HMCPSI) & Her Majesty's Inspectorate of Constabulatory (HMIC) (2016), *Delivering Justice in A Digital Age – A Joint Inspection of Digital Case Preparation and Presentation in The Criminal Justice System*. London: HMCPSI & HMIC. https://www.justiceinspectorates.gov.uk › uploads [15. 7. 2022].

2. House of Commons Justice Committee – HCJC (2009), The Crown Prosecution Service: Gatekeeper of the Criminal Justice System, 9th Report of Session 2008-2009, 15. July 2009, https://publications.parliament.uk/pa/cm200809/cmselect/cmjust/186/186.pdf [15. 7. 2022].
3. Data in Government (2022), UK government, https://dataingovernment.blog.gov.uk/make-a-plea-self-certification/ [15. 7. 2022].
4. NCJ Magistrat's Court of Victoria (2022), Australia, https://www.neighbourhoodjustice.vic.gov.au/knowledge-centre/our-service-innovation/online-pleas-innovation [15. 7. 2022].
5. Make a Plea (2022), UK government, https://www.gov.uk/make-a-plea [15. 7. 2022].
6. Online Dispute Resolution Outcomes (2022), https://getmatterhorn.com/static/Matterhorn_Outcomes_White_Paper.pdf [2. 8. 2022].
7. Quinsland Courts (2022), Plead guilty online, https://www.courts.qld.gov.au/going-to-court/plead-guilty-online [2. 8. 2022].

PLEA BARGAINING IN THE DIGITAL ENVIRONMENT

The paper examines the features of consensual negotiation in criminal matters (plea bargaining). The use of data-driven technology promotes revolutionary changes in the field of criminal justice, which were already caused by New Managerialism strategy. On examples from common law and continental legislation the author shows a different practice of plea bargaining. Based on foreign examples and considering an overview of the development of e-Administration and e-Judiciary in Serbia from 2018., the author concludes that it would be especially possible to improve the efficiency of the misdemeanor procedure.

KEYWORDS: *plea bargaining, New Managerialism strategy, misdemeanor procedure, e-Judiciary, digital environment.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.13

ZAŠTITA SVEDOKA U KRIVIČNIM POSTUPCIMA I PRIMENA TEHNOLOGIJE*

Olga Tešović*
Ivana Milovanović**

Pitanje primene tehnologije u krivičnim postupcima aktuelizovano je u Srbiji sa početkom pandemije Covid 19. Iako postojeća zakonska regulativa predviđa ovu mogućnost, šira primena tehnologije u krivičnim postupcima nije zapažena. Posmatrajući praksu sudova tehnologija se u Srbiji primenjuje jedino u krivičnim postupcima pred posebnim odeljenjima za suzbijanje organizovanog kriminala i ratnih zločina ali u redovnim krivičnim postucima se retko sreće. Sa druge strane, teorija je jedinstvena oko značaja primene tehnologije posebno u zaštiti svedoka i oštećenih u sudskim postupcima. Takođe, brojni međunarodni pravni akti koji sadrže odredbe o zaštiti svedoka u sudskim postupcima prepoznaju značaj korišćenja tehnologije radi izbegavanja brojnih negativnih konsekvenci sudskih postupaka i izbegavanja sekundarne viktimizacije. Međutim, i pored brojnih preporuka za ovakav vid ispitivanja primećeno je da se ona ne koristi u većem procentu u Srbiji i svakako ne u svim slučajevima u kojima je to neophodno ili korisno. Rad ima za cilj analizu pravnih normi koje se odnose na zaštitu svedoka u krivičnim postupcima sa posebnim akcentom na one koje predviđaju ili omogućavaju primenu tehnologije radi adekvatne zaštite na međunarodnom planu i Srbiji, obim primene tehnologije u praksi, razlozi za nedovoljnu primenu i preporuke za širom primenom.

KLJUČNE REČI: *zaštita svedoka i oštećenih, tehnička sredstva za prenos slike i zvuka, krivični postupak.*

* Doktor pravnih nauka, predsednica Osnovnog suda u Požegi. E-mail: *otolgates@gmail.com*

** Sudija i zamenica predsednika Osnovnog suda u Nišu. E-mail: *milovanovic.iva@gmail.com*

1. POJAM SVEDOKA I MODELI NJIHOVE ZAŠTITE

Značaj svedoka u krivičnom postupku ogleda se u činjenici da je iskaz svedoka najznačajnije i najučestalije dokazno sredstvo od najstarijih ljudskih civilizacija pa do danas. U teoriji ali i različitim zakonodavstvima postoje različite definicije svedoka ali se sve one gotovo slažu oko toga da je svedok lice koje poseduje informacije o činjeniama koje su od značaja za predmet postupka. Tako je i Zakonikom o krivičnom postupku RS[1] (u daljem tekstu: ZKP) propisano čl. 91 da je svedok lice za koje je verovatno da će dati obaveštenja o krivičnom delu, učiniocu ili o drugim činjenicama koje se utvrđuju u postupku.

Iako je iskaz svedoka najčešće (i u ne malom broju slučajeva jedino) dokazno sredstvo nesporo je da je to svakako najnepouzdanije dokazno sredstvo jer postoji mogućnost da, i pored zakonske obaveze svedoka da govori istinu, on to ne učini, odnosno, da pogrešno interpretira određene činjenice. Uzroci ovoga su različiti i ne moraju uvek zavisiti od volje samog svedoka, već i neke objektivne okolnosti mogu na to da utiču. Prema mišljenju autora, tri su grupe razloga zbog kojih svedoci ne govore istinu prilikom svedočenja:

1.1. Lična zainteresovanost za ishod postupka

Navedeno se najčešće odnosi na ispitivanje oštećenog u svojstvu svedoka imajući u vidu da je on uvek zainteresovan za ishod postupka s obzirom da je i sam pogođen izvršenjem krivičnog dela. Međutim, i ostali svedoci su u većini slučajeva zainteresovani za ishod postupka a razlozi za to mogu biti različiti: povezanost sa učiniocem, oštećenim ili nekim drugim učesnikom u postupku, posmatranje postupka iz perspektive sopstvenih interesa i dr. Nevezano da li se radi o posrednoj ili neposrednoj zainteresovanosti za ishod postupka to dovodi u većini slučajeva to toga da je iskaz, svesno ili nesvesno, delimično ili u celosti usmeren ka ishodu postupka koji je po mišljenju svedoka, posebno oštećenog, najpravičniji. U ovom kontekstu bitno je ukazati i na tzv. privilegovane svedoke, koji su gotovo uvek povezani sa postupkom ili učiniocem a neretko je njihov iskaz i jedino dokazno sredstvo u krivičnom postupku. Ono što se javlja kao veliki problem kod tzv. privilegovanih svedoka je korišćenje pravom da ne svedoče, što može (a što se i dešava u praksi) dovesti do obustave postupka ili oslobađajuće presude.

1.2. Pogrešno zaključivanje o određenim činjenicama i pogrešna percepcija događaja

Percepcija određenih događaja zavisi od individualnih karakteristika ličnosti svakog pojedinca. Dakle, svaki događaj različito utiče na različite ljude ali i činjenice koje su na prvi pogled nesporne ili očigledne mogu biti različito percipirane. Takođe, određeni

[1] Zakonik o krivičnom postupku, *Sl. glasnik RS*, br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - odluka US i 62/2021 - odluka US.

događaj budi različita osećanja ili stvara različita stanja kod ljudi u zavisnosti od karaktera posmatrača. Shodno svemu ovome, proizilazi da sve okolnosti slučaja i stanja koje događaj „stvara" kod ljudi mogu da dovedu do različitih zaključaka. Neretko se dešava da ljudi pod pritiskom različitih osećaja izgube svest o istini i pravilnom rasuđivanju, što svakako utiče na verodostojnost njihovih iskaza.

1.3. Zaštrašivanje svedoka

Nesporno je da učinioci krivičnih dela uglavnom znaju ko će biti ili ko su svedoci u postupcima protiv njih pa to samim tim stvara mogućnost uticaja na svedoke. Uticaj se može vršiti na različite načine: dogovorom, nuđenjem materijalne koristi ali i zastrašivanjem. Zastrašivanje svedoka može se podeliti u dve grupe: aktivno i implicitno. Aktivno zastrašivanje je putem otvorenih pretnji, primenom nasilja, dok je implicitno zastrašivanje prikriveno i proizilazi iz samog društvenog položaja lica koje zastrašuje (njegovog ranijeg kriminalnog ponašanja, društvenog statusa ili položaja, nadređenost u odnosu na svedoka i sl.) (Burnsajd, 2015).

Sve navedeno pokazuje da je najteži zadatak sudije prilikom sprovođenja postupka i donošenja odluke, zapravo, pravilna ocena iskaza svedoka. U tom smislu sukobljava se više teza: da je oštećeni uvek lično zainteresovan za ishod postupka te njegov iskaz treba sa posebnom opreznošću ceniti, sa druge strane teza da žrtvi/oštećenom treba da se veruje naročito kod „osetljivih" postupaka gde je to često i jedini dokaz, zatim, mogućnost da je izvršen uticaj na svedoka ali i individualne osobine svakog svedoka.

Imajući u vidu sve prethodno navedeno, a posebno značaj iskaza svedoka kao dokaznog sredstva, jasna je i potreba za zaštitom svedoka od raznih spoljašnjih uticaja ili faktora koji mogu u nekom pravcu uticati kako na sam iskaz svedoka, tako i na njegov život i bezbednost. Stoga je jasno da i pre samog krivičnog postupka mora dosta pažnje posvetiti zaštiti, pomoći i podrški svedocima jer je jasno da se preduzimanjem mera samo na glavnom pretresu ne može postići svrha. Navedeno ukazuje i na to da nije dovoljna samo procesna zaštita, već i razni vidovi podrške i pomoći kako bi svedok bio u mogućnosti da da dosledan i pravilan iskaz.

Radi pravilnog sagledavanja značaja primene tehnologije u zaštiti svedoka i oštećenih u krivičnim postupcima potrebno je ukazati na sve vidove zaštite svedoka. Modeli zaštite svedoka se mogu podeliti prema više kriterijuma ali najznačajnije i najuopštenije podele su:

1.4. Opšta i specijalna zaštita svedoka

Opšta zaštita svedoka se odnosi na sve svedoke u sudskim postupcima i njome se štite svi svedoci od bilo kakvih neprijatnosti u postupku i u vezi sa postupkom. Dakle, svaki svedok mora biti zaštićen od uvreda, bilo kakvih verbalnih ili fizičkih napada, nelagodnosti i neprijatnosti od strane bilo kog učesnika u postupku. Zaštitu je dužan da obezbedi organ postupka ali i sam svedok može preduzeti procesne radnje u cilju svoje zaštite.

Specijalna zaštita svedoka pruža se svedocima kojima je pored opšte zaštite potrebna i dodatna, specijalna zaštita. Potreba za specijalnom zaštitom može proisteći zbog same prirode izvršenog krivičnog dela, posebnih okolnosti ili načina izvršenja ali i posledica po oštećenog ali i zbog individualnih karakteristika svedoka. U krivičnom procesnom zakonodavstvu Srbije kao vidovi specijalne zaštite svedoka su posebna pravila zaštite posebno osetljivih svedoka i zaštićenih svedoka.

1.5. Procesna i vanprocesna zaštita svedoka

Procesna zaštita svedoka odnosi se na zaštitu svedoka tokom samog krivičnog postupka i mere se odnose na pomoć i podršku u vezi sa svedočenjem, s tim da je zabranjeno da se merama zaštite utiče i da se uopšte govori o predmetu svedočenja, i mere prilikom samog svedočenja, koje se odnose na mogućnost postavljanja pitanja, karaktera pitanja, zabrana suočenja, susret sa okrivljenim i sl.

Vanprocesna zaštita svedoka se odnosi na određene mere koje preduzimaju specijalizovani organi ili oraganizacije a tiču se zaštite svedoka van postupka, pre, tokom i nakon svedočenja. Ove mere se pre svega odnose na zaštitu života i bezbednosti svedoka i njima bliskih lica.

2. PRAVNA REGULATIVA ZAŠTITE SVEDOKA U KRIVIČNIM POSTUPCIMA – MEĐUNARODNOPRAVNA ZAŠTITA

Značaj pitanja zaštite svedoka u sudskim postupcima ogleda se između ostalog i u tome što je na međunarodnom planu doneto više akata kojima je regulisano pitanje zaštite svedoka u sudskim postupcima ali i većina najznačajnijih međunarodnih konvencija koje imaju za predmet druga pitanja, sadrže odredbe o zaštiti svedoka. U nastavku rada ukazaćemo na neke od najznačajnijih međunarodnih dokumenata, kojima je regulisano pitanje zaštite svedoka jer se primena tehnologije u zaštiti svedoka ne može posmatrati izolovano od ostalih oblika zaštite.

Kada se govori o zaštiti svedoka svakako na prvom mestu treba ukazati na Deklaraciju osnovnih pravnih principa za žrtve krivičnih dela i zloupotrebe moći.[2] Navedena Deklaracija treba da bude polazni dokument prilikom donošenja ili izmena nacionalnih zakona jer na sveobuhvatan način ukazuje na značaj i mere zaštite svedoka, kako u postupku, tako i van njega. Deklaracijom je proklamovano da se prema žrtvi mora obazrivo postupati uz puno poštovanje njenog dostojanstva. Neke od glavnih garancija žrtvama proklamovanih Deklaracijom su: da žrtve moraju biti obaveštene o svojim pravima, da imaju slobodan pristup pravosuđu, da imaju pravo na efikasno postupanje državnih organa prilikom odlučivanja, da imaju pravo na nadokandu svih vidova štete kao i zaštita od svakog vida viktimizacije žrtve. Posebno je značajno pomenuti da žrtvi mora biti omogućeno da iznese svoj stav, bez straha i svaka neprijatnost po žrtvu mora biti svedena na najmanju moguću meru.

[2] Generalna skupština Ujedinjenih nacija je usvojila Deklaraciju odlukom od 29.11.1985. godine.

Odredbe o zaštiti svedoka našle su se i u Konvenciji Ujedninjenih nacija protiv transnacionalnog organizovanog kriminala[3] koja je usvojena 22.06.2001. godine u Palermu. Sastavni deo konvencije su i Protokoli za prevenciju, suzbijanje i kažnjavžnje trgovine ljudskim bićima naročito ženama i decom i Protokol protiv krijumčarenja migranata, kopnom, morem u vazduhom, koji posebnu pažnju posvećuju zaštiti žrtava i to posebno zaštiti žena i dece. Akcenat je stavljen na zaštitu od odmazde ili zastrašivanja svedoka koji svedoče u krivičnim postupcima povodom krivičnih dela obuhvaćenim konvencijom ali i njihovim rođacima i drugim bliskim licima. Modeli zaštite svedoka su različiti i to može biti preseljenje, promena identiteta a predviđeno je i ispitivanje svedoka putem video linka tj. uz korišćenje tehničkih sredstava za prenos slike i zvuka.

Konvencija o pravima deteta[4] je nezaobilazni dokument kada se govori o zaštiti dece uopšte a samim tim i u sudskim postupcima. Konvencija sadrži osnovna prava koja moraju u državama potpisnicama biti obezbeđenjena svakom detetu. Sa aspekta zaštite dece u sudskim postupcima važno je ukazati na čl.12 Konvencije koji predviđa da detetu mora biti pružena mogućnost da bude saslušano u svim sudskim i administrativnim postupcima koji se tiču deteta, bilo neposredno ili preko zastupnika ili odgovarajućeg organa. Pored navedenog odredbama 40 i 41 Konvencije su posebno regulisana minimalna prava koja moraju biti obezbeđena maloletnicima u krivičnim postupcima.

Na području Evropske unije je takođe pitanje zaštite svedoka bilo aktuelno pa je tako 2005. godine Savet Evrope usvojio Preporuku R 9 o zaštiti svedoka i saradnika u pravosuđu.[5] Preporuka nema obevezujući karakter ali svakako da predstavlja smernice za države potpisnice u zaštiti svedoka ukazujući na potrebu maksimalne zaštite. Ono što je bitno istaći je da Preporuka ukazuje na potrebu da mere zaštite budu odabrane shodno individualnim karakteristikama ličnosti svedoka i prelagođene potrebama svakog pojedinačnog svedoka.

Kada se govori o dokumentima donetim na području Evropske unije potrebno je istaći Konvenciju o sprečavanju i borbi protiv nasilja nad ženama i nasilja u porodici (Istanbulska konvencija)[6] koja je usvojena 05.11.2011. godine u Istanbulu. Cilj Konvencije je, između ostalog, obezbeđivanje celokupne zaštite žrtvama rodno zasnovanog nasilja. Takođe, su čl.56 Konvencije propisane i posebne mere zaštite svedoka i oštećenih u ovim krivičnim potupcima od svih vidova sekundarne viktimizacije sa posebnim akcentom na to da je potrebno obezbediti u pravosudnim institucijama da ne dolazi do susreta između žrtava i učinilaca. U tom smislu u Konvenciji je izričito predviđeno da u skladu sa pravilima nacionalnog prava žrtva svedoči bez prisustva učinioca, naročito uz korišćenje odgovarajućih komunikacionih tehnologija, tamo gde su dostupne.

---

[3] Zakon o potvrđivanju Konvencije UN o transnacionalnom organizovanom kriminalu, *Sl. List SRJ*-Međunarodni ugovori, br.6/2001.

[4] www.unicef.org/serbia/media/3186/file, [7.10.2022.].

[5] www.pars.rs/images/biblioteka/smernice-o-merama-zastite-svedoka-u-medjunarodnom-pravu-i-pravu-RS.pdf, [7.10.2022.].

[6] www.coe.int/1680462540, [12.10.2022.].

Konvencija Saveta Evrope o zaštiti dece od seksualnog iskorišćavanja i seksualnog zlostavljanja[7] koja je usvojena 25.10.2007. godine na Lansarotu propisuje posebna načela i mere za zaštitu dece od svakog vida seksualnog zlostavljanja ali i mere prevencije koja je svaka država potpisnica u obavezi da preduzme. Konvencijom i nametnuta obaveza državama da u svoja krivična zakonodavstva inkriminišu krivična dela kojima se na posredan ili neposredan način deca seksualno iskorišćavaju i zlostavljaju. Pored navedenog, posebna pažnja je posvećena programima zaštite dece koji treba da budu usmereni na sve segmente života i funkcionisanja deteta. Takođe Konvencija predviđa pored opšte zaštite i zaštitu tokom krivičnog postupka koja između ostalog, obuhvata i zaštitu u vidu izbegavanja kontakta između žrtava i počinilaca na sudu ili u prostorijama policije osim ako nadležni organ ne proceni da je to u najboljem interesu detea ili kada je takav kontakt neophodan radi istrage i krivičnog postupka. Član 35 Konvencije propisuje posebna pravila razgovora sa detetom koja podrazumeva potpunu opreznost dok čl. 36 Konvencije predviđa mogućnost ispitivanja deteta putem tehničkih sredstava za prenos slike i zvuka.

Veoma važan dokument i može se reći vodilja prilikom postavljanja ciljeva u zaštiti svedoka u nacionalnom zakonodavstvu je Direktiva 2012/29/eu[8] evropskog parlamenta i evropskog saveta od 25. oktobra 2012. godine, kojom su zapravo uspostavljeni minimalni standardi o pravima, podršci i zaštiti žrtava kriminaliteta.

3. ZAŠTITA SVEDOKA U PRAVU REPUBLIKE SRBIJE

Posmatrajući standarde koji su postavljeni u navedenim ali i drugim međunarodnim aktima, može se zaključiti da su u pravnom sistemu Srbije u velikoj meri oni inkorporirani. U nastavku rada ukazaćemo na najznačajnije pravne akte Srbije iz oblasti kako opšte, tako i posebne zaštite svedoka, sa posebnim akcentom na odredbe koje se odnose na primenu tehnologije prilikom zaštite svedoka.

Sve mere procesne zaštite svedoka moraju biti propisane procesnim zakonima, što je i učinjeno Zakonikom o krivičnom postupku Srbije (ZKP) koji predviđa mere opšte i posebne zaštite svedoka u krivičnom postupku ali i upućuje na druge zakone kojima je regulisano pitanje vanprocesne zaštite svedoka.

Kao mere opšte zaštite svedoka potrebno je ukazati najpre na odredbe ZKP-a kojima su regulisane mere za održavanje reda na glavnom pretresu (čl. 369 do čl. 376), a kojima je predviđena dužnost suda da zaštiti ugled i bezbednost suda, stranaka i drugih učesnika u postupku od uvrede, pretnje i svakog drugog napada. Takođe, je čl. 371 ZKP izričito predviđeno da sud može okrivljenog udaljiti iz sudnice za vreme preduzimanja određene dokazne radnje ili do kraja dokaznog postupka i odrediti da on iz posebne prostorije putem tehničkih sredstava za prenos slike i zvuka prati tok postupka. Kao jedna od mera zaštite svedoka i oštećenih u postupku je mogućnost isključenja javnosti

[7] www.ravnopravnost.gov.rs/wpcontent/download/, [5.10.2022.].

[8] www.podrskazrtvama.rs/media/medjunarodni/DIREKTIVA-2012-29-EU.pdf, [29.9.2022.].

za ceo glavni pretres, ili jedan njegov deo (čl. 363 ZKP). Naime, između ostalog, kao razlozi za isključenje javnosti su zaštita interesa maloletnika i privatnost učesnika u postupku. Posebno značajne mere za zaštitu svedoka i oštećenih u krivičnom postupku su mere za obezbeđenje prisustva okrivljenog i nesmetano vođenje krivičnog postupka. Kao što je prethodno navedeno, jedan od mogućih razloga za neistinito, ili necelishodno svedočenje je mogućnost uticaja na svedoke. Upravo zbog toga je čl. 197 ZKP propisana mogućnost izricanja mere zabrane približavanja, sastajanja ili komuniciranja sa određenim licem u situaciji kada se proceni da postoje okolnosti koje ukazuju da bi okrivljeni mogao ometati postupak uticajem na oštećenog i svedoke, kao i okolnosti koje ukazuju da bi mogao ponoviti, dovršiti ili učiniti krivično delo. Ukoliko je stepen takve opasnosti viši, sud može shodno čl. 211 st. 2 tač. 2 ZKP odrediti i pritvor okrivljenom. Opšta zaštita svedoka je obezbeđena, ne samo u toku trajanja postupka, već i nakon njegovog okončanja i to ne samo izricanjem krivične sankcije, već i mogućnošću izricanja mere bezbednosti zabrana približavanja i komunikacije sa oštećenim (čl. 89a KZ).

Mere specijalne zaštite svedoka se odnose na odredbe ZKP-a kojima je regulisan procesni položaj posebno osetljivih svedoka i zaštićenog svedoka.

Zakonik o krivičnom postupku sadrži odredbe kojima je regulisano šta će se imati u vidu prilikom procene da li određenom svedoku treba dodeliti status posebno osetljivog. Stoga je propisano da organ postupka prilikom donošenja odluke o tome treba da uzme u obzir uzrast, životno iskustvo, način života, pol, zdravstveno stanje, prirodu ili posledice izvršenog krivičnog dela, odnosno druge okolnosti slučaja. Iz citirane zakonske odredbe proizilazi da svedok može dobiti status posebno osetljivog zbog određenih subjektivnih okolnosti kao što su pol, zdravstveno stanje, uzrast i sl. Međutim, i sama priroda krivičnog dela, okolnosti pod kojima je učinjeno, način izvršenja dela, odnos sa izvršiocem krivičnog dela mogu biti presudni za određivanje statusa posebno osetljivog svedoka.

Cilj određivanja statusa posebno osetljivog svedoka nekom licu sprovodi se kako bi se taj svedok zaštitio odnosno kako bi se njegovo ispitivanje sprovelo primenom posebnih mera zaštite. Najčešće se kao mere zaštite posebno osetljivih svedoka određuju postavljanje pitanja preko organa postupka, ispitivanje uz pomoć odnosno posredstvom stručnog lica, psihologa socijalnog radnika i dr., i zabrana suočenja sa posebno osetljivim svedokom. Najznačajniji vid zaštite posebno osetljivih svedoka je ispitivanje svedoka posredstvom tehničih sredstava za prenos slike i zvuka. Ispitivanje se sprovodi bez prisustva stranaka i drugih učesnika u postupku. Bitno je napomenuti da Zakonik o krivičnom postupku izričito navodi da se posebno osetljiv svedok može ispitati i u svom stanu ili drugoj prostoriji, odnosno ovlašćenoj instituciji koja je stručno osposobljena za ispitivanje posebno osetljivih lica. Najveći problem u vezi s primenom navedenog ogleda se u činjenici da ovaj način ispitivanja zahteva tehničku osposobljenost sudova koja je u većini sudova na teritoriji Republike Srbije na nezavidnom nivou.

Drugi vid specijalne zaštite svedoka po ZKP-u je dodeljivanje statusa zaštićenog svedoka. Zaštićeni svedok je zapravo svedok koji bi svojim iskazom ili odgovorom na pojedina pitanja sebe ili bliska lica izložio znatnoj opasnosti po život, zdravlje, bezbednost ili imovinu. Dakle, po svojim pravima i dužnostima zaštićeni svedok ima sva prava

i dužnosti kao i svaki drugi svedok, međutim, razliku čini to što je zaštićeni svedok izloženiji opasnostima zbog prirode svedočenja odnosno, ozbiljnosti krivičnog dela o kojem svedoči, učinioca i slično. Da bi jedan svedok uživao status zaštićenog svedoka o tome mora da postoji odluka nadležnog organa. Dakle, nije dovoljno da lice subjektivno smatra da je zbog svedočenja izloženo opasnosti već o tome mora odluku da donese sud. Određivanje statusa zaštićenog svedoka stvara mogućnost da se u cilju njegove zaštite primene mere posebne zaštite (čl. 106 ZKP), a njima se obezbeđuje da se istovetnost zaštićenog svedoka ne otkrije javnosti, a pod zakonom propisanim uslovima ni okrivljenom, ni njegovom braniocu. Radi realizacije ovih posebnih mera zaštite predviđeno je da se ispitivanje zaštićenog svedoka obavlja putem tehničkih sredstava za promenu zvuka i slike i njima rukuje stručno lice.

Kada se govori o pravnom okviru Srbije u zaštiti svedoka neophodno je ukazati na odredbe Zakona o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica.[9] U trećem delu ovog Zakona propisana su pravila o zaštiti maloletnih lica kao oštećenih u krivičnom postupku i okolnosti pod kojima se maloletno oštećeno lice ispituje u krivičnom postupku. Tako je članom 152. stav 3. Zakona o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica propisano da sudija može narediti da se maloletno lice sasluša upotrebom tehničkih sredstava za prenos slike i zvuka, a saslušanje se sprovodi bez prisustva stranaka i drugih učesnika postupka, u prostoriji u kojoj se svedok nalazi, tako da mu stranke i lica koja na to imaju pravo, pitanja postavljaju posredstvom sudije, psihologa, pedagoga, socijalnog radnika ili drugog stručnog lica. Članom 152. stav 4. predviđena je mogućnost da se maloletna lica koja su svedoci oštećeni u krivičnom postupku mogu saslušati i u svom stanu ili drugoj prostoriji, odnosno ovlašćenoj instituciji ili organizaciji, stručno osposobljenoj za ispitivanje maloletnih lica, pri čemu se mogu koristiti tehnička sredstva za prenos slike i zvuka.

Posebno je značajno ukazati da je Republika Srbija usvojila i Nacionalnu strategiju za ostvarivanje prava žrtava i svedoka krivičnih dela u RS[10] za period od 2020-2025. godine i Akcioni plan. Cilj strategije je da se svim žrtvama i svedocima krivičnih dela obezbedi adekvatan nivo procesnih prava, kao i sistemska, stručna i dostupna pomoć i podrška, kao i poseban nivo zaštite naročito ranjivim kategorijama žrtava. Pored ovog opšteg cilja Strategijom su postavljeni i posebni ciljevi i to: uspostavljanje mreže službi podrške, unapređenje dostupnosti, kvaliteta i efikasnsti primene mera zaštite žrtava i svedoka krivičnih dela u RS sa posebnom zaštitom posebno osetljivih kategorija žrtava i svedoka, podizanje svesti žrtava i svedoka o pravima koja im pripadaju kao i kontinuirano informisanje javnosti. Bitno je istaći da su u Starategiji u potpunosti inkoporirane odredbe Direktive UN(2012)29, što dodatno ukazuje na njen značaj. Sa aspekta primene tehnologije u zaštiti svedoka i oštećenih značajno je da njena primena u strategiji zauzima značajno mesto i da je predviđena kao jedan od glavnih vidova zaštite.

[9] Zakon o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica, *Sl.glasnik RS,* br.85/2005.

[10] www.mpravde.gov.rs/sr/tekst/30567/nacionalna-strategija-za-ostvarivanje-prava-zrtava-i-svedoka-krivicnih-dela-u-republici-srbiji-za-period-2020-2025-godine-19082020.php, [12.10.2022.].

4. PRIMENA TEHNOLOGIJE U ZAŠTITI POSEBNO OSETLJIVIH SVEDOKA U PRAKSI SUDOVA U SRBIJI

Sve prethodno navedeno ali i tumačenje suštine zaštite svedoka ukazuje da je primena tehnologije gotovo neophodna da bi se postigla potpuna zaštita. Navedeno, između ostalog, jer je izbegavanje kontakta učinioca i žrtve i davanje iskaza bez pritiska koji prouzrokuje prisustvo okrivljenog svakako neophodno radi izbegavanja sekundarne viktimizacije ali i iznošenja validnog i uverljivog iskaza.

Kao što je prethodno prezentovano pravni okvir Republike Srbije pruža mogućnost da se određeni delovi sudskih postupaka ne sprovode neposredno, već da se određene dokazne radnje sprovedu „na daljinu", odnosno, da svedok ne bude u prostoriji ili sudnici sa okrivljenim i ostalim procesnim subjektima već u posebnoj prostoriji. Međutim i pored ovakvih mogućnosti zapaža se da se primena tehnologije u sudskim postupcima ne koristi u dovoljnoj meri pa ni u zaštiti svedoka. Radi potvrđivanja navedene hipoteze ukazaćemo, a u odsustvu kompletnih podataka o primeni tehnologije u zaštiti svedoka, na istraživanje Foruma sudija Srbije u okviru projekta "Sudjenje na daljinu" tokom 2020. godine kojim je, između ostalog, ispitano koji je obim primene navedene tehnologije u zaštiti svedoka, zatim kakva je tehnička osposobljenost sudova za primenu, kao i kakva je zainteresovanost sudija za ovakvu vrstu ispitivanja (Krstić, 2021: 44).

Istraživanjem je obuhvaćeno 11 osnovnih sudova i 8 viših sudova na teritoriji Republike Srbije, u vremenskom periodu od 1. januara do 31. decembra 2019. godine, kao i od 1. januara do 31. decembra 2020. godine. Podaci su dobijeni slanjem zahteva za pristup informacijama od javnog značaja u navedenim sudovima.

Status posebno osetljivog svedoka može se dodeliti u svim predmetima, nezavisno od vrste krivičnog dela, pa je istraživanje suženo i fokusirano na ona krivična dela kod kojih se u svojstvu oštećenih najčešće javljaju lica koja se mogu smatrati posebno osetljivim.

Tako su iz nadležnosti osnovnih sudova analizirani predmeti gde je postupak pokrenut za krivično delo nasilje u porodici, iz člana 194. stav 3. KZ, krivično delo zapuštanje i zlostavljanje maloletnog lica iz člana 193. KZ i krivično delo nedozvoljene polne radnje iz člana 182. KZ. U višim sudovima analizirani su predmeti u kojima je postupak pokrenut zbog krivičnog dela silovanje iz člana 178. KZ, obljuba nad nemoćnim licem iz člana 179. KZ, obljuba sa detetom iz člana 180. KZ i trgovina ljudima iz člana 388. KZ.

Istraživanje je pokazalo da 58,33% osnovnih sudova i 87,5% viših sudova poseduje tehničke mogućnosti i posebnu prostoriju za ispitivanje svedoka primenom tehničkih sredstava, s tim da u određenom broju sudova postoji zajednička Služba za pomoć i podršku svedocima i oštećenima.

Tokom 2019. godine pred osnovnim sudovima je ukupno pravnosnažno okončano 172 predmeta za posmatrana krivična dela, a tokom 2020. godine 145 predmeta.[11] Od

[11] Pred osnovnim sudovima u 2019. godini pravnosnažno je okončano 27 postupaka zbog krivičnog dela iz člana 182. KZ, pet postupaka zbog krivičnog dela iz člana 193. KZ i 140 postupaka zbog krivičnog dela iz člana 194. stav 3 KZ. Tokom 2020. godine pravnosnažno je okončano 12 postupaka zbog krivičnog dela iz člana 182. KZ, četiri zbog krivičnog dela iz člana 193. KZ i 129 postupaka zbog krivičnog dela iz člana 194. stav 3. KZ.

sudova je zahtevana i informaciju o broju i strukturi oštećenih u postupku (žene, deca ili maloletnici), ali nije bilo moguće napraviti sistematizaciju zbog različito dostavljenih podataka ili neposedovanja takvih informacija u sudovima. Iz podataka koji su dostavljeni i koje je bilo moguće analizirati proizilazi da su se u navedenim predmetima završenim pred osnovnim sudovima kao oštećeni uglavnom javljale žene, maloletnici i deca.

Od ukupnog broja okončanih postupaka tokom 2019. godine pred osnovnim sudovima (151) samo je u trinaest oštećenima određen status posebno osetljivih svedoka, s tim da dva suda nisu posedovala evidenciju o tome. Ukupno je jedanaest svedoka ispitano putem tehničkih sredstava za prenos slike i zvuka, a u 22 predmeta oštećeni nisu saslušani na glavnom pretresu, već je vršen uvid u zapisnike o njihovom ranijem ispitivanju. Iz navedenog se zaključuje da je u 116 predmeta oštećeni saslušan na glavnom pretresu po opštim pravilima postupka za ispitivanje svedoka.

Identična je situacija u osnovnim sudovima i tokom 2020. godine: od ukupno 140 okončanih postupaka samo je u trinaest određen status posebno osetljivih svedoka, s tim da dva suda nisu posedovala evidenciju o tome. Ukupno je jedanaest svedoka ispitano putem tehničkih sredstava za prenos slike i zvuka, dok u 32 predmeta oštećeni nisu ispitani, već je vršen uvid u zapisnike o njihovom ranijem ispitivanju. Iz navedenog se zaključije je u 97 postupaka oštećeni saslušan na glavnom pretresu, po opštim pravilima postupka za ispitivanje svedoka.

Interesantan je podatak da je najveći broj postupaka u 2019. godini za krivično delo nasilje u porodici iz člana 194. stav 3. KZ završen pred jednim osnovnim sudom (80 postupaka), ali ni u jednom postupku nije oštećenom određen status posebno osetljivog svedoka, niti su korišćena tehnička sredstva za prenos slike i zvuka, uprkos činjenici da je u sedam postupaka dete bilo oštećeno.

Istraživanje je pokazalo da su samo dva osnovna suda iz uzorka tokom 2019. i 2020. godine koristila tehnička sredstva za prenos slike i zvuka, s tim da dva suda nisu posedovala evidenciju o tome, pa nisu ni dostavila podatke. U preostalih sedam sudova tehnologija nije korišćena.

Pred višim sudovima je tokom 2019. godine ukupno pravnosnažno okončano 35 postupaka, a tokom 2020. godine 28 postupaka.[12] Tokom 2019. godine kao oštećeni u navedenim postupcima završenim pred višim sudovima bilo je sedam oštećenih žena, sedam maloletnika i petoro dece, a tokom 2020. godine osam oštećenih žena, osam maloletnika i četvoro dece.

Od ukupnog broja analiziranih postupaka pred višim sudovima tokom 2019. godine, u sedam predmeta je oštećenima dodeljen status posebno osetljivih svedoka, a u deset predmeta su ispitani preko tehničkih sredstava za prenos slike i zvuka, dok u 21 predmetu nije korišćena tehnologija, a u četiri postupka nisu ispitivani.

[12] Zbog krivičnog dela silovanje iz člana 178. KZ, pred višim sudovima je u toku 2019. godine pravnosnažno okončano 20, a tokom 2020. godine ukupno 13 postupaka. Zbog krivičnog dela obljuba sa nemoćnim licem, pred višim sudovima je tokom 2019. godine pravnosnažno okončano četiri postupka, a tokom 2020. godina tri. Zbog krivičnog dela obljuba sa detetom iz člana 180. KZ tokom 2019. godine pravnosnažno je okončano četiri postupka, i isto toliko tokom 2020. U odnosu na krivično delo trgovina ljudima iz člana 388. KZ, tokom 2019. godine okončano je sedam, a tokom 2020. osam postupaka.

Tokom 2020. godine od ukupno 28 pravnosnažno završenih postupaka, u šest je oštećenima dodeljen status posebno osetljivog svedoka i ispitani su pomoću tehničkih sredstava za prenos slike i zvuka, dok u 16 predmeta nije korišćena tehnologija, a u četiri predmeta nisu ispitivani.

Što se tiče viših sudova tokom 2019. godine samo su u jednom višem sudu korišćena sredstva za prenos slike i zvuka, a tokom 2020. godine u dva suda, s tim da jedan sud nije posedovao podatke o tome. Iz navedenog proizlazi zaključak da tokom posmatranog perioda u pet viših sudova nije korišćena tehnologija za prenos slike i zvuka.

Iz svih navedenih podataka iz pomenutog istraživanja mogu se konstatovati sledeći zaključci:

1) Iako postoji zakonski osnov za upotrebu tehnologije za prenos slike i zvuka za ona krivična dela kod kojih se u svojstvu oštećenih najčešće javljaju lica koja se mogu smatrati posebno osetljivim, ova mogućnost se i dalje nedovoljno koristi u Republici Srbiji. Navedeni zaključak proizlazi iz činjenice da je istraživanje pokazalo da od 12 osnovnih sudova, 8 poseduje tehničke mogućnosti, a u posmatranom periodu tehnologija je korišćena u svega četiri tokom 2019. godine, odnosno u tri tokom 2020. godine. Situacija je identična i u višim sudovima gde od posmatranih 8 viših sudova 7 poseduje tehničke mogućnosti a tehnologija je korišćena u jednom tokom 2019. godine, odnosno u dva tokom 2020. godine;
2) Manji je procenat sudova koji nemaju tehničke mogućnosti za ispitivanje svedoka u posebnoj prostoriji primenom tehničkih sredstava za prenos slike i zvuka, te zato treba uložiti dodatna sredstva da i ovi sudovi dobiju takvu mogućnost;
3) U veoma malom procentu primenjuje se ispitivanje svedoka u posebnoj prostoriji za prenos slike i zvuka, kako u odnosu na ukupan broj predmeta, tako i na broj predmeta u kojima je svedocima dodeljen status posebno osetljivih svedoka. Ovaj podatak ukazuje da se sudije pretežno opredeljuju ili za klasičan način ispitivanja svedoka, ili za vršenje uvida u zapisnike o njihovom ranijem ispitivanju (što svakako pozitivno utiče na smanjenje rizika od sekundarne viktimizacije);
4) Određeni broj sudova ne poseduje evidencije o korišćenju posebnih prostorija za ispitivanje svedoka što posredno ukazuje da ne poseduju ni službe za pomoć i podršku žrtvama i svedocima krivičnih dela.
5) U većini postupaka gde se kao oštećeni pojavljuju maloletnici ili deca nije im dodeljen status posebno osetljivih svedoka, kao ni u slučaju krivičnog dela za nasilje u porodici.

ZAKLJUČAK

Imajući u vidu izloženi pravni okvir ali i rezultate citiranog istraživanja zaključuje se da u Srbiji postoji mogućnost primene mera zaštite svedoka i oštećenih primenom tehnologije ali isto tako ima dosta prostora za njihovo unapređenje.

U tom smislu smatramo neophodnim preduzimanje sledećih koraka:

1. povećanje broja sudova koji raspolažu tehničkim sredstvima za prenos slike i zvuka, osposobljavanje prostorija i modernizacija tehnologije;
2. unapređenje pravnog okvira i
3. odgovorajuća obuka nosilaca pravosudnih profesija ali drugih aktera (sudija, sudskog osoblja, tužilaštva i policije) o zaštiti svedoka primenom tehnologije.

Naime, iako većina sdova u Srbiji poseduje tehnologiju koju može primeniti u zaštiti i ispitivanju svedoka smatramo neophodnim povećanje broja sudova koji raspolažu ovom tehnologijom. Posebno je značajno ukazati da većina osnovnih sudova koristi prostorije i tehnologiju viših sudova što može dovesti do problema u vidu organizacije termina suđenja ali problem može predstavljati i udaljenost sudova. U ovom kontekstu treba imati u vidu i činjenicu da sadašnja tehnologija uglavnom omogućava da se posebno osetljivi svedoci ispituju putem tehničkih sredstava u istoj zgradi u kojoj je suđenje ali u različitim prostorijama. Stoga je potrebno modernizovati tehnologiju kako bi bilo moguće ispitivanje i svedoka koji se ne nalazi u zgradi suda, putem video linka. Ukazaćemo i na problem potrebe za modernizacijom tehnologije jer je samo određeni broj sudova u zemlji raspolaže inovativnom tehnologijom koja omogućava potpunu zaštitu svedoka. Takođe je značajno da ulazi u prostorije za ispitivanje posebno osetljivih svedoka budu odvojeni od prostora kojim će se kretati okrivljeni.

Iako je pravni okvir u Srbiji usaglašen u većoj meri sa međunarodnim standardima smatramo da je neophodno unaređenje određenih odredbi i to pre svega sa ciljem smanjenja broja ispitivanja posebno osetljivih svedoka. Zapaženo je da se čak i posebno osetljivi svedoci ispituju više puta tokom trajanja postupka pa u tom smislu smatramo potrebnim da se izričito ZKP-om dozvoli mogućnost uvida u snimak sa ispitivanja svedoka u prethodnim fazama postupka umesto ponovnog neposrednog ispitivanja.

Citirano istraživanje je pokazalo da sudije nisu u velikoj meri zainteresovane za primenu tehnologije. Ovome doprinosi svakako ne samo nepoznavanje mogućnosti i prednosti takvog načina ispitivanja već i nepoznavanje procedura za sprovođenje takvog načina ispitivanja. Određeni primeri iz sudske prakse ukazuju i na to da se ispitivanja svedoka putem tehnologije ne sprovede u skladu sa ZKP ili se pak načine određeni propusti što dovodi do zakonske obaveze ponovnog ispitivanja.[13] Takođe, značajna bi bila edukacija o tome kako identifikovati posebno osetljive svedoke imajući u vidu da je taj status u praksi jedino određivan deci i maloletnicima i izuzetno punoletnim žrtvama određenih

[13] Recimo, javljaju se slučajevi u kojima posebno osetljiv svedok vidi i čuje dešavanja u sudnici iako je određeno njegovo ispitivanje u posebnoj prostoriji uz pomoć psihologa.

krivičnih dela. Navedeno je osnova za sve dalje korake u zaštiti žrtve jer bez pravilne identifikacije na samom početku postupka, kasnije mere zaštite mogu ostati bez efekta.

Na kraju, se može zaključiti da je zaštita svedoka u krivičnim postupcima kompleksno pitanje, ali verodostojno svedočenje se može očekivati samo uz preduzimanje svih potrebnih mera zaštite koje su prilagođene svakom konkretnom svedoku i predmetu. Sa druge strane, nesporno je da država mora da u svakom pogledu zaštiti lice kome je izvršenjem krivičnog dela naneta šteta, pa sigurno nije potrebno a ni pravedno da trpi dodatnu štetu od strane sistema.

LITERATURA

1. Burnsajd, S. (2015) *Smernice o merama zaštite svedoka u međunarodnom pravu i Srbiji*, Winpro III.
2. Krstić I. i dr. (2021) "Sudjenje na daljinu, pravni okvir i praksa", Beograd: *Forum sudija Srbije*.
3. Zakonik o krivičnom postupku (*Sl. glasnik RS*, br. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 - odluka US i 62/2021 - odluka US).
4. Zakon o potvrđivanju Konvencije UN o transnacionalnom organizovanom kriminalu, (*Sl. List SRJ*-Međunarodni ugovori, br.6/2001).
5. Zakon o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica, (*Sl.glasnik RS*, br.85/2005).

Internet izvori

1. www.unicef.org/serbia/media/3186/file, [7.10.2022.].
2. www.pars.rs/images/biblioteka/smernice-o-merama-zastite-svedoka-u-medjunarodnom-pravu-i-pravu-RS.pdf, [7.10.2022.].
3. www.coe.int/1680462540, [12.10.2022.].
4. www.ravnopravnost.gov.rs/wpcontent/download/ [5.10.2022.].
5. www.podrskazrtvama.rs/media/medjunarodni/DIREKTIVA-2012-29-EU.pdf, [29.9.2022.]
6. www.mpravde.gov.rs/sr/tekst/30567/nacionalna-strategija-za-ostvarivanje-prava-zrtava-i-svedoka-krivicnih-dela-u-republici-srbiji-za-period-2020-2025-godine-19082020.php, [12.10.2022.].

PROTECTION OF WITNESSES IN CRIMINAL PROCEEDINGS AND APPLICATION OF TECHNOLOGY

The issue of the application of technology in criminal proceedings became topical in Serbia with the beginning of the Covid 19 pandemic. Although the existing legislation foresees this possibility, the wider application of technology in criminal proceedings has not been noticed. Observing the practice of the courts, the technology is used in Serbia only in criminal proceedings before special departments for the suppression of organized crime and war crimes, but it is rarely encountered in regular criminal proceedings. On the other hand, the theory is unique about the importance of the application of technology, especially in the protection of witnesses and victims in court proceedings. Also, numerous international legal acts that contain provisions on the protection of witnesses in court proceedings recognize the importance of using technology to avoid numerous negative consequences of court proceedings and to avoid secondary victimization. However, despite numerous recommendations for this type of examination, it was noticed that it is not used in a large percentage in Serbia and certainly not in all cases where it is necessary or useful. The aim of the paper is to analyze the legal norms related to the protection of witnesses in criminal proceedings with a special emphasis on those that foresee or enable the application of technology for adequate protection on the international level and in Serbia, the extent of the application of technology in practice, the reasons for insufficient application and recommendations for the wider application.

KEYWORDS: *witness and victim protection, technical means for image and sound transmission, criminal procedure.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.14

DIGITALIZACIJA U SISTEMU IZVRŠENJA KRIVIČNIH SANKCIJA REPUBLIKE SRBIJE*

Aleksandra Ilić**
Božidar Banović***

U radu autori razmatraju upotrebu moderne tehnologije u različitim aspektima sistema izvršenja krivičnih sankcija u Republici Srbiji. S jedne strane se analiziraju različiti oblici digitalizacije prisutni u zavodima za izvršenje krivičnih sankcija gde se izvršavaju kazna zatvora i druge krivične sankcije zavodskog karaktera, kao i mera pritvora koja predstavlja meru za obezbeđenje prisustva okrivljenog i nesmetano vođenje krivičnog postupka. S tim u vezi, autori analiziraju razlike koje, u vezi sa korišćenjem napredne tehnologije u kontroli zatvorenika, postoje u različitim zavodima, pri čemu se uzima u obzir podela zavoda s obzirom na stepen obezbeđenja. Autori polaze od pretpostavke da je najnapredniji vid digitalizacije prisutan u zatvorima zatvorenog tipa sa posebnim obezbeđenjem u kojima kaznu zatvora izdržavaju lica osuđena za najteža krivična dela, između ostalog i lica koja izdržavaju kaznu zatvora u skladu sa Zakonom o izvršenju kazne zatvora za dela organizovanog kriminala. S druge strane, autori razmatraju pitanje digitalizacije u izvršenju vanzavodskih sankcija i mera sa akcentom na onim sankcijama i merama gde dolazi u obzir primena elektronskog nadzora, poput kućnog zatvora ili kućnog pritvora. U vezi sa svim pomenutim aspektima digitalizacije u sistemu izvršenja krivičnih sankcija Republike Srbije, autori analiziraju dostupne statističke i druge podatke, a sve u cilju kritičke analize aktuelne situacije i definisanja eventualnih predloga za unapređenje stanja.

KLJUČNE REČI: *digitalizacija; izvršenje; krivične sankcije; mere; osuđenici; zatvor.*

---

* Rad je nastao u okviru projekta koji finansira Fond za nauku Republike Srbije u okviru Programa "IDEJE" - Management of New Security Risks - Research and Simulation Development, NEWSIMR&D, #7749151.

** Doktor pravnih nauka, vanredni profesor, Univerzitet u Beogradu, Fakultet bezbednosti.
E-mail: *alex.mag.ilic@gmail.com*

*** Doktor pravnih nauka, redovni profesor, Univerzitet u Beogradu, Fakultet bezbednosti.
E-mail: *bbvsup@yahoo.com*

UVOD

Proces digitalizacije, prisutan u svim segmentima društva, neophodno je sprovesti i u sistemu izvršenja krivičnih sankcija koji se ne može posmatrati izolovano u odnosu na druge elemente formalne socijalne kontrole koji čine još policija i pravosudni sistem (tužilaštvo i sudstvo). Ta povezanost bi trebalo da se ispolji i u sferi digitalizacije kako bi se olakšalo i učinilo efikasnijim funkcionisanje svih delova pomenutog sistema, ali i celine.

Digitalno osavremenjivanje sistema izvršenja krivičnih sankcija predstavlja jednu od prioritetnih aktivnosti i kontinuirani cilj naveden kako u Strategiji razvoja sistema izvršenja krivičnih sankcija u Republici Srbiji do 2020. godine (u daljem tekstu: Strategija)[1] tako i u Radnom tekstu Strategije razvoja sistema izvršenja krivičnih sankcija u Republici Srbiji za period 2021-2027. godine (u daljem tekstu: Radni tekst Strategije)[2]. Upravo se u Radnom tekstu Strategije ističe potreba razvijanja postojećih i uvođenje novih sistema i tehnologija kako bi se omogućilo jednoobrazno i sveobuhvatno prikupljanje potrebnih podataka, a sakupljeni podaci bili lako dostupni nadležnim organima i povezani sa sistemima sudova, tužilaštava, policije i drugih organa.

U radu će biti razmotreni različiti aspekti digitalizacije u sistemu izvršenja krivičnih sankcija. S jedne strane se analizira problematika digitalizacije u zavodima za izvršenje krivičnih sankcija koja se može istražiti iz dva osnovna ugla. Prvi se tiče digitalne opremljenosti zavoda za izvršenje krivičnih sankcija odnosno kvaliteta instaliranog informacionog softvera koji treba da omogući adekvatno i efikasno prikupljanje i distribuciju podataka kao i digitalnu opremljenost zavoda (instalirana oprema) koju prevashodno koristi služba za obezbeđenje. Drugi ugao podrazumeva upotrebu digitalne tehnologije kao vid pomoći osuđenicima prilikom ostvarivanja nekih njihovih prava odnosno generalno kao sredstvo koje treba da pomogne u procesu resocijalizacije.

Sistem izvršenja krivičnih sankcija sastoji se i iz segmenta izvršenja vanzavodskih sankcija i mera. Digitalizacija svakako nalazi svoju primenu i u toj oblasti odnosno u pogledu nekih vanzavodskih sankcija i mera pojavljuje se kao neophodan element u njihovom izvršenju – upotreba elektronskog nadzora. Ipak, očigledni praktični problemi u primeni zakonskih rešenja i široj primeni pojedinih vanzavodskih sankcija i mera uz elektronski nadzor zahtevaju detaljnu analizu i pronalaženje načina da se situacija popravi. S tim u vezi, u radu se ističu neki uporedni primeri dobre prakse koji bi mogli eventualno da budu primenjeni i u Republici Srbiji.

---

[1] Strategija razvoja sistema izvršenja krivičnih sankcija u Republici Srbiji do 2020. godine (*Službeni glasnik RS*, br. 114/2013).

[2] Radni tekst Strategije razvoja sistema izvršenja krivičnih sankcija u Republici Srbiji za period 2021-2027. godine. Dostupno na: https://www.mpravde.gov.rs/tekst/33173/strategija-razvoja-sistema-izvrsenja-krivicnih-sankcija-u-republici-srbiji-za-period-2021-2027-godina.php [14.10.2022.].

1. DIGITALIZACIJA U ZAVODIMA ZA IZVRŠENJE KRIVIČNIH SANKCIJA

Problematika digitalizacije u zavodima za izvršenje krivičnih sankcija se može razmotriti na više načina, u zavisnosti od više kriterijuma. Obično prva asocijacija na pomen upotrebe digitalne tehnologije je primena modernih digitalnih dostignuća u svrhu bolje i efikasnije kontrole lica lišenih slobode. Sistem nadzora i kontrole kretanja zatvorenika se unapređivao s vremenom kako su se događale značajne promene u sferi digitalizacije na opštem planu. U današnje vreme, nesumnjivo zahvaljujući tehnološkom napretku, u većini država zatvori raspolažu sa odgovarajućom modernom tehnologijom koja se koristi u različitim aspektima izvršenja sankcija i mera koje podrazumevaju lišenje slobode. S tim u vezi, u Republici Srbiji je u periodu primene Strategije bilo potrebno razviti softver za evidenciju lica lišenih slobode (SAPA) kao centralno mesto za prikupljanje podataka o licima lišenih slobode. Ovim softverom obuhvaćena je obrada matičnih podataka o licima lišenih sloboda kao i evidencija zdravstvenih, tretmanskih, bezbednosnih i dr. podataka od značaja za izvršenje krivičnih sankcija i mere pritvora. Takođe, sprovedena je i integracija softvera za evidenciju lica lišenih slobode (SAPA) sa centralnim softverom Ministarstva pravde Srbije. Izvršena je nabavka IT opreme za centralnu server salu, kao i opreme za potrebe WAN mreže Uprave za izvršenje krivičnih sankcija (u daljem tekstu: Uprava) kao osnove sistema, preko koje se odvija komunikacija sa softverima koji se koriste za potrebe zavoda[3].

Pored sistemskih novina u sferi informacione tehnologije na nivou celokupne Uprave i posebno sistema izvršenja zavodskih sankcija i mera, neophodno je obratiti potrebnu pažnju na problematiku digitalizacije u okviru konkretnih zavoda. Osnovni nosioci bezbednosti pa samim tim i primarni neposredni korisnici digitalne tehnologije u zavodima za izvršenje krivičnih sankcija su pripadnici službe za obezbeđenje koji su zbog prirode posla koji obavljaju ovlašćeni da preduzimaju različite mere kako bi kompleksna problematika kontrole u zatvorima funkcionisala. S tim u vezi, Zakon o izvršenju krivičnih sankcija[4] (u daljem tekstu: ZIKS) u članu 21. stav 1 propisuje da se služba za obezbeđenje, kao jedinstvena formacija Uprave, stara o bezbednosti ljudi i imovine u zavodu, sprovodi osuđena i pritvorena lica, učestvuje u utvrđivanju i sprovođenju programa postupanja prema osuđenom i obavlja druge poslove određene zakonom. U svrhu ostvarivanja svih zadataka koji su u njenoj nadležnosti, služba za obezbeđenje raspolaže sa odgovarajućom opremom koju, prema članu 33. Pravilnika o uniformi, oznakama, naoružanju, specijalnim vozilima i drugoj opremi u Službi za obezbeđenje u Upravi za izvršenje krivičnih sankcija[5] (u daljem tekstu: Pravilnik o UONSOZIKS) čine: lična oprema pripadnika službe, dodatna oprema za naoružanje, specijalna motorna vozila sa dodatnom opremom i uređajima i oprema koja je

[3] Radni tekst Strategije razvoja sistema izvršenja krivičnih sankcija u Republici Srbiji za period 2021-2027. godine. Dostupno na: https://www.mpravde.gov.rs/tekst/33173/strategija-razvoja-sistema-izvrsenja-krivicnih-sankcija-u-republici-srbiji-za-period-2021-2027-godina.php [14.10.2022.].

[4] Zakon o izvršenju krivičnih sankcija (*Službeni glasnik RS*, br. 55/14 i 35/19).

[5] Pravilnik o uniformi, oznakama, naoružanju, specijalnim vozilima i drugoj opremi u Službi za obezbeđenje u Upravi za izvršenje krivičnih sankcija (*Službeni glasnik RS*, br. 29/2016, 74/2016, 3/2017, 89/2017 i 7/2019).

instalirana ili se koristi u zavodu. Ukoliko se razmotri uticaj digitalizacije na sredstva kojima mogu raspolagati pripadnici službe za obezbeđenje, onda se akcenat mora staviti na specijalna motorna vozila sa dodatnom opremom i uređajima i opremu koja je instalirana ili se koristi u zavodu. Lična oprema i dodatna oprema za naoružanje, iako po pravilu usklađena sa aktuelnim standardima, ne predstavlja manifestaciju uticaja digitalizacije u ovoj oblasti.

Može se napraviti razlika između spoljašnjeg i unutrašnjeg aspekta kontrole bezbednosti u zavodima. Spoljašnji aspekt podrazumeva kontrolu ulaska i izlaska iz zavoda kako bi se onemogućio bilo kakav incident koji može da ugrozi adekvatno funkcionisanje konkretnog zavoda. Kontrola ulaska se vrši prevashodno kako bi se sprečilo unošenje nedozvoljenih stvari ali se kontrola nastavlja i tokom kompletnog boravka tih istih osoba. Za tako nešto digitalizacija je od velike pomoći zaposlenima u zavodima, posebno pripadnicima službe za obezbeđenje. U pogledu lica koja borave u zavodu, a da se ne radi o licima lišenim slobode, nema značaja osnov po kome se nalaze tamo: branilac okrivljenog, član porodice lica lišenog slobode, nastavnik ili student koji je u odobrenoj poseti...ili su u pitanju zaposlena lica (pedagozi, psiholozi, lekari...), svi ti subjekti se moraju podvrgnuti odgovarajućoj kontroli, naročito prilikom ulaska.

Ipak, većina zatvorskih sistema, kao uostalom i naš, pravi razliku između zavodskih ustanova prevashodno imajući u vidu propisan režim boravka osuđenika u njima. S tim u vezi u skladu sa, jednim od vodećih kriterijuma za kategorizaciju zatvorskih ustanova, stepenom obezbeđenja, većina država razlikuje ustanove koje karakteriše maksimalan stepen obezbeđenja i ustanove kod kojih je to prisutno u manjoj meri kao i ustanove kod kojih ne postoje bilo kakve prepreke za bekstvo, tzv. otvorene ustanove. Prema ZIKS-u (члан 14), svi zavodi za izvršenje krivičnih sankcija u Republici Srbiji se, s obzirom na stepen obezbeđenja, mogu svrstati u neku od četiri kategorije: zavodi otvorenog tipa, zavodi poluotvorenog tipa, zavodi zatvorenog tipa i zavodi zatvorenog tipa sa posebnim obezbeđenjem.

Jedan od segmenata u kojem dolazi do primene dostignuća moderne tehnologije u izvršenju kazne zatvora i drugih sankcija odnosno mera zavodskog karaktera je sprovod osuđenih i pritvorenih lica van zavoda odnosno radi povratka u zavod, što se može dogoditi iz različitih razloga (na suđenje, u zdravstvenu ustanovu radi lečenja ili pružanja hitne medicinske pomoći...). Pravilnik o načinu obavljanja poslova u službi za obezbeđenje u zavodima za izvršenje krivičnih sankcija[6] (u daljem tekstu: Pravilnik o NOPSOZIKS) definiše sprovod kao svako odvođenje ili dovođenje lica lišenih slobode (osuđenika, pritvorenika i drugih lica lišenih slobode) iz zavoda odnosno u zavod pri čemu se sprovod lica lišenih slobode vrši na osnovu naloga za sprovod koji izdaju upravnik zavoda ili načelnik službe za obezbeđenje u zavodu (član 25. Pravilnika o NOPSOZIKS). S druge strane ZIKS u članu 21. stav 1 neprecizno govori o sprovođenju samo dve kategorije lica lišenih slobode: osuđenih i pritvorenih lica, zaboravljajući na lica koja su u stanju neuračunljivosti učinila protivpravno delo koje je u zakonu predviđeno kao krivično delo, što je svakako pravilno navedeno u Pravilniku o NOPSOZIKS (Ilić, 2022: 82).

[6] Pravilnik o načinu obavljanja poslova u službi za obezbeđenje u zavodima za izvršenje krivičnih sankcija (*Službeni glasnik RS*, br. 21/2016 i 104/2016).

Sprovođenje mora da bude u skladu sa zahtevima neometane i efikasne realizacije odnosno principima bezbednog ostvarenja tog zadatka i važnosti kontrole svih mogućih rizika što se, s jedne strane, u skladu sa članom 21. stav 2. ZIKS postiže korišćenjem službenih vozila koja su opremljena uređajima za davanje posebnih svetlosnih i zvučnih signala pri čemu ta vozila treba da imaju propisanu ventilaciju i osvetljenje što može biti teže nego kod običnih vozila s obzirom na to da se radi o vozilima specijalne namene koja su drugačije konstruisana primarno u cilju ostvarenja pomenutog zadatka bezbedne realizacije sprovođenja. To svakako ne umanjuje važnost da i takva vozila imaju neophodnu ventilaciju i osvetljenje (Ilić, 2022: 82). Pravilnik o UONSOZIKS[7] u članu 2. stav 6. definiše pojam specijalnih motornih vozila kao motornih vozila koja služe za prevoz lica lišenih slobode, koja su opremljena uređajima za davanje posebnih zvučnih i svetlosnih signala, propisanom ventilacijom, osvetljenjem i instaliranom opremom (video nadzor). U članu 36. st. 1. i 2 Pravilnik o UONSOZIKS precizira da u takvom vozilu može postojati sistem za video nadzor radi kontrole lica tokom transporta i sistem za daljinsko praćenje vozila pri čemu su vozila specijalne namene plave ili plavo bele boje i imaju obeležja Uprave na prednjoj maski, prednjim i zadnjim vratima.

Pravilnik o NOPSOZIKS takođe reguliše pitanje ventilacije i osvetljenja službenih vozila u članu 26, gde se ističe da se sprovođenje čini, po pravilu, specijalnim službenim vozilima koja su obeležena oznakama Uprave, opremljena uređajima za davanje posebnih svetlosnih i zvučnih signala, propisanom ventilacijom, video – nadzorom i osvetljenjem smeštajnog prostora za lica lišena slobode. U odnosu na ZIKS, postoji izvesna razlika u obaveznosti odredbe o korišćenju specijalnih službenih vozila jer Pravilnik o NOPSOZIKS ističe da se to čini po pravilu, što znači da su moguća i odstupanja koja su i regulisana u stavu 3. istog člana. U tom smislu moguće je izuzetno da pripadnici službe za obezbeđenje, u skladu sa prirodom zadatka, po naredbi direktora Uprave ili upravnika zavoda, vrše sprovod u neobeleženim službenim vozilima i civilnom odelu. Ovaj izuzetak se može protumačiti u svetlu važnosti ostvarenja osnovnog cilja sprovoda odnosno bezbedne i efikasne realizacije zadatka, pa ako je procena da je to jedino moguće učiniti neobeleženim službenim vozilom od strane pripadnika službe za obezbeđenje koji su obučeni u civilno odelo, onda opravdanost takvog izuzetka ne treba dovoditi u pitanje (Ilić, 2022: 83). Pravilnik o NOPSOZIKS takođe razrađuje odredbu o upotrebi zvučne i svetlosne signalizacije, postavljajući određena ograničenja. Posebni zvučni i svetlosni znakovi smeju se upotrebljavati samo kada je to neophodno za efikasno i bezbedno izvršenje službene radnje koja ne trpi odlaganje (član 26. stav 2. Pravilnika o NOPSOZIKS). Drugim rečima, nije dozvoljeno bespotrebno korišćenje signalizacije samo zato što je specijalno službeno vozilo time opremljeno (Ilić, 2022: 83). Ratio legis pomenutog ograničenja je sprečavanje moguće zloupotrebe zvučne i svetlosne signalizacije odnosno njihovo korišćenje onda kada to nije nužno a radi ostvarivanja nekog drugog cilja koji nije povezan sa sprovodom lica lišenih slobode.

[7] Pravilnik o uniformi, oznakama, naoružanju, specijalnim vozilima i drugoj opremi u Službi za obezbeđenje u Upravi za izvršenje krivičnih sankcija (*Službeni glasnik RS*, br. 29/2016, 74/2016, 3/2017, 89/2017 i 7/2019).

Na kraju treba se osvrnuti na problematiku opreme koja je instalirana u zavodu a čija je osnovna svrha održavanje reda i dicipline u cilju očuvanja bezbednosti. Prema Pravilniku o UONSOZIKS (član 37) opremu instaliranu u zavodu čine: 1) *uređaji za video nadzor i perimetrijsku zaštitu* (alarmi za obezbeđenje objekata i prostora i druge vrste zaštite); 2) *uređaji za održavanje veze,* i to: (1) radio uređaji, (2) satelitski uređaji, (3) interfonski uređaji; 3) *uređaji za otkrivanje i prepoznavanje nedozvoljenih metalnih predmeta i ostalih nedozvoljenih supstanci*, i to: (1) skener ručnog prtljaga, (2) ručni detektor metala, (3) vrata za prolaz lica sa integrisanim detektorom metala, (4) ručni uređaj za otkrivanje i prepoznavanje eksploziva i drugih nedozvoljenih supstanci; 4) *uređaj za otkrivanje i blokiranje signala uređaja za komunikaciju na daljinu*; 5) *sistem hidrantske mreže* (šmrkovi sa vodom) i 6) *sistem za kontrolu pristupa i identifikaciju pomoću biometrijskih i drugih čitača*.

Pomenuta oprema predstavlja okvir u kojem svaki zavod za izvršenje krivičnih sankcija može da izvrši potrebno planiranje i nabavku s obzirom da se potrebe zavoda razlikuju na šta najviše utiče stepen obezbeđenja zavoda. Najveće potrebe nesumnjivo imaju zavodi zatvorenog tipa sa posebnim obezbeđenjem: Kazneno-popravni zavod Beograd – Padinska skela i Kazneno-popravni zavod u Požarevcu - Zabela kao i Posebna pritvorska jedinica Okružnog zatvora u Beogradu koja se nalazi na dve lokacije: Bačvanska i Ustanička (zgrada Specijalnog suda).

Pravilnik o UONSOZIKS u članu 38 propisuje da načelnik službe za obezbeđenje, u skladu sa vrstom i tipom zavoda, poslovima i zadacima službe za obezbeđenje, dostavlja upravniku zavoda obrazložen plan potreba i predlog za nabavku opreme. Pre sačinjavanja plana, načelnik službe za obezbeđenje, prethodno pribavlja mišljenje stručno-tehničke komisije za nabavku opreme koju obrazuje direktor Uprave. Nakon toga, upravnik zavoda, po izvršenoj analizi predloga, daje saglasnost na plan i predlog i iste, uz obrazloženje dostavlja direktoru Uprave. Precizira se i da se u skladu sa potrebama službe i novim naučno-tehničkim dostignućima i međunarodnim standardima, može planirati i nabavljati i drugu opremu koja je iste namene i svrhe. Odluku o nabavci opreme donosi direktor Uprave, u skladu sa zakonom (član 39. Pravilnika o UONSOZIKS). Instaliranu opremu održavaju ovlašćeni serviseri i Odeljenje za informatiku i analitiku u Upravi – podcentrima i radnici na poslovima održavanja (član 55. Pravilnika o UONSOZIKS).

Prema podacima iz Radnog teksta Strategije[8], došlo je do određenog napretka u digitalizaciji pojedinih zavoda za izvršenje krivičnih sankcija tokom sprovođenja Strategije[9]. U Kazneno-popravnom zavodu Niš izgrađen je objekat za dežurnu službu sa operativnim centrom dok je novoizgrađeni Kazneno-popravni zavod u Pančevu snabdeven najnovijim sistemom bezbednosne zaštite. Pored toga, Uprava je saopštila u maju 2021. godine da je u Okružnom zatvoru u Beogradu instaliran moderan video-nadzor, čime

[8] Radni tekst Strategije razvoja sistema izvršenja krivičnih sankcija u Republici Srbiji za period 2021-2027. godine, dostupno na: https://www.mpravde.gov.rs/tekst/33173/strategija-razvoja-sistema-izvrsenja-krivicnih-sankcija-u-republici-srbiji-za-period-2021-2027-godina.php [14.10.2022].

[9] Strategija razvoja sistema izvršenja krivičnih sankcija u Republici Srbiji do 2020. godine (*Službeni glasnik RS*, br. 114/2013).

je još više unapređena bezbednost ove ustanove i osoba lišenih slobode[10]. Uprava takođe ističe da je nova savremena oprema u najvećoj pritvorskoj jedinici u zemlji, osim bezbednosnog aspekta, važna i za poslove koji se svakodnevno obavljaju u monitoring centru, koji predstavlja „žilu kucavicu" Okružnog zatvora u Beogradu. S tim u vezi, ukazuje se da se monitoring sprovodi isključivo iz bezbednosnih razloga i u skladu sa propisima, bez narušavanja prava na privatnost zaposlenih i lica lišenih slobode.

Iako sve šira upotreba video-nadzora i znatna ulaganja u usavršavanje i implementiranje novih tehnologija nisu zasnovana na čvrstim empirijskim dokazima o efektivnosti ove mere u unapređivanju bezbednosti, ipak se na osnovu dosadašnjih istraživanja može izvesti zaključak o izvesnim pozitivnim promenama u ponašanju osuđenika koje se mogu pripisati upotrebi video-nadzora (Kovačević-Lepojević i Žunić-Pavlović, 2012: 335).

2. DIGITALNA TEHNOLOGIJA I RESOCIJALIZACIJA OSUĐENIKA

Pored bezbednosnog aspekta upotrebe digitalne tehnologije u zavodima za izvršenje krivičnih sankcija, gde su glavni akteri te upotrebe pripadnici službe za obezbeđenje u odnosu na lica lišena slobode u različitim situacijama kao i u odnosu na druga lica koja po različitim osnovama borave u zavodima, značaj digitalizacije u zavodskim ustanovama se može razmotriti i drugačije. U pitanju je upotreba digitalizacije u kontekstu lakšeg ostvarivanja pojedinih prava osuđenika odnosno generalno u procesu resocijalizacije kao pomoćno sredstvo u postizanju pojedinih ciljeva iz programa postupanja.

Naše krivično izvršno pravo ne prepoznaje mogućnost upotrebe digitalne tehnologije kao sredstva koje bi se moglo iskoristiti u svrhu resocijalizacije, kao deo programa postupanja, ili u sklopu ostvarivanja nekog prava osuđenika. S druge strane, ne postoji ni zabrana korišćenja digitalne tehnologije pa je konkretna upotreba digitalizacije siva zona odnosno područje u vezi sa kojim postoji pravna praznina koja se može tumačiti na različite načine. Činjenica je da digitalizacija prožima život savremenog čoveka na različite načine, počevši od toga da gotovo svi danas imamo mobilni telefon i da je to osnovni način komuniciranja sa drugim ljudima ali i informisanja. Imajući u vidu život savremenog čoveka moramo se zapitati da li bi trebalo revidirati postojeće okvire izvršenja krivičnih sankcija zavodskog karaktera kako bi se realnost digitalizacije u određenoj meri inkorporirala i u život lica lišenih slobode. Ako se pođe od osnovne svrhe izvršenja kazne zatvora odnosno resocijalizacije koja podrazumeva između ostalog i pripremu osuđenika za život na slobodi, onda se nameće logičan zaključak da adekvatne pripreme za slobodu nema bez vođenja računa o tome kako život na slobodi stvarno izgleda.

Jedan od prvih primera *ad hoc* digitalizacije u zavodima za izvršenje krivičnih sankcija kod nas, kao načina olakšavanja života osuđenicima, posebno onima koji se nalaze u zatvorenom režimu, je omogućavanje korišćenja modernih digitalnih platformi za igranje igrica, poput Xbox ili SonyPlaystation. S obzirom da nije izričito zabranjeno,

[10] Vlada Republike Srbije https://www.srbija.gov.rs/vest/545005/okruzni-zatvor-u-beogradu-dobio-savremenu-monitoring-opremu.php [12.10.2022.].

neke zavodske ustanove su omogućile ograničeno, u toku slobodnog vremena, korišćenje takvih uređaja, podrazumeva se isključivo u offline režimu. Pristup internetu bi predstavljao značajan rizik.[11] Nabavka tih uređaja pada na teret osuđenika odnosno bliskih lica jer izlazi iz okvira onoga što predstavlja obavezu države.

Momenat koji je podstakao intenzivnija razmišljanja na temu korišćenja digitalne tehnologije od strane osuđenika je pandemija korona virusa koja je bila okidač za razmatranje prednosti korišćenja nekih aspekata digitalne tehnologije u svrhu olakšavanja održavanja kontakta osuđenika sa članovima porodice. Jedno od osnovnih prava lica lica lišenih slobode je pravo na posete koje je regulisano u ZIKS-u. U skladu sa zakonskim rešenjem osuđeni (odnosno druga lica lišena slobode u zavodskim ustanovama) ima pravo da ga dvaput mesečno posete: bračni drug, deca, roditelji, usvojenici, usvojitelji i ostali srodnici u pravoj liniji i u pobočnoj liniji do četvrtog stepena krvnog i tazbinskog srodstva, kao i hranitelji, hranjenici i staratelji (član 90. ZIKS). Restriktivniju mogućnost ostvarivanja kontakata sa bliskim licima imaju osuđenici u režimu izvršenja kazne zatvora prema Zakonu o izvršenju kazne zatvora za krivična dela organizovanog kriminala[12] (u daljem tekstu: ZIKZOK) koji imaju pravo na posetu bliskih srodnika samo jednom mesečno (član 37. stav 1) pri čemu se tok posete audio-vizuelno nadzire i snima, osim u slučaju posete branioca, Zaštitnika građana i predstavnika međunarodnih organizacija koje se bave zaštitom ljudskih prava, u skladu sa međunarodnim ugovorom (član 37. stav 4).

Bez obzira na propisan režim poseta, svaki osuđenik na to ima pravo pa su okolnosti izazvane pandemijom koronavirusa, kada se pomenuto pravo naročito u početku nije moglo realizovati na uobičajen način, podstakle da se pronađe neko rešenje kako bi osuđenici ipak održavali kontakt sa bliskim osobama. S tim u vezi, u avgustu 2020. godine, Ministarstvo pravde Vlade Republike Srbije saopštilo je da su osuđenici u deset kazneno-popravnih ustanova počeli da koriste programe „Skajp" (Skype) i „Vajber" (Viber) za kontakt sa članovima svojih porodica u cilju dodatne psihosocijalne podrške tokom pandemije koronavirusa[13]. Prema podacima iz tog perioda, video komunikaciju su mogli da koriste osuđenici u kazneno-popravnim zavodima u Sremskoj Mitrovici, Nišu, Pančevu, Padinskoj skeli, Specijalnoj zatvorskoj bolnici u Beogradu i okružnim zatvorima u Beogradu i Kragujevcu, zatim štićenici u Vaspitno-popravnom domu u Kruševcu i Kazneno-popravnom zavodu za maloletnike u Valjevu, kao i osuđenice u Kazneno-popravnom zavodu za žene u Požarevcu. Za ovu vrstu kontakta se koriste uređaji tablet koje

[11] S tim u vezi zabeležen je interesantan slučaj iz prakse francuskih sudova. Jedan francuski zatvorenik dobio je sudsku zabranu korišćenja Playstationa 3 u svojoj ćeliji. Umesto toga dodeljen mu je Xbox 360 zbog toga što jedna od njegovih verzija nema mogućnost povezivanja sa lokalnom WiFi mrežom za razliku od Playstation 3 koji u svakoj svojoj verziji poseduje tu mogućnost. Konkretno, radi se o staroj verziji Xboxa za koju je trebalo kupovati eksterni WiFi adapter. Slim verzija je to rešila, ali ta verzija svakako ne bi mogla da dođe u ruke zatvorenika. Ipak nejasno što se uopšte o tome raspravljalo kada je zatvorenicima inače onemogućeno da uhvate WiFi signal ali je francuski sud procenio da bi i načelna takva mogućnost bila previse opasna. https://www.vijesti.me/vijesti/280932/play-station-zabranjen-u-zatvoru-xbox-nije [15.10.2022.].

[12] Zakonu o izvršenju kazne zatvora za krivična dela organizovanog kriminala (*Službeni glasnik RS*, br. 72/2009 i 101/2010).

[13] https://www.srbija.gov.rs/vest/482074/osudjenici-koriste-skajp-i-vajber-za-kontakt-sa-porodicom-tokom-pandemije.php [10.10.2022.].

je zavodima donirala nemačka nevladina organizacija „Help", dok osuđenici u Kazneno-popravnom zavodu u Pančevu koriste postojeće računare. Zaposleni u službi za tretman od marta 2020. godine za osuđena lica sprovode pojačanu psihosocijalnu podršku koja je od ključnog značaja za svaku stresnu situaciju pa se smatralo da će ovaj vid kontakta pomoći zatvorenicima da se umanji briga za članove njihovih porodica. U Radnom tekstu Strategije[14] se takođe pominje upotreba tableta u vreme pandemije korona virusa ali samo u jednom zavodu za izvršenje krivičnih sankcija – Vaspitno-popravnom domu u Kruševcu. U vezi sa tim ističe se kako je bila omogućena redovna komunikacija maloletnika koji se nalaze na izdržavanju vaspitne mere sa porodicom i bliskim licima, čak i u okolnostima koje su otežane zbog potrebe poštovanja epidemioloških mera u kontekstu borbe protiv pandemije virusom COVID 19.

Ipak, upotreba dostugnuća moderne tehologije, poput pomenutih tableta, u nekim državama nije povezana samo sa specifičnim okolnostima tokom pandemije koronavirusa. Te države su prepoznale prednosti digitalizacije u postupanju sa osuđenicima i u redovnim okolnostima. Treba pomenuti Sjedinjene Američke Države u kojoj je, prema dostupnim novinarskim podacima, dvanaest država omogućilo zatvorenicima da koriste tablet uređaje (Finkel & Bertram, 2021)[15]. S tim u vezi, četiri velike tehnološke kompanije popunile su tehnološku prazninu u zatvorima tako što su stvorile „tablete za popravljanje" (correction-grade tablets), namenjene isključivo zatvorenicima. To su kompanije: JPay, GTL, Edovo, i American Prison Data Systems (APDS, n.d.; Edovo, n.d.; GTL, n.d.; JPay, Inc., n.d.). JPay i GTL prave tablete za zatvorenike u svrhu njihove komunikacije sa spoljašnjim svetom putem e-mejlova, e-kartica, videograma ili video poziva. Ti tableti se istovremeno mogu iskoristiti i za neke druge stvari, poput slušanja muzike, igranja igrica, praćenja obrazovnog sadržaja, gledanja vesti ili filmova, pretraživanja pravnih dokumenata, podnošenja pritužbi i/ili dostavljanja zahteva zatvorskom osoblju. S druge strane, kompanije Edovo, i American Prison Data Systems prave tablete u kojima su instalirani različiti kursevi: obrazovne prirode, kursevi za profesionalnu obuku ili rehabilitacioni kursevi, takođe namenjeni zatvorenicima. Generalno gledano, tableti koje prave kompanije Edovo i American Prison Data Systems kupuju zatvori koje potom zatvorski službenici daju zatvorenicima za vreme sprovođenja obrazovnog, radnog ili rehabilitacionog procesa. Nasuprot tome, tableti JPay kompanije takođe nabavljaju zatvori ali se oni čine dostupnim zatvorenicima kroz kioske koji su postavljeni u okviru dela zatvora gde su spavaonice. Na kraju, tableti GTL kompanije se jedino mogu nabaviti privatnim putem, odnosno mogu ih kupiti članovi porodice ili druge bliske osobe zatvorenika za njihovu ličnu upotrebu, u skladu sa navedenim sadržajima koje mogu imati (Mufarreh, Waitkus & Booker, 2021: 411).

Iako upotreba tableta na prvi pogled deluje kao značajan korak u poboljšanju položaja osuđenika na njihovom putout popravljanja i prilagođavanja životu na slobodi,

[14] Radni tekst Strategije razvoja sistema izvršenja krivičnih sankcija u Republici Srbiji za period 2021-2027. godine. Dostupno na: https://www.mpravde.gov.rs/tekst/33173/strategija-razvoja-sistema-izvrsenja-krivicnih-sankcija-u-republici-srbiji-za-period-2021-2027-godina.php [14.10.2022.].

[15] https://www.prisonpolicy.org/blog/2019/03/07/free-tablets/ [11.10.2022.].

treba biti svestan i mogućih negativnih posledica njihove upotrebe odnosno problema zloupotrebe moderne tehnologije koja neretko postoji i u redovnim okolnostima, van zatvorskog sistema.

S jedne strane, kada su u pitanju "besplatni" tableti odnosno oni koje nabavlja država, u mnogim slučajevima, na pomenutom primeru Sjedinjenih Američkih Država, ispostavlja se da nisu sasvim besplatni jer se njihovim korisnicima odnosno zatvorenicima naplaćuju usluge u svakoj prilici, što često podrazumeva nametanje cena iznad tržišnih za telefonske pozive, video ćaskanje i medije. Čak i slanje e-pošte zahteva plaćeni „pečat". Na osnovu analize ovih ugovora može se zaključiti da su interesi zatvorenika na poslednjem mestu, daje se prioritet uštedi troškova i u krajnjoj liniji bitni su interesi provajdera. Istovremeno sa uvođenjem tableta, mnogi američki zatvori ukidaju neke tradicionalne, osnovne usluge, poput pravnih biblioteka, knjiga u fizičkom obliku (jedan zatvor na Floridi je čak ukinuo Bibliju u parirnoj verziji i zamenio lošijom verzijom e-Biblije na tabletu) i mogućnosti slanja i primanja klasične pošte (Finkel & Bertram, 2021)[16].

Ni šira javnost nije baš naklonjena procesu digitalizacije među osuđenicima. Iako nema puno istraživanja u vezi sa tim, jedno od najnovijih sprovedeno u Velikoj Britaniji potvrđuje početnu konstataciju o načelnom nezadovoljstvu zbog tendencije da se zatvorenicima omogući pristup digitalnoj tehnologiji. Više od polovine (54%) ispitanika u anketi su istakli da su protiv toga da se zatvorenicima dozvoli upotreba digitalne tehnologije. Na primer, ispitanici u velikom procentu smatraju da mejlovi treba da se uvek proveravaju (73%). Takođe, više od polovine ispitanika smatra da digitalni pristup mora da se zaradi (57%) – veruju da je digitalna tehnologija luksuz i da ne bi trebalo da bude „besplatna" odnosno bez nekakvih troškova. Nasuprot tome, manji procenat (42%) smatra da je nerazumno tretirati upotrebu digitalne tehnologije kao luksuz (Hadlington & Knight 2022: 245).

Kod nas se o značaju digitalnog opismenjivanja osuđenika i uopšte važnosti digitalizacije u životima lica lišenih slobode slabo govori. Naša šira javnost, slično poput britanske, ne gleda blagonaklono na "privilegije" koje se omogućavaju zatvorenicima. Opšta tendencija retributivno orijentisane javnosti je insistiranje na sve strožijem i restriktivnijem zatvorskom režimu. Ne razmišlja se o jednostavnoj činjenici da će velika većina zatvorenika, jednog dana, izaći iz zatvora u svet koji je u svim svojim segmentima prožet digitalnom tehnologijom. Ako se ne omogući osuđenicima makar minimalan pristup toj tehnologiji, otežaće se značajno proces prilagođavanja životu na slobodi, što bi trebalo da bude osnovna zamisao resocijalizirajućeg tretmana u zatvorima. Kako bi se atmosfera promenila, onoliko koliko je moguće, potrebno je raditi na edukaciji šire javnosti o značaju pripreme osuđenika za život na slobodi, kako bi se povećale šanse za njihovo bolje uklapanje kada dođe vreme za izlazak iz zatvora.

[16] https://www.prisonpolicy.org/blog/2019/03/07/free-tablets/ [11.10.2022.].

3. DIGITALIZACIJA U IZVRŠENJU VANZAVODSKIH SANKCIJA I MERA

Pored izvršenja zavodskih sankcija i mera, uticaj digitalizacije se manifestuje i u okviru sistema izvršenja vanzavodskih sankcija i mera koji se takođe nalazi u nadležnosti Uprave. Izvršenje vanzavodskih sankcija i mera je prevashodno regulisano u Zakonu o izvršenju vanzavodskih sankcija i mera[17] (u daljem tekstu: ZIVSIM) uz shodnu primenu ZIKS-a kao osnovnog zakona u oblasti izvršenja krivičnih sankcija. Poslove izvršenja vanzavodskih sankcija i mera sprovodi Poverenička služba kao organizaciona jedinica Uprave (član 3. stav 1. ZIVSIM).

Poslovi izvršenja u nadležnosti Povereničke službe su raznovrsni i međusobno dosta različiti ali neke od njih spaja mogućnost upotrebe digitalne tehnologije u njihovoj realizaciji. Reč je o sistemu elektronskog nadzora koji se može primeniti prilikom realizacije poslova izvršenja u vezi sa pojedinim vanzavodskim sankcijama i merama. To su: izvršenje mere zabrane napuštanja stana (kućni pritvor), organizacija, sprovođenje i praćenje izvršenja kazne zatvora u prostorijama u kojima osuđeni stanuje (kućni zatvor) i nadzor nad uslovno otpuštenim licem.

U pogledu kućnog pritvora, ako sud donese odluku da se ta mera izvršava uz primenu elektronskog nadzora, oprema za elektronski nadzor aktivira se odmah posle dostavljanja odluke suda o primeni mere kućnog pritvora. Uređaj za lociranje okrivljenog (odašiljač sa pratećom opremom), koji je neškodljiv po zdravlje, postavlja stručno lice, koje pri tome daje potrebno uputstvo okrivljenom o načinu rada uređaja. Poverenička služba upravlja i uređajem kojim se daljinski prati kretanje okrivljenog i njegov položaj u prostoru (član 17. st. 4. i 5. ZIVSIM).

Kad je u pitanju kućni zatvor, u slučaju da sud odredi da se izvršenje te sankcije sprovodi sa primenom mere elektronskog nadzora, primenu sprovodi Poverenička služba, u saradnji sa policijom. Postavljanje uređaja za lociranje osuđenog (odašiljač sa pratećom opremom) obavlja se na isti način kao i u slučaju izvršenja mere kućnog pritvora sa elektronskim nadzorom (član 22. ZIVSIM).

Elektronski nadzor je moguće uspostaviti i prilikom vršenja poslova nadzora nad izvršenjem mera određenih uz uslovni otpust. U slučaju da je sud doneo odluku o uslovnom otpustu kojom je odredio da je osuđeni dužan da ispuni obaveze predviđene krivičnopravnim odredbama uz primenu elektronskog nadzora, elektronski nadzor ne može trajati duže od jedne godine, niti duže od trajanja uslovnog otpusta. Na primenu elektronskog nadzora shodno se primenjuju odredbe ZIVSIM kojima se uređuje izvršenje kućnog zatvora sa elektronskim nadzorom (član 46. ZIVSIM).

U cilju unapređenja tehničkih kapaciteta, 2019. godine zaključen je ugovor o novom sistemu elektronskog nadzora, tako da je do kraja 2020. godine, nabavljeno 3000 jedinica za elektronsko praćenje[18]. Na taj način je prevaziđen inicijalni deficit uređaja, što je bio

[17] Zakon o izvršenju vanzavodskih sankcija i mera (*Službeni glasnik RS*, br. 55/2014 i 87/2018).

[18] Radni tekst Strategije razvoja sistema izvršenja krivičnih sankcija u Republici Srbiji za period 2021-2027. godine, dostupno na: https://www.mpravde.gov.rs/tekst/33173/

jedan od primarnih generatora povećanja broja predmeta koji čekaju na izvršenje, a koji je 2019. iznosio oko 1.000 (Kolaković-Bojović, Batrićević i Matić-Bošković, 2022: 26).

Još jedan od ključnih problema u pogledu tehničkih kapaciteta Povereničke službe, ogledao se u činjenici da Uprava nije posedovala jedinstveni informacioni (case management) sistem. Ovo se višestruko negativno odražavalo na rad Povereničke službe, budući da su prikupljanje i obrada statističkih podataka a time i praćenje statističkih parametara bili značajno otežani. Pored toga, potpuna centralizacija poslovnih procesa podrazumevala je da se kompletna komunikacija i razmena dokumenata u procesu izvršenja vanzavodskih sankcija i mera odvija putem pošte i elektronske pošte, usled čega je bio nemoguć pregled stanja u realnom vremenu (Kolaković-Bojović, Batrićević i Matić-Bošković, 2022: 26). S tim u vezi, u okviru novog jedinstvenog informacionog sistema Uprave u delu izvršenja vanzavodskih sankcija i mera učinjen je značajan napredak u vođenju evidencija, dosijea i promena u izvršenju, što će u mnogome olakšati rad poverenika u administrativnom delu[19].

Na kraju se treba osvrnuti na jednu vanzavodsku sankciju koja se ne nalazi u režimu mogućeg elektronskog nadzora – uslovna osuda sa zaštitnim nadzorom. U pitanju je krivična sankcija koja se nažalost, prema zvaničnim statističkim podacima, veoma retko izriče, iako bi je trebalo smatrati jednom od osnovnih vanzavodskih krivičnih sankcija s obzirom na načelni potencijal koji ima. Podaci o njenom izricanju i izvršenju u periodu od 2015. do 2020. godine su poražavajući. Naime, u periodu od 2015. do 2017. godine, izricano je do 30 uslovnih osuda sa zaštitnim nadzorom, da bi se pozitivan trend javio u periodu 2017-2019. Pad tokom 2020. godine je u skladu sa padom broja predmeta i zastojima u radu pravosuđa uzrokovanim pandemijom COVID 19 (Kolaković-Bojović, Batrićević i Matić-Bošković, 2022: 44). Poverenici koji su u praksi sprovodili nadzor nad ovom merom, izrazili su mišljenje da uslovna osuda sa zaštitnim nadzorom na adekvatan način utiče na pozitivne promene u ponašanju osuđenih lica, te da je korektivni efekat ove sankcije veći nego kod ostalih vanzavodskih sankcija i mera ali su takođe istaknuti i problemi koji poverenicima otežavaju ili sasvim onemogućavaju efektivan nadzor nad izvršenjem ove mere (Kolaković-Bojović, Batrićević i Matić-Bošković, 2022: 45).

Iako su prisutni mnogobrojni problemi koji se ističu u sprovođenju uslovne osude sa zaštitnim nadzorom, u literaturi se mogu pronaći neka rešenja za poboljšanje primene ove sankcije a koja su zasnovana na upotrebi digitalne tehnologije. U pitanju je praksa prisutna u Sjedinjenim Američkim Državama a tiče se upotrebe kioska za prijavljivanje osuđenika kao vid elektronskog izveštavanja koji smanjuje potrebu da se prestupnik sa niskim rizikom sastane licem u lice sa službenikom za uslovnu kaznu odnosno poverenikom. Kiosk identifikuje osuđenika koristeći biometrijske mere (skeniranje otiska dlana ili prsta) i od njega se traži da da informacije o kojima bi obično razgovarao sa poverenikom (Ahlin, Hagen, i Crosse, 2016: 688). Informacije o ispitanicima uključuju podatke o mestu

strategija-razvoja-sistema-izvrsenja-krivicnih-sankcija-u-republici-srbiji-za-period-2021-2027-godina.php [14.10.2022.].

[19] Radni tekst Strategije razvoja sistema izvršenja krivičnih sankcija u Republici Srbiji za period 2021-2027. godine, dostupno na: https://www.mpravde.gov.rs/tekst/33173/strategija-razvoja-sistema-izvrsenja-krivicnih-sankcija-u-republici-srbiji-za-period-2021-2027-godina.php [14.10.2022.].

stanovanja i radni status kao i eventualne nedavne kontakte osuđenika sa sistemom krivičnog pravosuđa (npr. hapšenja). Mnogi kiosci takođe dozvoljavaju osuđenicima da plaćaju račune i kazne deponovanjem sredstava u bezbednu kutiju za zaključavanje pričvršćenu za kiosk mašinu. Nakon što ispitanik odgovori na tražena pitanja, kiosk se može programirati da izda potvrdu za posetu i da pruži obaveštenje osuđeniku da se prijavi na test na drogu ili da poseti poverenika kada je to neophodno (Ahlin, Hagen, Harmon & Crosse, 2016: 690). Na ovaj način se poverenički sistem rasterećuje u pogledu niskorizičnih osuđenika a resursi usmeravaju više ka kontroli visokorizičnih osuđenika.

ZAKLJUČAK

Nekolike značajne promene su usledile poslednjih godina u sferi digitalizacije sistema izvršenja krivičnih sankcija i mera. Jedna od njih je uvođenje jedinstvenog informacionog sistema u čitavoj Upravi što predstavlja izuzetno bitan korak ka povezivanju svih aktera krivičnog progona ali istovremeno to ima značaj i za efikasnije funkcionisanje kako same Uprave tako i njenih delova: zavoda za izvršenje krivičnih sankcija i Povereničke službe.

U zavodima za izvršenje krivičnih sankcija digitalizacija nalazi svoje mesto već dugi niz godina, kroz sve modernije sisteme kontrole i nadzora kako njenih stanovnika - lica lišenih slobode tako i svih ostalih koji po nekom osnovu borave u zavodu. Napredak u digitalizaciji je ovde naročito vidljiv, pa tako polako ali sigurno tehnika postaje dominantan činilac u obezbeđivanju zavoda odnosno održavanju reda i bezbednosti u njima. Ipak, bez obzira na sve sofisticiranija digitalna rešenja, njima upravlja čovek, koji i dalje ostaje osnovni faktor održavanja reda i bezednosti u zavodima. U svakom slučaju moderna tehnologija značajno olakšava kompleksan posao pripadnika službi za obezbeđenje u različitim zavodima a naročito u zavodima zatvorenog tipa sa posebnim obezbeđenjem.

Jedno od najznačajnijih polja primene digitalne tehnologije u sistemu izvršenja krivičnih sankcija je u okviru procesa resocijalizacije osuđenika. Prednosti digitalizacije treba iskoristiti u korist osuđenika kako bi se na najbolji mogući način pripremili za život na slobodi koji je u velikoj meri digitalizovan. Iako na prvi pogled davanje „privilegija“ osuđenicima kroz upotrebu digitalnih uređaja mnogim građanima deluje kao luksuz koji ne bi smeo da se praktikuje, u današnje vreme nikako se to ne može smatrati luskuzom već važnim delom života osuđenika. Pandemija korona virusa je otkrila dve važne stvari: pokazala je koliko je važno prilagoditi se novonastalim i nepredvidivim okolnostima ali je ukazala i na važnost digitalnog opismenjavanja pojedinaca. Takav zaključak bi morao da se primeni i u odnosu na osuđenike kojima se mora dati prilika da pod kontrolom neka svoja prava ostvare digitalnim putem.

U pogledu izvršenja vanzavodskih sankcija i mera takođe je jasan značaj digitalizacije za efikasnije funkcionisanje tog sistema. Pored šire primene elektronskog nadzora, treba razmisliti i o nekim drugim modalitetima digitalizacije u ovom segmentu, koji bi možda konačno podstakli značajnije korišćenje alternativa kazni zatvora, nego što je to slučaj u ovom trenutku.

LITERATURA

1. Ahlin, E.A., Hagen, C.A., Harmon, M.A. & Crosse, S. (2016) „Kiosk Reporting Among Probationers in the United States", *The Prison Journal,* 96(5), 688-708.
2. Ilić, A. (2022) *Komentar Zakona o izvršenju krivičnih sankcija*. Beograd: Službeni glasnik.
3. Kovaćević-Lepojević i Žunić-Pavlović (2012) „Primena video-nadzora u kontroli kriminala", *Specijalna edukacija i rehabilitacija*, 11(2), 325-345.
4. Kolaković-Bojović, M., Batrićević, A. i Matić-Bošković, M. (2022) *Analiza uticaja primene alternativnih sankcija i mera u Republici Srbiji u period od 2015. do 2020. godine*. Beograd: Institut za kriminološka i sociološka istraživanja i misija OEBS u Srbiji.
5. Mufarreh, A., Waitkus, J. & Booker, T.A. (2022) „Prison Officials Perception of Technology in Prison", *Punishment & Society,* 24(3), 410-432.
6. Finkel, M. & Bertram, W. (2021) "More states are signing harmful "free prison tablet" contracts", Prison Policy Initiative. Available at: https://www.prisonpolicy.org/blog/2019/03/07/free-tablets/ [11.10.2022].
7. Hadlington, L. & Knight, V. (2022) „Public Acceptability of Prisoners'Access and Use of Digital Technologies in the UK", *The Prison Journal*, 102(2), 237–255.

Pravni i drugi izvori

1. Strategija razvoja sistema izvršenja krivičnih sankcija u Republici Srbiji do 2020. godine (*Službeni glasnik RS*, br. 114/2013).
2. Strategija razvoja sistema izvršenja krivičnih sankcija u Republici Srbiji za period 2021-2027. godine, dostupno na: https://www.mpravde.gov.rs/tekst/33173/strategija-razvoja-sistema-izvrsenja-krivicnih-sankcija-u-republici-srbiji-za-period-2021-2027-godina.php [14. 10.2022.].
3. Zakon o izvršenju vanzavodskih sankcija i mera (*Službeni glasnik RS*, br. 55/2014 i 87/2018).
4. Zakon o izvršenju kazne zatvora za krivična dela organizovanog kriminala (*Službeni glasnik RS*, br. 72/2009 i 101/2010).
5. Zakon o izvršenju krivičnih sankcija (*Službeni glasnik RS*, br. 55/14 i 35/19).
6. Pravilnik o načinu obavljanja poslova u službi za obezbeđenje u zavodima za izvršenje krivičnih sankcija (*Službeni glasnik RS*, br. 21/2016 i 104/2016).
7. Pravilnik o uniformi, oznakama, naoružanju, specijalnim vozilima i drugoj opremi u Službi za obezbeđenje u Upravi za izvršenje krivičnih sankcija (*Službeni glasnik RS*, br. 29/2016, 74/2016, 3/2017, 89/2017 i 7/2019).
8. Vijesti online (12.04.2013) *Play Station zabranjen u zatvoru, Xbox nije*, https://www.vijesti.me/vijesti/280932/play-station-zabranjen-u-zatvoru-xbox-nije [15.10.2022].
9. Vlada Republike Srbije – Saopštenje Ministarstva pravde (10.08.2020) Osuđenici koriste „Skajp" i „Viber" za kontakt sa porodicom tokom pandemije https://www.

srbija.gov.rs/vest/482074/osudjenici-koriste-skajp-i-vajber-za-kontakt-sa-porodicom-tokom-pandemije.php [10.10.2022.].

10. Vlada Republike Srbije – Saopštenje Ministarstva pravde (13.05.2021.) *Okružni zatvor u Beogradu dobio savremenu monitoring opremu* https://www.srbija.gov.rs/vest/545005/okruzni-zatvor-u-beogradu-dobio-savremenu-monitoring-opremu.php [12.10.2022.].

DIGITALIZATION IN THE SYSTEM OF EXECUTION OF CRIMINAL SANCTIONS IN THE REPUBLIC OF SERBIA

In the paper, the authors consider the use of modern technology in various aspects of the system of execution of criminal sanctions in the Republic of Serbia. On the one hand, the different forms of digitalization present in institutions for the execution of criminal sanctions are analyzed, where prison sentences and other criminal sanctions of an institutional nature are carried out, as well as the measure of detention, which is a measure to ensure the presence of the accused and the smooth conduct of criminal proceedings. In this regard, the authors analyze the differences in the use of advanced technology in the control of prisoners that exist in different prisons, taking into account the division of prisons according to the level of security. The authors start from the assumption that the most advanced type of digitalization is present in closed type prisons with special security (supermax prisons) in which prison sentences are served by persons convicted of the most serious crimes, including persons serving prison sentences in accordance with the Law on Execution of Prison Sentences for Organized Crime. On the other hand, the authors consider the issue of digitalization in the execution of non-custodial sanctions and measures with an emphasis on those sanctions and measures where the application of electronic surveillance comes into play, such as house arrest or house prison. In connection with all the mentioned aspects of digitalization in the system of execution of criminal sanctions of the Republic of Serbia, the authors analyze the available statistical and other data, all with the aim of critically analyzing the current situation and defining possible proposals for improving the situation.

KEYWORDS: *digitalization, execution, criminal sanctions, measures, convicts, prisons.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.15

A REVIEW OF THE EFFICIENCY OF JUSTICE AND OTHER ELEMENTS OF THE 2022 – 2025 CEPEJ ACTION PLAN: "DIGITALISATION FOR A BETTER JUSTICE"

Marko Novaković*

CEPEJ (European Commission for the Efficiency of Justice) on the 20th anniversary of its work adopted the Action plan for the period 2022-2025 named "Digitalisation for a better justice". Digitalisation has been playing an increasingly important role in the justice system in recent years, but its significance erupted during the COVID-19 pandemic. Since digitalization is our present but even more our future, CEPEJ rightfully decided to focus its Action plan on this aspect of the judiciary. The author will review all aspects of the CEPEJ action plan, but the focus will remain on the efficiency of justice. One of the main conclusions is that the digitalisation of justice is an absolute necessity and all stakeholders should put it among their priorities (in a similar manner as CEPEJ did) but the process of digitalization should be conducted diligently and with proper assessment of its effects. Otherwise, digitalization might have the opposite effect in many areas of society, even leading to the denial of justice.

KEYWORDS: *CEPEJ, Digitalisation, Justice, Efficiency, judges,*

* PhD, Senior Research Fellow, Insitute of International Politics and Economics, Belgrade.
E-mail: *marko@diplomacy.bg.ac.rs*

INTRODUCTION

At the 37th CEPEJ (European Commission for the Efficiency of Justice) plenary meeting, which was held on 8 and 9 December 2021 both on-site in Strasbourg in person and online, CEPEJ has adopted an Action plan for the period 2022 – 2025 regarding digitalization in justice (CEPEJ, 2021). This adoption occurred on the 20th anniversary of CEPEJ, which was a good reminder that CEPEJ's work includes numerous guidelines and tools, including 15 on mediation, 16 on quality and efficiency, 5 on e-justice; more than 20 groups of indicators based on more than 300 questions also make it possible to better evaluate European judicial systems, but also well beyond. CEPEJ relevance in this field stems from its history, transparent methodology of work, and wide membership – which will be briefly revisited in the following chapter.

1. HISTORY AND CEPEJ MEMBERS

The European Commission for the Efficiency of Justice (CEPEJ) was established 20 years ago, on September 18th, 2002 (Res 2002). In the quest for improving the rule of law and fundamental rights in Europe, the efficiency of justice plays a crucial role. Hence, the aim of the CEPEJ is set as a two-folded task: on the one side is "to improve the efficiency and the functioning of the justice system of member states, with a view to ensuring that everyone within their jurisdiction can enforce their legal rights effectively, thereby generating increased confidence of the citizens in the justice system" and on the other "to enable a better implementation of the international legal instruments of the Council of Europe concerning efficiency and fairness of justice" (Statute of the CEPEJ, Article 1).

However, in order to achieve goals, any organization has to determine methods and steps that will lead to the accomplishment of its (predetermined) objectives. CEPEJ is no different and already in its Statute, concrete methods for reaching goals were set. Those methods are:

1) identifying and developing indicators, collecting and analyzing quantitative and qualitative data, and defining measures and means of evaluation;
2) drawing up reports, statistics, best practice surveys, guidelines, action plans, opinions, and general comments;
3) establishing links with research institutes and documentation and study centers;
4) inviting to participate in its work, on a case-by-case basis, any qualified person, specialist, or non-governmental organization active in its field of competence and capable of helping it in the fulfillment of its objectives, and holding hearings;
5) creating networks of professionals involved in the justice area (Statute of the CEPEJ, Article 3).

The creation of the CEPEJ demonstrates the will of the Council of Europe to promote the rule of law and fundamental rights in Europe, on the basis of the European Convention on Human Rights, and especially its Articles 5 – Right to liberty and security, 6 – Right to a fair trial, 13 – Right to an effective remedy, 14 – Prohibition of discrimination (CEPEJ – About the CEPEJ). The Council of Europe has initiated a reflection on the efficiency of justice and adopted Recommendations that contain ways to ensure both its fairness and efficiency. The establishment of CEPEJ, which is ensured by the Directorate General of Human Rights and Legal Affairs, shows the intention of the Council of Europe not only to elaborate international legal instruments but also to promote a precise knowledge of the judicial systems in Europe and of the different existing tools which enables it to identify any difficulties and facilitate their solution (*Ibid.*). The CEPEJ will have, among other duties, the task of continuing the ongoing reflection about the potential offered by new information technologies (IT) to improve the efficiency of justice. The functioning of the CEPEJ is governed by its Statute (Statute of the CEPEJ).

2. CEPEJ METHODOLOGY

CEPEJ is constantly working on improving its own methodology. These kinds of methodological reassessments are necessary, if CEPEJ, or any other organization for that matter, wants to stay relevant and fulfill its purpose effectively in the ever-changing world. In the Action plan "Digitalisation for a better justice", the following improvements in the CEPEJ methodology were proposed:

1) Giving more importance to networking and exchange of good practices;
2) Better in-house co-ordination at the Council of Europe: the Department for the Execution of judgments of the ECHR and the ECHR could use the CEPEJ indicators while providing the CEPEJ with useful information on dysfunctions within the judicial systems of the member states, the CAHAI for questions on artificial intelligence, the CDCJ and CDPC for coordination on the respective tools concerning the field of justice, etc.;
3) Ensuring synergies between CEPEJ intergovernmental activities and cooperation activities, as well as between cooperation activities (2022 – 2025 CEPEJ Action plan).

As we can see, the second proposed methodology improvement is the only mythological improvement *stricto sensu*. The first one is just emphasizing networking and the exchange of good practices. This is the aspect of CEPEJ work that is always one of the focuses but this emphasis obviously indicates the need to increase effort in that area, while the third one is focused on the synergy between CEPEJ's activities.

3. CEPEJ MEMBERS

The CEPEJ is a forum of experts with expertise in various fields in line with the CEPEJ Statute. Every Council of State member State (there are 46 of them currently) is represented by experts. Overall administration and assistance to the experts are provided by a CEPEJ Secretariat. Apart from them, observers are also *de facto* members of CEPEJ. Currently, observers' statuses have Holy See, Canada, Japan, Mexico, United States of America (CEPEJ – Map & Members). On top of that, the Committee of Ministers granted observer status to the additional five countries: Guatemala, Israel, Kazakhstan, Morocco, and Tunisia (CEPEJ – About the CEPEJ).

Apart from states, the following international organizations, and institutions representing judicial professionals, as well as partners have the status of observers of the CEPEJ: European Union (EU), Council of the Bars and Law Societies of Europe (CCBE), Council of the Notariat of the European Union (CNUE), European Union of Rechtspfleger and court Clerks (EUR), European networks of Councils for the Judiciary (ENCJ), European Association of Judges (EAJ), Association of European administrative judges (AEAJ), European Judicial Training Network (EJTN), European Expertise and Expert Institute (EEEI), International Union of Judicial Officers (UIHJ), Organisation for Economic Co-operation and Development (OECD), *Magistrats européens pour la Démocratie et les Libertés* (MEDEL) and World Bank (*Ibid.*).

4. ELEMENTS OF THE CEPEJ ACTION PLAN FOR DIGITALISATION

Acting in accordance with its Statute which provided that "The use of information and communication technologies shall be promoted in order to strengthen the efficiency of justice, in particular in order to facilitate access to justice, speed up court proceedings, improve the training of legal professionals, as well as the administration of justice and management of courts" (Statute of the CEPEJ) the CEPEJ created an Action plan for digitalization that is the topic of this paper. To accompany the ongoing digitalisation of judicial systems, while always ensuring that justice is human, efficient and of high quality, the CEPEJ should take into account the following orientations:

4.1. Efficiency of justice

The main focus of this article is the first "orientation" that was listed in the Action plan – Efficiency of justice. The efficiency of justice should be achieved through "Supporting digitalization of the administration and management of courts/ prosecution services. The transition from paper to digital court files is ongoing and necessary. Also, the administration of justice must use information technology to optimize its operations, as well as the interconnection links between the various judicial institutions. It is necessary to ensure that the tools chosen by States and courts are the most appropriate

and compatible with quality, efficient, accessible, and impartial justice. The digitalisation of procedures must improve their efficiency, but also the quality of the work to be carried out by judges, prosecutors, the teams assisting them, and lawyers" (2022 – 2025 CEPEJ Action plan).

The court systems throughout the world are notorious for their lack of adaptability to new technologies, often justifying this reluctance to engage in an overhaul of digitalization as concern for privacy and prevention of disinformation (Eltis, 2011). However, most of those claims and concerns were based on scenarios in which digitalization of court proceedings would create an infringement of somebodies rights, while in reality, no clear argument against digitalisation as a general process was demonstrated. Despite this reluctance, court systems throughout the world were forced to accept numerous virtual and digital solutions in order to continue with their work during COVID19 pandemic since reduced activities in courts and lockdown measures have an impact on court operations. The majority of countries were looking for solutions that would limit interaction with courts and suspension of non-urgent cases was one of the applied measures. To enable the functioning of the courts, countries where the level of information technology development allowed introduced modalities of online hearings and/or other use of modern technologies during proceedings like electronic filing. The promotion of alternative dispute resolution and court settlement was also a tool used in some of the countries (Matić Bošković & Novaković, 2021, pp. 188-201). However, in that small sample more digitalized justice system, while general access to justice is improved by virtual courts there was one major exception – it did not help the people that do not have access to the internet, computers on technology in general.

While this concern might seem like an exaggeration in what seems like a more digitalized world, the magnitude of that problem can be grasped only once actual data and information are inspected and elaborated. The International Telecommunication Union's (ITU) statistics shed an important light and perception on the prospects of digitalization and important consideration regarding current possibilities and potential issues. According to the International Telecommunication Union's estimate of 2.7 billion people unconnected compares with an updated estimate of 3 billion people unconnected worldwide in 2021. This demonstrates that digitalization is not a linear process and it should consider and adjust to trends in order to avoid denial of justice. The problem and aspects to consider are not only the sheer number of "connected" people but also its distribution.

In 2019, prior to the COVID pandemic, an estimated 3.6 billion people, or nearly half the world's population, were unconnected. Globally, the number of Internet users grew by 7 percent, and the share of individuals using the Internet – grew by 6 percent between 2021 and 2022 (International Telecommunication Union, 2022). However, growth is unevenly distributed across regions. Areas with a low share of individuals using the Internet have achieved the fastest growth over the past year – following a typical diffusion pattern for new and emerging technologies. Africa, the least connected of ITU's six world regions, achieved 13 percent year-on-year growth in the share of individuals using

the Internet. Today, 40 percent of the population in Africa is online. The Arab States showed robust growth, with the Internet now reaching 70 percent of the population. In Asia and the Pacific, Internet penetration grew from 61 percent in 2021 to 64 percent in 2022, relative to the region's population. The Americas, the Commonwealth of Independent States, and Europe each achieved 3 percent growth, with more than 80 percent of the population online in each region while Europe remains the most connected region globally, with 89 percent of its population online.[1] The COVID-19 outbreak also has an impact on the exercise of procedural rights of suspects and accused persons. Direct communication with lawyers, interpreters, or with third persons (while the suspects or accused persons are deprived of liberty) is more difficult. In the Netherlands, stakeholders have raised concerns about the effective safeguarding of the right to a fair trial and quality of justice during COVID pandemic (The Netherlands Committee of Jurists for Human Rights, 2020), since the prosecution service has announced plans to make an increased use of its power to decide itself on certain criminal cases.[2] This could have an impact on the right to a fair trial if citizens are not adequately informed.

Research conducted in smaller regions but in more detail also confirms this disparity. A good example is a rather comprehensive research on this topic that has been conducted by Pew Research Center in the USA, which demonstrates some alarming data regarding racial and social disparities (Pew Research Center, 2020). Pew Research Center reported on the results of the disparity in access to computers and broadband connections at home. According to their research, about eight-in-ten whites (82%) report owning a desktop or laptop computer, compared with 58% of blacks and 57% of Hispanics. There are also substantial racial and ethnic differences in broadband adoption, with whites being more likely than either blacks or Hispanics to report having a broadband connection at home. There were not enough Asian respondents in the sample to be broken out into a separate analysis (Matić Bošković & Novaković, 2021, pp. 181-201). When it comes to social disparity, roughly two-thirds of rural Americans (63%) say they have a broadband internet connection at home, up from about a third (35%) in 2007, a Pew Research Center survey conducted in early 2019 concluded (*Ibid.*). Rural Americans are now 12 percentage points less likely than Americans overall to have home broadband; in 2007, there was a 16-point gap between rural Americans (35%) and all U.S. adults (51%) on this question (*Ibid.*). Finally, Pew Research Center reported that disabled Americans are about three times as likely as those without a disability to say they never go online (23% vs. 8%), according to a Pew Research Center survey conducted in the fall of 2016. When compared with those who do not have a disability, disabled adults are roughly 20 percentage points less likely to say they subscribe to home broadband and own a traditional computer, a smartphone, or a tablet (*Ibid.*).

Some concerns regarding achieving universal connectivity were emphasized by the ITU as it was presented in this chapter. While two-thirds of the world can be considered connected, bringing the remaining one-third of humanity online presents a

[1] Share of individuals using the Internet.

[2] Such decisions by the prosecution service cannot impose a prison sentence and can be contested in court.

daunting task. The hardship lies in the fact that most of those still offline generally live in remote, hard-to-reach areas (International Telecommunication Union, 2022). It also has to be considered that there is a difference between basic and meaningful connectivity. Transferring to meaningful connectivity in which people not only have ready access to the Internet but are able to use it regularly and effectively to improve their lives – is even more challenging (*Ibid*.) since the absolute number of people with internet access will be naturally remedied to a point through continuous urbanization process at least to a point. ITU has listed a useful and exhaustive (but not complete) list of barriers in that quest for global, useful connectivity that includes: slow Internet speed; limited affordability of hardware and subscription packages; inadequate digital awareness and skills; and linguistic and literacy barriers, as well as issues like gender discrimination or the lack of reliable a power source. All these need to be addressed if everyone is to enjoy equitable access to online resources (International Telecommunication Union, 2022).

4.2. Transparency of justice

CEPEJ will stem towards more transparent justice through "*Promoting digitalisation to improve knowledge on justice in general, in particular on the length of proceedings. New technologies must provide users with better knowledge of procedures, judicial institutions and the respective roles of each of the justice professionals. Each court must have dashboards enabling it to monitor and manage its case flow; this makes it possible to identify and limit potential backlogs, to respect reasonable timeframes, and to better manage the workload of justice professionals*" (2022 – 2025 CEPEJ Action plan).

Despite the fact that it deals with a very important topic, this point hardly deserves a special place in this Action plan. On the one side, it is too vague and provides a rather strict formulation that digitalization must provide users with better knowledge of procedures. It would be more rational to state that digitalization should enable users to understand the procedure better since ultimately, it is on users themselves to decide whether will use it to acquire more knowledge on any matter. On the other hand, the provision that "each court must have dashboards enabling it to monitor and manage its case flow" (*Ibid*.) is too specific and does not leave space to consider the financial restrictions of many courts and provides pointless limitations for more technically advanced countries, where monitoring and managing case-flow might be conducted in a more advanced way.

4.3. Collaborative justice

Another interesting part is named "collaborative justice" and it encompasses setting up relevant digital tools for interconnectivity between participants in the judicial proceedings (judges, prosecutors, lawyers, other justice professionals, and users). All justice professionals contribute to the same public service, that of justice at the service of the user; they must therefore have easy-to-use, compatible, and efficient communication tools (*Ibid*.)

There are numerous perspectives and views stating that access to justice will be substantially improved by the digitalization of the court and the justice system in general. Virtual courts are seen as one of the main tools to connect justice participants. Some research, even before the COVID-19 pandemic supported this. The experiment conducted by the Montana Legal Services Association has included tests of court appearances by video, staff, and continuing legal education training, meetings, client interviews, mediation, and client self-help clinics. Data includes observation and surveys. The overall conclusion is that the use of video makes a contribution to access to justice (Zorza, 2007, 1, 3). Even earlier, in the late XX century, Even Lederer was contemplating virtual courtrooms, he emphasized that "…we may well be able to substantially enhance access to justice for those who today have little or no access at all. (Lederer, 2018)". While virtual courtrooms are just the first step and a small part of the digitalization of justice – it comes with the same potential issues if not implemented properly as the ones that were presented in the part regarding the efficiency of justice.

4.4. Human and People-centered justice

The human-centered justice part focuses on adequate support of the judges, prosecutors, their teams, and all other justice professionals to help them adapt their essential roles to the digital environment. In its, rather short, elaboration, the focus is given to two aspects. The first one is positive and proclaims the rising efficiency of justice as the main goal of digitalization. However, in the same sentence, a sort of disclaimer is made that, despite digitalization, judges shall remain central figures of the judicial procedures and that digitalization must never seek to replace the judge (2022 – 2025 CEPEJ Action plan).

The second one named people-centered justice is closely correlated with the previous one. The efficiency of justice is revisited again, in the context of digitalization, but this time with more focus on users and justice professionals. *Supporting justice professionals and users with training in order to make full use of digital tools. The training of justice professionals, including lawyers, in the process of digital transformation, is vital because it contributes not only to the efficiency of justice but also to the independence of justice, in that it allows them to act with full knowledge of the law and procedures. Users who so wish should be supported in this digital environment, in particular by training sessions, but proficiency in these digital tools cannot become a condition for access to justice.*

Educating judges in a digital context means just that – adapting them to the digital environment. This is not only desirable but absolutely necessary. There is no doubt that it is more pressing to conduct this education regarding more senior judges, the ones that did not grow in a digital age, and they are the vast majority today, in 2022. This situation will remedy itself to a certain degree in time,[3] but in the current times, some researchers noted that questions such as "…whether judges and lawyers are culturally and mentally ready for the delivery of justice outside a brick-and-mortar courtroom once

[3] With more members of younger generations that grew up in digital world are becoming judges, a higher level of general digital literacy is expect.

the emergency is over" (Fabri, 2021, p. 2). The level of digital literacy will be an ever-expanding endeavor, since more and more cases will have digital aspects as a part of it, and judges will need to have more understanding of technology than simply use of the computers and court systems (Brookings Institution, 2019).

With that in mind, educating upcoming generations of judges early in their careers is very important. This education should encompass not only digital tools used in courts but particularly educating them to understand more complex digital aspects of crimes. This ability to understand and analyse digital aspects of crimes will be crucial for their ability to deliver justice, as more and more crimes have digital dimensions and crimes related to the digital world are getting more complex every day.

4.5. Informed Justice and Responsible and reactive CEPEJ

Finally, the last two points in the report are related to informed justice (*increasing the use of the results of the CEPEJ evaluation of judicial systems and other tools. To increase the visibility, understanding; and use of the results of the evaluation exercise, CEPEJ should provide more analyzed information and respond to other requests for specific analyses whenever possible* (2022 – 2025 CEPEJ Action plan) and responsible and reactive CEPEJ (*ensure the visibility of its tools so that they are accessible to all and reflect the expertise of those who developed them The CEPEJ is at the service of justice professionals and users, who can ask, to create specific tailored tools, for a better justice. Its mission is to use all of the expertise at its disposal to answer their request promptly, concretely and efficiently* (*Ibid* .).

Those actions are formulated in relation to CEPEJ – on the one side to promote and direct the usage of CEPEJ work by others and on the other to clarify actions that should be taken by CEPEJ to improve its visibility. While those points need to be further elaborated and might be a more natural part of the "methodological" section of the Action plan, one has to commend CEPEJ for constantly reassessing itself and striving to improve its work and adjust it to the needs of the ever-changing world.

CONCLUSION

Most widely known for its reports on the efficiency and quality of justice in Europe, the CEPEJ helps to ensure that the public service of justice is efficient, accessible, and of better quality, by placing the needs of the user at the center of the judicial process. The CEPEJ's expertise includes numerous guidelines and tools for courts and justice professionals, including 16 on quality and efficiency, 15 on mediation, and 5 on e-justice; more than 20 groups of indicators based on more than 300 questions also allow for a better evaluation of judicial systems. The ongoing and future work of the CEPEJ is part of the action plan 2022-2025 dedicated to "digitalisation for a better justice".

The action plan for 2022-2025 – "Digitalisation for a better justice" puts digitalisation in a center of attention – and rightfully so. Digitalisation is not an option, it is a

prerequisite for justice in modern times. However, a diligent analysis is necessary for its introduction in any part of justice – and the pace of its implementation can differ from region to region and even from court system to court system. If it is not conducted in that manner, a noble quest to improve efficiency and other aspects of justice via digitalization can backfire and endanger primarily the ones who need the justice system the most – low-income citizens and the underprivileged groups.

REFERENCES

1. 2022 – 2025 CEPEJ Action plan: "Digitalisation for a better justice". Adopted at the 37th CEPEJ plenary meeting Strasbourg and online, 8 and 9 December 2021. Available at: https://rm.coe.int/cepej-2021-12-en-cepej-action-plan-2022-2025-digitalisation-justice/1680a4cf2c [06. 09. 2022].
2. CEPEJ – About the CEPEJ. Available at: https://www.coe.int/en/web/cepej/about-cepej [05.09.2022].
3. CEPEJ – Map & Members. Available at: https://www.coe.int/en/web/tbilisi/the-coe/objectives-and-missions#:~:text=46%20member%20countries%3A,of%20T%C3%BCrkiye%20in%20August%201949 [05. 09. 2022].
4. CEPEJ. 2021. 37th plenary meeting – Abridged report. Available at: https://rm.coe.int/cepej-2021-17-en-37-cepej-plenary-meeting-report-dec-2021/1680a4cf83 [05. 09. 2022].
5. Council of Europe, Resolution Res(2002)12 of the Committee of ministers establishing the European Commission for the efficiency of justice (CEPEJ). Adopted by the Committee of Ministers on 18 September 2002 at the 808th meeting of the Ministers' Deputies. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804ddb99 [05. 09. 2022].
6. Eltis, K. (2011) "The Judicial System in the Digital Age: Revisiting the Relationship between Privacy and Accessibility in the Cyber Context", *McGill Law Journal*, 56(2), 289-316. DOI: https://doi.org/10.7202/1002368ar.
7. Fabri, M. (2021) "Will COVID-19 Accelerate Implementation of ICT in Courts?" *International Journal for Court Administration*, 12(2), DOI: http://doi.org/10.36745/ijca.384.
8. Horowitz Menasce, J. Igielnik, R. and Kochhar, R. Pew Research Center, January 9, 2020, *Most Americans Say There Is Too Much Economic Inequality in the U.S., but Fewer Than Half Call It a Top Priority*, Available at: https://www.pewresearch.org/social-trends/2020/01/09/most-americans-say-there-is-too-much-economic-inequality-in-the-u-s-but-fewer-than-half-call-it-a-top-priority/ [06.09.2022].
9. International Telecommunication Union. Available at: https://www.itu.int/en/mediacentre/Pages/PR-2022-09-16-Internet-surge-slows.aspx [26. 9. 2022].

10. Lederer, F. I. (2018) "Improving Access to Justice via Technology", *Popular Media*. 427. Available at: https://scholarship.law.wm.edu/popular_media/427/ [26. 09. 2022].
11. Matić Bošković, M. and Novaković, M. (2021) "Adaptation of Judicial Systems to the Global Pandemic – a Short and Long-term Impact of COVID-19 on Judicial Systems", *John Marshall Law Journal*, XIV (2), 188-201.
12. Statute of the CEPEJ. Appendix 1 to Resolution Res(2002)12. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804ddb99 [05. 09. 2022].
13. The Netherlands Committee of Jurists for Human Rights. 2020. Letter on concerns about corona measures in criminal justice. Available at: https://njcm.nl/wp-content/uploads/2020/05/NJCM-brief-aan-minister-Grapperhaus-gewijzigde-aanhef.pdf [26.09.2022].
14. Whitney, M. How to improve technical expertise for judges in AI-related litigation Brookings Institution. Available at: https://www.brookings.edu/research/how-to-improve-technical-expertise-for-judges-in-ai-related-litigation/ [24. 09. 2022].
15. Zorza, R. 2007. Video Conferencing for Access to Justice: An Evaluation of the Montana Experiment, Legal Services Corporation. Available at: https://docplayer.net/3126017-Video-conferencing-for-access-to-justice-an-evaluation-of-the-montana-experiment-final-report.html [27.9.2022].

PREGLED EFIKASNOSTI PRAVOSUĐA I DRUGIH ELEMENATA AKCIONOG PLANA CEPEJ 2022-2025: "DIGITALIZACIJA ZA BOLJU PRAVDU"

Evropska komisija za efikasnost pravosuđa (CEPEJ) je na svoju dvadesetu godišnjicu rada usvojila Akcioni plan za period 2022-2025 pod nazivom "Digitalizacija za bolju pravdu".

Digitalizacija ima sve značajniju ulogu u pravosudnom sistemu poslednjih godina, ali je njen značaj povećan tokom pandemije izazvane virusom COVID-19. Pošto je digitalizacija kako naša sadašnjost, tako i budućnost, CEPEJ je opravdano odlučio da svoj Akcioni plan fokusira na oblast digitalizacije u pravosuđu.

U ovom radu autor razmatra aspekte CEPEJ Akcionog plana, ali je u najvećoj meri fokusiran na efikasnost pravosuđa. Jedan od osnovnih zaključaka u radu je da je digitalizacija pravosuđa neophodna i da bi svi akteri u toj oblasti trebalo da je posmatraju kao prioritet na sličan način na koji je to uradila Evropska komisija za efikasnost pravosuđa. Međutim, proces digitalizacije treba uspostavljati marljivo uz odgovarajuću procenu njenih efekata. U suprotnom digitalizacija bi mogla da ima negativan efekat u različitim društvenim oblastima, a mogla bi čak da doprinese i uskraćivanju pravde.

KLJUČNE REČI: *CEPEJ, digitalizacija, pravda, efikasnost, sudije.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.16

CHANGES OF CONFIDENTIALITY DUTY IN THE DIGITAL LEGAL ERA

Olga Sovova*
Miroslav Sova**

The article deals with the phenomenon of the third millennium, which is the onset of generalised digitalisation in the public and private spheres. The provision of legal services by the state or private persons, legal advisors, is not an exception. The use of social networks, the automated creation of contracts, blockchains, cloud repositories, virtual databases and various online conference platforms touch on the natural subtlety of the state administration, legal representatives and their relationship with clients. The paper examines the core of professional duties in legal services: the duty of confidentiality. The paper compares two types of confidentiality duty. The first one is the confidentiality duty of state officers, including judges. The second one is the attorney's professional duty. The paper highlights standard and general requirements for all professionals. Based on the author's experience as an attorney and university law teacher, the paper points out the risks and benefits of digitalisation in maintaining confidentiality obligations.

The paper argues that digital legal services and justice are an inevitable need for the new era of digitalisation. The paper concludes with proposals to comply with the requirements for protecting social and private interests when delivering digital legal services. The author uses the method of desk research and analysis of documents and practical examples.

KEYWORDS: *digitalisation, digital legal services, confidentiality duty, state administration, attorney, judge, desk research.*

* Associate Professor, Police Academy of the Czech Republic in Prague, CZ.

ORCID 0000-0001-9651-0686

E-mail: *sovova@polac.cz* • *olga.sovova@seznam.cz*

** Master of Information Technologies.

ORCID 0000-0002-9358-8362

INTRODUCTION

The third millennium, often labelled as the era of digitalisation, especially the COVID-SARS 19 pandemic (pandemic), offered new communication possibilities. Also, the public administration or private persons provided legal services moved to the online world. Social networks, automated creation of contracts, blockchains, cloud repositories, virtual databases and various online conference platforms touch on the natural subtlety of the public administration, legal representatives and their relationship with clients. In connection with their jobs and positions, public administration officers, employees, legal advisers and members of their teams get acquainted with private and sensitive information. High-ranking civil servants, officers in the army corps, and attorneys-at-law work with confidential information and know-how. So as part of their job, they must protect the information and communicate it to third persons only if the law provides it. That is why the confidentiality duty in various legal forms and regulations was imposed on them. In the last three years, the duty of confidentiality, privileged communication and information protection got new because of the possibilities mentioned above of digitalisation.

The paper highlights the mandatory confidentiality imposed on state officers and the professional confidentiality of the regulated helping professions. The author examines the relationship between the attorney and the client, including the communication privilege in the digital framework.

1. GENERAL REMARKS ON CONFIDENTIALITY AND PRIVACY

Theory and practice distinguish between the term "privacy" and "confidentiality". Privacy and its protection focus on acquiring information, while confidentiality focuses on communicating information; however, both concepts complement and overlap. The European concept of privacy and confidentiality aims at protecting a person's dignity. The doctrine and practice in the USA understand the right for privacy as a part of human liberty (Whitman, 2004).

Even though the legal entity has no right to privacy, keeping information about its activities confidential is core and inevitable. That is why the confidentiality duty applies to the knowledge about private and publicly owned legal entities.

The duty of confidentiality might be private, based on civil law regulations or mandatory, based on public law requirements.

Mandatory confidentiality serves in the legal order to protect societal and individual interests. Confidentiality could be defined as a legal institution, the task of which is to protect the legitimate interests of persons by the fact that another person, whether natural or legal, through its statutory bodies, employees or associates, does not disclose sensitive or private information. This obligation continues even after the end of the given job or profession.

The mandatory confidentiality violation can be punished even after the activity is no longer performed. The duty of confidentiality prevents the misuse of protected knowledge, so the holder cannot acquire unauthorised advantages in his job or business.

> *"The definition of confidentiality is not included in the Czech legal system, so it is necessary to base it on the general understanding of this concept. Confidentiality can be understood as the obligation of a specific natural person to act in such a way that the protected information ... is not learned by a third person who is not authorised to do so. Compliance with the obligation of confidentiality is primarily connected with the expected passivity of a specific natural person, his failure to act, or refraining from a specific action.* "(Janeckova, 2019: 216)

Despite the lack of legal definition mentioned above, the Czech legal order took two approaches to the confidentiality duty.

The first one is the mandatory confidentiality imposed by the state on its officers or other persons to protect the public interest.

However, the professional literature and practice are relatively inconsistent regarding what the state should consider mandatory confidentiality. Part of the practice and theory underlines that only the obligation to maintain confidentiality in the public interest forms this type of confidentiality. The duty of confidentiality of judges, public attorneys, tax or police officers forms one of the most critical obligations connected with their job positions, as they get acquitted with compassionate information. Some authors also consider obligations imposed by international treaties to be a particular type of mandatory confidentiality.

Obligatory confidentiality for members of regulated professions or clergy connected directly with information obtained in their job is then the state recognised confidentiality.

Only the person for whose benefit it is imposed can agree with disclosing information. Another authority, e.g. a superior or the court, may replace the consent of the person concerned. In some cases, mandatory confidentiality may be breached if the holder is exposed to the risk of criminal prosecution concerning the exercise of his profession. The possibility of providing information otherwise protected by mandatory confidentiality must be enshrined in law.

The law defines mandatory confidentiality by its material and personal scope. The personal scope of mandatory confidentiality refers to the designation of entities bound by confidentiality. The protected information forms its material scope.

Private confidentiality duty aims to cover business activities, like know-how, material procedures or contractual obligations and rights.

The Czech legal regulation differentiates between the rights and obligations imposed on the holder of the duty of confidentiality according to the legal nature of the duty. The law limits the protection of private confidentiality. Mandatory obligations enjoy a wide range of protective measures in public and private law, including procedural rights.

The confidentiality duty is imposed on the so-called regulated professions, like medical doctors, public notaries, or attorneys-at-law.

> *"Confidentiality is a fundamental attribute of the provision of legal services and duty that binds every attorney in all the steps he takes in the practice of law. Despite this, or precisely because of this, we have recently noticed repeated attempts to break or limit lawyer confidentiality duty.* (Kejhova & Rydlova, 2019)

2. DUTY OF CONFIDENTIALITY IN THE DIGITAL ERA

2.1. Confidentiality duty and reporting obligations

Working with information is one of the fundamental areas of activities within legal services. The main switch is connected with the introduction of artificial intelligence in daily practice, as contemporary society is based on technologies and knowledge. Modern technologies enable a much more service user-oriented approach and complete access to data sharing. Files are kept either in paper or electronic format. The case documentation is mainly kept in both formats.

Protecting personal data and providing information about a case is the most critical legal services challenge. The client-attorney privilege covers communication and the exchange of information. However, the scope of the mentioned privilege is questionable in theory, especially in practice. The legal regulation and the rule of law require the traceability of information, especially concerning sensitive financial matters.

The prevailing public interest, for example, in criminal proceedings, may permit access without the consent or even knowledge of the person concerned. Numerous legal requirements for breaching confidentiality reduce the clarity and effectiveness of the legal order and endanger the rule of law. In practice, confidentiality is not sufficiently respected in terms of its scope, which in the past happened mainly due to ignorance of the legislation. Currently, frequent legislation changes, media pressure, or publicly watched cases can contribute to the efforts of healthcare workers to violate mandatory confidentiality.

The reporting obligation or notification, when the law stipulates that confidentiality can be broken for other reasons, is enshrined in European and national legislation, especially in tax cases. Specific sanctions secure communication of certain facts to designated authorities.

The Czech Criminal Code, Act No. 40/2009 Coll., stipulates the reporting obligation in § 368 and crime prevention in § 367. These provisions include a wide range of offences and crimes, including the most severe crime against life and society- for example, murder, pornography, child abuse, hostage taking, fraud and money laundering. The mentioned obligations do not interfere with the attorney and clergy's professional confidentiality. If they provide legal aid in such a case, the attorneys, colleagues, or employees are exempted from the reporting or crime prevention obligations.

Other regulated professions and public officers have the reporting and prevention duty according to the Criminal Code. They could be held administrative or criminally liable if they evade it. The threat of death, bodily harm, another serious detriment, or administrative or criminal prosecution exempts them from this obligation.

However, the exemption of legal advisors is not absolute in financial matters. The anti-money laundering legislation- the Act. No. 253/2008 Coll., on Selected Measures against Legitimisation of Proceeds of Crime and Financing of Terrorism, requires the attorney to report the suspicion about the client to the professional bar. The Czech Bar Association issued the AML application methodology and the questionnaire for clients, which helped to identify the possible risk. The use of the methodology and the questionnaire is not compulsory. However, the attorney is responsible for compliance with legal regulations. The Czech Bar Association then decides if the case would be reported to the Ministry of Finance's state authority. If the attorney deposits money for clients, she must cooperate with the bank when identifying the source of the client's money. The same legal regulation applies to public notaries according to § 27 of the Act. No. 253/2008 Coll.

2.2. Breach of professional confidentiality

Due to the social importance of mandatory confidentiality and the need for increased personal data protection, sensitive data, legal and ethical standards establish liability for breach of obligations imposed in connection with compulsory confidentiality. Liability is not only a legal phenomenon or a subject of legal investigation. Many normative systems operating in society often emphasise responsibility for a specific type of behaviour more strongly than legal norms.

The breach of professional confidentiality and privacy protection is a professional or administrative offence. According to the Czech Criminal Code, § 180, a person or legal entity could be held responsible for the crime of unauthorised use of personal data. This crime also includes the breach of professional confidentiality duty. The crime of violation of the confidentiality of conveyed messages, § 182 of the Criminal Code, stipulates for misuse or illegal download of stored or transferred data.

This offence or crime applies to public officers, including judges or prosecutors. The public administration and the justice sector belong to the state's critical infrastructure, not only because of the large amount of personal and sensitive data stored but also because of its irreplaceability in the rule of law states.

As mentioned, public servants have disciplinary responsibilities. That is why the breach of the confidentiality duty might be a misdemeanour, which is punished in the disciplinary proceedings. The Supreme Administrative |Court is the respective body for the disciplinary delicts of judges, public prosecutors, and executors. The Court found a judge, who accessed a case file, assigned to another judge, and informed the third party guilty of the confidentiality breach (13Kss 2/2020).

The Anglo-American legal system underlines that the rules concerning confidentiality form the core of the adversarial system (Kaufman, 1984: 187). But the theory, as

well as the practice, recognises that the role of the attorney (advocate) is much more complex in the relationship with the client.

> *"In the discharge of his duty, an advocate knows but one person in all the world, at that is his client. To save that client by all means and expedients, and all hazards and costs to other persons, and among them to himself, is his first and only duty".* (Kaufman, 1984: 254)

Czech law, especially professional practice, understands the lawyer-client relationship mentioned above. The Czech Bar Association strictly punishes the attorneys' confidentiality duty violations. The following disciplinary decisions provide some examples.

The attorney was stroke out from the bar:

> *„It is a disciplinary delict if a lawyer, as a defence attorney, provides a television with photographs from the criminal file without being released from the obligation of confidentiality".* (K 103/2015)

Communication with the police might be not only prohibited but also punished by a fine:

> *„It is a disciplinary offence if the lawyer, not being released from the obligation of confidentiality by his client, adds information about his defence and their mutual relations to the record of the Police of the Czech Republic".* (45/16)

The attorney should always be aware that the information about legal services, their type, scope and price is confidential data. General provision of Section 21, Paragraph 1 of the Advocacy Act No. 85/1996 Coll. stipulates that the advocate shall maintain confidentiality about all facts she learns about regarding legal service provision.

Nevertheless, almost everybody needs advice or support from colleagues or partners. That is why an attorney might break confidentiality. The wrongdoing often does not happen intentionally or out of carelessness, but rather to find a solution in a complex case or personal situation.

The following survey in chapter four examines issues of breaching the confidentiality duty from the attorneys' perspectives.

3. SURVEY

The master's student of the Police Academy of the Czech Republic, Ms Patricie Chudackova, surveyed the challenges of the duty of attorneys 'confidentiality. The first author supervised the thesis, which the student successfully defended in May 2022. The student processed the data collected and then worked on her diploma thesis — Duty of tackiness in tax procedure from the tax subject's point of view and the lawyer's representative.

The student, who works as a paralegal in an attorney's office, utilised her practical experience, giving them a theoretical basis, which she acquired by studying at university. She would reuse the knowledge she had processed and transformed in her profession.

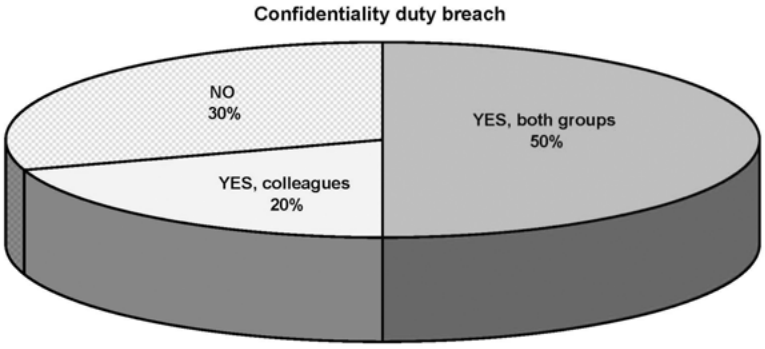
The survey's main goal was to determine to what extent client confidentiality is violated in legal practice and whether these acts are penalised. The student surveyed in February 2022 among ten respondents - lawyers with diverse years of experience in various law branches, like business, finance or labour law, to obtain different views.

The respondents answered the following four questions:

- Have you encountered a breach of confidentiality on your part or colleagues during your legal practice?
- If so, in what matter and to what extent was confidentiality violated?
- Did the body of the professional chamber detect this violation?
- If so, was it penalised?

The survey was conducted through a questionnaire sent to respondents by e-mail. Seven men and three women answered. These were primarily lawyers with more than ten years of experience, but the respondent's shortest legal experience was two years, and conversely, the longest was 20 years.

Graph No. 1 shows the survey results.



Source: Chudackova, 2022, survey results

The survey specifically revealed that seven out of ten respondents confirmed the breach of confidentiality on their part and the part of their colleagues. The lawyers usually discuss the case with the opposing party without the client's prior consent. They often seek advice or opinions from their colleagues who are not involved in providing legal aid. They usually discuss more general or psychological issues with the partner, especially if the case is emotionally strained or exhausting.

> *"A certain moral dispute of a lawyer regarding the preservation of confidentiality can also be represented by cohabitation with his partner. A lawyer must constantly evaluate whether or not it is appropriate and safe to keep electronic devices with confidential*

information in the home environment. The mentioned problem is relevant, especially nowadays, when most lawyers depend on working from home. Primarily when his partner works in the same profession, in such a case, the so-called home office can represent a particular form of danger since the other partner can easily access e-mail communication and phone calls with the client". (Jirounkova, 2021)

Other examples of breaching professional confidentiality are identifying the client when dissolving cases with former colleagues. Very often, attorneys disclose the terms of the transaction to a third party, who then uses it to her advantage.

The survey confirmed that breach of confidentiality is a widespread phenomenon representing some breach of the code of ethics and the law to some extent.

However, professional authorities do not detect most mandatory confidentiality breaches. Disciplinary action is, therefore, exceptional and only if an attorney violates confidentiality intending to harm the client.

4. DIGITAL LEGAL SERVICES

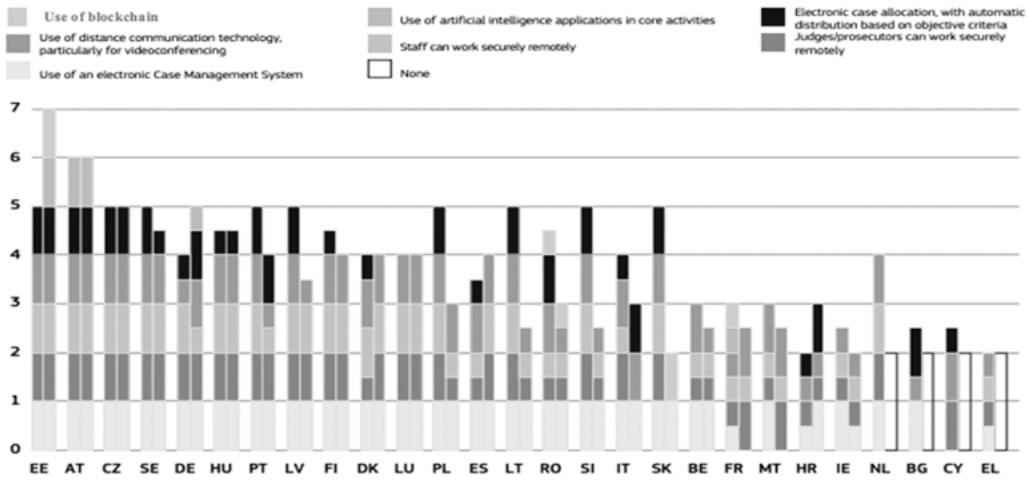
In recent years, both scholars and industry analysts have predicted a worldwide transformation of digital public services from a traditional paradigm of use of technologies in which public administration provides a "use-case-centric" electronic access to information, registration services, payment of fees, e-health, etc. towards a new paradigm, which promotes consolidated, multi-channel, user-centric ("as easy as online shopping"), services. Digital public services that follow the new paradigm may span not only many governmental agencies but also be open to "smart" application and user interface development by external (private or public) service providers (Velicogna, 2017, Daub *et al*. 2020). Furthermore, the adoption of the new paradigm may contribute to the creation of a "once-only government", in which "*citizens and businesses need to provide their data only once before it is shared across departments with appropriate privacy protections*." (EU knowledge4policy).

While ongoing digitalisation of court administration and court proceedings is already taking place in almost all European countries (EU scoreboard 2021), the resulting digital services mostly follow the "traditional" paradigm of standalone "use-case-centric" portals. For example, the prevalence of this approach is evident in the digital services provided by the Nordic and Baltic (pub.norden, 2022) as well as Czech judicial portals (justice.cz).

A future transition towards the new paradigm, which encourages the participation of third-party service providers, may inevitably transform the landscape of public digital legal services in countries around Europe and accelerate the adoption of modern technological capabilities, such as blockchain-based digital legal tools, by lawyers, law firms, and their clients by making them more available and accessible. According to the 2021 EU Justice Scoreboard, making blockchain-based tools widely available requires

further attention to improve the quality of courts and prosecution services through digitalisation. "*While most Member States have case-management systems, videoconferencing systems and the possibility for teleworking, there is still a need for further progress in making automatic case allocation systems, artificial intelligence and blockchain-based tools more widely available*".

Use of digital tools by courts and prosecution services



NOTE: left column = courts, right column = prosecution services, *Source:* https://ec.europa.eu/info/sites/default/files/eu_justice_scoreboard_2021.pdf

The adoption of blockchain-based tools has increased to help establish trust and transparency in public administration services. "*Blockchain is a system of recording information in a way that makes it difficult or impossible to manipulate, and distributed ledger technology is a system for recording the transaction details of assets in multiple places simultaneously, with no central data store or administration functionality. These might be used as a new information infrastructure that could support and ensure the safe exchange of information between public administrations, citizens and businesses*". (EU knowledge4policy)

The following examples are the possible emerging applications of blockchain technologies in digital legal services that impact how lawyers, legal firms and individuals interact with public administration.

4.1. Land Registries

Progressive digitisation of land registration services, including the introduction of electronic land registration proceedings and digital signatures, as well as research in digital identity such as self-sovereign identity (SSI) lays solid grounds for the

application of blockchain-based tools. (Shualb *et al*. 2022) Blockchain-based land registries are being explored and prototyped, for example, in Canada (blockchain.ubc.ca) and can be a significant step toward land registry digitalisation in developing nations where land ownership is less documented, and citizens may not have access to land registries. Using blockchain in land registries results in "*transparency, increased trust, increased predictive capability, reliability, increased control, cost reduction, reduced energy consumption, security, ease of access, privacy, reducing corruption, and error reduction*". (Shualb *et al*. 2022)

The Czech Republic introduced the digital land registry in 2001. Since 2014 the land registry, which records legal relations to real estate property, maps and boundaries between real estates, has played an essential role in private law. Records are publicly available via websites. The publicity principle applies. What is entered in the registry is considered legally binding until proven otherwise. Remote access is either limited without information about the personal data of owners or paid with the identification of the accessing person. Such a person can also get legal documentation connected with the property and all details about the owner.

4.2. Smart contracts

A blockchain-based tool adopted in land registries and property sales is smart contracts. Smart contracts are the blockchain form of conventional contracts. "*A smart contract can execute and enforce itself autonomously and automatically, without intermediaries and is valid, without depending on authorities or third parties by consensus of network users eliminating bureaucracy given the decentralised, immutable and transparent nature of Blockchain technology.*" (Casalas et al., 2020). Smart Contracts can be applied in the process of property registration, where they open possibilities for real-time property sales. Smart Contracts in property registration serve as a means of automatically verifying the identity of the property owner (including their claims for being the true property owner) and buyer and that all contract terms have been met based on defined criteria, and then executing the payment and registering the property on behalf of the new owner." (Casalas *et al.* 2020, Table II). However, as smart contracts are still contracts, preparing and reviewing the contract terms and criteria requires lawyer involvement.

4.3. Decentralised justice platforms

Traditional dispute resolution methods such as state courts and international arbitration have proven ineffective in handling the growing amount of small value claims in online transactions across national borders. Decentralised justice platforms, such as Kleros, Aragon and Jur, offer an innovative, more efficient, cost-effective and transparent approach to online dispute resolution. Decentralised justice platforms leverage smart contracts - they "*combine blockchain, crowdsourcing and game theory in order*

to produce resolution systems which are radically more efficient than existing methods." (Aioudef *et al.* 2022). In the upcoming years, decentralised justice platforms will realise adoption in disputes, where the involvement of legal professionals is not suitable due to their high cost.

Since the future digital legal services will be online (cloud-based) platforms open to third-party service providers and will not only be consumed by lawyers and law firms but will likely become part of their own digital legal service offerings, strong cybersecurity practices inside law firms are a key requirement. In the USA, according to the American Bar Association (ABA), cloud services play a crucial role in the IT resources of lawyers and law firms. The biggest concern for lawyers regarding cloud computing is confidentiality and security, followed by a lack of control over data. Additionally, in their 2021 Cybersecurity report, ABA reported that 25% of attorney respondents had experienced a data breach at some point and that "*clients are increasingly focusing on the cybersecurity of law firms representing them and using approaches like required third-party security assessments, security requirements, and questionnaires.*" (Kennedy, 2021). Cybersecurity and confidentiality are crucial demands of clients on law firms and place a demand on law firms to implement sophisticated security programs and policies. ABA recommends that law firms' leadership take on such programs and policies, not only IT departments and technology consultants. Such programs and policies affect online legal services offered through online platforms.

Law firms must consider a full spectrum of cloud systems they use to provide legal services through online platforms. According to the Czech Bar Association, legal firms should consider an online legal service offered through an online platform (web or mobile) if the online platform is used for delivering information to clients, is used for communication between the lawyer as the provider and the client as the recipient of the legal service and the legal service is invoiced, or possibly paid, through an online platform. *"A lawyer providing such a legal service ... must at the same time ensure that third parties do not compromise this data. The lawyer is responsible for securing the communication and confidentiality of the online platform…." (Czech Bar Association, 2018)*

CONCLUSION

The authors identified several risks and challenges in the digital legal service:

- Uncritical reliance on technology. It might be pretty difficult to get fixed the erroneous data. GDPR protects personal rights and data but not business and property rights.
- The human factor can fail. The negligence in entering, changing or protecting data can lead to third-party injury. The possibility to search and surf via various state-administered registers, especially when those are not publicly available, might lead to corruption and the discharge of data. The authors examined the breach of the duty of confidentiality in part three.

- Registers do not communicate because, in the past, each public administration body developed its digital network. The user of the public administration must ask for more documents. The unnecessary circulation of data might endanger their confidentiality.
- The public administration does not have sufficiently strong protection against cyber-attacks because of the lack of money or system obsolescence. The contracts are concluded for long-time periods, and any change needs public tender. The legal requirements for public procurement are rigorous in the European Union and lead to protractions. Public authorities often keep their systems intact as long as possible.

Digitalisation and data transfer via the Internet or cloud storage attract cybercrime. It is tough to disclose a computer crime, as it is always hidden and silent with no violence. The data could be sold anonymously through unidentifiable computers and banks in states without the obligation to report money laundering.

The AI enables any legal services provider to compile, process and share enormous amounts of data (big data) and information quicker, in more detail and much greater extent than man can. The machine learns itself and improves processes. AI facilitates keeping records in electronic form and sending them to any place in the world, for example, data collected during trials. Blockchain technologies solve issues of transparency, costs and confidentiality. The authors underline that this is how the client of digital legal services will be a subject in the case, not only an object in data circulation.

The critical issue to examine in the future is how to balance the competing interests of privacy and data-sharing and not exclude the client or public services user as a holder and owner of the information. Further, the public service user must be able to settle the matter and communicate personally with the public authority. The public service needs to be closer to smaller communities and older persons or persons with impairments. Even modern and digitised legal services are based not only on modern technologies but also on human interaction.

The judge, the attorney, the prosecutor, and other public officers can access confidential information. The possibilities to influence public space and individual destinies via social networks, and misusing professional knowledge, are immense. That is why it is necessary to emphasise not only education and digital literacy but also advocates' and public servants' moral integrity and human values. Digitalisation can only support the rule of law by cooperating with all procedural parties.

REFERENCES

1. Aouidef, Y., Ast, F., Deffians, B. (2021) *Decentralised Justice: A Comparative Analysis of Blockchain*, Online Dispute Resolution Projects.
2. Casallas, J.A. T., Cueva-Lovelle, J. M., Molano Rodríguez, J. I. (2020) „Smart Contracts with Blockchain in the Public Sector", *International Journal of Interactive Multimedia and Artificial Intelligence,* In Press:10. DOI:10.9781/ijimai.2020.07.005. Available at: https://www.researchgate.net/publication/343884451_Smart_Contracts_with_Blockchain_in_the_Public_Sector. [1.9.2022].
3. Chudackova, P. (2022) "Duty of tackiness in tax procedure from the tax subject's point of view and the lawyer's representative", *Diploma thesis*. Prague: Police Academy of the Czech Republic, Available on request at: knihovna@polac.cz.
4. Daub, M., Domeyer, A., Lamaa, A., Renz, F. (2020) *Digital public services. How to achieve fast transformation in scale*. Available at: https://www.mckinsey.com/industries/public-and-social-sector/our-insights/digital-public-services-how-to-achieve-fast-transformation-at-scale. [1.9.2022].
5. Janeckova, E. (2019) *GDPR: řešení problémů v praxi obcí,* Prague: Grada Publishing.
6. Jirounkova, K. (2021) „Elektronické důkazní prostředky v souvislosti s výkonem advokacie a vztahem advokáta a klienta", *Právní rozhledy* No. 23-24. Available at: Beck-online.cz. [1.9.2022].
7. Kaufman, A. L. (1984) Problems in Professional Responsibility., 2nd Edtion, Toronto: Little, Brown and Company.
8. Kejhová, H. and Rýdlová, H. (2019) „Ztratí-li se důvěra v advokátní mlčenlivost, už se nikdy nevrátí" *Advokátní deník,* Prague: Czech Bar Association. Available at: https://advokatnidenik.cz/2019/04/17/ztrati-li-se-duvera-v-advokatnimlcenlivost-uz-se-nikdy-nevrati/. [1.9.2022].
9. Kennedy, D. (2021) Cloud Computing. Available at: https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cloudcomputing/ [1.9.2022].
10. Shualb, M., Hassan, N. H., Usman, S., Alam, S. (2022) *Identity Model for Blockchain-Based Land Registry System: A Comparison.Wireless Communications and Mobile Computing* DOI:10.1155/2022/5670714. Available at: https://www.researchgate.net/publication/358508950_Identity_Model_for_Blockchain-Based_Land_Registry_System_A_Comparison [1.9.2022].
11. Velicogna, M. (2017) *In Search of Smartness: The EU e-Justice Challenge. Informatics* 4(4):38 DOI:10.3390/informatics4040038. Available at: https://www.researchgate.net/publication/320938829_In_Search_of_Smartness_The_EU_e-Justice_Challenge [1.9.2022].
12. Whitman, J. Q. (2004) „The Two Western Cultures of Privacy: Dignity versus Liberty", *Faculty Scholarship Series*. Paper 649. USA: Yale Law School. Available at: http://digitalcommons.law.yale.edu/fss_papers/649 [1.9.2022].

Internet sources:

1. AML Application of the Czech Bar Association, Available at: https://www.cak.cz/scripts/detail.php?id=24763. [1.9.2022].
2. Blockchain.ubc.ca. Available at: https://blockchain.ubc.ca/research/bc-land-title-survey-authority-ltsa-digital-id-design-challenge-diac. [1.9.2022].
3. Front. Blockchain.Sec. Blockchain for Good. Available at: https://www.frontiersin.org/articles/10.3389/fbloc.2021.564551/full#B5 [1.9.2022].
4. Nordic and Baltic judicial portals. Available at: https://pub.norden.org/temanord2022-518/temanord2022-518.pdf [1.9.2022].
5. Official website of the European Union: https://knowledge4policy.ec.europa.eu/foresight/digital-transformation-public-administration-services_en [1.9.2022].
6. https://ec.europa.eu/info/sites/default/files/eu_justice_scoreboard_2021.pdf, pg. 33, Figure 41 [1.9.2022].

Legal sources:

1. Act No. 253/2008 Coll. on Selected Measures against Legitimisation of Proceeds of Crime and Financing of Terrorism, Available at: https://www.cnb.cz/en/supervision-financial-market/legislation/money-laundering/laws-and-regulations/-working translation for information. [1.9.2022].
2. Act No. 253/2008 Coll. on Selected Measures against Legitimisation of Proceeds of Crime and Financing of Terrorism, Available at: https://www.cnb.cz/en/supervision-financial-market/legislation/money-laundering/laws-and-regulations/-working translation for information. [1.9.2022].
3. Criminal Code of the Czech Republic, 2009, Available at: https://www.ejtn.eu/PageFiles/6533/Criminal%20Code%20of%20the%20Czech%20Republic.pdf [1.9.2022].
4. Czech Bar Association, Decision K 103/2015 of 14 December 2015. Available at: https://www.cak.cz/assets/komora/bulettin-advokacie/sbirka_2016-2018.pdf [1.9.2022].
5. Czech Bar Association, Decision 45/16 of 7 June 2015. Available at: https://www.cak.cz/assets/komora/bulettin-advokacie/sbirka_2016-2018.pdf. [1.9.2022].
6. Czech Bar Association. 2018. Online legal platforms-explanatory statement. Available at: https://www.cak.cz/assets/12_pravni-sluzby-prostrednictvim-on-line-platforem_01-04-2018.pdf [1.9.2022].
7. Supreme Administrative Court, Czech Republic, Decision 13 Kiss 2/2020 of 5 November 2020. Available at: https://vyhledavac.nssoud.cz/DokumentOriginal/Text/657085. [1.9.2022].

PROMENA OBAVEZE POVERLJIVOSTI U DIGITALNOJ ERI

Autori se u radu bave fenomenom trećeg milenijuma, a pod kojim se podrazumeva generalizovana digitalizacija u javnoj i privatnoj sferi. Ona je prisutna i u oblasti pružanja pravnih usluga od strane države ili privatnih lica. Korišćenje društvenih mreža, automatizovano kreiranje ugovora, blokčejn, Cloud repozitorijumi, virtuelne baze podataka i razne online konferencijske platforme utiču na odnos državne administracije i pravnih zastupnika sa građanima ili klijentima. Fokus istraživanja u ovom radu je obaveza zaštite poverljivosti podataka od strane državnih službenika, uključujući i sudije, kao i obaveza zaštite poverljivosti podataka od strane advokata. U radu se ukazuje na standardne i opšte zahteve kojih moraju da se pridržavaju u svom radu svi profesionalci, kao i na rizike i prednosti digitalizacije u pogledu obaveze poverljivosti. U radu su primenjeni metodi kabinetskog istraživanja i analize sadržaja različitih dokumenata. Na osnovu analize rezultata istraživanja, autori u radu iznose predloge za unapređenje uslova zaštite društvenih i privatnih interesa prilikom pružanja digitalnih pravnih usluga.

KLJUČNE REČI: *digitalizacija, digitalne pravne usluge, obaveza poverljivosti, državna uprava, advokat, sudija.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.17

DIGITALIZATION IN GERMAN CRIMINAL PROCEEDINGS AND ACCOMPANYING FUNDAMENTAL RIGHTS ASPECTS*

Manfred Dauster**
Julia Aileen Kreutz***

Digitalization is also increasingly reaching the field of criminal procedure law. This contribution studies the handling of digitalization in the German Code of Criminal Procedure. The focus lies on the recent legal amendments, particularly regarding electronic file management and electronic file transfer between courts and law enforcement authorities. However, the article also covers the examination of the effectiveness of the long-established and largely unchanged procedural rules and maxims of German criminal procedure in the context of digitalization and digital evidence. The article questions if and how the digitalization of criminal procedural law is compatible with German fundamental rights, proving that many investigative measures, when applied to digital evidence, can easily violate fundamental rights, and that the digitalization of criminal court proceedings may not be exclusively beneficial. Considering the dangers to fundamental rights, it calls for a responsible and considerate approach to digitalization and proves that more digitalization-related amendments are required to protect the rights of the persons involved in digitalized criminal proceedings, particularly those of the accused or the defendant.

KEYWORDS: *digital evidence, investigative measures, electronic file management, fundamental rights, right to privacy of communications.*

* This year's conference of the Institute of Comparative Law and the Institute of Criminological and Sociological Research will deal with the topic "Digitalization in Penal Law and Judiciary". This is an urgent topic that a German contribution can only partially cover. According to German understanding, the digitalization of court administration must be strictly separated from the digitalization that the digitalization of procedural rules will bring. The latter is aimed at the administration of justice, the former is part of the judicial executive in the hands of the (state) judicial administrations. It lacks direct reference to procedural law and, in particular, does not affect the legal position of individual parties to the proceedings. It cannot be dealt with here because otherwise, in accordance with the constitutional distribution of competences in Germany, the regulations of 17 judicial administrations at the level of the German federal state and the 16 Länder would have to be discussed. This cannot be done in a conference contribution, even not briefly. This contribution therefore deals with the digitization projects in German criminal procedural law as a whole and accepts the fact that interesting perspectives beyond procedural law are left out.

** PhD, Presiding Judge of the Bavarian Supreme Court (ret.), Munich, Judge of the Court of Bosnia and Herzegovina, Sarajevo, Member of the Institute for Economic Criminal Law, International and European Criminal Law at Saarland University, Saarbrücken. E-mail: *saarlouis10@hotmail.com*

*** Research assistant at the Chair of German and European Criminal Law and Criminal Procedure Law including Economic Criminal Law, held by Prof Dr Marco Mansdörfer, at Saarland University, Saarbrücken.

E-mail: *j.a.kreutz@t-online.de*

INTRODUCTION

There is no clear definition of the term "digitalization". Depending on the context, it can take on several meanings. In the original sense, digitization means the conversion of analogue information into digital formats, which can then be processed by information technology. Another meaning of digitalization is digital revolution, also referred to as digital change or digital transformation. Digital transformation describes the processes of change triggered by digitalization in society, including the economy, culture, education and politics. In the latter understanding of the term, it is also to be understood here when placed in a relationship with criminal law and criminal justice. The latter are only marginal elements of a much broader digital trend setting that reaches beyond state reform processes and encompasses the economy as well as society and ultimately includes the re-writing of a process through which analogue products (paper, files, communication) are converted with the help of electronic data processing into formats (files) that are in turn accessible to electronic data processing. The accompanying effects of such digitization are expected to be facilitation and acceleration of communication between those involved in the conversion process, personnel savings and (after amortization of the considerable investment costs) general cost savings.

At the same time, we must not forget that, in terms of cultural history, it was a very long way before we were able to talk about the digitalization of social processes. It took thousands of years for mankind to break away from baked clay tablets with the cuneiform writings of Mesopotamia or from Egyptian papyri. The invention of the printing press by Johannes Guttenberg was revolutionary in its own right, leaving behind the monastic writing rooms in which monks did nothing but handwrite (sacred and other) texts on calf parchment for years. Even the judiciary of the late Middle Ages, which until then had cultivated a working method based essentially on oral (transmission) traditions, increasingly wrote things down and created registers and files. What was not written in these could easily be ignored ("Quod non est in actis, non est in mundo."). With the now-more-printed paper, information poured in on people, the extent of which could not have been imagined before the printing press, and in addition, books (and other writings) also became relatively cheap and thus accessible to individual and no longer just privileged consumption. The beginnings of (legal) scientific writing as we know it today lie in this period and are actually inconceivable without the printing press. The invention of the typewriter, the photocopier and the personal computer, in their way, gave a further innovative boost to everyday life in courts, public prosecutors' offices and law firms in particular. Judges' desks without personal computers are no longer imaginable in the 21st century. Computers have even found their way into courtrooms. Nevertheless, no legal workplace today can do without paper files. Even the lawyer of the 21st century can still hide behind mountains of paper in the form of files. Digitization wants to put an end to this. When people talk about it, the results they present include, in particular, adding these paper files to the clay tablets, papyri and parchments. Our forests will thank us for this endeavor. But digitization is also about networking between and

with authorities within national borders and beyond, i.e. about facilitating communication. Within the state, however, it is also about reforming legal transactions between individuals (citizens) and the state, between state authorities and all their members. If you like, digitalization also gives itself the appearance of increasing, speeding up, improving overall efficiency between the state, its authorities and its citizens. With an electronic "click", the citizen sets administrative and judicial processes in motion, which then produce results without leaving paper traces behind. That this is also more cost-effective in the end is the hope that dies last, as we all know.

Covid-19 hit us unexpectedly, but all the harder for it. Unprepared as the world was at the outbreak of the infectious disease, it seriously looked at times as if all public life would have to be halted to contain the pandemic. With regard to the judiciary, it seemed as if the immediate standstill of the administration of justice was threatening across borders (Dauster, 2022: 248-271). After all, digitalization had progressed so far that even the judiciary could switch to domestic workplaces and audio-visual proceedings where they were legally permissible and tried and tested. The rule of law bumped a bit at times, but continued to function (*Ibid.*). The pandemic situation from 2020 until today has contributed significantly to convincing the last digitalization sceptics that digitalization also has good sides for the administration of justice[1].

Digitization goes in parallel with the broader time phenomenon of globalization and can no longer be stopped. It is an almost techno-philosophical question whether one is even conceivable without the other. No answer can be given here. In the present context, we can only touch on the question of the consequences of occupational medicine and psychology for the individual and then for society when the digitalization of justice is completed. The time of the pandemic gave us a rough foretaste, when judges and public prosecutors were also required to work from their home offices if at all possible. The social communication and interaction we had been used to until then only took place at the Sparflammen level. Digitalization is perhaps similar to fire. When our human ancestors understood how to make fire and use fire to prepare their food, they paved the way nutritionally for the development of homo sapiens as we know it today. This was not revolutionary on their part. We do not know whether the results of a completed digitalization, which in future will only have to be adapted to technical developments, will bring about a new homo sapiens or rather conditions that evoke memories of the science fiction novella 1984 by George Orwell. When we think of the judiciary, it is not so much Orwell's Big Brother that evokes horror, but the automaton judge who, fed with data, produces a judicial decision at the end of a split-second processing process within the framework of the matrix given to him. National fundamental and international human rights should always be taken into account in digitalization, because they could prevent the worst excesses from occurring. Some aspects of digitalization that are relevant to fundamental rights will be presented here. In the presentation, the work must essentially be guided by the considerations on German criminal procedure. The other

[1] In 2021, more than 50.000 online hearings have taken place in German civil proceedings (Rebehn, S. (2022) "Mehr als 50.000 Videoverhandlungen in 2021", *DRiZ*, 150 et seq.).

German procedural systems can at best be touched upon. Digitalization is a cross-border phenomenon. It is not possible within the framework of this conference contribution to consider its effects on procedural positions under European law or even to make comparative legal considerations. In this respect, the conference contribution only provides an insight from the perspective of German criminal procedural law.

1. DIGITALIZATION IN GERMAN CRIMINAL PROCEDURE

The influence of electronic and digital information technology is ever-growing. Today, the creation and sharing of electronic documents has become an established practice in most areas of public and private communication. Digital data files have become a means of working and a work product for many modern employees. The expanding importance of computers and the internet, the creation of more internet connected devices ("Internet of things"[2]) and the resulting inflow of new users are causing a steady growth in this area. Never has so much information about the public been available in form of personalized digital footprints (Blecschmitt, 2018: 361) This phenomenon has become known as "Big Data". The most used definition for the term Big Data assigns three specific properties to it: Volume, velocity, and variety (Dorcshel, 2015: 6). Volume means the exponential growth of computing power that, according to Moore's Law (Moore, 1965: 114), doubles within a certain period of time, which is directly connected to the volume of data available worldwide, velocity the speed at which data is processed, and variety the diversity of data sources and data formats (Dorschel, 2015: 7). An estimated amount of 33 zettabytes of digital data existed in the world in 2018 and until the year 2025, the global data volume is projected to further accelerate exponentially and surpass 175 zettabytes (Reinsel, Gantz, Rydning, 2018). In addition, in 2022, there will be an estimated 13.1 billion interconnected (IoT) devices in the world (Valishery, 2021) and with the worldwide fiberglass network ever-growing, the transfer of more and increasingly bigger files will be possible. Today, digital evidence plays an increasingly bigger role in criminal proceedings, and the number of proceedings based (almost) exclusively on digital evidence, especially with regards to Cybercrime, is also increasing. For example, these two court cases have lately attracted the attention of the German public: A man was found guilty of killing a woman based on an audio recording made by Amazon's voice assistant "Alexa" in the victim's flat (LG Regensburg, verdict of 16 December 2020 – file no.: Ks 103 Js 28875/19) and a man was found guilty based on location data collected by his Mercedes car (OLG Frankfurt a.M., decision of 20 July 2021, file no.: 3 Ws 369/21). And digitalization is also appearing in the court proceeding itself, a development that has only been accelerated by the Covid-19 pandemic. Digitalization does not only bring challenges, but also opportunities an "easier" execution of criminal proceedings. How this makes digitalization into a double-edged sword will be discussed in this contribution.

[2] „Internet of things" (IoT) is a term used to describe a network of physical objects that are equipped with network capability in such a way that data can be exchanged between them. These devices range from ordinary household items (smart fridges, smart home) to smart cars and sophisticated industrial tools.

The German Code of Criminal Procedure is the Strafprozessordnung (StPO). It regulates the entire criminal proceeding, most notably the criminal investigation, during which evidence is gathered, and the main proceeding, which usually ends in judgment or acquittal. In the context of digitalization, there have been and will be several interesting legal amendments to the StPO, the most important of which we will now discuss.

If we focus on the measures of criminal investigation first, one must differentiate between so-called open investigation measures and secret investigation measures. This assignment depends on whether the defendant must be informed of the measure or not. Open investigative measures include Sicherstellung and Beschlagnahme (Section 94 StPO), both measures that can be translated as forms of seizure. Sicherstellung means that objects which may be of importance as evidence for the investigation may be confiscated or secured otherwise, while Beschlagnahme is applicable to such objects that are in possession of a person and are not voluntarily surrendered. The only condition for conducting a seizure is the presence of "initial suspicion", a sufficient factual indication that a possible criminal act might have occurred, which is a rather low requirement (Bildner, 2021: 8), but they have to be ordered by a judge. Both Sicherstellung and Beschlagnahme have been around and largely unchanged for a long time and have not yet been amended with regards to digitalization, but their scope has grown to include digital data. Germany's Federal Constitutional Court, the Bundesverfassungsgericht (BVerfG), has ruled that not only physical objects like hard drives, optical drives or other storage devices, but also non-physical objects such as raw data can be seized under Sections 94 et seqq. StPO as long as the seizure only comprises past data and not data which is yet to be produced in real-time or in the future (BVerfGE 113, 29 (50); BVerfGE 124, 43 (60 et seq.). It has also ruled that the measures of seizure in Sections 94 et seqq. StPO can be used to seize digital telecommunication like e-Mails or chat messages (BVerfGE 124, 43). According to adjacent Section 95 StPO, anyone who possesses any of the aforementioned objects or data has to produce and deliver it on demand or else coercive measures can be taken against them. This rule, which was created in a time when the age of digitalization was not yet foreseeable, can be used to oblige cloud storage providers to look for, find and reveal what the prosecutor's office is asking them to release ("production order)" (Jahn & Brodowski, 2020: 81). Since 2021, it is also not entirely correct to label Sicherstellung und Beschlagnahme as open investigation measures anymore. By the Act on the Further Development of the Code of Criminal Procedure and the Amendment of Other Provisions, a new Section 95a StPO was introduced which enables the court to defer noticing the accused if the relevant item is not in possession of the accused, a significant crime is concerned, and a notice would be likely to jeopardize the purpose of the investigation. This amendment is especially intended to improve criminal prosecution when it comes to accessing electronic evidence.[3] The court may also order any third party that is in possession of the evidence to not inform the accused of the ongoing investigation. And there's another problem with digital evidence: Before a court

[3] Bundesregierung, Entwurf eines Gesetzes zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften, 2021, https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_StPO_Fortentwicklung.pdf;jsessionid=0AD68B160A82CD29C47A01C33721AB8D.2_cid334?__blob=publicationFile&v=2, 69.

orders a seizure of certain items, the persons involved in the investigation must first know if these items are worth seizing. For this purpose, Section 110 StPO enables the police and the public prosecutor's office to review any files of a person who has been subjected to a raid pursuant to Section 103 StPO and decide whether they should be seized or not. Simply said, Section 110 StPO is a precursor measure to a seizure. With the 2021 amendment, Paragraph 3 of this rule was explicitly expanded to digital files which are not present at the location of the raid, enabling law enforcement authorities to access cloud storages elsewhere through the searched device.

Then, there's the secret investigation measures. The most important ones are Quellen-TKÜ (Section 100a Paragraph 1 sentences 2, 3 StPO) and Online-Durchsuchung (Section 100b StPO). Quellen-TKÜ enables the police to monitor and record encrypted telecommunications by exploiting security gaps or installing malware to the accused person's personal device without their knowledge. 100b StPO enables authorities to access any information technology system that's being used by the accused and to access and search all past, current, and incoming data as well as cloud storage on that system. Both measures are only possible if certain serious criminal offences have been committed and if other ways of investigation promise little success. While these measures have been implemented recently and have already been amended several times, much like the older legal regulations of Sections 94 et seqq. StPO, Sections 100a et seqq. StPO are also scrambling to keep up with the reality of criminal prosecution and the tools that are used to screen or observe the persons accused of a crime. For example, law enforcement agencies may use a "silent SMS", a text message without any contents, to ping the location of a cellphone belonging to a person they are interested in. The usage of Silent SMS has to this day not been explicitly regulated. Many courts, including the German Federal Supreme Court of Justice (Bundesgerichtshof [= BGH]) resort to interpreting or even combining existing legal basis to legitimize the use of these techniques, and in the case of the Silent SMS, the BGH ruled that Section 100i StPO, which had not been created for the purpose, was suitable (BGH NStZ 2018, 611). It is true that the legislator often cannot keep up with all the new developments in digital police work, but a bad taste remains, also with regard to fundamental rights, which we will discuss later.

Let us now look beyond the criminal investigation and focus on the criminal proceeding itself. This previously paper-heavy enterprise is currently experiencing digitalization. With the 2017 Act on the Introduction of the Electronic File in the Judiciary and on the Further Promotion of Electronic Legal Transactions, among other things, changes were made to the StPO. Since 2018, there is now the possibility of a fully electronic file management and electronic file transfer between courts and law enforcement authorities. According to Section 32 StPO, the electronic file-keeping and file management regarding criminal files (eStrafakte) is still optional but will become mandatory in 2026. This means that by that year, all German states ("Länder") must introduce a secure digital system that allows for safe receiving, sending, storing, or editing digital court files. The system will save the entire proceeding from the first document onwards, including all the summons, notices, writs (warrants and subpoenas) and court papers. The accused

can also make digital objections and appeal acts that infringe their rights electronically. Section 32a StPO defines which requirements must be met by the electronic file and its contents and by the system used to transfer it, and Section 32e StPO rules that all files that do not meet the requirement (either because they are printed or because they do not have the correct file type) must be converted to digital form. Section 32b StPO rules that whenever an electronic criminal file is created, all persons involved must provide a qualified electronic signature. While the transfer of these files between law enforcement agencies and courts is currently still optional, it too will become mandatory from 2026 onwards. And the communication between defense attorneys and the court is also set to change. According to Section 32b StPO, since January 1st, 2022, certain communication like motions or declarations between the defense attorney and the court shall now be also submitted electronically, with an exception for situations in which the digital transfer is malfunctioning. Any appeals (Berufung, Revision) and their grounds as well as the bringing of private prosecution or accessory prosecution even must be submitted electronically. Section 32f StPO declares that access to the electronic criminal file is granted by making the file available for retrieval or by transmitting it via a secure channel. The government draft explicitly states that for the question of whether file inspection was granted, it does not matter whether the inquirer has actually inspected the files or not.[4] Usually, the inquirer will be the defense attorney, but if the accused does not have a defense attorney, he or she shall personally be granted access to the files or to view evidence insofar as the purpose of the evidence is not jeopardized or overriding interests of third parties worthy of protection do not conflict with this, according to Section 147 Paragraph 3 StPO. Legislators have realized that criminal files can easily grow to a considerable size and can, especially if they were obtained through any of the previously named investigative measures, also contain third party data. Therefore, the law states that technical and organizational measures must be taken to ensure that third parties cannot gain knowledge of the contents of the files, and any person whom file inspection is granted must be made permanently recognizable to anyone viewing the file. Furthermore, a person to whom inspection is granted may not publicly disseminate files, documents, printouts, or copies that have been provided to them or make them available to third parties for purposes unrelated to the proceedings.

To round this off, in Sections 496 et seqq. StPO, an entire segment was dedicated to the handling of personal data that will undoubtedly be kept in electronic criminal files. The processing and use of personal data is only permitted to the extent necessary for the purpose of criminal proceedings and measures must be taken to meet the requirements of data protection and data security. Since third parties like providers or specialized IT developers are often contractually involved in the management and the storage of criminal electronic files, the law states that the storage of these files may only be entrusted to non-public bodies if a public body exclusively controls access to and use of the data in

[4] Bundesregierung, Entwurf eines Gesetzes zur Einführung der elektronischen Akte in Strafsachen und zur weiteren Förderung des elektronischen Rechtsverkehrs, 2016, https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RegE_elektronische_Akte_in_Strafsachen.pdf;jsessionid=1C6B8B276254404EFF4141343E2EBD9F.2_cid334?__blob=publicationFile&v=1 , 61.

the processing facilities. Any electronic file copies that have been taken from the original file must be deleted immediately once they are no longer required.

Digitalization is also present elsewhere in German law. The Law on the Execution of Criminal Sanctions (Strafvollzugsgesetz [= StVollzG]) was altered by the 2017 legislative amendment, too. According to Section 110a StVollzG, the electronic criminal file will also make an entrance in this area. Here, digitalization may prove a challenge for detainees who are not represented by a defense attorney. During pre-trial detention, the above-mentioned rules (Sections 32 et seqq. StPO and Section 147 StPO) apply and provide them with a right to inspect the electronic criminal file, but they do not grant the pre-trial detainee a right to participate in electronic legal traffic while they are in detention – therefore giving them a right that they may not be able to exercise considering detainees' restricted internet access (Esser, 2020: 220).

Other procedural Codes were also updated. Among others, the Code of Civil Procedure (Zivilprozessordnung), the Administrative Court Act (Verwaltungsgerichtsordnung), the Labor Court Act (Arbeitsgerichtsgesetz) as well as the Administrative Offences Act (Gesetz über Ordnungswidrigkeiten) all received changes that implement the voluntary use of electronic file management for now and mandatory electronic file management from 2026 onwards. Therefore, it is safe to say that almost the entirety of German courts, prosecutors's offices and law enforcement agencies will go fully "digital" in 2026. The new German file-keeping system might also boost the exchange of information with other European countries. Currently, a "European Criminal Records Information System" (EPRIS-ADEP) is in a first trial phase. This system will enable police in all participant countries to check whether a criminal investigation has already been filed against a certain person. However, this system will not enable foreign authorities to have direct access to the underlying files. Access will require an application within the framework of European mutual legal assistance in criminal matters, but due to time constraints, we will leave it at that.

2. LEGAL LIMITS OF DIGITALIZATION

To begin this chapter, we will talk about the basics of German criminal procedure. The German criminal proceeding is characterized by its maxims, the most important of which we will briefly touch upon. According to Section 160 StPO, as soon as the public prosecutor's office becomes aware of the suspicion of a criminal offense either through a report or through other means (this cognizance is referred to as "initial suspicion"), it must investigate the facts of the case for the purpose of deciding whether to file a public action or not. In compliance with Section 152 Paragraph 2 StPO, the public prosecutor's office is obligated to intervene for all prosecutable criminal offenses if there have been sufficient indications brought to light by the investigation that make it seem likely that a crime has taken place ("adequate suspicion"). In that case, Sections 152 and 170 StPO oblige the public prosecutor's office to bring the action because according to Section 151 StPO, there can be no criminal court proceeding without a previous indictment. Maxims also apply to

the main proceeding. Namely, the Principle of the Public Nature of Proceedings applies. It states that any hearing before a (criminal) court shall be public, which includes releasing the judgment and orders to the public. This allows citizens to control the judiciary to some extent, admittedly not so much regarding legal niceties, but to prevent "backroom courts" and blatantly unjust proceedings. And finally, there's the Principle of Orality, which states the judge may only rule based on what was presented orally at the main hearing. Even in the case of documentary evidence, the relevant documents must in principle be read out loudly in the main trial (Section 249 StPO), and according to Section 249 Paragraph 1 Sentence 2 StPO, electronic documents can and must be read out loudly, too. Pursuant to Section 261 StPO, the court must then judge based on its free conviction drawn from the essence of the trial. A conviction shall only be made if the court is fully convinced that of the defendant's guilt based on the findings made in the main hearing. In the trial, according to Section 244 Paragraph 2 StPO, to ascertain the truth, the court shall therefore, of its own motion, extend the taking of evidence to all facts and evidence relevant to the decision. In this regard, the Principle of Immediacy applies, which means that evidence may not be substituted by other, less direct evidence (e.g.: hearing a witness testimony about a conversation instead of interviewing the speaker himself). However, the court may not choose freely what evidence it can review and in which form, since there are only certain and specific means of evidence ("Strengbeweis") that may be used in a German criminal proceeding. The means of evidence ("Beweismittel") are limited to visual inspection (Inaugenscheinnahme), documentary evidence (Urkundenbeweis), witnesses (Zeugenbeweis), expert evidence (Sachverständigenbeweis) and the statements of the defendant.

If we focus on visual evidence, we run into the first issue with digitalization: Despite the name, Inaugenscheinnahme means perception of any kind of evidence not only through eyesight, but also by hearing, smelling, tasting or feeling (BGHSt 18, 51 (53).). In terms of visibility, digital data is not directly perceptible to the human eye and has to go through several processing steps before it appears on a screen of a given device or before it is printed from that device (Bildner, 2021: 5). Digital evidence can also not be experienced with all human senses. For example, a court may find themselves having to rule based on a screenshot of an e-mail, a screenshot of a website, a video that has been downloaded from an online source or taken from a hard drive, a voice recording, a text file or an image file or a screenshot of a chat log. These are either visible or audible or, in lucky instances, both. But digital evidence is never perceptible to touch and smell. If a judge touches bank bills, he or she can notice that they are counterfeit based on the weight and the feeling of the paper of the way the light reflects off the coating. This is not possible if the judge is only given a digital picture of the counterfeit bills. It may also be difficult to determine the authenticity of digital evidence. For example, videos can be altered using Deep Fake software and images may be edited or distorted. Websites such as "fakewhats.com" enable anyone to easily create a fake chat log. Even captures or printouts of websites are not safe from forgery because the appearance of websites can be edited with tools that are built into every internet browser. In the StPO, no procedure for ensuring the authenticity of data is provided, and in practice, checks are rarely made.

As for documentary evidence, Section 249 StPO regulates that all documents that are part of evidence must be read out in the trial. Documentary evidence comprises written documents that are readable and suitable for providing evidence through their content (BGHSt 27, 135 (136)). Previously, when digital documents were concerned, all of them had to be printed before to the trial. Since 2018, Section 249 Paragraph 1 Sentence 2 StPO allows for digital documents to be read out from a digital screen without the need to print. This does not necessarily create more risks, because while the display on the screen may be incorrect due to a technical error, an unintentional change of the contents of the file was also possible in the previously stipulated printing process. The trouble with digital documents lies in their fleeting nature. In documentary evidence, the authenticity of the document is not important to the decision of whether it can be read out aloud. Unlike in electronic communication between the court and the defense attorney (Section 32a StPO), a qualified electronic signature on documentary evidence is not required, but the probative value is also not increased if such a signature is present (Möllers, Salemi, Schliwinski, 2022: 176). This is a difference to civil procedure law, where according to Section 371a of the Code of Civil Procedure (Zivilprozessordnung – ZPO), a qualified electronically signed document is presumed to be true unless proven otherwise. This means that documentary evidence has a high probative value, but only provides little evidence of authenticity. To find the truth, which the court is called upon, it is however of the utmost importance that the digital data is genuine and has not been altered. While the threat of fake evidence has historically always been looming, it has increased with the rise of digital files. The fact that the evidence must go through several hands (law enforcement agencies, possibly third parties) before it is presented to the court in the trial can already be a source of error because every transfer poses a risk of data corruption (Jahn & Brodowski, 2020: 92). All people involved in the transfer chain must be qualified to handle digital evidence and every collection, preparation or evaluation of the evidence should be documented. To assess whether a digital file has been altered, it is possible to rely on the use of hash values, which will provide an insight into whether a file has been edited. This however requires that a first hash value is taken soon after the evidence is collected (Fährmann, 2020: 230). Digital documents are also susceptible to forgery, as PDF files can be easily altered with specialized software and changing a Microsoft Word (.docx) file is almost comically easy (Möllers, Salemi, Schliwinski, 2022: 177).

Within the framework of expert evidence, expert opinions on matters that are not are not known to the court are prepared and introduced into the trial in written form (Section 75 StPO). In accordance with the Principle of Immediacy, the expert must however also be heard in the main trial and explain his findings orally (Section 250 StPO). Experts may be heard on the quality or content of data sets that are part of visual or documentary evidence.

Regarding witnesses, it is important to realize that the testimony is limited to whatever that person has witnessed, either through vision, hearing, touch, or smell, and is therefore not direct evidence, and that the witness may have an incomplete or incorrect memory. A witness cannot talk about any digital evidence directly, but only report

how they have witnessed it, which makes witness evidence less desirable in the court if the evidence can be viewed straightforwardly.

On a side note. critics have also condemned how the reasons for the judgment and the evidence are listed in the judgement. According to Section 267 Paragraph 1 StPO, the judgment must state the facts that are considered proven on which the verdict is based. These grounds must be reproduced in words, and the only exception are illustrations or photos which may be directly attached to the file. This descriptive technique is very time-consuming and often cannot replace the direct display of the relevant evidence, like the original document or video (Matthias Jahn & Brodowski, 2020: 95). Since digital evidence is not attachable to a physical judgement file, digital evidence must be described in all cases. And when it comes to the appeal, the court can only rely on the judgment and the files that are attached to it. Other sources of knowledge, like the investigation file, are not accessible (*Ibid:* 98). This means that the description of digital evidence in the judgement must be as precise as possible. Some therefore call this rule obsolete.

It appears that digital evidence brings about new challenges for criminal proceedings and that the traditional German means of evidence, while still largely up to the task, may need to be revised in the future, either through updating the existing means or by introducing a new category for digital evidence.

The recollection of how a criminal proceeding starts leads us to another legal limit. The principle which calls on the public prosecutor's office to investigate to determine whether a crime has occurred when an initial suspicion has arisen (Legalitätsprinzip) may prove challenging in the context of digitalization. First, it obligates the legislator to implement instruments for law enforcement to be enabled to investigate. A thorough investigation might warrant an extensive search of the suspect and his belongings, including his (personal) digital data, which might interfere with the suspect's fundamental rights, and which we will touch upon in the next chapter. When it comes to reviewing digital evidence, the Legalitätsprinzip quickly snowballs out of control. Searching a single suspect's phone might lead to the discovery of other possible crimes or suspects, and even a single online patrol on a criminal platform conducted by a police officer will quickly produce several suspected cases, which quickly pushes the public prosecutors' offices and the police to their limits. In practice, only a prioritization on serious crimes and pooling of resources is possible to solve this issue (Rückert, 2020: 16).

Finally, there's the question of whether criminal trials should be possible via video conferencing in the future. As of now, the StPO knows no such possibility. In German Civil Procedure Law, however, such a rule has existed since as early as 2002. Section 128a ZPO enables the court, on application or of its own motion, to permit the parties to be absent from the oral proceedings and to join the trial via video conference in the courtroom. From what we have learned, it is currently very difficult to implement video conferencing into German criminal proceedings. The Principle of Immediacy demands the court to form a personal impression on the defendant, the experts and the witnesses who all must be "present" in the courtroom pursuant to Sections 230, 250 ZPO. Transferring trials into a digital environment also brings challenges for the Principle of the

Public Nature of Proceedings. Besides, video conference trials have quite a different "atmosphere" to a trial which is held in presence. Through the webcams, not all expression lines will be visible in the faces of the participants, and the conversation might be less lively as if everyone was sitting in the same room. Consequently, many critics argue that it is significantly harder for participants in a video call to assess their opposites than in real life. For example, if the defendant is likely to be sent to a psychiatric facility and the judge has to substantially base his or her decision on the impression of the defendant during the trial and the defendant does not say a single word, that decision will be even harder if the defendant is only visible to the judge on a screen. But a largely overlooked first step in the direction of video conferencing has already been taken. Since 2021, according to Section 463e StPO, within the framework of the penal system, when certain decisions (for example decisions about the suspension of the remainder of the sentence to probation) need to be taken, there is a possibility of hearing the convict orally by video conference. The decision whether to hold an oral hearing in person or by remote transmission is in the discretion of the court, but the order is inadmissible if a life sentence or placement in a psychiatric hospital is to be enforced. The convict must also be present in the office of a defense attorney or in an office (of the penitentiary) at the time of the video conference. This rule, which was passed in light of the Covid-19 pandemic, is thus still quite restrictive, but possibly points the way in which direction the StPO might develop if digital trials were to be introduced.

The greatest legal challenge in the context of digitalization is the dichotomy between data protection laws and the interests of law enforcement. The criminal proceeding must not become a toothless tiger, but citizens must also not become transparent. The Code of Criminal Proceedings has to reconcile both interests. The large and growing amount of data is causing more and longer criminal investigations, and the sheer amount of personal data is improving investigations more than any other form of police investigation could have ever dreamed of. Since more data means that more and possibly longer investigations are necessary, technological advances which are meant to aid the authorities work with data are being introduced (Schneider, 2020: 80). This includes the software-based evaluation of mass evidence through machine learning or the use of IT-forensics (Bildner, 2021: 16). How this struggle for power presents itself in the light of fundamental rights will be discussed in the next chapter.

3. FRICTIONS WITH FUNDAMENTAL RIGHTS

The German constitution (Grundgesetz [= GG]) contains the fundamental rights (most of them) in its articles 1-19. An in-depth analysis of the complex German fundamental rights system is not possible here, but a short and insightful introduction into how the fundamental rights balance digitalization shall be given.

Art. 1 GG famously states that the dignity of the human being is inviolable, and part of this guarantee of human dignity is the protection of the so-called core part of the

way of living (Kernbereich privater Lebensgestaltung) against government interventions (BVerfGE 109, 279. This core part is of a highly personal nature and the affected person usually prefers the contained information to stay a secret (for example, a person's health data, private conversations between spouses, or a person's sexuality). Many of the aforementioned investigative measures have provisions that are intended to protect this core area. For example, any core data that is obtained during Online-Durchsuchung or Quellen-TKÜ must be deleted immediately, measures must be taken that limit the amount of impacted core data to a minimum and any investigation which would only produce findings from this core area is entirely forbidden (Section 100d StPO). The practical problem with protecting this fundamental right is that only by coming across sensitive data can the assessment be made that this data cannot be used (BVerfGE 109, 279 (313). On top of that, there is no such rule when it comes to seizures (Bildner, 2021: 14) However, any evidence that contains information about this protected area is not admissible as evidence in a criminal proceeding (BVerfGE 124, 43 (70).

Probably the most important fundamental right in the context of digitalization is the right to informational self-determination, derived from Art. 1 GG (human dignity) in connection with Art. 2 GG (right to free development of personality).[5] The right to informational self-determination is the authority of the individual to decide for himself, on the basis of self-determination, when and within what limits information about his private life should be communicated to others. This protection also applies to less personal data and not just the core part of living (BVerfGE 120, 274 (312)). At first glance, it completely bans any use of personal data that is not permitted by the impacted individual and therefore as good as forbids digitalization. But unlike the unrestricted right to human dignity, it is accessible to restrictions in case of overriding public interest. Therefore, it allows for balancing of the interests of the individual and the interests of the public. The public interest in the prosecution of offenders can in principle justify an interference with this right (BVerfGE 130, 151 (187)). For example: Data that has been obtained via Online-Durchsuchung or Quellen-TKÜ can be kept for some time but must be deleted as soon as it is not relevant to prosecution (a public interest) anymore, Section 101 Paragraph 8 StPO. This also applies to any data collected during the proceedings, with certain exceptions (Sections 483 ff., 489 StPO). When it comes to the (digital) criminal file, the right to informational self-determination determines what can be included and what cannot be included and who can read the contents of the file and when. According to Section 353d of the Criminal Code (Strafgesetzbuch – StGB), the indictment or other official court documents may not be published before they have been publicly discussed in the trial or before the proceedings have been concluded, and any offense is prosecutable. This law intends to protect the fundamental personality rights of the accused who is innocent until proven guilty (BVerfG NJW 2015, 2777). The right to informational self-determination also restricts the circle of people who are allowed to inspect the criminal file: Pursuant to Sections 147, 406e StPO, only the defendant, the defense attorney, the victim, the victim's attorney, and the joint plaintiff are allowed to view it, but not the public. Private citizens can also request access pursuant

[5] First defined by the Bundesverfassungsgericht in BVerfGE 65, 1.

to Section 475 StPO, but this access can be denied. If any trade secrets are relevant for the criminal proceeding, the (casual) disclosure of these may also infringe the affected person's Right to Occupational Freedom (Art. 12 GG) and therefore, the court must exercise its discretion in such a way that these secrets are not violated. During the investigation of data, especially when accessing communication, authorities gain information about the personality of the person affected, but also information about third parties whose right to informational self-determination is then also affected and who are especially protected because their data plays no role in the criminal proceeding. When a residence is searched for (digital) evidence, the fundamental right to inviolability of the home (Art. 13 GG) is relevant, and in the case of seizure or confiscation of physical objects, so is the right to property (Art. 14 GG).

The right to informational self-determination also limits if and to what extent personal data can be shared with other authorities, and it is relevant in the context of upcoming software solutions to solve the problem of mass evidence. Today, there is a plethora of software available that can analyze and categorize digital data. Large software providers have long discovered the need for specialized software (Schneider, 2020: 81). The possibilities for predictive policing are growing and modern software is able to teach itself based on the data fed to it (machine learning) and even predict behavioral patterns (predictive policing) (*Ibidem*.). This software will filter and read large quantities of possibly sensitive data. This can have a serious impact on the fundamental right to informational self-determination, which also forbids the evaluation of any personal data. Any corresponding laws will have to go way beyond just the general investigative clauses of the StPO. There will at the very least have to be rules for conduct and statutory requirements to protect core data. The requirements must be even higher if the data is outsourced to third party software developers who are under contract with the authorities.

On top of that, and closely related to the right to informational self-determination, there is the right of confidentiality and integrity of IT systems.[6] It concerns the usage and the functions of IT systems and the trust of the user that the program is safe to use and protects their data, directly restricting the possibilities of law enforcement agencies to gain information through the usage of spyware, like Quellen-TKÜ and Online-Durchsuchung.

Furthermore, whenever telecommunication data of any kind are affected, the right to privacy of correspondence, posts and communications (Art. 10 GG) is in question. It primarily protects the content of the communication, but also the circumstances of the communication, like the connection data, any device-ID identifiers or numbers. It is however notable that this fundamental right only protects the communication as long as it is ingoing, not after it has ended (BVerfGE 115, 166.). For example, an e-Mail is protected under this fundamental right while it is still in transfer or if it is temporarily stored by the provider, but it falls out of protection if it reaches once it is printed or stored (Bildner, 2021: 9).

Art. 103 GG furthermore grants all participants in a proceeding the right of access to the case. This includes the right to review the files, the right to comment, the right that these comments will be minded, and the right to be notified about important developments.

[6] First defined by the Bundesverfassungsgericht in BVerfGE 120, 274.

Here, there are a few possible friction points with regard to the digitalization of criminal proceedings: The mandatory use of the (digital criminal) file will complicate legal communications for eldery people or people without internet access. The use of different file types might make it difficult to acknowledge files that require special software to open. In the criminal proceeding, the right to access to the case is meant to enable an appropriate defense of the defendant. If data has been processed in the investigation, then both the input data and the software need to be made known to the defendant or his defense attorney in order for the defendant to comprehend the result (Basar & Hiéramente, 2018: 685). This is not in the interest of the software developer, who is interested in not having their program's source code made available (and whose respective fundamental rights must be respected), and the police also won't like seeing their ways of working leaked to possible criminals.

As with every interference with fundamental rights, they must be proportionate. Proportionality means that the interference needs to follow a legitimate goal and is suitable and necessary to reach that goal, and especially there must not be any measures that can reach the same goal but are more lenient. Furthermore, the interests of the public in undertaking a measure must outweigh the interests of the individual of not being subjected to it. In this regard, already the interference should be kept as low as possible, and only data relevant to the case should be obtained. In practice, it is getting increasingly more difficult to separate important data from useless data, which is why more and more investigators are employing the "vacuum cleaner method": confiscate all available data and separate later (Basar & Hiéramente, 2018: 681). If possible, less stringent measures should be used to determine where stronger measures are later required. The textbook example for this is the preliminary inspection of data before a possible seizure, Section 110 StPO. But this measure, which is generally seen as the "lesser evil", may enable authorities to do a "complete screening" on the person concerned, and the conditions to deploy it are lesser than with the less intrusive measure of seizure (Peters, 2017: 473), proving that not all measures work the way the legislator envisioned them.

CONCLUSION

To conclude, digitalization in criminal proceedings has the potential to improve criminal proceedings for all involved, but also bears the risk of interfering with fundamental rights of the accused and of third parties. In contrast to the past, when intel about persons of interest had to be meticulously figured out and uncovered, the modern citizen produces more personal data on his own power than the prosecution authorities could have ever dreamed of, and often, this data can be intentionally or unintentionally incriminating. Separating the data relevant to a criminal investigation from personal data is a massive challenge and very sensitive with regard to fundamental rights. Furthermore, the digitalization of court proceedings may not be as inclusive and easy as one might think at first glance. It is seldom advisable to close your mind to new technology and new opportunities, but there must be no digitalization at all costs.

REFERENCES

1. Bassar, E., Hiéramente, S. (2018) „Datenbeschlagnahme in Wirtschaftsstrafverfahren und die Frage der Datenlöschung", *NStZ,* 681-687.
2. Bildner, A. (2021) „Zugriff auf Auswertung von Massendaten im Strafverfahren", *KriPoZ Sammelband Digitalisierung im Straf- und Strafprozessrecht*, 3-21.
3. Blechschmitt, L. (2018) „Auswirkungen des stetigen Datenaustauschs auf das strafrechtliche Ermittlungsverfahren", *MMR*, 361-366.
4. Dauster, M. (2022) "Criminal Proceedings in Times of Pandemic", In: University of Latvia (ed.), *New Legal Reality: Challenges and Perspectives*. II. Collection of research papers in conjunction with the 8th International Conference of the Faculty of Law of the University of Latvia, Riga: University of Latvia Press, 248 – 271.
5. Dorschel, J. (2015) *Praxishandbuch Big Data*, Wiesbaden: Springer Gabler.
6. Esser, R. (2020) „Digitalisierung und Strafvollzug", In: *Digitalisierung und Strafverfahren*, (Elisa Hoven, Hans Kudlich (eds.)), Baden-Baden: Nomos, 217-246.
7. Fährmann, J. (2020) "Digitale Beweismittel und Datenmengen im Strafprozess", *MMR,* 228-233.
8. Jahn, M., Brodowski, D. (2020) „Digitale Beweismittel im deutschen Strafprozess – Ermittlungsverfahren, Hauptverfahren und Revision", In: *Digitalisierung und Strafverfahren*, (Elisa Hoven, Hans Kudlich (eds.)), Baden-Baden: Nomos, 67-102.
9. Möllers, F., Salemi, S., Schliwinski, N. (2022) In: *Recht Digital – 25 Jahre* (Schweighofer Erich, Kummer Franz (eds.)), Tagungsband des 25. Internationalen Rechtsinformatik Symposions Bern: IRIS, 169-178.
10. Moore, G. E. (1965) "Cramming more components onto integrated circuits", In: *Electronics*, Vol. 38, Issue 8.
11. Rebehn, S. (2022) "Mehr als 50.000 Videoverhandlungen in 2021", *DRiZ*, pp. 150.
12. Reinsel D., Gantz, J., Rydning, J. (2018) *Data Age 2025: The Digitization of the World From Edge to Core*, IDC White Paper.
13. Rückert, C. (2020) „Herausforderungen der Digitalisierung für das Strafverfahren", In: *Digitalisierung und Strafverfahren*, (Elisa Hoven, Hans Kudlich (eds.)), Baden-Baden: Nomos, 9–38.
14. Peters, K. (2017) „Anwesenheitsrechte bei der Durchsicht gemäß § 110 StPO: Bekämpfung der Risiken und Nebenwirkungen einer übermächtigen Ermittlungsmaßnahme", *NZWiSt* 2017, pp. 465-473 (p. 473).
15. Schneider, F. (2020) „Auswirkungen der Digitalisierung auf das Ermittlungsverfahren, ZIS 02/2020, pp. 79-83 (p. 80).
16. Vailshery, L. S. (2021) *IoT and non-IoT connections worldwide 2010-2025*, https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

Other sources

1. LG Regensburg, verdict of 16 December 2020 – file no.: Ks 103 Js 28875/19.
2. OLG Frankfurt a.M., decision of 20 July 2021, file no.: 3 Ws 369/21.
3. BGHSt 18, 51.
4. BGHSt 27, 135.
5. BVerfGE 65, 1.
6. BVerfGE 109, 279
7. BVerfGE 113, 29.
8. BVerfGE 115, 166.
9. BVerfGE 120, 274
10. BVerfGE 124, 43.
11. BVerfGE 130, 151.
12. BVerfG NJW 2015, 2777.

DIGITALIZACIJA U NEMAČKOM KRIVIČNOM POSTUPKU I PRATEĆI ASPEKTI OSNOVNIH LJUDSKIH PRAVA

Digitalizacija sve više dopire i do oblasti krivčnog procesnog prava. Predmet ovog rada je ukazivanje na korišćenje digitalizacije u krivičnom postupku prema odredbama nemačkog Zakonika o krivičnom postupku. Fokus rada je na nedavnim zakonskim izmenama, a koje se odnose na elektornsko upravljanje dosijeima i elektronski prenos dosijea između sudova i organa za sprovođenje zakona. Osim toga, autori u ovom radu analiziraju efikasnost davno uspostavljenih i uglavnom nepromenjenih proceduralnih pravila i načela nemačkog krivičnog postupka u kontekstu digitalizacije i digitalnih dokaza. U radu se postavlja pitanje da li je i kako digitalizacija krivično procesnog prava kompatibilna sa nemačkim osnovnim pravima, dokazujući da mnoge istražne mere kada se primenjuju na ditialne dokaze mogu lako da ugroze osnovna ljudska prava, pa stoga digitalizacija krivičnog sudskog postupka ne može biti isključivo korisna. Uzimajući u obzir navedenu mogućnost, potrebno je da se prema digitalizaciji zauzme odgovoran i pažljiv pristup, a što ukazuje da je neophodna izmena postojećeg zakonodavstva u vezi sa digitalizacijom kako bi se zaštitila prava lica uključenih u digitalizovan krivični postupak, a posebno okrivljenih ili optuženih lica.

KLJUČNE REČI: *digitalni dokazi, istražne mere, elektronsko upravljanje fajlovima, osnovna prava, pravo na privatnost komunikacija.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.18

THE RIGHT TO A FAIR TRIAL IN THE ERA OF DIGITALIZATION

Bianca Mirabela Șerb*

The right to a fair trial represents one of the elements of the principle of ensuring the rule of law in a democratic society. Article 6 of the European Convention on Human Rights, entitled "Right to a fair trial", designates, on the one hand, all the procedural guarantees set out expressly by that provision and, on the other hand, the general and implied guarantee to a fair trial. In order to deliver a fair, efficient, and accessible justice - a crucial component of the rule of law - the use of information and communication technologies has become indispensable to the modernization of justice. This facilitates access to courts, reduces delays, boosts the quality-of-service delivery, and brings citizens closer to trusted justice systems.

KEYWORDS: *European Convention on Human Rights (ECHR), European Court of Human Rights (ECHR), European Commission for the efficiency of justice (CEPEJ), proceedings, fair trial.*

* Ph.D, West University of Timișoara – Faculty of law, Coordinator: professor Valentin Constantin.
E-mail: *bianca.serb94@e-uvt.ro*

INTRODUCTION

This article proposes an analysis of the procedural guarantees enshrined in art. 6 of the European Convention on Human Rights and their appliance in the era of digitalization. The paper is centered around the principle of a fair trial. The article begins with a chapter that contains some general information concerning the right to a fair trial. The next chapter offers a more detailed analysis of art. 6 of the Convention, presenting both the expressed and implied guarantees of the right to a fair trial based on their scope and content. The chapter is based on the ECtHR interpretation and has references to the legal literature. The next chapter presents CEPEJ as a body of the European Counsel. The fourth chapter embodies a short analysis of some of the guarantees of the right to a fair trial which are commonly manifested in the digitalized era.

1. GENERAL ASPECTS REGARDING THE EUROPEAN CONVENTION ON HUMAN RIGHTS AND THE RIGHT TO A FAIR TRIAL

Article 6 of the European Convention on Human Rights[1] has its origins in the texts of art. 10 and art. 11 (1) of the Universal Declaration of Human Rights. According to art. 10 of the Declaration, "Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him." and Article 11 (1) provides that "Everyone charged with a penal offense has the right to be presumed innocent until proved guilty according to the law in a public trial at which he has had all the guarantees necessary for his defence."

The Convention must be regarded as a system of objective protection of human rights (EctHR, *Case of Sporrong and Lonnroth v. Sweden*, Case No. 7151/75, point 12). The constant concern of the ECtHR is to protect rights that are "practical and effective as opposed to theoretical and illusory" (ECtHR, case of Mehmet Eren v. Turkey, Case No. 32347/02 , point 50). This means giving priority to the effectiveness of the protection rather than to legal formalism. The Convention regulates, in principle, rights with substantially "material" content, which can be invoked directly in the internal order of the Contracting States. In addition to these substantial rights, such as the right to life, liberty, and security, the right to freedom of thought, conscience and religion, etc., the Convention regulates two procedural rights, which do not consider certain freedoms of a person, but it consists in guarantees regarding the enhancement of the rights and freedoms that are recognized before the courts.

The right to a fair trial is one of the components of the principle of ensuring the rule of law in a democratic society. As the ECtHR pointed out, the Member States have decided to take all necessary measures to effectively defend the rights enshrined in the Universal Declaration of Human Rights, "because of their sincere attachment to the principle of the rule of law." (Birsan, 2005: 357).

[1] Hereinafter reffered to as the Convention.

Art. 6 enjoys significant autonomy within the national laws of the Contracting States, including its substantive as well as procedural provisions. Therefore, a procedural error within the meaning of national law will not necessarily amount to a breach of the art. 6. Art. 6 is essentially concerned with whether an applicant was afforded ample opportunities to state his case and contest the evidence that he considered false, and not with whether the national courts reached a right or wrong decision (ECtHR, case of Karalevičius v. Lithuania, Case No. 53254/99).

Article 6 does not enable the ECtHR to act as a supreme (higher) court which may re-establish the facts of the case or re-examine the alleged breaches of national law (ECtHR, case of Bernard v. France, Case No. 22885/93, points 37-41), nor to rule on the admissibility of evidence (ECtHR, case of Bernard v. France, Case No. 22885/93, points 37-41). The jurisdiction of the ECtHR is governed by the principle of subsidiarity. However, the ECtHR has occasionally found violations of art. 6 on the account of the persistence of conflicting court decisions on the same issue made within a single court of appeal, or by the different district court's ruling on appeal, stressing that the "profound and long-standing" nature of the divergences at issue was incompatible with the principle of legal certainty in its broad meaning. At the same time, the Grand Chamber stressed that it was not the Court's function under art. 6 to compare different decisions of national courts – even if given in apparently similar proceedings – save in cases of evident arbitrariness (Rónai: 2013).

The right established by the text of art. 6, about its substance, is a procedural right but seen as an obligation of the Member States, it can also be analyzed as a real substantive right, with the specific sanction - the international liability of the states concerned - in case of non-compliance with one of its components. The Contracting States are required by Article 1 of the Convention to organize their legal systems to ensure compliance with art. 6 (Birsan, 2010: 357). According to the principle of autonomous interpretation of Article 6, the ECtHR decides the question of applicability of this provision under civil rights and obligations. Applicability of this article to pre-trial, appeal, and other review stages is established based on non-autonomous criteria and depends to a large extent on the existence of accessible remedies in national law (ECtHR, case of Delcourt v. Belgium, Case No. 2689/65, points 23-26).

1.1. Article 6 of the European Convention on Human Rights

Article 6 paragraph 1 provides:

"In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order, or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."

The main difference between the requirement of "fairness" and all the other elements of art. 6 is that "fairness" concerns the procedure as a whole and not just in the light of a particular incident or a procedural error.

The concept of "fairness" has autonomous meaning being irrelevant to the meaning of this concept under the national law system of the Member States. Therefore, there may be situations in which, although there is a violation of the domestic procedural rules - even a flagrant one – from the perspective of the Convention the trial would be considered fair and vice versa (ECtHR, case of Gafgen v. Germany, Case No. 22978/05, points 162-188).

There were also situations in which the Court declared the national proceedings unfair due to the cumulative effect of the procedural errors, although each error considered individually would not have constituted a violation of art. 6 (ECtHR, case of Barbera, Maessegue and Jabardo v. Spain, Case No. 10590/83).

When analysing whether the condition of "fairness" is met, the ECtHR is concerned with verifying whether the parties have had sufficient opportunities to prepare and defend their case, leaving the Member States a considerable margin of discretion regarding the procedural rules if the trial itself, as a whole, is not affected and meets the conditions laid down by the Convention.

In the system established by the European Convention, the right to a fair trial can be viewed in a broad sense, but if we limit ourselves strictly to the first paragraph, we observe that it contains a list of general guarantees - the right to a fair trial, the right to a public hearing within a reasonable time by an independent and impartial tribunal established by law. These procedural guarantees can be divided into two categories: express and implied.

The first category includes the right to be judged within a reasonable time; the right to be judged by an independent and impartial tribunal established by law; the publicity of the procedure (except in cases where access to the courtroom is prohibited to the press, the public or a party to the proceedings, in the interests of morality, public order or national security, in order to protect the interests of minors or the privacy of the parties involved in the proceedings, or when advertising could harm the interests of justice). These guarantees are expressly stated in art. 6 and can be considered absolute in the sense that depriving a person of such rights would inevitably lead to an unfair trial.

Guarantees that are not expressly mentioned by the text of art. 6, stem from its interpretation and were developed by the ECtHR through its case law. The implied guarantees are the right to have access to justice, the principle of contradictoriality, the principle of equality of arms, the right to a reasoned decision, and the obligation to ensure the enforcement of the judgment. These guarantees are not absolute hence non-compliance or limitation of these rights in some situations does not automatically lead to an unfair trial. Moreover, the ECtHR has emphasized in many of its judgments that its role is to determine whether the procedure as a whole was fair. It does not replace a national court and does not analyse the merits of the case, it does not become a jurisdiction of the fourth degree, but analyses aspects related to procedural issues strictly.

Concerning the implied guarantees, no precise distinction can be made between them. Moreover, the case law of the ECtHR is not consistent in making a clear distinction between the principle of equality of arms and the principle of contradictoriality. The ECtHR pointed out that the principle of equality of arms is an element of the broader notion of a fair trial, which also encompasses the fundamental principle of contradictoriality, emphasizing that the principle of equality of arms does not exhaust the entire content of paragraph 1 of art. 6. Equality of arms is only one aspect of the much broader notion of a fair trial before an independent and impartial tribunal.

2. DIGITALIZATION OF THE JUDICIAL SYSTEM IN EUROPE

In 2002, the Committee of Ministers of the Council of Europe established the European Commission for the Efficiency of Justice (hereinafter CEPEJ) as an innovative body for improving the quality and efficiency of the European judicial systems and strengthening the court users' confidence in such systems.

According to Resolution Res (2002)12 when creating the CEPEJ, the Member States considered that the rule of law principle cannot be ensured without a fair, efficient, and accessible judicial system.

The CEPEJ's mission is to enhance the effectiveness and operation of the judicial system in the Member States and to advance the application of the Council of Europe's adopted instruments in this regard.

The European Council of Europe's desire to advance the rule of law and fundamental rights in Europe is evident in the creation of the CEPEJ, which is based on the European Convention on Human Rights, particularly Articles 5 (Right to liberty and security), 6 (Right to a fair trial), 13, and 14 (Right to an Effective Remedy) (Prohibition of discrimination).

The creation of CEPEJ, which is supported by the Directorate General of Human Rights and Legal Affairs, demonstrates the Council of Europe's intention to develop not only international legal instruments but also to advance a thorough understanding of the European judicial systems and the various tools currently in use, allowing it to recognize any challenges and aid in their resolution.

The CEPEJ will be tasked with, among other things, carrying on the ongoing discussion about the opportunity presented by modern information technology (IT) to enhance the effectiveness of justice. The CEPEJ's Statute governs how it operates (see Appendix 2 to Resolution Res(2002)12).

The statute of the CEPEJ places a strong emphasis on judicial system comparisons and the sharing of information about how they operate. This comparison highlights justice's effectiveness and quality rather than "just" efficiency in the limited sense.

To carry out these responsibilities, the CEPEJ has established a regular process for assessing the judicial systems of the Council of Europe's member states. A series of Working Group has been established, among which we mention (CEPEJ-GT-EVAL, CEPEJ-COLLET, CEPEJ-STAT, SATURN etc).

During their meeting in Istanbul for the 30th Conference (24–26 November 2010), the Ministers of Justice of the Council of Europe's member states adopted Resolution No. 1 on a modern, transparent, and efficient justice. This resolution "invited the Committee of Ministers to build on the work of the SATURN Working group within CEPEJ, further developing its capacity to acquire a better understanding of the time required for judicial proceedings in the Member States, with a view to developing tools to enable the Member States to better meet their obligations under Article 6 of the ECHR regarding the right to a fair trial within a reasonable time".

„Digitalization for a better justice" is the name of the CEPEJ`s Action plan for 2022-2025. The Action Plan has been adopted at the 37th CEPEJ plenary meeting in Strasbourg on 8 and 9 December 2021. According to this plan, the priority of the CEPEJ for the next four years is to accompany States and courts in a successful transition towards digitalization of justice in line with European standards and in particular Article 6 of the European Convention on Human Rights.

3. ARTICLE 6 AND THE DIGITALIZED JUDICIARY

Many deeply ingrained expectations and notions about court proceedings exist in modern society. Our moral compass directs us to the definition of a fair trial when defining these expectations. We may all agree that courts should follow the principle to a fair trial when conducting their activities. In this section, we examine a few particular aspects of the fair trial principle by examining potential obstacles that might intervene as a result of digitalization.

Some of the core aspects of a fair trial, as defined by Article 6 of the European Convention on Human Rights, are a public hearing, the right to have access to justice, and the personal participation of the parties in the proceedings. Although the ECtHR's case law provides us with specific guidance on the demands resulting from this principle, we must keep in mind that the interpretation of the Convention and, consequently, of Article 6 will always be subject to present-day conditions. The idea that the ECHR is a "living instrument" implies that its rules, principles, and standards are not static and that how they are applied must consider social and economic changes (See: ECtHR, Case of Tyrer v the United Kingdom).

3.1. Public hearing

It was held by the Court that the right to a public hearing would be devoid of substance if a party to a case were not apprised of a hearing in such a way as to have an opportunity to attend it, should he or she decide to exercise the right to appear that is established in the domestic law (ECtHR, case of Yakovlev v. Russia, Case No. 72701/01).

As regards notifications of proceedings and service of decisions in the context of procedural rights protected by Article 6 of the Convention, the Court held that Article 6

§ 1 cannot be construed as conferring on litigants the right to obtain a specific form of service of court documents, such as by registered post (ECtHR, case of Kolegovy v. Russia, Case No. 15226/05). Nonetheless, the Court considered that in the interests of the administration of justice a litigant should be notified of a court hearing in such a way as to not only have knowledge of the date, time, and place of the hearing but also to have enough time to prepare his or her case and to attend the court hearing (ECtHR, case of Aždajić v. Slovenia, Case No. 71872/128).

3.2. Access to justice

In order to prevent the parties from committing too many procedural errors, the practice has been to provide the parties with pre-determined forms for drafting their submissions. The idea behind this is that it is easier to obtain properly drafted pleadings if the parties work from a template. The use of forms, especially where this is mandatory, is not something that appears in the published case law of the European Court of Human Rights. However, given that the Court itself imposes the lodging of applications by means of forms, it is unlikely that making them mandatory can be regarded as a disproportionate restriction on the right of access to a court guaranteed by Article 6 paragraph 1 ECHR.

3.3. Personal participation of the parties in the proceedings

The Court has not addressed this issue extensively. ECtHR`s case law does not consider that the right to a fair trial goes so far as to enshrine the right to personal participation by the parties in the proceedings (ECtHR, case of Karpenko v. Russia, Case No. 5605/04). Participation via a representative – such as a lawyer – is in principle sufficient in civil matters (ECtHR, case of Khuzhin v. Russia, Case No. 13470/02), unless the proceedings relate more specifically to the character, lifestyle, or conduct of one of the parties (ECtHR, case of Urbšienė and Urbšys v. Lithuania, Case No. 16580/09). Apart from these particular situations, the Court does not lay down a requirement for the personal participation of the parties in the proceedings. This means that civil proceedings can take place without the judge ever meeting the parties, without the parties being allowed to speak at a hearing, or even without them having a real understanding of the issues at stake and how the proceedings unfold (CEPEJ, Guidelines and comparative study centrality user, P.19).

In the most recent years, the use of new information and communication technologies (ICTs) and the shift to Cyberjustice, which can be seen in the generality of the CoE countries, have had a significant impact on the effectiveness of the user's right to obtain adequate information about the procedure that concerns him/her. Beyond the general online information about the extent of the rights of litigants and the procedural ways to implement or defend them, users can increasingly obtain, through dynamic questionnaires that help them better clarify the dispute in question, personalized and

contextualized information allowing them to continue their institutional journey with the appropriate institutions. Above all, the user now has the opportunity to follow online the progress and the status of his "procedure" (stages, schedule of hearings, deadlines provided) with the competent court, as long as the competent court uses a computer system in the management of cases (CEPEJ, Guidelines and comparative study centrality user, P.20).

Moreover, as regards the right to a fair trial and effective legal assistance when the applicant's participation in the hearings in criminal proceedings against him is limited to videoconference, the Court has held that while such participation was not, as such, contrary to the right to a fair trial, arrangements had to be made for the applicants to follow the proceedings, to be heard without technical impediments, and to communicate effectively and confidentially with their lawyer. In case of *Sakhnovskiy* (ECtHR, case of Sakhnovskiy v. Russia (GC), Case No. 21272/03), the applicant had been able to communicate with the lawyer for only fifteen minutes, immediately before the start of the hearing. The Court held that given the complexity and seriousness of the case, the time allotted had not been sufficient for the applicant to discuss the case and make sure that the lawyer's knowledge of the case and legal position were appropriate. Moreover, it was questionable whether communication by video link, installed and operated by the State, had offered sufficient privacy. The applicant might legitimately have felt ill at ease when he discussed his case with the lawyer. The Court noted that the Government had not explained why it had been impossible to make different arrangements for the applicant's legal assistance and held it has been a violation of Article 6 paragraphs 1 and 3 c) of the Convention (ECtHR, The Rule of Law and Justice in a digital age, 2021).

CONCLUSION

In order to make sure that their judicial systems run in accordance with ECHR`s standards and satisfy the needs of persons seeking justice, Member States get assistance from the European Commission for the Efficiency of Justice (CEPEJ) of the Council of Europe.

The public interest in justice must be upheld to the greatest extent possible, and this includes facilitating access to justice through alternative channels like online services or enhancing informational accessibility via court websites and other channels of communication (phone, email, etc.).

In order to deliver a fair, efficient, and accessible justice - a crucial component of the rule of law - the use of information and communication technologies has become indispensable to the modernization of justice. This facilitates access to courts, reduces delays, boosts the quality of service delivery, and brings citizens closer to trusted justice systems.

The public service of justice has the chance to continue operating thanks to the use of digital technologies. However, both its quick development and overuse could have detrimental effects. Future developments in digital justice, including online services, distant hearings, and videoconferences, must always uphold fundamental rights and the rules of a fair trial.

REFERENCES

1. Bîrsan, C. (2005) *Convenția europeană a drepturilor omului. Comentariu pe articole*, Volumul II, Drepturi și libertăți, București: Ed. C.H. Beck.
2. Bîrsan, C. (2010) *Convenția europeană a drepturilor omului. Comentariu pe articole*, Ediția 2, București: Ed. C.H. Beck.
3. ECtHR, Background paper for the Judicial Seminar 2021: The Rule of Law and Justice in a digital age, 1st of July 2021.
4. ECtHR, case of Aždajić v. Slovenia, Case No. 71872/128.
5. ECtHR, case of Barbera, Maessegue and Jabardo v. Spain, Case No. 10590/83.
6. ECtHR, case of Bernard v. France, Case No. 22885/93ECtHR, case of Delcourt v. Belgium, Case No. 2689/65 .
7. ECtHR, case of Gafgen v. Germany, Case No. 22978/05.
8. ECtHR, case of Karalevičius v. Lithuania, Case No. 53254/99.
9. ECtHR, case of Karpenko v. Russia, Case No. 5605/04.
10. ECtHR, case of Khuzhin v. Russia, Case No. 13470/02.
11. ECtHR, case of Kolegovy v. Russia, Case No. 15226/05.
12. ECtHR, case of Mehmet Eren v. Turkey, Case No. 32347/02.
13. ECtHR, case of Sakhnovskiy v. Russia (GC), Case No. 21272/03.
14. ECtHR, case of Schenk v. Switzerland, Case No. 10862/84.
15. ECtHR, case of Sporrong and Lonnroth v. Sweden, Case No. 7151/75.
16. ECtHR, case of Urbšienė and Urbšys v. Lithuania, Case No. 16580/09.
17. ECtHR, case of Yakovlev v. Russia, Case No. 72701/01.
18. Rónai, O. (2013) "A general overview of Article 6 I. of the ECHR", *Conference: Doktorandusz Fórum at: Miskolc, Hungary*, retrieved from https://www.researchgate.net/publication/258963140_A_general_overview_of_Article_6_I_of_the_European_Convention_on_Human_Rights.

PRAVO NA PRAVIČNO SUĐENJE U ERI DIGITALIZACIJE

Pravo na pravično suđenje predstavlja jedan od elemenata principa vladavine prava u demokratskom društvu. Član 6. Evropske konvencije o ljudskim pravima, pod nazivom „Pravo na pravično suđenje" s jedne strane podrazumeva sve procesne garancije izričito utvrđene tom odredbom, a sa druge strane opštu garanciju za pravično suđenje. Da bi se obezbedila pravična, efikasna i dostupna pravda kao ključna komponenta vladavine prava, korišćenje informacionih tehnologija postalo je neophodno. Ono je ujedno od značaja i za modernizaciju pravosuđa i podrazumeva olakšan pristup sudovima, unapređuje efikasnost suđenja, povećava opšti kvalitet pružanja usluga i unapređuje dostupnost pravosuđa građanima, a što ujedno i povećava njihovo poverenje u rad pravosuđa.

KLJUČNE REČI: *Evropska konvencija o ljudskim pravima (ECHR), Evropski sud za ljudska prava (EctHR), Evropska komisija za efikasnost pravosuđa (CEPEJ), postupak, pravično suđenje.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.19

PRIMENA DIGITALNE TEHNOLOGIJE U KONTEKSTU KRIVIČNOPRAVNE REAKCIJE NA KRIMINAL I PRAVO NA POŠTOVANJE PRIVATNOG ŽIVOTA: RASKORAK U BALANSIRANJU IZMEĐU JAVNOG I PRIVATNOG INTERESA
sa posebnim osvrtom na praksu Evropskog suda za ljudska prava

Nikola Paunović*

Svakodnevni razvoj digitalnih tehnologija i nove mogućnosti koje pružaju umnogome oblikuju naše delovanje podstičući nas da se navikavamo i da usvajamo trenutna tehnološka dostignuća. Jedna od mnogih oblasti u kojoj primena digitalnih tehnologija dobija na sve većem značaju jeste i kriminalistička praksa, što omogućava nadležnim organima korišćenje savremenijih metoda i tehnika u otkrivanju i evidentiranju podataka od krivičnopravnog značaja. Polazeći od toga da izložena tendencija usmerena ka digitalizaciji kriminalističkog postupanja poprima sve šire razmere, u radu se nastoje analizirati najzastupljenija tehnološka dostignuća koja nalaze svoju primenu u ovoj oblasti, sa posebnim osvrtom na praksu Evropskog suda za ljudska prava, kako bi se uvideli njihovi potencijalni rizici. U zaključnim razmatranjima se ističe da primena digitalnih tehnologija u kriminalističkoj praksi osim što nadležnim organima donosi niz novih mogućnosti u praktičnom radu, istovremeno stvara i brojne rizike od arbitrarnog i prekomernog zadiranja u osnovna prava i slobode ljudi. Stoga se naglašava da imperativ pre i za vreme njihovog sprovođenja mora biti usmeren ka pravilnom odmeravanju balansa između javnog interesa koji nalaže njihovu primenu radi sprečavanja nereda ili kriminala i privatnog interesa građana koji diktira da njihova zajemčena prava ne smeju biti povređena odnosno ugrožena.

KLJUČNE REČI: *digitalne tehnologije, kriminal, Evropski sud za ljudska prava, javni interes, pravo na poštovanje privatnog života.*

* Treći sekretar u Ministarstvu spoljnih poslova Republike Srbije i doktorand Pravnog fakulteta Univerziteta u Beogradu. E-mail: *dzoni925@gmail.com*

UVOD

Svedoci smo vremena u kojem se neprestano odvija rapidni razvoj digitalne tehnologije čija primena ispunjava čitave sfere društvenog života, stvarajući brojne nove mogućnosti za obavljanje niza aktivnosti u virtuelnom prostoru. U eri informatičkog društva čiji smo savremenici tradicionalne metode i tehnike za otkrivanje i registrovanje krivičnih dela se uveliko zamenjuju inovativnim tehnološkim dostignućima. Sve evidentnija potreba za primenom tehnoloških dostignuća u svakodnevnom radu nije zaobišla ni sferu kriminalističke prakse u kojoj se primećuje da proces digitalizacije metoda i tehnika koji se koristi u cilju otkrivanja krivičnih dela dobija na posebnom značaju (Kostić & Mrvić- Petrović, 2021: 51).

Navedena činjenica uticala je i na sve učestaliju prisutnost diskusija u stručnim i naučnim krugovima o mogućnostima i rizicima korišćenja digitalnih tehnologija. Mogućnosti koje one pružaju u kontekstu detekcije kriminala je teško pobrojati na jednom mestu budući da lista potencijalnih metoda i tehnika zavisi od vrste kriminaliteta koje je predmet istražnog postupka, ali i od raspoloživih tehnoloških kapaciteta sa kojim raspolažu nadležni organi, budući da je nivo razvijenosti i dostupnosti tehnoloških inovacija različit od zemlje do zemlje. Imajući u vidu navedeno, u radu se nastoje analizirati savremena dostignuća koja su nastala kao rezultat tehnoloških inovacija, pri čemu svoju primenu nalaze u kontekstu otkrivanja i registrovanja krivičnih dela. Osim toga, razmatraju se i potencijalne implikacije koje mogu nastati na planu legaliteta njihove primene kao rezultat njihove primene u svrhe otkrivanja i evidentiranja krivičnih dela. Navedeno naročito dolazi do izražaja u slučaju narušavanja ravnoteže između javnog interesa oličenog u potrebi primene digitalnih istražnih metoda u cilju prevencije kriminala i privatnog interesa lica prema kojima se one preduzimaju koji diktira zaštitu njihovog privatnog života od neopravdanog i preteranog zadiranja u njihova zajemčena prava (Kostić & Jelisavac-Trošić, 2017: 33).

Kako bi se došlo do pravog odgovora na predmetno pitanje i time sprečile povrede prava na privatni život potrebno je u svakom slučaju voditi računa o tome da li su metode koje se koriste u kontekstu otkrivanja i evidentiranja krivičnih dela preduzete u skladu sa zakonskim okvirima koji propisuju uslove za njihovu primenu, te da li se njihovim sprovođenjem ostvaruje legitimni cilj u meri u kojoj je to neophodno u demokratskom društvu (Council of Europe, 2020: 23-30). Upravo o navedenom pitanju koje nalaže pravilno odmeravanje ravnoteže između javnog i privatnog interesa u slučajevima primene digitalnih tehnologija u kontekstu otkrivanja i registrovanja krivičnih dela bilo je reči u čitavom nizu predmeta koji su rešavani pred Evropskim sudom za ljudska prava (u daljem tekstu: Sud). U tom smislu, u daljim redovima, potrebno je analizirati koje uslove Sud vrednuje u procesu donošenja zaključka da li je bilo povrede prava na privatni život usled primene digitalnih tehnologija. Ovom prilikom treba ukazati da Sud podvodi predmetne slučajeve pod član 8 Konvencije za zaštitu ljudskih prava i osnovnih sloboda (u daljem tekstu: Konvencija) koji propisuje da svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske. S tim u vezi, javne vlasti neće se mešati u

vršenje ovog prava sem ako to nije u skladu sa zakonom i neophodno u demokratskom društvu u interesu nacionalne bezbednosti, javne bezbednosti ili ekonomske dobrobiti zemlje, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili morala, ili radi zaštite prava i sloboda drugih.[1]

1. PRAVO NA POŠTOVANJE PRIVATNOG ŽIVOTA U KONTEKSTU OTKRIVANJA PODATAKA OD KRIVIČNOPRAVNOG ZNAČAJA PRIMENOM DIGITALNE TEHNOLOGIJE

Nadležni organi u cilju otkrivanja krivičnih dela i identifikacije potencijalnih osumnjičenih sprovode niz kriminalističkih operativnih radnji putem kojih dolaze do podataka od značaja za pokretanje i vođenje krivičnog postupka (Škulić, 2011: 213). Jedna od najzastupljenijih savremenih tehnoloških dostignuća koja omogućava prikupljanje potrebnh informacija jeste primena *metode globalnog pozicionog sistema* koja omogućava praćenje targetiranih osoba u prostoru i vremenu. O iznetom pitanju bilo je reči u predmetu *Uzun protiv Nemačke* u kome se podnosilac predstavke, osumnjičen za umešanost u bombaške napade, žalio da je njegovim praćenjem putem GPS-a i korišćenjem podataka dobijenih na taj način u krivičnom postupku koji se vodio protiv njega povređeno pravo na poštovanje privatnog života. Sud je smatrao da nije došlo do povrede člana 8. Konvencije, nalazeći da su nadležni organi primenom ove metode, uprkos tome što su GPS nadzor, kao i obrada i korišćenje podataka dobijenih na taj način ometali pravo podnosioca predstavke na poštovanje njegovog privatnog život, težili ostvarivanju legitimnih ciljeva zaštite nacionalne bezbednosti, javne bezbednosti i prava žrtava, kao i sprečavanja kriminala. Pored toga Sud je utvrdio da je primena ove metode bila proporcionalna cilju koji se želeo ostvariti, što svedoči iz činjenice da je GPS nadzor naložen tek nakon što su se druge istražne metode pokazale nedovoljnim, te da je sproveden u relativno kratkom periodu (oko tri meseca). Konačno, Sud je našao da je njena primena bila mera koja je neophodna u demokratskom društvu, budući da se istraga ticala veoma teških zločina (European Court of Human Rights, 2022A: 12).[2] Takođe, o predmetnoj problematici bilo je reči u predmetu *Ben Faiza protiv Francuske* koji se odnosio na primenu mere GPS nadzora preduzete protiv podnosioca predstavke u krivičnoj istrazi o njegovoj umešanosti u izvršenje krivičnih dela trgovine drogom. Podnosilac predstavke je naveo da je primena ove mere predstavljala mešanje u njegovo pravo na poštovanje njegovog privatnog života. Sud je smatrao da je došlo do povrede člana 8. Konvencije nalazeći da relevantni zakoni nisu sadržali odredbe o tome u kojoj meri i u kojim slučajevima su vlasti imale pravo da koriste svoje diskreciono pravo u pogledu određivanja primene GPS nadzora. Iz tog razloga, u ovom slučaju, podnosilac predstavke nije uživao minimalnu zaštitu neophodnu u demokratskom društvu (European Court of Human Rights, 2022A: 12).[3]

[1] Konvencija za zaštitu ljudskih prava i osnovnih sloboda Rim, 4. novembra 1950.

[2] Uzun v. Germany, application no. 35623/05, Judgment 2 September 2010.

[3] Ben Faiza v. France, application no. 31446/12, Judgment 8 February 2018.

Osim primene metode globalnog pozicionog sistema, u kriminalističkoj praksi se u velikom broju slučajeva koriste i *tehnike tajnog audio i/ili video snimanja* targetiranih lica (Škulić, 2015: 24). O navedenom pitanju bilo je reči u predmetu *Perri protiv Ujedinjenog Kraljevstva* u kome se podnosilac predstavke žalio da mu je povređeno pravo na privatni život time što ga je policija tajno snimala u policijskoj stanici u svrhu identifikacije zbog sumnji da je izvršilac čitavog niza krivičnih dela razbojništva. Sud je smatrao da je došlo do povrede člana 8. Konvencije budući da je uočeno da podnosilac predstavke nije mogao naslutiti da će ga snimati u policijskoj stanici. Iz navedenog proizilazi da predmetno zadiranje u pravo na privatni život podnosioca nije bilo u skladu sa zakonom jer policija nije ispoštovala važeće propise koji su nalagali da se pre prethodnog snimanja pribavi saglasnost podnosioca predstavke, da je neophodno to lice obavesti da će se pristupiti snimanju, te da se informiše o njegovim pravima u tom pogledu (European Court of Human Rights, 2022A: 27).[4]

S druge strane, o primeni metode video snimanja targetiranih lica svedoči slučaj *Gorlov i drugi protiv Rusije* u kome su se podnosioci predstavke žalili da je usled stalnog nadzora njihovih ćelija njihovo pravo na poštovanje privatnog života bilo povređeno. Sud je smatrao da je došlo do povrede člana 8 Konvencije, nalazeći da predmetna mera nije bila u skladu sa zakonom. Ovo stoga što se iako moglo prihvatiti da je bilo potrebno stalno video snimati određene delove kazneno-popravnih ustanova ili određene pritvorenike, činjenica je da relevantni pravni okvir u Rusiji nije pružao dovoljno jasne, precizne i detaljne garancije za zaštitu od proizvoljnog mešanja javnih vlasti u pravo na poštovanje privatnog života (European Court of Human Rights, 2022A: 29).[5] O metodi video snimanja od strane nadležnih organa bilo je reči i u predmetu *Vasilica Mocanu protiv Rumunije* u kome se podnosilac predstavke žalio da je tokom zadržavanja u policijskim prostorijama njegova ćelija bila pod video nadzorom. Sud je smatrao da je došlo do povrede člana 8 Konvencije, nalazeći da nadzor podnosioca predstavke video kamerom koja je bila instalirana u ćeliji u kojoj je bio smešten nije bio u skladu sa domaćim zakonom (European Court of Human Rights, 2022A: 28).[6]

Osim tajnog snimanja u kriminalističkoj praksi se često koristi i *metoda tajnog nadzora ostvarenih komunikacija* o čemu je bilo reči u slučaju *Karabejoglu protiv Turske* koja se sprovodila u kontekstu krivične istrage protiv predmetnog lica u cilju daljeg korišćenja tako dobijenih informacija u istrazi. Sud je smatrao da nije bilo povrede člana 8. Konvencije u vezi sa prisluškivanjem telefona za potrebe krivične istrage, ali da je došlo do povrede člana 8. u pogledu korišćenja informacija dobijenih prisluškivanjem u disciplinskom postupku. Sud je posebno utvrdio da je tokom krivične istrage podnosilac predstavke uživao minimalni stepen zaštite koji je neophodan u demokratskom društvu, budući da je prisluškivanje naređeno na osnovu objektivno opravdane sumnje i da je izvršeno u skladu sa relevantnim zakonodavstvom. Osim toga, po mišljenju Suda,

[4] Perry v. the United Kingdom, application no. 63737/00, Judgment 17 July 2003.

[5] Gorlov and Others v. Russia, application no. 27057/06 and 2 others, Vakhmistrov v. Russia application no. 56443/09, Sablin v. Russia application no. 25147/14, Judgment 2 July 2019.

[6] Vasilică Mocanu v. Romania, application no 43545/13, Judgment 6 December 2016.

zadiranje u pravo podnosioca predstavke na poštovanje njegovog privatnog života bilo je neophodno u interesu nacionalne bezbednosti i radi sprečavanja nereda i zločina. Međutim, korišćenje tako dobijenih informacija u kontekstu disciplinske istrage nije bilo u skladu sa zakonom, usled toga što je relevantno zakonodavstvo prekršeno u pogledu zabrane korišćenja informacija u druge svrhe osim onih za koje su prikupljene, ali i kršenju obaveze uništavanja prikupljenih podataka u za to predviđenom roku po okončanju krivične istrage (European Court of Human Rights, 2022B: 17-18).[7]

O navedenoj metodi bilo je reči i u slučaju *Figueiredo Teikeira protiv Andore* u kome se podnosilac predstavke, osumnjičen za krivično delo trgovine drogom, žalio da je skladištenje podataka koji se odnose na njegovu telefonsku komunikaciju predstavljalo neopravdano mešanje u njegovo pravo na poštovanje njegovog privatnog života. Sud je smatrao da nije došlo do povrede člana 8. Konvencije budući da je našao da je u ovom slučaju ispoštovana ravnoteža između prava podnosioca predstavke na poštovanje njegovog privatnog života i javnog interesa oličenom u potrebi sprečavanja krivičnih dela. Prema shvatanju Suda, nadležni organ je pravilno procenio neophodnost i proporcionalnost naloga za tajni nadzor komunikacije u svetlu prikupljenih dokaza i ozbiljnosti krivičnog dela u pitanju. S druge strane, podnosilac predstavke je imao na osnovu nacionalnog pravnog okvira pravne mogućnosti i zaštitne mehanizme da preispita ovu odluku nadležnog organa, što sve zajedno dovodi do zaključka da njegovo pravo na privatni život nije bilo povređeno u ovom slučaju (European Court of Human Rights, 2022B: 18).[8]

Osim tajnog snimanja u policijskim stanicama u praksi nije redak slučaj i primena metode presretanja telefonskih razgovora advokata sa svojim klijentom. Upravo o ovoj problematici je bilo reči u predmetu *R.E. protiv Ujedinjenog Kraljevstva* u kome se podnosilac predstavke, koji je uhapšen i pritvoren zbog sumnji za izvršenje ubistva službenika policije, žalio na režim primene tajnog nadzora konsultacija između pritvorenika i njegovih advokata. U ovom slučaju, Sud je smatrao da je došlo do povrede člana 8. Konvencije u pogledu tajnog nadzora pravnih konsultacija, nalazeći da relevantne odredbe domaćeg zakona koje su bile na snazi u to vreme nisu pružale dovoljne garancije za zaštitu obavljanja razgovora između podnosioca predstavke i njegovog advokata (European Court of Human Rights, 2022B: 6).[9] Pored izložene situacije, pritvorenici su neretko izloženi i tajnom snimanju razvogora sa svojim rođacima. O ovome je bilo reči u predmetu *Visse protiv Francuske* u kome su se podnosioci predstavke, uhapšeni zbog sumnje da su izvršili razbojništvo i stavljeni u istražni zatvor, žalili da je snimanjem telefonskih razgovora između njih i njihovih rođaka u prostorijama za posete zatvora, a po nalogu istražnog sudije povređeno njihovo pravo na poštovanje privatnog i porodičnog života. Sud je smatrao da je došlo do povrede člana 8. Konvencije, nalazeći da francuski zakon nije dovoljno jasno ukazao na to pod kojim uslovima i u kojoj meri vlasti mogu da se mešaju u privatni život pritvorenika, niti je definisao obim i način vršenja svojih diskrecionа ovlašćenja u toj sferi. Shodno tome, podnosioci predstavke nisu uživali minimalni

[7] Karabeyoğlu v. Turkey, application no. 30083/10, Judgment 7 June 2016.

[8] Figueiredo Teixeira v. Andorra, application no. 72384/14, Judgment 8 November 2016.

[9] R.E. v. the United Kingdom application no. 62498/11, Judgment 27 October 2015.

stepen zaštite koji je neophodan u demokratskom društvu. Sud je posebno primetio da je sistematsko snimanje razgovora u prostoriji za posete u druge svrhe osim obezbeđenja zatvora, lišilo sobe za posete njihovog jedinog razloga postojanja, koji se sastoji u tome da se pritvorenicima omogući da zadrže određeni stepen privatnog života, uključujući privatnost razgovora sa svojim porodicama i rođacima (European Court of Human Rights, 2022B: 5).[10]

U prilog tome da je za zakonitost primene mere tajnog nadzora komunikacija potrebno da postoje adekvatni zakonski mehanizmi zaštite od eventualnih zloupotreba svedoči i slučaj *Sabo i Visi protiv Mađarske*, u kome su se podnosioci predstavke žalili da su bili podvrgnuti neopravdanim i nesrazmernim merama u okviru mađarskog pravnog okvira o tajnom nadzoru u svrhe nacionalne bezbednosti, budući da je ovaj pravni okvir podložan zloupotrebama, posebno zbog nedostatka sudske kontrole. U ovom slučaju Sud je smatrao da je došlo do povrede člana 8. Konvencije. Iako je Sud našao da suprotstavljanje današnjim oblicima terorizma zahteva pribegavanje najsavremenijim tehnologijama, uključujući masovno praćenje, u cilju sprečavanja izvršenja terorističkih akata, zaključio je da predmetni pravni okvir ne pruža dovoljne garancije za izbegavanje potencijalnih zloupotreba, s obzirom na to da bi opseg mera mogao da obuhvati praktično svakoga u Mađarskoj, pa čak i osoba izvan prvobitnog opsega delovanja. Štaviše, naređivanje takvih mera odvijalo se u potpunosti u nadležnosti izvršne vlasti i bez procene da li je presretanje komunikacija bilo striktno neophodno i bez ikakvih delotvornih zaštitnih mera (European Court of Human Rights, 2022A: 4-5).[11]

Iz prethodnog slučaja proizilazi da je za primenu mera tajnog nadzora komunikacija neophodno da su nadležni organi imali sudski nalog kojim se odobrava njeno sprovođenje. U prilog ovome svedoči i slučaj *Hambardzumjan protiv Jermenije* u kome je podnosilac predstavke navela da policija nije imala ovlašćenja da je stavi pod tajni nadzor tokom krivične istrage, zbog čega se žalila da je usled neovlašćene primene tajnog nadzora bilo povređeno njeno pravo na privatni život. Sud je smatrao da je došlo do povrede člana 8. Konvencije, nalazeći da mera nadzora upotrebljena protiv podnosioca predstavke nije imala odgovarajući sudski nadzor i da nije bila u skladu sa zakonom. Posebno je konstatovano da nalog nije bio dovoljno precizan u pogledu toga koja osoba je bila predmet mere nadzora, što je bilo neprihvatljivo kada je u pitanju tako ozbiljno mešanje u pravo na poštovanje privatnog i porodičnog života kao što je primena tajnog nadzora. Štaviše, u nalogu nisu bile navedene ni konkretne mere koje je trebalo preduzeti protiv podnosioca predstavke (European Court of Human Rights, 2022B: 8).[12]

[10] Wisse v. France, application no 71611/01, Judgment 22 December 2005.

[11] Szabó and Vissy v. Hungary, application no. 37138/14, Judgment 12 January 2016.

[12] Hambardzumyan v. Armenia, application no. 43478/11, Judgment 5 December 2019.

2. PRAVO NA POŠTOVANJE PRIVATNOG ŽIVOTA U KONTEKSTU DIGITALNOG REGISTROVANJA PODATAKA OD KRIVIČNOPRAVNOG ZNAČAJA

Problematika vezana za potrebu balansiranja između javnog i privatnog interesa kada je reč o rizicima od zloupotrebe prava na privatni život usled primene digitalne tehnologije u cilju sprečavanja kriminala, osim u kontekstu otkrivanja krivičnih dela dolazi do izražaja i u sferi registrovanja prikupljenih podataka. Prikupljani podaci se radi preglednosti i sistematičnosti pohranjuju u odgovaravajuće baze podataka kojima rukuju nadležni organi. Ove baze podataka mogu biti prilično brojne, tako da se obično dele po kriterijumu predmeta podataka koje se u njih unose. U tom smislu, opšte je poznato da postoje baze podataka o DNK profilu koje sadrže informacije o bioloških tragovima ili baze podataka o registrovanim učiniocima krivičnih dela. Pored ovih baza podataka, treba imati u vidu da se u zavisnosti od potreba zaštite interesa nacionalne bezbednosti mogu voditi i drugi registri primera radi o potencijalno bezbednosno interesantnim licima. Prilikom evidentiranja predmetnih podataka od krivičnopravnog značaja pitanja koja su u centru pažnje odnose se na rokove čuvanja pohranjenih podataka, mogućnosti za podnošenje zahteva za brisanje zadržanih podataka po okončanju postupka, mogućnosti za odbijanje zahteva za dostavu podataka u zavisnosti od prirode i težine krivičnih dela koji se stavljaju na teret, kao i na imperativ postojanja minimalnih zaštitnih mehanizama protiv zloupotreba prava na poštovanje privatnog života. Upravo o navedenim pitanjima se u bogatoj sudskoj praksi izjašnjavao i Evropski sud za ljudska prava.

O tematici vezanoj za rokove čuvanja DNK profila u odgovarajućim bazama podataka svedoči slučaj *S. i Marper protiv Ujedinjenog Kraljevstva* u kome su podnosioci predstavke smatrali da je usled neograničenog zadržavanja u bazi podataka njihovih otisaka prstiju, uzoraka ćelija i DNK profila i to nakon što je krivični postupak okončan oslobađajućom presudom i obustavom postupka povređeno njihovo pravo na poštovanje privatnog života iz člana 8 Konvencije. Sud je analizirajući činjenično stanje u ovom slučaju našao da je došlo do povrede člana 8 uzimajući u obzir da opšta i neselektivna priroda ovlašćenja koja se ogledala u zadržavanju otisaka prstiju, uzoraka ćelija i profila DNK osoba osumnjičenih, ali neosuđivanih za krivična dela, kako je primenjena u ovom konkretnom slučaju, nije uspela da obezbedi pravičnu ravnotežu između javnog i privatnog interesa. S tim u vezi, Sud je naglasio da se upotreba savremenih naučnih tehnika u sistemu krivičnog pravosuđa ne može dozvoliti po bilo koju cenu i bez pažljivog balansiranja potencijalnih koristi od široke upotrebe takvih tehnika sa interesima zaštite privatnog života. Iz tog razloga, prema shvatanju Suda potrebno je da nadležni organi u svakom konkretnom slučaju odmere i postignu pravu ravnotežu između ova dva suprotstavljena interesa (European Court of Human Rights, 2022A: 1).[13] U prilog navedenom svedoči i slučaj *M.K. protiv Francuske* u kojem su nadležni organi odbili da na zahtev podnosioca predstavke odobre brisanje biometrijskih podataka koji su

[13] S. and Marper v. the United Kingdom, application nos. 30562/04 and 30566/04, Judgement 4 December 2008.

uzeti radi otkrivanja činjenica od značaja za vođenje postupka, i to uprkos tome što su postupci završeni oslobađajućom presudom, kao i obustavom postupka. Sud je smatrao da je došlo do povrede člana 8. Konvencije, nalazeći da je zadržavanje podataka predstavljalo nesrazmerno mešanje u pravo podnosioca predstavke na poštovanje njegovog privatnog života, usled čega se ne može reći da bi to bilo neophodno u demokratskom društvu. Sud je posebno primetio da je francuska država prekoračila svoje polje slobodne procene u ovom pitanju jer pravni okvir koji je dozvoljavao zadržavanje otisaka prstiju osoba osumnjičenih za krivično delo, ali i neosuđenih lica, o čemu je bilo reči u ovom slučaju, nije u skladu sa imperativom odmeravanja pravične ravnoteže između suprotstavljenih javnih i privatnih interesa (European Court of Human Rights, 2022A: 2-3).[14]

Takođe i slučaj *Gaughran v. the United Kingdom* se ticao problematike neograničenog zadržavanja ličnih podataka i to DNK profila, otisaka prstiju i fotografija podnosioca predstavke. Sud je i u ovom slučaju smatrao da je došlo do povrede člana 8 zaključivši da je Ujedinjeno Kraljevstvo prekoračilo prihvatljivo polje slobodne procene i da je zadržavanje u pitanju predstavljalo nesrazmerno mešanje u pravo podnosioca predstavke na poštovanje privatnog života, što se ne može smatrati neophodnom merom u demokratskom društvu. Sud je posebno podvukao da nije bilo odlučujuće trajanje zadržavanja podataka, već odsustvo određenih zaštitnih mera. U slučaju podnosioca predstavke, njegovi lični podaci su čuvani na neodređeno vreme bez obzira na težinu njegovog dela, bez potrebe za neograničenim zadržavanjem i bez ikakve stvarne mogućnosti revizije, zbog čega nije postignuta pravična ravnoteža između suprotstavljenih javnih i privatnih interesa (European Court of Human Rights, 2022A: 7).[15]

U slučaju *Aycaguer v. France* bilo je reči o tome da li je moguće odbiti zahtev nadležnih organa za dostavu traženih podataka u zavisnosti od prirode i težine krivičnih dela koji se stavljaju na teret. Naime, u predmetnom slučaju podnosilac predstavke je naveo da je došlo do povrede njegovog prava na poštovanje privatnog života zbog činjenice da je njegovo odbijanje da se povinuje nalogu za dostavu bioloških uzoraka rezultiralo krivičnom osudom. Sud je smatrao da je došlo do povrede člana 8 nalazeći da nacionalni propisi ne normiraju odredbu koja pravi razliku u periodima skladištenja DNK profila u zavisnosti od prirode i težine učinjenih krivičnih dela, zbog čega nije postignuta pravična ravnoteža između suprotstavljenih javnih i privatnih interesa. Do navedenog zaključka Sud je došao tim pre budući da je Ustavni savet doneo odluku kojom je uslovio primenu odredbi o nacionalnom DNK registru prethodnim određivanjem trajanja čuvanja takvih ličnih podataka u zavisnosti od svrhe dosijea i prirode i/ili težine krivičnih dela o kojima je reč (European Court of Human Rights, 2022A: 5-6).[16]

S druge strane, u slučaju *Peruzzo i Martens* protiv Nemačke podnosioci predstavke, koji su osuđeni za teška krivična dela, žalili su se da im je pravo na poštovanje privatnog života povređeno time što su domaći sudovi naložili da se od njih prikupi ćelijski materijal i da ga pohrane u bazu podataka u obliku DNK profila u svrhu olakšavanja istrage

[14] M.K. v. France, application no. 19522/09, Judgement 18 April 2013.

[15] Gaughran v. the United Kingdom, application no. 45245/15, Judgement 13 February 2020.

[16] Aycaguer v. France, application no. 8806/12, Judgement 22 June 2017.

budućih zločina. Sud je predstavku proglasio neprihvatljivom kao očigledno neosnovanu, našavši da mere na koje su se podnosioci predstavke žalili predstavljaju srazmerno mešanje u pravo podnosilaca predstavke na poštovanje njihovog privatnog života i da su neophodne u demokratskom društvu (European Court of Human Rights, 2022A: 3).[17]

Osim prikupljanja i čuvanja podataka o DNK profilima u odgovarajućim registrima, nadležni organi u cilju prevencije kriminala i vođenja evidencije o registrovanim učiniocima krivičnih dela kreiraju i rukovode i drugim potrebnim digitalnim bazama podataka. Jedna od takvih baza podataka jesu registri u koje se unose podaci o evidentiranim krivičnim delima i njihovim učiniocima. O ovom pitanju bilo je reči u predmetu *Brunet protiv Francuske* u kome se podnosilac predstavke žalio da je usled zadržavanja podataka u registru evidentiranih krivičnih dela koja je sadržala informacije iz istražnih izveštaja, uz navođenje involviranih lica i to nakon što je postupak protiv njega okončan, povređeno njegovo pravo na privatni život. Sud je smatrao da je došlo do povrede člana 8 Konvencije, zaključivši da je prekoračeno diskreciono pravo države odnosno polje njene slobodne procene. Sud je našao da zadržavanje predmetnih podataka nakon okončanja postupka nije bilo neophodno u demokratskom društvu. Pri tome je posebno problematično bilo to što podnosilac predstavke nije imao realnu mogućnost da traži brisanje iz baze podataka informacija koje se odnose na njega, kao i to što je bila propisana neopravdano dugački vremenski okvir čuvanja tih podataka, 20 godina, koji se mogao poistovetiti i sa njihovim neograničenim zadržavanjem (European Court of Human Rights, 2022A: 3-4).[18]

Takođe, postoje i baze podataka u koje je registruju učinioci pojedinih grupa krivičnih dela, kao što su učinioci krivičnih dela protiv polne slobode. U prilog navedenom svedoči i slučajevi *B.B. protiv Francuske, Gardel protiv Francuske i M.B. protiv Francuske* u kojima su se podnosioci predstavke žalili na njihovo uvrštavanje u nacionalnu bazu podataka o seksualnim prestupnicima. Sud je smatrao da nije došlo do povrede člana 8 Konvencije, zauzimajući stav da dužina čuvanja podataka, maksimalno 30 godina, nije bila nesrazmerna u odnosu na cilj kojem se teži oličen u sprečavanju kriminala. O tim pre što je uvid u takve podatke od strane suda, policije i upravnih organa bio uslovljen obavezom čuvanja poverljivosti i ograničen na tačno utvrđene okolnosti (European Court of Human Rights, 2022A: 1).[19]

U pojedinim slučajevima nadležni organi vode odgovarajuće baze podatake koji su specifične po tome što se u njima ne registruju podaci o licima protiv kojih se vodi krivični postupak, već pre svega o potencijalno bezbednosno interesantnim licima. U tom smislu, postavlja se pitanje usklađenosti između javnog interesa koji nalaže da se ove baze podataka vode i privatnog interesa oličenom u potrebi zaštite privatnog života involviranih lica. O predmetnom pitanju bilo je reči u predmetu Šimovolos protiv Rusije u kome se podnosilac predstavke žalio da su nadležni organi prikupljali informacije o

[17] Peruzzo and Martens v. Germany, application no. 7841/08 and 57900/12, Decision on the admissibility 4 June 2013.

[18] Brunet v. France, application no. 21010/10, Judgment 18 September 2014.

[19] B.B. v. France, application no. 5335/06, Gardel v. France, application no. 16428/05, and M.B. v. France no. 22115/06, Judgements 17 December 2009.

njegovom kretanju i podatke unosili u odgovarajuću bazu podataka o ostvarenom nadzoru. Sud je smatrao da je došlo do povrede člana 8 Konvencije, uočivši da su kreiranje i održavanje baze podataka i postupak njenog rada bili regulisani naredbom ministarstva koja nikada nije objavljena ili na bilo koji drugi način učinjena dostupnom javnosti. Pored toga, Sud je utvrdio da domaći zakon nije dovoljno jasno definisao obim i način vršenja diskrecionog prava koje je dato domaćim vlastima da prikupljaju i čuvaju informacije o privatnom životu pojedinaca, niti su bili predviđeni makar minimalni zaštitni mehanizmi protiv zloupotreba (European Court of Human Rights, 2022A: 1-2).[20] O navedenoj problematici svedoči i slučaj *Khelili protiv Švajcarske* u kome je bilo reči o tome da se podnositeljka predstavke žalila da je ženevska policija neosnovanim vezivanjem njenog imena za zanimanje prostitutke u za to predviđenoj bazi podataka povredila njeno pravo na poštovanje privatnog života. Sud je smatrao da je došlo do povrede člana 8. Konvencije, nalazeći da je čuvanje u policijskim evidencijama ovih podataka koji se tiču njene privatnosti prekršeno pravo podnosioca predstavke na poštovanje privatnog života. Prema shvatanju Suda zadržavanje reči „prostitutka" godinama nije bilo ni opravdano ni neophodno u demokratskom društvu, tim pre jer je ta reč mogla naštetiti ugledu podnosioca predstavke i učiniti njen svakodnevni život problematičnijim. Iz tog razloga, podnosilac predstavke je u ovom slučaju imao značajan interes da se reč „prostitutka" ukloni iz policijskih evidencija (European Court of Human Rights, 2022B: 16).[21]

ZAKLJUČAK

Poštovanje privatnog života je, kako je to pokazala goresprovedena analiza, zajemčeno pravo svakog pojedinca u koje se javne vlasti ne bi smele mešati. Ipak, ovu načelnu odredbu treba shvatati uslovno, budući da je zadiranje javnih vlasti u vršenje ovog prava od strane pojedinaca relativizovano mogućnošću da se nadležni organi mešaju u njihovo pravo na privatni život ako je to između ostalog potrebno radi sprečavanja nereda i kriminala. Međutim, treba imati da predmetno zadiranje u pravo na privatni život ne sme da bude proizvoljno, već naprotiv u skladu sa zakonom i u meri u kojoj je to neophodno u demokratskom društvu. Upravo, s tim u vezi javlja se i problem u praksi koji se tiče balansiranja između javnog i privatnog interesa. Drugim rečima, javlja se dilema gde postaviti granicu ispod koje mešanje javne vlasti ne bi predstavljalo nedozvoljeno zadiranje u pravo na privatni život pojedinaca, odnosno u kojim slučajevima bi ta granica bivala prekoračena. Iako se na prvi pogled čini da je jednostavno postaviti ovu granicu, to ipak nije tako, budući da odgovor na postavljeno pitanje zavisi od pojedinačnog slučaja i od izloženog činjeničnog stanja koje se vezuje za predmetni slučaj. S druge strane, ono što se može uraditi po ovom pitanju jeste da se postave odgovarajuće smernice koje nadležni organi treba da cene prilikom odlučivanja da li u konkretnom slučaju prevagu treba da odnose javni ili privatni interes. U tom smislu, potrebno je voditi računa pre

[20] Shimovolos v. Russia, application no. 30194/09, Judgement 21 June 2011.

[21] Khelili v. Switzerland 18 October 2011, application no. 16188/07, Judgement 18 October 2011.

svega o tome da li je predmetno mešanje u skladu sa zakonom. Ukoliko nije, onda nije ni potrebno ispitivati ispunjenost ostalih uslova. Ukoliko je predmetno mešanje u skladu sa zakonom, onda se pristupa ustanovljavanju da li je to zadiranje opravdano postizanjem nekog legitimnog cilja, da bi se u slučaju kada i ako se to utvrdi prešlo na izjašnjavanje da li je mešanje zaista bilo neophodno u demokratskom društvu.

U vezi sa iznetim najviše dilema u praksi izaziva primena mera tajnog nadzora, prilikom čijeg određivanja odnosno tokom čijeg sprovođenja može doći do povreda prava na privatni život pojedinaca. Iz tog razloga, potrebno je imati u vidu da se primena mera tajnog nadzora može sprovoditi samo u meri koja je nužna i neophodno potrebna u demokratskom društvu i to samo na osnovu i u skladu sa zakonom. Osim primene mera tajnog nadzora tokom kojih dolazi do prikupljanja podataka o ličnosti, poseban problem izaziva i problematika zadržavanja prikupljenih podataka u odgovarajućim bazama podataka. U vezi sa ovim pitanjem treba praviti razliku između svrhe radi koje se podaci čuvaju, te svojstva lica u odnosu na koje se podaci odnose te optimalnog vremenskog okvira unutar kojeg je dozvoljeno čuvati podatke.

U svakom slučaju treba konstatovati, a što jasno proizilazi i iz analizirane sudske prakse Evropskog suda za ljudska prava, da primena digitalnih tehnologija u kontekstu krivičnopravne reakcije na kriminal ne može biti selektivna niti zasnovana na arbitrarnom postupanju, već treba da bude sprovedena na način koji pruža mogućnosti za balansiranje između javnog i privatnog interesa. Na putu ka postizanju ovog cilja nadležni organi treba da uživaju polje slobodne procene kako bi im se pružio prostor za uspostavljanje pravične ravnoteže između javnog i privatnog interesa. U tom procesu balansiranja nadležni organi bi trebalo da izvagaju potencijalne koristi koje ima primena digitalnih tehnologija u kontekstu krivičnopravne reakcije na kriminal u svakom pojedinačnom slučaju, s jedne strane, i moguće zloupotrebe prava na privatni život koje mogu nastati usled njihove primene. Prilikom odgovora na ovo pitanje treba voditi računa o tome da li se njihovom primenom ostvaruje legitimni cilj oličen u potrebi sprečavanja kriminala, te ukoliko je to slučaj da li je to neophodno u demokratskom društvu. Jedinstvenih obrazaca za rešavanje predmetnog pitanja nema, ali iznete smernice mogu poslužiti kao stabilan osnov za ostvarenje ideala da svaki pojedinac bude zaštićen od arbitrernog zadiranja u njegovo pravo na privatni život.

LITERATURA

1. Kostić J., Mrvić Petrović N., (2021) „Digital Evidence and Criminal Law cooperation in the Digital Age", International Scientific Conference *Archibald Reiss Days* (N. Koropanovski ed.) Belgrade, 9-10 November 2021. Belgrade: University of Criminal Investigation and Police Studies, 43-54.
2. Kostić J., Jelisavac-Trošić, S. (2017) „Digital Forensic Procedures f European Anti-fraud Office and protection of personal data", *EU and Comparative Law Issues and Challenges, Series (Eclic 1) - Procedural Aspects of EU Law*, (Dunja Duić, Tunjica Petrašević (eds.), Osijek: Josip Juraj Stossmayer University of Osijek, Faculty of Law, 6 -7 April 2017, 32-47.
3. Škulić, M. (2011) „Specijalne istražne tehnike u funkciji suzbijanja organizovanog kriminaliteta", U: *Društveni aspekti organizovanog kriminaliteta* (Aleksandar Fatić i Božidar Banović (ur.), Beograd: Institut za međunarodnu politiku i privredu, 201-225.
4. Škulić, M. (2015) „Tajni audio i video nadzor kao posebna dokazna radnja u Zakoniku o krivičnom postupku", *Tužilačka reč*, No. 28. 24-49.

Legal and other sources

1. Aycaguer v. France, application no. 8806/12, Judgement 22 June 2017.
2. B.B. v. France, application no. 5335/06, Gardel v. France, application no. 16428/05.
3. Ben Faiza v. France, application no. 31446/12, Judgment 8 February 2018.
4. Brunet v. France, application no. 21010/10, Judgment 18 September 2014.
5. Council of Europe (2020) Guide to the Case-Law of the European Court of Human Rights. Council of Europe, Strasbourg.
6. European Court of Human Rights (2022A). Factsheet – New technologies. European Court of Human Rights, Strasbourg.
7. European Court of Human Rights (2022B). Factsheet – Personal data protection. European Court of Human Rights, Strasbourg.
8. Figueiredo Teixeira v. Andorra, application no. 72384/14, Judgment 8 November 2016.
9. Gaughran v. the United Kingdom, application no. 45245/15, Judgement 13 February 2020
10. Hambardzumyan v. Armenia, application no. 43478/11, Judgment 5 December 2019.
11. Karabeyoğlu v. Turkey, application no. 30083/10, Judgment 7 June 2016.
12. Khelili v. Switzerland 18 October 2011, application no. 16188/07, Judgement 18 October 2011.
13. Konvencija za zaštitu ljudskih prava i osnovnih sloboda Rim, 4. novembra 1950.
14. M.B. v. France no. 22115/06, Judgements 17 December 2009.
15. M.K. v. France, application no. 19522/09, Judgement 18 April 2013.

16. Peruzzo and Martens v. Germany, application no. 7841/08 and 57900/12, Decision on the admissibility 4 June 2013.
17. Perry v. the United Kingdom, application no. 63737/00, Judgment 17 July 2003.
18. S. and Marper v. the United Kingdom, application nos. 30562/04 and 30566/04, Judgement 4 December 2008.
19. Sablin v. Russia application no. 25147/14, Judgment 2 July 2019.
20. Shimovolos v. Russia, application no. 30194/09, Judgement 21 June 2011.
21. Szabó and Vissy v. Hungary, application no. 37138/14, Judgment 12 January 2016.
22. R.E. v. the United Kingdom application no. 62498/11, Judgment 27 October 2015.
23. Uzun v. Germany, application no. 35623/05, Judgment 2 September 2010.
24. Vakhmistrov v. Russia application no. 56443/09.
25. Vasilică Mocanu v. Romania, application no 43545/13, Judgment 6 December 2016.
26. Wisse v. France, application no 71611/01, Judgment 22 December 2005.

THE APPLICATION OF DIGITAL TECHNOLOGY IN THE CONTEXT OF CRIMINAL LAW RESPONSE TO CRIME AND THE RIGHT TO RESPECT FOR PRIVATE LIFE: A GAP IN BALANCING BETWEEN PUBLIC AND PRIVATE INTEREST

with special reference to the practice of the European Court of Human Rights

Daily development of digital technologies and the new opportunities they provide greatly shape our actions, encouraging us to get used to and adopt current technological achievements. One of the many areas in which the application of digital technologies is gaining ever greater importance is the criminal law field, which enables competent authorities to apply more sophisticated methods and techniques in discovering and recording data of criminal law significance. Starting from the fact that the exposed tendency towards the digitization of criminal law response to crime is taking on greater significance, the paper analyzes the most common technological achievements that find their application in this area, with special reference to the practice of the European Court of Human Rights, in order to recognize their potential risks. In the concluding remarks, it is emphasized that the application of digital technologies in practice, in addition to bringing a number of new opportunities in practical work to competent authorities, also creates numerous risks of arbitrary and excessive encroachment on the basic rights and freedoms of people. Therefore, properly weighing the balance, between the public interest that mandates their application to prevent disorder or crime and the private interest of citizens that dictates that their guaranteed rights must not be violated or endangered, should be respected in each case.

KEYWORDS: *digital technologies, crime, European Court of Human Rights, public interest, right to respect for private life*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.20

UNDERNEATH THE ROBOT JUDGE'S ROBE: DEMYSTIFYING THE USE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL JUSTICE THROUGH A GLOBAL SOUTH PERSPECTIVE

Leonardo Simões Agapito*
Matheus de Alencar e Miranda**
Túlio Felippe Xavier Januário***

Scientific and technological developments in the field of autonomous systems and artificial intelligence have provided and boosted their use in the most varied sectors of society. It is no different with activities carried out within the scope of criminal justice. Examples of these technologies being used in criminal investigations and procedures, including in assisting judgments, are increasingly frequent. However, it did not take long for questions to be raised regarding the limits of these systems and their possible impacts on the individuals' guarantees. Although we cannot deny that some particularities of these technologies, especially of AI (such as the opacity and unpredictability of its output), pose risks to some fundamental guarantees in criminal proceedings, there is, in our view, at the basis of many doctrinal criticisms, a certain misunderstanding on what these technologies actually are, how they operate and how they are being used in the justice system. In view of this scenario, the aim of the present paper is precisely to investigate how artificial intelligence and autonomous systems have been used in criminal justice, so that we can identify what are, in fact, their potential impacts on Defendants' rights and guarantees. For this, we will initially study the concept and operation of these technologies, so that we can understand their particularities. Subsequently, we will analyze their concrete application in the judicial sphere. For that, we will adopt as object of study, two of the best known systems of judicial assistance – HART and COMPAS – and the system used in Brazil, namely, the VICTOR. From the conclusions reached in the first two topics and applying the deductive methodology, we will seek to demystify some legends related to the so-called "robot judge", identifying what are, in fact, its potentials and limits and which are the guarantees that are at stake.

KEYWORDS: *artificial intelligence; robot judge; decoloniality; global south.*

* PhD Student in Latin American Integration, University of São Paulo (Brazil).
E-mail: *leoagapito@gmail.com*

** PhD Candidate in Criminal Law, State University of Rio de Janeiro (Brazil).
E-mail: *matheus.alencarm@gmail.com*

*** PhD Fellow, Fundação para a Ciência e a Tecnologia (FCT), University of Coimbra (Portugal).
E-mail: *tuliofxj@gmail.com*

INTRODUCTION

Scientific and technological developments in autonomous systems and artificial intelligence have provided and boosted their use in the most varied sectors of society (Januário, 2020b: 95ff; Estellita, Leite, 2019: 15; Hilgendorf, 2020: 43; Januário, 2020a; Januário, 2022; Pereira, 2021: 235; Machado, 2019: 101; Januário, 2021c; Rodrigues, 2021a.). It is no different with activities carried out within the scope of criminal justice.

Examples of these technologies being used in criminal investigations and procedures, including in assisting judgments, are increasingly frequent. However, it did not take long for questions to be raised regarding the limits of these systems and their possible impacts on the individuals' guarantees.

Although we cannot deny that some particularities of these technologies, especially of AI (such as the opacity and unpredictability of its output), pose risks to some fundamental guarantees in criminal proceedings, there is, in our view, at the basis of many doctrinal criticisms, a certain misunderstanding on what these technologies actually are, how they operate and how they are used in the judicial system. Nevertheless, questions about the criminal procedure model itself need to be asked previously.

In this scenario, the present paper's objective is to investigate the criticisms that can effectively be directed to the use of technology in judicial activity in the criminal sphere. To do this, we will initially do a brief study on the concepts and operation of these technologies so that we can understand their particularities and concrete application in the judicial sphere. Subsequently, we will analyze in detail the criminal procedural model and the criticisms that can be directed at it. To do so, we will make a case study of some Latin American examples of alternative criminal procedures. In the end, we want to demonstrate that, although there are pertinent criticisms that are directed to the so-called "robot judges", which point out problems that in fact must be faced so that there is a fair and adequate application of these technologies in the criminal justice system, there are even more fundamental problems in the criminal procedural model itself, which must be rethought to become a truly democratic instrument.

1. TECHNOLOGY IN JUDICIARY SYSTEM: CONCEPTS, LIMITATIONS AND THE CRITICS DIRECTED AT IT

The automation of repetitive tasks that require the processing of a large amount of data has become increasingly common in the most diverse sectors of activities, including in the scope of investigations and criminal proceedings. It is important to note that this automation still occurs mainly through autonomous systems, although there is undeniable room for expanding the application of artificial intelligence[1] (A.I.).

[1] According to Fabiano Hartmann and Roberta Zumblick, artificial intelligence operates through the identification of patterns in the available database, prioritizing, from them, behaviors that have positive effects related to the objective sought. Widely used to find patterns and classify documents, this

In this scenario, some questions arise due to the implementation of this level of automation in the "typically human" Judiciary System, mainly in criminal issues, where the individualization of every case and person is most likely expected. These questions come in an even larger number when the technology used is the A.I., concerning its specific problems. The journey of this criticism will be explained here, but first, it is necessary to understand *if* A.I. is the key factor to pose new challenges and how the technology capable of autonomous decision-making is inserted into the criminal system as a whole.

In the distinction between A.I. and autonomous systems, it is important to note that the European Commission (2018) defines artificial intelligence as 'systems that display intelligent behavior by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals'. They 'can be purely software-based, acting in the virtual world' (e.g. voice assistants) or 'embedded in hardware devices (e.g. autonomous cars).

Despite some lingering discussion on this topic (Santosuosso, Bottalico, 2017: 35ff), we can consider A.I. as machine intelligence, capable of solving problems in a way similar to a human being. In other words, with the purpose of solving a problem, it has the ability to understand its environment through data inputs and, based on them, choose a course of action. It is undeniably an 'umbrella concept', which encompasses several subfields such as robotics, machine learning, and natural language processing (Calo, 2017; Peixoto & Silva, 2019: 75; Agapito, Miranda, Januário, 2021).

This definition is somewhat close to the classification proposed by the European Commission's High-Level Expert Group on Artificial Intelligence (2018: 7), which is intended precisely to improve the abovementioned concept. According to them, the comprehension of A.I. can involve two perspectives: by I) *Artificial Intelligence as "systems",* we can understand softwares or hardwares that, to achieve a complex goal, perceive their environment, interpret the collected data, reason on this data and decide the best action(s) to take (according to pre-defined parameters) in the physical or digital world. Besides that, some can also learn to adapt their behavior according to their previous experiences. II) As a scientific discipline, A.I. encompasses several approaches and techniques, such as machine learning, machine reasoning, and robotics.

Although the "intelligence" of these systems is sometimes impressive, A.I. is not the only specie of technology capable of autonomous decision-making (without immediate human intervention). There are several algorithms able to do it, despite being the product of pure human previous programming, not using the ability of A.I. to reprogram itself to adjust precision.

As such, we can understand pre-programmed automation (P.P.A) the systems capable of autonomous decision-making but are products of pure human previous programming[2]. In other words, they have the ability to react to the environment without

technology has expanded to other functions as well. See: Peixoto; Silva, 2019: 63ff. See also: Agapito; Miranda; Januário, 2021: 89.

[2] We are aware of the use of heuristic algorithms in the IT language and in another opportunity, we used the terminology "autonomous system". See: Agapito, Miranda, Januário, 2021. We are also aware both terminologies are correct, but this time we preferred to use pre-programmed automation for law science

the need for human intervention (therefore, autonomous, like A.I.), but cannot select a course of action or elaborate a new solution to a problem (therefore, not intelligent). They only present a pre-programmed response according to the environment identified (Hilgendorf, 2015; Peixoto & Silva, 2019; Agapito, Miranda, Januário, 2021: 89-90).

It is important to mention that when these technologies are applied in the Judicial System, many critics arise, mainly around the A.I. The first concern regards the data used as *input*. Since artificial intelligence depends on processing a huge amount of data, their security, reliability, and lawfulness become an important issue, especially if we consider the risks of violation of the holders' rights and data bias, which may reflect developers' prejudices and discriminations (Agapito, Miranda, Januário, 2021: 96; Mulholland, Frajhof, 2019; Yapo, Weiss, 2018: 5366; Peixoto, Silva, 2019: 34-35; Januário, 2021b; Miranda, Januário, 2021: 286ff.)

In other words, scholars point out that, contrary to what happened in the past, when data sharing depended on minimal conscious conduct by data subjects, they are shared massively and depend on a simple active conduct of their holders. Based on that observation, there is a justified concern that there will be an ever-increasing intrusion on people's intimacy and privacy on the grounds of arguments such as greater efficiency in police activities and in the criminal justice system (Miró Llinares, 2018: 114ff).

Besides that, there is a concern regarding the eventual accentuation of criminal selectivity to the detriment of certain groups. Using factors such as ethnicity, race[3], gender, place of residence, and profession to determine greater or lesser preventive policing or the risk of recidivism and whether a specific citizen is entitled to a certain alternative penalty or precautionary measure will definitely demonstrate a sort of *algorithm discrimination* (Miró Llinares, 2018: 120ff).

Finally, data may end up being inaccurate or invalid. This can happen when the data employed for training the algorithm is poorly applied by the programmer, when they are collected in a very strict period, or when they are not representative enough. With poor data being used as input, poor outputs will be achieved, increasing the chances of errors and perpetuation of discrimination and prejudice (Miró Llinares, 2018: 122ff).

Another concern is related to the *opacity* of artificial intelligence. By that, we mean that the comprehension of the relationships between a given input and an achieved output, especially the foundations of a decision made by the algorithm, is very difficult. A.I. is often compared with black boxes since the conditions for fully understanding the outputs' "how" and "why" are very limited (Burrell, 2016: 1; Price II, 2017: 2; Wimmer, 2019; Rodrigues, 2020b: 25.).

Furthermore, we cannot disregard the issues related to the *unpredictability* of these systems. Once their algorithms have the ability to learn from their previous experiences

because it is the best technical expression for a legal system, considering the potential of communication of the meaning of the technology in terms of its production and consequences for the law.

[3] As explained by Anabela Miranda Rodrigues (2020a: 233), it is important to point out that the variable "race" is not expressly used by these systems. However, other elements are applied and end up implicitly reflecting racial prejudice.

and adapt themselves to achieve their goals better, the output reached by A.I. sometimes cannot be foreseen even by its programmers.[4]

For those reasons, far beyond the relevant controversies in evidentiary matters that A.I. raises (Quattrocolo, 2020: 37ff; Gless, 2020: 202ff; Fidalgo, 2020: 129ff; Canestraro, Januário, 2022), some scholars sustain that its application in criminal justice system itself, depending on its form and intensity, could represent a violation on some of the defendant's rights and guarantees, such as his right to a defense, to a public trial, and the right to appeal[5].

As we can see, P.P.A. and artificial intelligence, when applied in the most varied phases of criminal prosecution, spark endless debates regarding their feasibility, limits, and implications (Kehl, Guo, Kessler, 2017; Chiao, 2019). We believe, however, that despite the adequacy and fairness of many of the critics directed to technology in the criminal justice system, some of them are built on premises that are, in our view, inaccurate. Briefly, we understand that there is a misunderstanding of how these technologies are really applied in practice, besides suggesting that they have been applied (and consequently disturbed) in an effective criminal procedure model. It disregards, therefore, that many of the problems observed reflect a more significant issue related to the criminal justice system itself.

First, it must be noted that all critics are generally directed to A.I., ignoring that P.P.A is also part of the same problem, with similar consequences. The difference between them is much more related to how to address responsibility to people involved in each case, bringing specific and controversial problems. As explained by Cathy O'Neil (2016), more than the distinction between A.I. and P.P.A., what is relevant to consider is the mathematic models, the algorithms, and the way they are built.

Regarding human responsibility, however, it is very important to understand the different types of technology and how they are applied to the Criminal Justice System. In other words, if the system is fully pre-programmed, it is necessary to find the decision-makers that decide how the machine would automate decisions. On the other hand, if the machine learns how to improve itself and solve different problems, it is necessary to identify the ones that were responsible for the definition of the objectives, path, and testing of A.I.

Finally, it is important to note that some of the critics seem to understand that the application of these technologies restrains their sentencing when they would be

[4] Susana Aires de Sousa (2020: 64) highlights that the specificity of autonomous systems is precisely their ability to reach outputs with no interference of the programmer, but only through information and experiences acquired by them. Therefore, they are able to obtain answers that were not even imagined by the individuals and make decisions that can even be against the law.

[5] According to Anabela Miranda Rodrigues (2020a: 230ff), due to algorithms' opacity, relevant decisions to the Defendants are taken without them having the opportunity to know their foundations. Besides that, the development of these technologies is under the charge of private companies, which have no interest in disclosing the particularities of their operation. This causes difficulties in the public control of judicial decisions and a certain "unaccountability" on the part of the judges, which no longer see the decisions as their own. Luís Greco (2020: 43ff.) also sees in the lack of a person accountable for the decisions, the main issue with the so-called "robot judges".

"deciding" similarly or instead of a judge. However, as we emphasized before (Agapito, Miranda, Januário, 2021), the decision-making capacities of A.I. and P.P.A. are helpful in several other procedural phases when a decision has to be made, such as surveillance, intelligence, investigation and sentence serving.

These misunderstandings on the concrete applications of technology end up limiting the scientific capacity to analyze and propose valid changes in this scope. In fact, instead of this consolidated idea of systems that judge and hinder and that must be excised from criminal justice, we should accept that some of these technologies are already a reality in the criminal justice system and that would be much more productive to direct our energy on identifying which kind of technology and decision-making processes are (and should be) accepted according to law and the protection of human dignity.

However, as we briefly addressed in the introduction, these scientific guidelines are dependent on the accommodation of another stodgy reality: criminal justice system is not even close to being satisfactory in terms of peace building and conflict overcoming. This is what we will seek to demonstrate through the case study in the next topic.

2. LONG BEFORE THE ARRIVAL OF TECHNOLOGY: SCRUTINIZING PROBLEMS OF CRIMINAL PROCEDURE IN LATIN AMERICA

Brazilian contemporary criminal justice system has unquestionably perpetuated the Portuguese institutions, the influence of German and French concepts, and, more recently, a considerable alignment to the United States' common law. Herman Dooyeweerd (2015) explains that western law relies on an ancient Roman tradition, which divides public and private law. For Dooyeweerd, this separation has its legitimation in the Roman society organization by "families". This family concept included much more relatives than nowadays and had a leader, the "paterfamilias", who was not only the decision-maker, the head, and the legal representant of this large group, but also its priest, responsible for spiritual ceremonies and guardian of family's gods, ancestor's worship, knowledge, and traditions. There was a division between private gods (family's worship) and public gods (the gods of the State, "imperium", like Caesar himself), both with an ancient common origin (no hierarchy between public and private forums). In other words, the conflicts inside the family were legally solved by the "paterfamilias", but the conflicts with the State might be solved by public institutions with "religious status". It is no surprise that Braithwaite (2014) sees in western criminal systems the sobriety (seriousness) of a cult, or, we should say, of a Roman Christian cult.

The first response to this perspective could be that only an unreligious procedure (empty of any transcendent content) would be able to answer different religious perspectives at once. So, a great effort would be made to exclude every religious reference and traditional symbols without any success for at least four main reasons: a) because every action will always be interpreted by the interested parties of the procedure by religious

meanings (*e.g.* revenge from gods, divine will, or universal balance); b) the separation of religious authorities and political authorities is far from being a consensus for a large number of non-Christian traditions, which see peace and reconciliation as spiritual experiences; c) the rituals became empty without a transcendent meaning, which depends on creating a whole new perspective to the interested parties (without significance it is harder to obtain collaboration); d) all religions deals with similar concepts that are substantially important to a criminal procedure (*e.g.* justice, truth, revenge, forgiveness, an reconciliation) which might build bridges in conflicts.

In fact, the superficial discourse of secularism, liberal principles of tolerance by "equal distance" and neutrality of institutions is at least a great part of the reason why: a) criminal justice struggle to legitimate itself in different communities (not only on rural areas, but also in urban peripheral communities); b) criminal system may judge damages caused against companies and accept a "business ethics" and "corporate citizenship" faith, but it still blinds to all the complexity of environmental harm for indigenous people; c) legal reforms debates are more about efficiency and "war on crime" by criminal procedure than safety consensus and peacebuilding. Criminal justice is not using socially meaningful instruments and are not able to listen to people's real expectations on criminal cases.

The religious intolerance in Brazil have still been an issue since the Colonization. It would be naïve to ignore all the current violence and racism against Indigenous and African beliefs. But there are plenty of examples of resistance inside symbols and religious rituals. The "rustic Catholicism" (*catolicismo rústico*)[6] has been important to preserve traditional knowledges from ancient communities. The Brazilian "benzeideras", the use of images identified as Catholic saints and African gods, even folk stories about how World was corrupted or saved (Bosi, 1992: 54). Syncretism is not a "case of complete success", but it demonstrates that different cultures are able to dialogue and survive.

By not listening to religious traditions, along many other cultural forms of expression, the criminal system has not allowed minorities to create something new, to express themselves, to show its pain. It has not allowed resistance. The "so-called" neutral justice is a monopoly of narratives. The criminal system needs to re-fund its rituals and symbols, which are the social meaning and territorial values shared. More than that, it needs to find new (actually, they are meaningful ancient) perspectives of justice, retribution, and restauration for a more effective system, identified with its society.

2.1. Decolonization: how deep should we go?

The Constitution of the "*Estado Plurinacional de Bolívia*", from 2009, is a great example of this syncretism on Law and its institutions. In the preamble, it proposes to overcome the "colonial state", building a "Social Unitarian State under Plurinational

[6] See: Queiroz, 1968: 106. The author explains that African cultures could resist better in urban areas, while indigenous traditions had a better chance to survive in distant areas. However, the folklore and traditional celebrations may reveal deeper roots.

Community of Law", re-founding the country "with the strength of Pachamama and the grace of God". To ensure the protection of diversity, art.30, II, guarantees the recognition of indigenous community institutions as part of the general structure of the State (5) and the "exercise of political, legal and economic systems according to their worldview" (14). There is also the guarantee of due legal process in a "plural justice" (art.115, II) and the exercise of the adversary by ordinary means or by indigenous justice (119, I). In the art. 28 of the Bolivian Criminal Procedure Code (Law n.1970 of March 25, 1999), "community justice" is recognized with the same value as the ordinary justice system in cases involving members of the same community.

It is important to remember that the criminal procedure is not about punishment or guilt attribution. It is about solving conflicts, social pacification. It is about understanding injury, the leading cause and what might be done. In simple words, criminal procedure has the mission of finding the truth and to decide how to respond to it. To build this "truth", all the affected agents will intent to expose their perspectives and narratives. A consensus might be necessary in some communities or democratic systems and reparation, retribution and restoration might be possible if one of these makes some sense for this specific community.

Néstor García Canclini (1989: 263), writing about culture in Latin America, investigated a particular aspect of regions' identity, the hybridization of traditions of different origins, classes, and nations, which directly affects the dynamics of power. The dispute in urban public spaces between old statues, graffiti, social movement's signs, and advertisements is a great example of what it means to have a "dispute for a narrative", construction of meaning, and legitimacy. In this scenario, the author notes an ostensive fragmentation of messages and the surpass of territory as a fundamental element of cultural restrictions. To the author, Latin America has a long story of cultural hybridization. However, new technologies speeded this phenomenon in a particular way that overshadowed the difference between mass culture and popular culture, allowing individuals to create unlimited contents and variations.

In this scenario, a plural criminal procedure is not only about parallel systems. It is about social participation, new instruments, new dynamics built by community and new consequences for each process model. The process is not an island in society, it is also a great opportunity to rethink relations and social needs. In that way, it is important to observe what has already been made in the Plurinational State of Bolivia, and the different great proposes of John Braithwaite, as: a) the need for a double consciousness; b) the dialogue through symbols and myths; c) the pursue for cultures of reconciliation and long-term projects. However, we also need to take a better look at the specificities of Brazilian conflicts.[7]

[7] These topics were explored in detail at: Braithwaite, 2014. The present paper intents to make a review applied for Latin American context.

a. Double consciousness

The recognition of communitarian institutions in Bolivia is extremely important for enhancing community identity, protecting its members, and maintaining social cohesion. As presented by Donna Lee Van Cott (2006), the processes of independence in general, guided by liberalism and positivism, did not bring recognition of the diversity of legal systems. Despite that, the systems continued to exist. As a consequence, we may assume that Brazil has already had many different legal systems, even without formal recognition. Isolated communities have their means of settling disputes, which tend to be as much freer as their seclusion. In this scenario, it would be naive to think that formal judicial institutions can be better for the community where there is not even formal health care service and essential medicines.

Although the Bolivian model brought autonomy and recognition, Braithwaite (2014) made an important observation about "vernacularizing" institutes. When assimilating procedures, new issues might be caused, as the reduction of effectiveness of sanctions and consequent naturalization of causing injury, especially against vulnerable people, such as women and children.[8] But also, traditional procedures may not have enough guarantees or know-how to judge new kinds of harms as economic frauds, crimes against consumers, and intellectual property violations. As an example, both traditional institutions (unprepared or without recognition) and formal institutions (absents) are not able to protect isolated communities from harms produced by companies, such as soil and water pollution. Traditional justice must be evaluated by its social impacts, just like any other criminal policy.

As proposed by Braithwaite (2014: 220), an open dialogue between members of different communities is essential to the development of a "double consciousness". Both sides need to investigate together which one considers a harm and what kind of response is expected for those who violate it. In some cases, members of an isolated community might discover new standards and harms that cannot be accepted anymore and also how serious this harm really is for them. A great example of this "double consciousness" was demonstrated in 2019, in the first "*Marcha das Mulheres Indígenas*", occurred in Brasília, which produced a final report about female leadership, matriarchal traditions and education. In this document, the violence against women is presented as a consequence of colonization, but also as cultural heritage that needs to be transformed. The event became the biggest feminist protest in Brazilian history after the indigenous feminist movements also invited many other feminist movements to join them. In other words, the greatness of the event became from the huge support given to indigenous women to use their own voice for their own demands.

In summary, different than the Bolivian proposal, it is the conflicts between different communities that demand hybrid processes, that better listen to the victims, better meet the defendant needs and may offer an adequate integration. Criminal justice is also

[8] Braithwaite (2014) presents the institute of Bulubulu, which was a meaningful ritual of reconciliation and reparation, but it became an authorization for rapes when applied for sexual violence.

about social awareness and social engagement to present complaints and to demand reparations. Hybrid procedures might develop instruments more accessible than formal justice, but also use the duties and protections offered by formal procedures (*e.g* whistleblowing protection, identities secrecy or even bodyguards for defendants) (Schavelzon: 2016).[9]

b. Dialoguing by symbols and myths

When a dialogue is proposed, there are instruments to investigate, but also important roles to be played and respected. Community leaders are not "representants" of a group. They may be judges, mayors, or priests. Some roles are too complex and depend on a deep understanding of the community for a meaningful role assignment on criminal procedure. It is not a simple "talk". A hybrid procedure depends on hybrid institutions, and hybrid Courts. International criminal law and post-conflicts Courts already discussed it a lot. However, the biggest difference here is not identity and representativeness, although those elements remain important. As demonstrated by Braithwaite (2014), the complexity of harm and the plurality of its meanings (as sensitive cultural and spiritual consequences) create a social claim for responses that might only be satisfied by those particular roles.

A great example, is the Plan de Sánchez massacre, judged in 2004 by the Inter-American Court of Human Rights (IACHR)[10], revealed different forms of violence perpetrated by public officers during the criminal investigation. At first, members of the Guatemalan army invaded different communities and killed children and the elderly, sexually assaulted women, and disposed the bodies in mass graves. When a community member died, these communities had traditional ceremonies that should take weeks before a burial. Also, family members had to be buried close to their homes, for different spiritual reasons. In the following months, those villages were supervised by the Guatemalan army, which forbade religious rituals and limited their daily activities. Twelve years later, when the State started to investigate the massacre, the bodies were removed and manipulated without any special consult of families and local religious leaders, which the community interpreted as a repetition of violence. Paying attention to customs and practices prevents revictimization by judicial procedures.

On the other hand, as observed by Braithwaite (2014: 223), the penalties applied can also generate good or bad spiritual consequences, for example, a "new balance between different worlds" or "attracting the fury of the gods". Again, communitarian justice mechanisms should not be implemented without thinking about their political-criminal effects, yet, choices must be made collectively after all the consequences

[9] The author explains the risk of popular lynching and the use of traditional justice as an excuse for pure revenge, as might had occurred with Bolivian ex-vice President Víctor Hugo Cárdenas.

[10] See: Inter-American Court of Human Rights (IACHR) (2004). By the time of the trial, many traditions had been lost by the death of ancient members and the fear of survivors. Many of them had already accepted the Christian faith to be included in a new community in cities (looking for social acceptance). On this matter, see: YATES, 1984. The documentary presents the growth of Pentecostal churches during the U.S. endorsed military coup.

are exposed and considered. Criminal sanctions are not like math to be applied by an isolated judge, an autonomous island of reason. In this aspect, except in simple cases or special jurisdictions, the Bolivian penal procedure code provides a Judgment Council, joined by a technical judge and two random citizens (art.53 and 57, Bolivian Code of criminal procedure).

Finally, Braithwaite (2014) also made an excellent observation about myth and law enforcement. A criminal procedure may also incorporate the spiritual consequences to encourage compliance. To restore peace, different commitments and promises are made between the convicted person, the victims and their communities. If a commitment is violated by someone, what could happen to them? The myth might be able to discourage revenge, to create satisfaction on shareholders and to establish insurances. The myth communicates social perspectives, but it also illustrates how this group would deal with betrays and lies.

Of course, there will also be new reactions during these rituals and procedures. Western courts tend to be rigid and serious, without much space for laughter or even tears. As demonstrated before, the way in which western courts carry out their acts is intrinsically linked to the Roman religiosity of the "imperium", which was sober. This same logic is not present in other cultures, where activities can oscillate between comedy and tragedy, as presented by Braithwaite (2014: 230). Again, an immersion into Latin American religiosity and plurality is necessary to see that emotions tend to be exposed as a demonstration of commitment and personal concern.[11]

The end of apartheid in South Africa is a demonstration of how essential emotions are. Desmond Tutu (2000) narrates the 27th of April 1994, the first time that the country's black population could vote, as a day of joy, prayers, clapping, singing, and dancing. The pain of centuries was not easily overcome, overcoming requires intensity. Emotions are natural, unavoidable, but also symbolic. As presented by Braithwaite (2014: 230), during his experience on East Timor Commission for Reception, Truth and Reconciliation, the public joined the sections and testimonies, saluting with applauses and gestures of respect for those who confessed and laughing at those who lied.

The procedure, in the search for a better understanding of the facts that occurred, must be prepared for the unspoken, for the internal demands of the parties, for the social feeling of vulnerability. Moreover, during these sections, a much more violent feeling might grow on each side. How to deal with the unforgivable? Braithwaite's proposal relies on the surpass of a spiral of shame, anger, and violence. According to the author, the criminal procedure must interrupt this circle, so that the defendant does not need to fear the truth and its consequences. Thus, not all human feelings might help, so the myths should encourage collaboration and integrity, but also it needs to reward them.

And how to reward the defendant that pleads guilty? The myth might offer some possibilities.

[11] As an example, see: the Inter-American Court of Human Rights (IACHR), 2013: 90. The relatives demanded a "public act" that would dignify the life of Jeremias Osório. Memory, visibility, non-repetition. The requests of the victims of the Inter-American Court will exemplify a subjective world that demands externalization. Image restoration, confession and commitment.

c. Peacebuilding as a long journey

Padilla (2005: 214) made an interesting report about a case that occurred in 2003, in Totonicapán, Guatemala when two members of an indigenous community were caught trying to rob a house in another community. Initially, the community to which these individuals belonged felt extremely ashamed and proposed the sentence of twenty years in prison, without any right to defense. However, the dialogue turned in a different direction after many manifestations. The community started to reflect on reasons to rob and their needs, their hunger, and which values must prevail. The conclusion was that "punishment does not clear the mind, work does." The community decided that both defendants must clean their names and repair the invaded community with voluntary work. Reparation, honor, work became more important than revenge, blood, and fear. The turning point emerged with the question: which values may create a stronger community?

By this report, it is possible to conclude that reconciliation and other restorative justice values are not exactly "natural", but they are possible. During debates, there is much to hear and evaluate, because society does not feel the act by itself, but the complexity of causes and its consequences, mainly when harm became common. Why did police shoot again? Why have companies always ignored the risks they are aware of? Why would people burn a bus? Why have people been living in a piece of land that does not belong to them? The judicial procedure become nonsense without these answers.

Colonized procedures are long, formal, and limited. They search for an episodical solution. Traditional justice also offers a great opportunity to revisit institutions, rebuild solidarity, and create new relations. In this scenario, it becomes impossible to simply compare the formal justice system and traditional instruments of conflict resolution. However, as proposed by Braithwaite (2013), there will be no better moment to discuss what is expected of government and corporations as during the criminal procedure. Liability must be evaluated not only by what was done (wrongdoing), but actually by what should be done (compliance). Criminal procedure is a lesson for the future, a journey for the truth and for a better society, with mature individuals and stronger connections.

Every society has its own myths about this journey. The hero that was not prepared for the challenge. The defeat and the pain. The supporters, the wisdom, the lessons. The reborn, return of a king (queen), and a final victory when everything becomes better than ever. This is the story of Moses, Hercules, and even Anakin Skywalker, as demonstrated by Campbell (1997). The journey is a symbol of all people's life. The struggles, the "no comeback point". Of course, there will be fear and anger, shame, and regret. But the myth has the keys to salvation, regeneration, forgiveness, and remission. It demands a complex process and is far from being fast. No journey is easy or simple, but it might be possible.

As demonstrated before, all interested parties must join this process to compose the truth with their fragments (in different forms), and to build a new solution with their needs. But the truth will not always be revealed by spoken dialogues. As exposed

by Braithwaite (2014), Indonesia's peacemaking process "dismissed" the search for truth by long and diverse testimonies, deciding to pass through a reconciliation agreement that was radically embraced by sharing tasks and voluntary services. The "unspeakable" was said by sharing each other's pain on service. By the other hand, every IACHR decision says that "this judgment is, *per se*, a form of reparation", which is false. The Courts opinion can not heal anything by itself, especially when this opinion occurs far from the place where the harm was made. Healing comes through the journey, by social engagement, even media accountability, public acts.

For Braithwaite, this limitation of criminal procedure, especially in international courts, is the reason why "justice" might be pursued by many doors. Parallel initiatives from different actors, pursuing public awareness, recognition, and forgiveness. Justice must find its own multiparty way. In the author's words:

"For this we need a formalism of criminal law that enables informalism, and an informalism that enables formalism. This is so if there can be strength in the convergence of weaknesses of formalism and informalism in the longue dure´e of international justice." (Braithwaite, 2020: 26)

In conclusion, when comparing the formal criminal system and traditional justice, we may find ourselves comparing things that are very different because communitarian decisions have a much bigger meaning; or, because communitarian instruments are also part of something bigger. Decolonizing criminal justice means that our justice standards must grow in a more diverse and complex reality (Haesbaert, 2021: 318).[12] Decolonizing also means surpassing modernity and its fragmented worldview. And, if "justice comes from many doors", as Braithwaite said, those should also be respected and accepted by the same criminal system.

d. Criminal procedure tendencies in Brazil

Despite what we have exposed, the Brazilian judicial system has been following a different direction. The latest criminal procedure reform is a big example of the principal value followed by legislators and legal practitioners: "efficiency" (*e.g.,* Law 13.964/2019).

As demonstrated, the criminal procedure must allow all interested parties to join it. However, the United States' influence pushed legislators to adopt a new perspective, where efficiency means "quick procedures and easier solutions", reducing "legal guarantees" and "impunity". Suddenly, the criminal procedure became an uncomfortable detail before tougher sanctions.

In that case, different bargain solutions were implemented to dismiss a more prolonged investigation (e.g., Art.28-A, *Brazilian Criminal Procedure Code*). A shorter process is not only a good deal for judges and public prosecutors, whose careers are benefited from productivity, but also for companies. In Brazil, a corporation can only be charged by environmental crimes, where quick procedures will not be able to demonstrate all

[12] The author demonstrated the importance of local radio station to build reconciliation and social pacification.

the consequences of a disaster (as a dam rupture or an oil leak). On the other hand, quick procedures and short investigations limit the collection of evidence in financial crimes, which allows companies to use compliance programs and internal investigations to transfer liability to lower employees (Laufer, 1999).

Of course, nobody would benefit from a long-life criminal procedure where confused and empty acts are repeated with no special reason than legitimate itself. Brazilian judiciary has many investigations standing in cabinets, waiting months and years in an infinite line to be presented to a judge. Efficiency should not be faced as "a cleaning operation". Proposals should reflect on urgency (not hurry, but an active posture by the judiciary), plural participation, and social engagement, not simply on the lapse of time. Why does a fast decision matter without hearing the victims? After a year or even eight years, the feeling will be the same: abandonment.

In the opposite direction, there is no contemporary legal reform proposal for corporate criminal procedures. In Brazilian criminal law, there are no more than five articles about legal consequences for corporate crimes (Lei n.9.605/1998). Simultaneously, administrative and civil liabilities may also be negotiated by fines and compliance commitments, although all the challenges faced by victims and public authorities to enforce fulfillment. The Brazilian judicial system needs to adopt a new and socially meaningful procedure without easy solutions for corporate abuses.

CONCLUSION

Considering what we have emphasized in the last topic, we understand that it is necessary to address the question of technology in the criminal justice system through a different perspective from now on. We still agree that the main challenge in dealing with autonomous decisions in criminal justice is to secure transparency and accountability - through the disclosure of autonomous decision steps – and also the elimination of data bias, which might guarantee a more reliable A.I.

However, overcoming these issues does not necessarily make A.I. more legitimate when applied in the criminal justice system. Technology *per se* is very effective in achieving greater efficiency in some activities that demand the processing of a massive amount of data in a reduced time. However, it does not necessarily secure fairer decisions and, even less, peacemaking between the parties, especially if applied in a criminal procedure model that is ineffective in achieving these goals. In other words, technology is not the cause of several problems pointed by some scholars, but it will not be the solution to them as well, unless it is accompanied by structural changes in the criminal justice system.

As some kinds of technology have an undeniable disruptive capacity, they have the potential to be an important tool in overcoming traditional, expensive, and ineffective legal procedures. The technology of the future should therefore be seriously investigated and applied to support a more democratic, plural, and effective procedure in conflict resolution.

As we demonstrated through the Latin America's case study, traditional justice instruments are inadequate for countries that face a large number of violent deaths per year, high crime rates, and demand fast decisions every day in a judicial routine. They need exactly the opposite than merely fast decisions in a judicial routine. There is a social claim for justice, but isolated judges are not able to understand and political judges are to dangerous to have this power. New policies need to be developed and corporations need to be charged for real. Traditional justice instruments might offer new answers for questions that the judicial system has only worked to silence.

Most important, traditional justice is not an alternative path. It is the community's identity, the legitimated way, and the autonomy to say what matters to society. Justice is a deeper concept than academic graduation. It is created from the community's values, built by ancestors, shared by dear ones, and chosen by dialogue. Justice is a living heritage. Furthermore, technology should help those in need of Justice find its best-inherited version.

REFERENCES

1. Agapito, L. S., Miranda, M. A., Januário, T. F. X. (2021) "On the Potentialities and Limitations of Autonomous Systems in Money Laundering Control", *RIDP* 92(1), 87-108.
2. Braithwaite, J. (2013) "Does restorative justice work?" in: Johnstone, G. *A restorative justice reader*. 2.ed. London: Routledge, 320-352.
3. Braithwaite, J. (2014) "Traditional justice" in: Llewellyn et. al. (eds.). *Restorative Justice, Reconciliation and Peacebuilding*. New York: Oxford University Press, 214-239.
4. Braithwaite, J. (2020) "Many doors to international criminal justice", *New Criminal Law Review*, 23(1), 1-26.
5. Bosi, A. (1992) *Dialética da colonização*. São Paulo: Companhia das Letras.
6. Burrell, J. (2016) "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms", *Big Data & Society*, 3(1), 1-12.
7. Calo R. (2017) "Artificial Intelligence Policy: A Primer and Roadmap", *UC Davis Law Review,* 51(2), 399-435, https://lawreview.law.ucdavis.edu/issues/archive.html.
8. Campbell, J. (1997) "O herói de mil faces" São Paulo: Cultrix/Pensamentos.
9. Canestraro, A. C., Januário, T. F. X. (2022) "Inteligência artificial e programas de compliance: uma análise dos possíveis reflexos no processo penal", in: D'Ávila, F. R., Amaral, M. E. A. (orgs.). *Direito e Tecnologia: Anais do I Colóquio Nacional do IEDC*. Porto Alegre: Citadel, 363-392.
10. Chiao, V. (2019) "Fairness, Accountability and Transparency: Notes on Algorithmic Decision-Making in Criminal Justice", *International Journal of Law in Context*, 15(2), 126-139.
11. Conselho Indigenista Missionário (2019) *Documento final da Marcha das Mulheres indígenas: "Território: Nosso Corpo nosso espírito",* https://cimi.org.br/2019/08/

marcha-mulheres-indigenas-documento-final-lutar-pelos-nossos-territorios-lutar-pelo-nosso-direito-vida/.
12. Dooyeweerd, H. (2015) *Raízes da cultura ocidental: as opções pagã, secular e cristã.* São Paulo: Cultura cristã.
13. Estellita, H., Leite, A. (2019) "Veículos Autônomos e Direito Penal: uma introdução" in: Estellita, H., Leite, A. (orgs.) *Veículos Autônomos e Direito Penal.* São Paulo: Marcial Pons, 15-35.
14. European Commission (2018) "Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe: COM/2018/237 final", https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN.
15. Fidalgo, S. (2020) "A Utilização de Inteligência Artificial no Âmbito da Prova Digital – Direitos Fundamentais (Ainda Mais) Desprotegidos' in: Rodrigues, A. M. (coord.), *A Inteligência Artificial no Direito Penal.* Coimbra: Almedina, 129-161.
16. Garcia Canclini, N. (1989) *Culturas Híbridas: estrategias para entrar y salir de la modernidad*. México, D.F.: Grijalbo.
17. Gless, S. (2020) "AI in the Courtroom: A Comparative Analysis of Machine Evidence in Criminal Trials", *Georgetown Journal of International Law,* 51(2) 195-253.
18. Greco, L. (2020). *Poder de julgar sem responsabilidade de julgador*: *a impossibilidade jurídica do juíz-robô.* São Paulo: Marcial Pons.
19. Haesbaert, R. (2021) *Território e descolonialidade: sobre o giro (multi)territorial/de(s) colonial na América Latina*. Buenos Aires: CLACSO.
20. Hilgendorf, E. (2015) "Recht und autonome Maschinen – ein Problemaufriβ" in: Hilgendorf, E.; Hötitzsch, S. (eds.) *Das Recht vor den Herausforderungen der modernen Technik.* Baden-Baden: Nomos.
21. Hilgendorf, E. (2020) "Sistemas Autônomos, Inteligência Artificial e Robótica: uma orientação a partir da perspectiva jurídico-penal" in: Hilgendorf, E., Gleizer, O. (eds.) *Digitalização e Direito.* São Paulo: Marcial Pons, 43-59.
22. Inter-American Court of Human Rights (IACHR) (2004). *Case of Plan de Sánchez Massacre vs. Guatemala***.** 19 November 2004. http://www.corteidh.or.cr/docs/casos/articulos/seriec_116_ing.pdf.
23. Inter-American Court of Human Rights (IACHR) (2013). *Case of Osorio Rivera y relatives vs. Peru*. 26 November 2013. https://www.corteidh.or.cr/docs/casos/articulos/seriec_274_esp.pdf.
24. Januário, T. F. X. (2020a) "Inteligência Artificial e Responsabilidade Penal no Setor da Medicina", *Lex Medicinae: Revista Portuguesa de Direito da Saúde,* 17(34), 37-63, https://www.centrodedireitobiomedico.org/publica%C3%A7%C3%B5es/revistas.
25. Januário, T. X. (2020b) "Veículos Autónomos e Imputação de Responsabilidades Criminais por Acidentes" in: Rodrigues, A. M. (coord.) *A Inteligência Artificial no Direito Penal.* Coimbra: Almedina, 95-127.

26. Januário, T. F. X. (2021a) "Cadeia de Custódia da Prova e Investigações Internas Empresariais: Possibilidades, Exigibilidade e Consequências Processuais Penais de sua Violação", *Revista Brasileira de Direito Processual Penal,* 7(2), 1453-1510, https://doi.org/10.22197/rbdpp.v7i2.453.
27. Januário, T. F. X. (2021b) "Considerações Preambulares Acerca das Reverberações da Inteligência Artificial no Direito Penal" in: Comério, M. S.; Junquilho, T. A. (eds.) *Direito e Tecnologia: um debate multidisciplinar.* Rio de Janeiro: Lumen Juris, 295-314.
28. Januário, T. F. X. (2021c) "Inteligência artificial e manipulação do mercado de capitais: uma análise das negociações algorítmicas de alta frequência (High-Frequency Trading – HFT) à luz do ordenamento jurídico brasileiro", *Revista Brasileira de Ciências Criminais*, 29(186), 127-173.
29. Januário, T. X. (2022) "Inteligência artificial e direito penal da medicina", in: Rodrigues, A. M. (coord.), *A inteligência artificial no direito penal, Volume II*. Coimbra: Almedina, 125-173, forthcoming.
30. Kehl, D., Guo, P., Kessler, S. (2017) "Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing", *Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School*, 2017. http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746041.
31. Laufer, W.S. (1999) "Corporate Liability, Risk Shifting, and the Paradox of Compliance", *Vanderbilt Law Review*, 52, 1341-1420.
32. Lee Van Cott, D. (2006) "Pluralismo legal y administración de justicia comunitaria informal en América Latina". in: *Antología: Grandes temas de la antropología jurídica.* Oaxtepec: Red latinoamericana de antropología jurídica, 2006, 209-237.
33. Machado, L. S. (2019) "Médico robô: responsabilidade civil por danos praticados por atos autônomos de sistemas informáticos dotados de inteligência artificial", *Lex Medicinae: Revista Portuguesa de Direito da Saúd*e, 16(31), 101-114.
34. Miranda, M. A.; Januário, T. F. X., "Novas tecnologias e justiça criminal: a tutela de direitos humanos e fundamentais no âmbito do direito penal e processual penal", in: Moreira, V. Et. al. (orgs.), Temas de Direitos Humanos do VI CIDH Coimbra 2021, Brasílica / Edições Brasil, Campinas / Jundiaí, 2021, 284-298.
35. Miró Llinares, F. (2018) "Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots", *Revista de Derecho Penal y Criminología*, 3(20), 87-130.
36. Mulholland, C.; Frajhof, I. Z. (2019) "Inteligência Artificial e a Lei Geral de Proteção de Dados Pessoais: Breves Anotações Sobre o Direito à Explicação Perante a Tomada de Decisões por Meio de Machine Learning" in: Frazão, A.; Mulholland, C. (eds.). *Inteligência Artificial e Direito: Ética, Regulação e Responsabilidade.* São Paulo: Thomson Reuters Brasil.
37. O'Neil, C. (2016), *Weapons of math destruction: how big data increases inequality and threatens democracy.* New York: Crown Publishers.
38. Padilla, G. (2005) "Pluralismo jurídico y paz en Guatemala", *Revista IIDH,* 41, 209-223.

39. Peixoto, F. H.; Silva, R. Z. M. (2019) *Inteligência Artificial e Direito.* Curitiba: Alteridade Editora, 2019.
40. Pereira, A. G. D. (2021) "Inteligência Artificial, Saúde e Direito: considerações jurídicas em torno da medicina de conforto e da medicina transparente", *Julgar,* 45, 235-261.
41. Price II, W. N. (2017) "Artificial Intelligence in Health Care: Applications and Legal Issues", *U of Michigan Public Law Research Paper*, 599, 1-7.
42. Quattrocolo, S. (2020). *Artificial Intelligence, Computational Modelling and Criminal Proceedings: A Framework for a European Legal Discussion.* Cham: Springer.
43. Queiroz, M.I.P. (1968) "O catolicismo rústico no Brasil", *Revista do Instituto de Estudos Brasileiros,* 5, https://doi.org/10.11606/issn.2316-901X.v0i5p,104-123.
44. Rodrigues, A. M. (2020a) "A questão da pena e a decisão do juiz - entre a dogmática e o algoritmo", in: Rodrigues, A. M. (coord.), *A Inteligência Artificial no Direito Penal*, Coimbra: Almedina, 219-244.
45. Rodrigues, A. M. (2020b) "Inteligência Artificial no Direito Penal – A Justiça Preditiva entre a Americanização e a Europeização", in: Rodrigues, A. M. (coord.), *A inteligência artificial no direito penal*. Coimbra: Almedina, 11-58.
46. Rodrigues, A. M. (2021a) "Os crimes de abuso de mercado e a «Escada Impossível» de Escher (o caso do Spoofing)", *Julgar,* 45, 65-86.
47. Santosuosso, A.; Bottalico, B. (2017) "Autonomous Systems and the Law: Why Intelligence Matters" in: Hilgendorf, E.; Seidel, U. (eds.), *Robotics, Autonomics, and the Law: Legal Issues Arising from Industry 4.0 Technology Programme of the German Federal Ministry for Economic Affairs and Energy.* Baden-Baden: Nomos, 27-58.
48. Schavelzon, S. (2016) "La justicia comunitaria en Bolivia y la ocupación de la casa de Víctor Hugo Cárdenas", *Direito e Democaria*, 17(1) 43-63.
49. Sousa, S. A. (2020) "Não fui eu, foi a máquina": teoria do crime, responsabilidade e inteligência artificial", in: Rodrigues, A. M. (coord.), *A inteligência artificial no direito penal*. Coimbra: Almedina, 59-93.
50. The European Commission's High-Level Expert Group on Artificial Intelligence (2018) *A Definition of AI: Main Capabilities and Scientific Disciplines: Definition Developed for the Purpose of the Deliverables of the High-Level Expert Group.* Brussels: European Commission, 2018. https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf.
51. Tutu, D. M. (2000) *No future without forgiveness*. Nova Iorque: Doubleday.
52. Wimmer, M. (2019) "Inteligência artificial, algoritmos e o direito. Um panorama dos principais desafios", in: Lima, A. P. C., Hissa, C. B., Saldanha, P. M. (coords.), *Direito digital: debates contemporâneos*. São Paulo: Thomson Reuters Brasil, 15-30.
53. Yapo, A; Weiss, J. (2018) "Ethical Implications of Bias in Machine Learning" in: *Proceedings of the 51st Hawaii International Conference on System Sciences,* 5365-5372.
54. Yates, P. (dir.) (1984) *Cuando las montañas tiemblam*. Guatemala, Espanha: Skylight, 1984, (84min). https://www.youtube.com/watch?v=5FIHfM2E2PQ&t=2122s&gt.

ISPOD TOGE SUDIJE ROBOTA: DEMISTIFIKACIJA UPOTREBE VEŠTAČKE INTELIGENCIJE U KRIVIČNOM PRAVU U ODNOSU NA GLOBALNU PERSPEKTIVU JUGA

Naučni i tehnološki razvoj u oblasti autonomnih sistema i veštačke inteligencije omogućili su i podstakli njihovu upotrebu u različitim društvenim oblastima. Oni su počeli da se koriste i u okviru krivičnog pravosuđa. Sve su češći primeri njihovog korišćenja ne samo u krivičnim istragama i postupcima, već i prilikom donošenja presuda. Međutim, nije prošlo mnogo vremena, a da se ne postave pitanja u vezi sa granicama tih sistema i njihovim mogućim uticajem na prava pojedinaca. Iako ne možemo poreći da neke specifičnosti ovih tehnologija, posebno veštačke inteligencije (kao što su npr. nejasnoća i nepredvidivost učinka), predstavljaju rizik za neke fundamentalne grancije u krivičnom postupku. Po našem mišljenju, u osnovi mnogih dokritriniranih kritika, prisutno je izvesno nerazumevanje šta su ove tehnologije, kako funkcionišu i kako se koriste u pravosudnom sistemu. S obzirom na navedeno, autori u ovom radu nastoje da istraže kako su veštačka inteligencija i autonomni sistemi korišćeni u krivičnom pravosuđu kako bismo mogli da identifikujemo koji su u stvari njihovi potencijalni uticaji na prava i garancije okrivljenih. Zbog toga ćemo prvo proučiti koncept i rad ovih tehnologija kako bismo razumeli njihove posebnosti, a zatim ćemo analizirati njihovu konkretnu primenu u sferi pravosuđa. Stoga ćemo se opredliti za predmet proučavanja dva najpoznatija sistema sudske pomoći – HART i COMPAS, kao i sistem koji se koristi u Brazilu, odnosno VICTOR. Na osnovu zaključaka i primenom deduktivnog metoda, nastojaćemo da demistifikujemo neke stavove vezane za tzv. "sudiju robota" identifikujući koji su njegovi potencijali i granice, a naročito kada su u pitanju pravne garancije.

KLJUČNE REČI: *veštačka inteligencija, robot, sudija, dekolonijalnost, globalni jug.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.21

KRIVIČNA PRAVDA U ERI VEŠTAČKE INTELIGENCIJE

Svetlana Nenadić*
Ivana Miljuš**

Autorke polaze od pretpostavke da veštačka inteligencija (AI), kao ekstenzija digitalne transformacije društva, postaje sastavni deo krivične pravde. Rad predstavlja prikaz moguće upotrebe AI u krivičnom pravu, ali i rizika koje njegova upotreba nosi po krivično pravo. Polazeći od teze da tehnologija AI dovodi do uklanjanja barijera između mašina i čoveka tako što veštačka inteligencija prestaje da bude prosti objekt u rukama čoveka i postaje subjekat društvenih interakcija, autorke zaključuju da AI nije samo prosto oruđe krivične pravde već i put ka transformaciji krivičnog prava.

Rad polazi od pojma AI i njegovog uticaja u svetu interneta stvari (IoT) na način otkrivanja krivičnih dela, prevenciju i procenu stepena rizika recidivizma. Pametni algoritmi veštačke inteligencije mogu da deluju nezavisno od ljudi, generišući aktivnosti u ime čoveka, bez njegovog neposrednog znanja ili odobrenja. Međutim, kako je AI sklona predrasudama (AI bias), algoritmi softvera „predvidive pravde" mogu da imaju diskriminatorski efekat, koji je potrebno identifikovati. U pravosudnim sistemima tehnološki razvijenih država AI dobija i funkciju da pomogne sudiji da brže i efikasnije obavlja sudijski posao. Primena tehnologije „učenja mašina" radi automatskog generisanja presuda za sudije dovodi do brojnih rizika, naročito naglašenih u krivičnim predmetima. Postavljaju se pitanja preoblikovanja uloge sudije („instrumentalizacije sudija"), nepristrasnosti suda, prava na informisanje o logici odlučivanja, prava na osporavanje naučne validnosti algoritma i prekomerne standardizacije sudskih odluka. S obzirom na karakter autonomnosti AI, neminovno se postavlja pitanje da li postoji krivična odgovornost veštačke inteligencije, u kom obimu i na koji način i da li je potrebno kreiranje novih oblika odgovornosti i novih subjekata odgovornosti u kaznenom pravu?

KLJUČNE REČI: *krivična pravda; veštačka inteligencija (AI); internet stvari (IoT); predrasude veštačke inteligencije (AI bias); subjekti krivične odgovornosti.*

* Doktor pravnih nauka, zamenik javnog tužioca u Tužilaštvu za ratne zločine.
E-mail: *svetlananenadic11@gmail.com*

** Doktor pravnih nauka, docent na Univerzitetu u Beogradu – Pravnom fakultetu.
E-mail: *miljusivana85@gmail.com*

UVOD

Veštačka inteligencija[1] (sistem veštačke inteligencije) podrazumeva raznolik stepen upotrebe nauka i tehnologija radi omogućavanja mašinama da preduzimanjem radnji koje zahtevaju inteligenciju postignu određene ciljeve kao što je pobeda šampiona u šahu, vožnja automobila, razgovori sa ljudima (European Commission for the Efficiency of Justice (CEPEJ), 2019: 30). Dostignuće razvoja kompjuterske tehnologije je oblikovanje formi veštačke pravne inteligencije[2] – „mešavine veštačke inteligencije i prava", koja prognozira, savetuje, pruža pravnu pomoć, pomaže policiji u sprečavanju i otkrivanju krivičnih dela i u izvesnoj, manjoj ili većoj meri, pruža pomoć i podršku sudiji učestvovanjem u postupku odlučivanja pred sudom. Razvoj veštačke pravne inteligencije ima ambiciju i da zamenjuje aktivnost sudije.

Definicije veštačke inteligencije su raznolike i neusklađene. Radi analize efekata veštačke inteligencije na ljudska prava u pravnim postupcima, pogodnom se smatra određenje pojma veštačke inteligencije od strane Komesara za ljudska prava. Veštačka inteligencija je, prema ovoj definiciji, mašinski sistem koji „izrađuje preporuke, predviđanja ili odluke za određeni set ciljeva" prema sledećem pojednostavljenom obrascu: 1. *korišćenje mašinskog i/ili ljudskog učešća da sagleda stvarna i/ili virtuelna okruženja*; 2. *pretvaranje ovih percepcija u modele* (bilo ručno ili automatski); 3. *izvođenje ishoda iz modela* (bilo preko čoveka ili automatizovanim putem), u formi preporuka, predviđanja ili odluka (Komesar za ljudska prava, 2019: 5).

Iskustva upotrebe veštačke inteligencije u pravosudnim sistemima različita su po osnovu usluge koje ona pruža. U naučnoj i stručnoj literaturi i uporednopravnim izveštajima posvećuje se naročita pažnja naprednim obrađivačima sudske prakse, davanju sudskih odluka u otvorenim podacima, za koje se koristi neka obrada AI, analizama rizika budućeg ponašanja okrivljenih i osuđenih (algoritmi i alati za analizu – „prediktivni alati"). Iako je koncept „predvidive pravde" („*predictive justice*")[3] značajno širi, jer generalno podrazumeva predviđanje ishoda (uspeha/neuspeha) određenog predmeta ili odgovarajuće faze postupka, zvanično se u domaćim medijima naglašava njena svrha da pomogne sudijama da odlučuju o saobraćajnim prekršajima (Toskić Cvetinović, 2021). Kada je reč o korišćenju veštačke inteligencije u postupku odlučivanja, upotreba veštačke

[1] Veštačka inteligencija se u stranoj literaturi jednoobrazno označava skraćenicom „AI" („*Artificial Intelligence*"), a u tekstovima na srpskom jeziku pronalazi se i skraćenica „VE". Autorke su se opredelile za skraćenicu „AI" zbog dominantnog označavanja pojma veštačke inteligencije kao oblasti računarstva, ovom skraćenicom.

[2] U literaturi se pronalazi izraz „veštačka pravna inteligencija" („*artificial legal intelligence*") (Shi i dr., 2021: 1). Osim ovog izraza, upotrebljava se i izraz „pravda veštačke inteligencije" (*Artificially Intelligent Justice*). (Re i Solow-Niederman, 2019: 242)

[3] Prediktivni softeri razvijeni su za potrebe privatnog sektora pre svega pravnih službi, osiguravača i osiguranika, kao i advokata (predviđanje ishoda parnica). Njihov cilj je da umanje pravnu nesigurnost i nepredvidivost budućih sudskih odluka. Teorijske funkcionalnosti softvera „predvidive pravde" ogledaju se u utvrđivanju verovatnoće uspeha ili neuspeha nekog predmeta pred sudom, do koje se dolazi putem statističkog modeliranja prethodnih odluka korišćenjem informatičkih metoda obrade „prirodnog jezika" i „mašinskog učenja" (European Commission for the Efficiency of Justice (CEPEJ), 2018: 29)

inteligencije modifikuje način rada sudija i uopšte pravnika, a potencijalno preti da razori sudijsku ulogu i načela na kojima počiva savremena krivična procedura. Postupci odlučivanja značajno se menjaju i mogu da preoblikuju ulogu sudije i eliminišu uključivanje emocija i saosećanja prilikom odlučivanja (Sourdin, 2018: 1129). Još uvek u teorijskom smislu je krajnji cilj razvoja veštačke inteligencije da se stvori tzv. „jaka" veštačka inteligencija, a to je u suštini „mašina za samoučenje sposobna da automatski razume svet uopšte, u svoj svojoj složenosti" (European Commission for the Efficiency of Justice (CEPEJ), 2019: 30).

Živimo u svetu gde mašine međusobno komuniciraju. U nama nevidljivom, svetu „interneta stvari" intenzivno razmenjuju, selektuju i ocenjuju podatke koje sami pribavljaju, a pribavljene informacije obrađuju u svojim neuralnim mrežama i iz njih uče, odnosno izvode zaključke na osnovu kojih usmeravaju svoje aktivnosti. Suština ideje *machine learning* je eliminisanje čoveka iz jednačine, jer veštačka neuralna mreža uči da izvodi zadatke razmatrajući primere i zaključujući iz njih, a da nije prethodno programirana pravilima izvođenja određenog zadatka (Završnik, 2020: 658). Informacije koje mašine obrađuju tiču se sveta oko njih, pa samim tim i nas, kao njihovog prirodnog okruženja.

Veštačka inteligencija poseduje jednu značajnu inherentnu manu koja je prepreka za širu upotrebu ove tehnologije, naročito iz ugla zaštite ljudskih prava. Po svojoj prirodi je pristrasna. Pristrasnost, koja se može ogledati u predrasudama, sklonostima ili predubeđenjima, predstavlja naročit problem kod upotrebe veštačke inteligencije u raznim aktivnostima vezanim za sprovođenje „krivične pravde". Na primer, kod procene opasnosti od recidivizma ili obrazlaganja presude. Krivično pravosuđe, kao mehanizam koji društvu nudi garancije „krivične pravde", mora da predstavlja bedem zaštite od bilo kog oblika diskriminacije svakog pripadnika društva, tako da je postojanje bilo kog oblika pristrasnosti u ovom složenom mehanizmu nedopustivo. Razmatraćemo koje sve vrste pristrasnosti veštačke inteligencije postoje i zašto je ovaj problem važan sa stanovišta krivičnog prava. Radi ilustracije kako predrasude veštačke inteligencije mogu da se reflektuju u krivičnom pravu, predstavićemo jedno istraživanje iz SAD koje se ticalo analize pristrasnosti veštačke inteligencije.

Mogućnost mašina da donose odluke umesto nas ili da deluju umesto ili mimo nas, dovodi do osećaja anksioznosti koji proizilazi iz ljudskog straha od koegzistencije sa veštačkom inteligencijom (Hallevy, 2013: 14). Ovaj strah je čest motiv ostvarenja naučne fantastike sa temom budućnosti u kojoj mašine vladaju ljudima.[4] Mračna distrofična budućnost iz umetničkih ostvarenja je još uvek daleko od nas. Međutim, pred pravnicima se nalazi realan i aktuelan problem, a to je pitanje krivične odgovornosti kod krivičnih dela izvršenih od strane veštačke inteligencije, odnosno, pred pravnicima je dilema – postoji li *machina sapiens criminalis* (Hallevy, 2013: 14).

[4] Strah od „robota" leži u korenu tri zakona Isaka Asimova iz njegovog čuvenog dela „Ja, robot".
Prvi zakon: Robot ne sme da povredi ljudsko biće ili, nečinjenjem, dozvoli ljudskom biću da se povredi.
Drugi zakon: Robot mora da se povinuje naredbama koje mu daju ljudska bića, osim ako bi takva naređenja bila u suprotnosti sa Prvim zakonom.
Treći zakon: Robot mora da štiti sopstvenu egzistenciju sve dok takva zaštita nije u suprotnosti sa Prvim ili Drugim zakonom. (Asimov, 1950: 40)

1. UPOTREBA VEŠTAČKE INTELIGENCIJE U KRIVIČNOM PRAVOSUĐU

Veštačka inteligencija i algoritmi primenjuju se široko u sferama društvenog i ličnog života. U naučnim radovima ova pojava označava se trendovima „vladavine algoritama", „pojačanog uticaja matematike" na sve životne oblasti, kao i dela „solicionizma" koji slede tehnološke kompanije nudeći tehnička rešenja za sve društvene probleme, uključujući i kriminalitet (Završnik, 2019: 624). Ideja funkcije algoritma je da eliminiše predrasude svojstvene ljudskom rasuđivanju i odlučivanju ukazivanjem poverenja razumu, nauci i objektivnosti, ali njeno sprovođenje u delo upravo vodi suprotnim dejstvima.

Duboko u pozadini, kroz istoriju su poznate zamisli da se krivična pravda ograniči isključivo na razum odnosno „čistu nauku" (Završnik, 2019: 637). Dostizanje objektivnosti u odlučivanju odnosno eliminisanje subjektivizma u odlučivanju jedan je od temelja zagovaranja upotrebe veštačke inteligencije u postupku sudskog odlučivanja. Teoretičari ukazuju da ipak postoje različiti aspekti subjektivnosti, najmanje dve, prvi koji su štetni i za njih nema mesta u pravnom rezonovanju, i drugi koji obogaćuju pravne odluke jer su kompatibilni sa osnovnim pravnim vrednostima (Plesničar i Šugman Stubbs, 2018: 158).

Poruka menadžera kreatora algoritama, koja naročito deluje na društva koja građani doživljavaju diskriminatorskim, glasi da su postojeći pravni mehanizmi za obezbeđenje nepristrasnosti sudija nedovoljni odnosno nedovoljno pouzdani i nedolotvorni, a da veštačka inteligencija upravo nudi objektivno naučno odlučivanje.

1.1. Upotreba „algoritama za prognoziranje" u cilju sprečavanja i otkrivanja krivičnih dela, procene stepena rizika od bekstva i recidivizma

Plod razvoja informacione tehnologije i veštačke inteligencije je upotreba tzv. „prediktivnih alata" – alata za prognoziranje da li postoji rizik da će lice postati učinilac („potencijalni učinilac") ili žrtva („potencijalna žrtva") pojedinih krivičnih dela ili krivičnih dela određene prirode ili grupe. „Prediktivni alati" podržavaju „*pre – crime* koncept" krivičnog prava. Koncept podrazumeva ulogu krivičnog prava da se bavi budućim krivičnim delima služeći se anticipatornom logikom, tj. logikom predviđanja, a počiva na pojmu „*pre – crime*" kojim se kritički opisuje preokupacija društva budućim krivičnim delima odnosno budućnošću i bezbednošću, kao i tendencija krivičnopravnog sistema da se bavi anticipiranjem krivičnih dela (Nenadić, 2021: 269).

Kreiranje algoritama za preciznije prognoziranje budućeg ponašanja okrivljenih (alati za procenu rizika) dovodi do zabrinutosti naučnih radnika i profesionalnih pravnika da li interesi poslovanja privatnih tehnoloških kompanija koje stvaraju algoritme imaju prioritet u odnosu na interese krivične pravde.[5]

[5] Sumnju potkrepljuje i deo analize netransparentnog postupanja profitne kompanije „Northpointe", u pogledu rada njenog algoritma za ocenu rizika, od strane neprofitne organizacije *Pro Publica:* „Kompanija ne objavljuje javno kalkulacije koje su korišćene da bi se došlo do ocena rizika okrivljenih, tako da nije moguće da okrivljeni i javnost vide šta bi moglo dovesti do razlika"....."Nije podelila konkretne proračune, za koje je rekla da su vlasnički." (ProPublica).

Osnovna pretpostavka policijskih alata za prognoziranje je da su određena krivična dela, kao što su krađa i razbojništvo, u velikoj meri predvidiva, jer učinioci krivičnih dela sa prepoznatljivim profilom imaju tendenciju da čine istovrsna krivična dela, na približno istoj lokaciji i u isto doba dana (Peeters i Schuilenburg, 2018: 272). Predviđanje pojedinih krivična dela kao što su provaljivanja/obijanja stambenih objekata (*residential burglary*) i nasilja bandi (*gang violence*) popularnim alatom „*PredPol*" počiva na primeni modela predviđanja zemljotresa na predviđanje krivičnih dela. Model analizira pojavu zemljotresa kao „pozadinskih događaja" ili „naknadnih potresa", što se projektuje na pomenuta krivična dela.[6]

Predviđanje u operativnom radu policijskih službenika obuhvata jednostavnije poduhvate kao što je korišćenje alata kompjuterske statistike koji obrađuju velike količine podataka iz policijskih izveštaja o hapšenjima, a zatim predviđaju buduće koncentracije kriminala ili „vruće tačke" („*hot spots*") odnosno dolazi do „predvidivog mapiranja krivičnih dela" radi bržeg reagovanja policije. Negativni efekti aktivnosti ovih alata su prekomerna kontrola pojedinih geografskih oblasti, te posledično nedovoljna kontrola drugih geografskih oblasti, što utiče i na doživljaj građana da u društvu vlada diskriminacija i nejednaka pravda.

Pojam „*predictive policing*" vezuje se analitičke alate, prikupljanje, a potom analizu podataka, te rezultat analize – anticipiranje krivičnih dela, vremena i mesta izvršenja potencijalnih budućih krivičnih dela. U skladu sa tim prognozama, prilagođavaju se operacije policije odnosno menjaju se odluke policije i raspored policijskih službenika u rizičnim oblastima. Posledično, javljaju se promene u okruženju i sledi ponovno prikupljanje podataka (Bennett Moses i Chan, 2018: 807 – 808).

Softveri sa algoritmom za prognoziranje budućih krivičnih dela podrazumevaju analizu velike količine „razbacanih" podataka na osnovu koje se izračunava da li postoji povećan stepen rizika od izvršenja krivičnih dela. Ovi instrumenti za predviđanje rade u cilju sprečavanja izvršenja budućeg krivičnog dela (*ex – ante preventivne mere*) zalažењem u pripremnu fazu ostvarivanja krivičnog dela i u cilju otkrivanja već učinjenog krivičnog dela (*ex – post reaktivne mere*). U pogledu alata koji imaju funkciju da deluju preventivno razlikuju se oni koji se fokusiraju na „rizične" pojedince – generisane liste koje identifikuju ljude koji će najverovatnije učiniti krivična dela (tzv.„*heat lists - algortihm*") i koji se fokusiraju na rizična mesta („*hot spot policing*") (Završnik, 2020: 570).

Prediktivni alati dovode u pitanje suštinsko ostvarivanje ljudskih prava, jer se na bazi njihovih rezultata preduzimaju aktivnosti prema licima koja se ne smatraju osumnjičenima. Ne postoji sumnja da su ova lica učinila krivično delo, već isključivo sumnja da će u budućnosti učiniti krivično delo. Nalazi se da je načelno „preventivna pravda na suprotnom polu od pretpostavke nevinosti" (Report of Open Society Justice Initiative`s Criminal Justice Program, 2014: 97). Procena rizika na osnovu okolnosti koje se ne odnose na radnje lica već isključivo druge faktore kao što su sredina u kojoj živi, mogu ga okvalifikovati opasnim po društvo i staviti pod nadzor policije.

[6] Određena krivična dela deluju kao „samopobuđena", slično naknadnim potresima zemljotresa. Predviđanje se bazira na sledećem poređenju: „Zemljotres ili krivično delo može biti „pozadinski događaj" ili „naknadni potres" ili „skoro ponavljanje drugog zemljotresa"/"krivičnog dela blizu u prostoru i vremenu" (Bennett Moses i Chan, 2018: 808).

Alati čija je funkcija da izvode automatizovane zaključke o kriminalitetu na osnovu slika lica koja svojim većim stepenom varijacija u izgledu lica odnosno pojedinim karakteristikama lica odudaraju od slika lica ljudi koji poštuju zakon, iako primenjuju kontrolisano mašinsko učenje, isključivanje pristrasnosti subjektivnih sudova ljudi kao posmatrača i kontrolisanje po rasi, polu i starosti i izrazu lica (Wu i Zhang, 2016: 1), kritikovani su jer se ipak suštinski, samo u novom ruhu, vraćaju pseudonauci frenologiji, kontraverznim istraživanjima i teorijama o urođenim svojstvima zločinca i predrasudama o krivičnom delu.

Sistem *National Data Analytics Solution* (NDAS) u Velikoj Britaniji, za koji se prognozira da bi trebalo da bude dostupan u skoroj budućnosti u svakoj policijskoj upravi u ovoj zemlji, koristi se za izgradnju, na osnovu raspoloživih podataka, prototipa ponašanja kriminalaca i žrtava, koji se zatim upoređuje sa podacima o građanima radi procene rizika da li će pojedinačni građanin postati žrtva nasilja, nekog oblika modernog ropstva ili potencijalni učinilac krivičnih dela (Nenadić, 2021: 272). Predstavnici Nacionalnog instituta za veštačku inteligenciju „Alan Tjuring" izrazili su zabrinutost za funkcionisanje ovog sistema, po osnovu niza etičkih pitanja. Izdvajamo osnovno: „Da li je moralno ispravno intervenisati kada pojedinac možda nije učinio krivično delo, a postoji verovatnoća da će to učiniti u budućnosti?" (Savetodavno mišljenje Instituta u pogledu ovog programa pod nazivom „*Independent Digital Ethics, Ethics Advisory Report for West Midlands Police*").

Sudovi u SAD primenjuju „prediktivne alate" (alate za procenu rizika – „*risk assessment algorithms*") u postupcima sudskog odlučivanja u krivičnom postupku koji prognoziraju („*predictive justice*"): 1. *rizike bekstva ili recidivizma u pogledu okrivljenih u procesnim fazama koje prethode suđenju*, *u proceduri odlučivanja o jemstvu*; 2. *verovatnoću recidivizma okrivljenih* u proceduri odlučivanja o krivičnoj sankciji; 3. *rizike u proceduri odlučivanja o uslovnom otpustu*.

Zagovornici upotrebe ovih alata ukazuju da je njihova svrha da se smanji kriminatitet odnosno da budu instrumenti kontrole kriminaliteta, da se eliminiše pristrasnost svojstvena ljudima i da postupci u kojima se odlučuje budu fer i efikasniji. Međutim, nalazi se da ovi alati veštačke inteligencije imaju tendenciju da daju prednost utilitarističkom konceptu pravde, koji favorizuje interese većine (zajednice) nad manjinom, nauštrb individualnih ljudskih prava (vidi Forest, 2021: 1- 9). Osnovni problemi algoritama su nedostatak informacija o njihovom dizajnu i funkcionisanju, kao i efekat uvećavanja predrasuda umesto njihovog gubljenja. Izveštava se da se ulazni podaci upravo izvode iz pristrasnog rada policije i rasno kompromitovanih podataka o ranijoj osuđivanosti, što neizbežno vodi rezultatu da će okrivljeni Afroamerikanci i Latinoamerikanci komjuteru delovati rizičniji u pogledu budućih hapšenja od okrivljenih belaca (Eckhouse, 2017).

Odlučivanje o slobodi okrivljenog pre suđenja podrazumeva ocenu dokaza i budućeg ponašanja okrivljenog, da li će okrivljeni pobeći, odazivati se pozivima suda, da li postoji verovatnoća da će učiniti novo krivično delo. Složenost odlučivanja podrazumeva da se određenoj okolnosti, kao što je na primer ranija osuđivanost, ne pridaje značaj *a priori*, nego u vezi sa svim okolnostima konkretnog slučaja u međusobnoj zavisnosti.

Neke od osnovnih kritika mašinskog odlučivanja pa i odlučivanje o jemstvu ili preventivnom lišenju slobode su da se sudske odluke svode na mašinsku logiku, te se do rezultata dolazi automatski, bez uzimanja u obzir društvene složenosti i okolnosti konkretnog slučaja. Praktično, odluka o pritvoru zavisi od određenog unosnog podatka i njegovog vrednovanja tako da neznatna razlika u numeričkom rezultatu može da svrsta okrivljenog među lica sa srednjim stepenom rizika, umesto među lica sa niskim stepenom rizika, te da realni ishod bude lišavanje slobode okrivljenog pre suđenja (Forest, 2021: 26 – 27). Pravičnost postupka odlučivanja povređuje se ako se ne dozvoli okrivljenom da preispituje konkretne unose, da li oni imaju diskriminatoski efekat odnosno nose sa sobom implicitnu pristrasnost (nevidljiv skup pretpostavki zasnovanih na rasi, klasi ili drugim faktorima), te vrednovanje unosa, od čega zavisi odluka o slobodi okrivljenog.

Iako alati formalno imaju ulogu pomoći sudijama, odlučivanje sudije protivno prognozi algoritma praktično nameće sudiji dodatni teret, veću odgovornost, zbog čega je realno predvideti da će se sudije povinovati rezultatu rada algoritma. Prednost odlučivanja ljudi je što se njihove odluke mogu zasnivati na vrednostima i društvenim razmatranjima koje se ne unose u mašinu. Tako se kao primer u literaturi praktično objašnjava da sudija može da odluči da odredi jemstvo okrivljenoj, u odnosu na koju postoji rizik od ponovnog izvršenja krivičnog dela, na osnovu hijerarhije vrednosti. Sudija može da pridaje veću pažnju njenoj ulozi majke i zaštitnika dece, dok algoritam ne bi mogao da radi na osnovu takve hijerarhije prioriteta, iako bi tačnije odredio rizik od ponavljanja krivičnog dela (European Commission for the Efficiency of Justice (CEPEJ): 2019, 54). Mašina nema svest. Nije etički niti društveni subjekt.

Zagovornici upotrebe algoritama za odlučivanje o jemstvu američke Arnold Fondacije isticali su nedostatke u praksi prilikom odlučivanja sudije/magistrata/državnog službenika odnosno komesara o jemstvu: zasnivanje odluke na okolnostima optužbe, prevelika relevantnost koja se pripisivala okolnostima kao što je zloupotreba alkoholnih pića i droga, upletenost u odlučivanje predrasuda na štetu siromašnih manjinskih grupa, a ne objektivna ocena rizika da će okrivljeni izvršiti novo krivično delo, povrediti nekoga odnosno da postoji povećan rizik od vršenja nasilja (krivičnih dela sa elementima nasilja) ili rizika izostanka sa suđenja. U praksi su se odluke zasnivale i na okolnostima ranije osuđivanosti (kriminalne istorije), što je zahtevalo vreme za utvrđivanje i angažovanje ljudskih resursa, okolnostima veza sa zajednicom i radnog statusa okrivljenog. Upotrebi algoritama pripisana je uloga sredstva u borba protiv implicitne pristrasnosti, nevidljivog skupa pretpostavki zasnovanih na rasi, klasnim i drugim faktorima koji mogu biti u igri", jer podrazumeva naučno potvrđenu ocenu rizika.[7] Primena algoritma je predviđena kao savetodavna i pomoćna, a ne kao zamena za sudsku ocenu.

Zakonodavnom reformom u Kaliforniji uveden je sistem jemstva koji se oslanja na algoritamsku procenu rizika. Predviđeno je diskreciono pravo viših sudova na lokalni

[7] Istraživači su otkrili da su manje od deset objektivnih faktora kao što su starosna dob, krivični dosije i prethodni izostanci okrivljenih sa ročišta pred sudom, uz pridavanje većeg značaja novijim krivičnim delima, bili najbolji za prognozu ponašanja okrivljenog (Dewan, 2015).

instrument za procenu rizika, ali koji je izabran sa liste alata prethodno potvrđenih od strane Sudskog saveta na nivou države (Re i Solow-Niederman, 2019: 287).

Algoritmi za ocenu verovatnoće recidivizma („*recidivism risk algorithms*“) koriste se pri odmeravanju zatvorskih kazni, odnosno njihovi rezultati su preporuka sudiji za odluku o izricanju kazne zatvora. Greške u ovoj proceduri imaju izuzetno teške posledice po društvo i individualne slobode, jer se na temelju osude odlučuje o slobodi okrivljenog, eventualnom izricanju kazne zatvora i njenom trajanju.[8] Zamisao funkcije algoritama je da se putem naučnih i tehničkih metoda dođe do konkretnog rezultata – krivične sankcije, te da se eliminišu razlike svojstvene sudijama kao ljudskim bićima i da se efikasnije odlučuje. Raznolikosti sudija posebno dolaze do izražaja u „*melting pot*“ američkom društvu, čak i kada se radi o sudijama istog distrikta. Sudije odlučuju u okviru diskrecione ocene i pod izvesnim uticajem različitih tradicija, raznolikih iskustava, vrednosti i etičkih principa koji dele, u istim ili sličnim situacijama donose neujednačene odluke. Međutim, zasnivanje odluka o kazni na statičkim faktorima i nepromenljivim karakteristikama (poput nivoa obrazovanja okrivljenog, socio-ekonomskog porekla ili sredine u kojoj živi) može da dovede do suprotnog efekta od predstavljenog željenog (Sourdin, 2021: 83). Ovi alati za predviđanje nose sa sobom inherentni potencijal da pogoršaju odnosno uvećaju neopravdane i nepravedne razlike, svojstvene društvima i pravosuđima u kojima je izražena diskriminacija među populacijom kao što je američko, u kojem se promovišu i u najširem obimu primenjuju.

Osnovni prigovori isticani protiv upotrebe algoritma „*Correctional Offender Management Profiling for Alternative Sanctions*“ (COMPAS) u proceduri izricanja kazni bili su tačnost informacija na kojima se temelji ocena rizika, tačnost programa i ostvarivanje prava okrivljenog da u potpunosti istraži i preispituje odluku o krivičnoj sankciji ocenom tačnosti rezultata, pretnja po realizaciju prava okrivljenog na individualizovanu kaznu i pitanje „predrasuda algoritama“ (Freeman, 2016: 91 – 100) odnosno tzv. „algoritmičkih predrasuda softvera“ ili „predrasuda automatizacije“.

Predstavićemo ukratko jedno istraživanje iz SAD koje se ticalo analize pristrasnosti veštačke inteligencije koja se bavila procenom stepena recidivizma osuđenih lica.[9] U svrhu istraživanja prikupljeni su podaci za 7.000 uhapšenih lica u okrugu Brauard, Florida za period 2013. i 2014. godinu. Cilj istraživanja je bio utvrđivanje u kojoj meri su procene softvera, baziranog na veštačkoj inteligenciji, koji je korišćen u cilju procene stepena recidivizma osuđenih lica, bile tačne. Prema rezultatima ovog istraživanja samo 20% ljudi za koje je softver procenio da će izvršiti krivično delo u skorijoj budućnosti je zaista to i učinilo. Kada su se u razmatranje uzeli i prekršaji, taj procenat je skočio na 50%. Istraživači zaključuju da je stepen tačnosti procene bio tek nešto bolji od stepena procene po principu pismo/glava. Pored toga, istraživači su utvrdili da su podaci koje

[8] O teorijskim razmatranjima u prilog isključenja automatizovanog odlučivanja u ovoj fazi (Sourdin, 2021: 251 – 252).

[9] Istraživanje je sprovela neprofitna organizacija koja se bavi istraživačkim novinarstvom u javnom interesu *Pro Publica* i istraživači Julia Angwin, Jeff Larson, Surya Mattu i Lauren Kirchner u maju 2016. godine. Istraživanje je objavljeno na sajtu ProPublica.

softver prikuplja netransparentni, kao i to da postoji prenošenje društvenih predrasuda, predubeđenja i stigmi sa društva na veštačku inteligenciju.[10]

Funkcija tzv „prediktivnog alata" HART („*Harm Assessment Risk Tool*"), koji se još uvek testira u Velikoj Britaniji i u eksperimentalnoj je fazi, te isključivo ima savetodavnu ulogu, je procena stepena rizika (nizak, srednji, visok) od ponovnog izvršenja krivičnog dela na osnovu tridesetak faktora od kojih pojedini nisu u vezi sa učinjenim krivičnim delom.

Korišćenje algoritma u postupku odlučivanja o uslovnom otpustu bazira se na preporuci ocene rizika od recidivizma osuđenog. Instrumenti mogu da mere osim trenutnih životnih uslova i ponašanja osuđenog i varijable koje su van njegove direktne kontrole, kao što je osuđivanost njegovih roditelja (Peeters, Schuilenburg, 2018: 272).

1.2. Predrasude veštačke inteligencije

Veštačka inteligencija je, po svojoj prirodi, sklona predrasudama. Problem predrasuda veštačke inteligencije je višeslojno analiziran u literaturi (tzv. „*AI bias*"). Funkcioniše po principima mašinskog učenja tako što mašine uče iz skupa podataka koji im je dat. Podaci o „stvarnom svetu" iz kojih mašine „uče", ne predstavljaju ništa drugo već sam „stvarni svet". Dakle, ukoliko postoji činjenica da se pripadnici određene rase A u zvaničnim evidencijama češće pojavljuju kao izvršioci krivičnih dela u odnosu na pripadnike druge rase B, mašine će u procesu učenja da dođu do zaključka da postoji veća verovatnoća da će pripadnik rase A izvršiti krivično delo nego pripadnik rase B. Zašto do ovoga dolazi? Naime, činjenica je da nejednakosti u društvu postoje. Pravni mehanizmi zaštite jednakosti u društvu postoje upravo zato što postoji nejednakost u društvu. Dakle, mašine samo uče iz onoga što „vide" u podacima. Mašine „vide" nejednakost i tu nejednakost „uče" kao zakonitost. Algoritmi mašinskog učenja nisu svesni, stoga nisu u stanju da se prilagode institucionalnim pristrasnostima ugrađenim u policijske podatke, a prisustvo pristrasnosti u početnom (trening) skupu podataka dovodi do predviđanja koja su podložna istim predrasudama koja već postoje u okviru skupa podataka (Isaac, 2018: 546). Veštačka inteligencija je dobra u predviđanju u onoj meri u kojoj su dobri podaci na osnovu kojih uči. Jednom kada veštačka inteligencija nauči diskriminatornu zakonitost iz podataka koji su joj dati, tada pristrasnost postaje njen stalni problem (Siau i Wang, 2020: 79).

1.2.1. Vrste pristrasnosti veštačke inteligencije

Pristrasnost veštačke inteligencije u teoriji je klasifikovana u pet kategorija (Chou i dr. 2017). Svih pet kategorija su od značaja za upotrebu veštačke inteligencije u krivičnom pravu.

Prva kategorija je *pristrasnost zasnovana na skupu podataka*. Ova pristrasnost nastaje kada se koristi limitiran skup podataka za mašinsko učenje, odnosno kada skup

[10] Kompanija „Northpointe", koja je kreirala navedeni softver, dala je odgovor na odov istraživanje navodeći da se ne slaže sa rezultatima analize, niti tvrdnjama iznetim na osnovu analize. Primedbe je moguće videti na sajtu ProPublica.

podataka iz kojih mašina uči ne predstavlja raznolikost stvarnog sveta o kome veštačka inteligencija zaključuje. „Hranjenje" veštačke inteligencije limitiranim skupom podataka zasigurno vodi ka predrasudama, tako što će veštačka inteligencija favorizovati samo one podatke koji su joj poznati, odnosno one kojima je naučena, a ignorisaće one podatke kojima nije naučena.

Druga kategorija je *pristrasnost udruživanja*. Ova pristrasnost suštinski predstavlja tendenciju veštačke inteligencije ka preslikavanju kulturoloških obrazaca jednog društva koje sadrže elemente predrasuda, kao na primer rodnih ili rasnih predrasuda.

Treća kategorija je *pristrasnost automatizacije* koja se ogleda u tome što veštačka inteligencija ima tendenciju generalizovanja i automatizovanja u odlučivanju zanemarujući ljudsku individualnost, želje, volju i slobodu u odlučivanju.

Četvrta kategorija je *pristrasnost interakcije*. Ova kategorija pristrasnosti nastaje kada je veštačkoj inteligenciji omogućeno da uči iz podataka koje sama pribavlja, a da prethodno algoritam nije isključio mogućnost učenja iz štetnih ili pogubnih uverenja. Ova kategorija potvrđuje pravilo da i za veštačku inteligenciju važi „S kim si, takav si". Dobar primer navedenog je četbot Tai, kompanije „Microsoft", koji je na Tviteru bio podučavan raznim uvredama i stereotipima, pa je nakon 24 sata „života na mreži" morao biti ugašen zbog psovki, rasističkih i zapaljivih političkih izjava (Wakefield**,** 2016).

Peta kategorija je *pristrasnost potvrde*. Do ove kategorije pristrasnosti dolazi u situaciji kada su informacije kojima se veštačka inteligencija „hrani" previše pojednostavljene. U tom slučaju veštačka inteligencija će rađe da pribegne rešenju koje odgovara pojednostavljenoj slici, pre nego što će da uzme u razmatranje one elemente koji nisu u punoj saglasnosti sa tako pojednostavljenom slikom. Odnosno, od veštačke inteligencije se ne može očekivati da ima „sluha" za alternativna rešenja ili ideje, kao ni za razne oblike ljudske kreativnosti koji izlaze iz okvira zadatog.

Postavlja se pitanje kako je moguće rešiti problem pristrasnosti veštačke inteligencije? Konačni cilj je stvaranje mašinske etike koja podrazumeva da će mašine jednog dana biti sposobne da samostalno slede idealan etički princip ili skup principa, odnosno da se, prilikom odlučivanja, samostalno rukovode etičkim principima i da u skladu sa njima preduzimaju moguće pravce delovanja (M. Anderson, S. L. Anderson, 2007: 15). Ovaj cilj više nije samo odraz pukog maštanja o budućnosti, on se ostvaruje kroz kreiranje algoritamskog etičkog kodeksa (više o tome Béranger, 2021a) koji treba da kreira društveno odgovornu veštačku inteligenciju[11]. On se ostvaruje kroz identifikaciju razloga zbog kojih je veštačka inteligencija pristrasna, potom klasifikaciju modela pristrasnosti i traganje za algoritamskim rešenjem koje bi za svaku kategoriju smanjilo, odnosno eliminisalo pristrasnost.

[11] Ideju „društveno odgovorne veštačke inteligencije" razradio je Béranger u svojoj knjizi *Societal Responsibility of Artificial Intelligence. Towards an Ethical and Eco-responsible AI* (vidi Béranger 2021b).

1.3. Pomoćna uloga veštačke inteligencije u postupku presuđenja i opasnosti automatski generisanih presuda

Upotreba veštačke inteligencije u postupku odlučivanja pravda se prevashodno razlozima bržeg rešavanja sporova, uštedama troškova kada su u pitanju jednostavniji predmeti, razlozima efikasnosti sudskog postupka i jednoobrazne primene prava. U teorijskom smislu, razlozi u prilog korišćenja AI u postupku odlučivanja su direktno pružanje pomoći sudijama u izradi nacrta sudskih odluka ili u procesu donošenja odluka, ili indirektna pomoć sudovima putem rasterećivanja od nepotrebnih sporova koji su „osuđeni na neuspeh" prema prognozama „prediktivnog softvera" u privatnom sektoru.[12] Veštačka inteligencija može da obezbedi relativno pojednostavljena sudska obrazloženja i standard evaluacije, da pruži sudiji sve slične predmete, zakone, propise i sudska tumačenja itd. (Cui, 2017). Međutim, temeljna opasnost uvođenja automatizovanih presuda u krivičnopravnoj materiji je da menjaju rad sudije za rad mašine i kreiraju neku potpuno različitu krivičnu "pravdu", jer nedostaje stručno rasuđivanje i odlučivanje.

U Kini, značajan broj sudova kupio je softver koji sudijama predlaže ishode predmeta ili kontroliše saglasnost sudskih odluka sa ranijim sudskim odlukama (Stern i dr., 2021: 539). Na kraju niza ideja razvoja veštačke inteligencije za potrebe pravosuđa su napredne aplikacije koje teže da pomognu u automatizaciji donošenja odluka. Upotreba veštačke inteligencije za automatsko generisanje presuda označava se izrazom tehnologije koje iskrivljuju/izobličavaju ili čak razaraju („*disruptive technologies*") postupak presuđenja, jer mogu da menjaju rad sudija i pružaju vrlo različite forme pravde, u kom slučaju se procesi znatno menjaju i mogu da preoblikuju ulogu sudije (Shi i dr., 2021: 1129).[13] Uloga veštačke inteligencije u postupku presuđenja u najmanjoj meri izobličava osnovna načela krivičnog postupka, pre svega načela slobodne ocene dokaza, slobodnog sudijskog uverenja i pravičnosti radi usklađivanja sudije sa algoritmom.

Postoje primeri testiranja donošenja automatizovanih presuda u prvostepenim postupcima u građanskopravnim sporovima, kada su u pitanju sporovi male vrednosti (projekat „robot sudija" u Estonija).[14] Prema mišljenju teoretičara, projekat potencijalno otvara vrata da se eksperimenti primene algoritama za donošenje odluka sprovedu uskoro i u krivičnoj materiji (Basile, 2019: 14). Najbolji primer da su prognoze na putu da se ostvare je i tzv. „Projekat 206" za sudove u Šangaju čija je uloga da standardizuje i pojednostavi

[12] Veštačka inteligencija kao instrument pružanja pomoći sudu može da bude i u funkciji prepoznavanja lica radi potvrde identiteta stranke, što je primenljivo pre svega u slučajevima *online* rasprava pred sudom.

[13] Tehnologija koja izobličava sudijsko odlučivanje je termin koji prema mišljenju autorki najviše odgovara opisu pojave da automatizacija u postupku odlučivanja u meri aktuelno dostignutog stepena upotrebe (pomoć sudiji tokom postupka odlučivanja), osim što izobličava odlučivanje po redovnom toku stvari, izobličava i ostvarivanje pojedinih osnovnih ustavnih prava i sloboda, naročito prava na odbranu. Izobličavanje, uz nedostatak neophodnih garancija za ostvarivanje suštine individualnih ljudskih prava, preti da ih razori. Osim toga, isključivo mašinsko odlučivanje razara ulogu sudije i suda.

[14] Projekat „robot sudija" u Estoniji osmišljen je radi rešavanja zaostalih sudijskih predmeta. „Robot sudija" dizajniran je da presuđuje u sporovima male vrednosti (vrednost predmeta spora manja od 7.000 evra), s tim što je predviđeno da o žalbi na presudu odlučuje čovek sudija.

prikupljanje dokaza, da unapredi doslednost u tretmanu sličnih slučajeva i poveća nadzor nad sudijama (Stern, 2021: 541). Projekat je inicijalno bio fokusiran upravo na krivične predmete. Sazvani su timovi stručnjaka da utvrde koji dokazi treba da se zahtevaju i kako da se postupa na taj način u 102 „rutinska" krivična predmeta (Stern, 2021: 541).

Osnovni argumenti u prilog upotrebe veštačke inteligencije u postupku odlučivanje su smanjivanje potencijalne sudske samovolje jačanjem kontrole nad radom sudija i omogućavanje sudiji da se striktno pridržava unapred određenih dokaznih pravila. Suštinski, uvođenje algoritama za proveru da li su dostavljeni svi prethodno zahtevani dokazi od policije i tužilaštva vodi upravo dezintegraciji načela slobodnog sudijskog uverenja i slobodne ocene dokaza i promovisanju formalne ocene dokaza u krivičnoj proceduri, elementa svojstvenog inkvizitorskom tipu krivičnog postupka. Sudija je vodeći se načelom slobodne ocene dokaza i svojim slobodnim uverenjem potpuno slobodan u izboru koje će se dokazne radnje preduzimati u konkretnom slučaju, te koji će se stepen dokaznog kredibiliteta pokloniti dokazima do kojih dođe na takav način (Škulić, 2021: 67).

S druge strane, ključni rizici generalne uloge AI u postupku odlučivanja su nerazumevanje odlučivanja, narušavanje sudske nepristrasnosti, rizici netransparentnosti odlučivanja algoritama, nepouzdanosti „pohranjenih podataka" i problem definisanja koji su subjekti odgovorni za donošenje odluke i kako je podeljena njihova odgovornost.[15] Načelno, pravni teoretičari ovakav proces donošenja odluka ne smatraju legitimnim i neautokratskim i dovode u pitanje ostvarivanje osnovnih prava i sloboda (Završnik, 2020: 568).

Uloga veštačke inteligencije da pruža potporu i pomoć[16] sudiji lako može prerasti u zamenu za sudiju. Lako je zamisliti da bi se sudije previše oslanjale na preporuke veštačke inteligencije i da bi nerado odstupale od njih, te korišćenje veštačke inteligencije u postupku odlučivanja dovodi u pitanje nepristrasnost suda, odnosno da li su te sudije efektivno „instrumentalizovane sudije" (Shi i dr., 2021: 17).

Teoretičari oštro kritikuju donošenje automatizovanih presuda formulišući pravo na neautomatizovano odlučivanje suda koje se temelji na povredi ljudskog dostojanstva presuđivanjem od strane mašine: „Mašina odlučuje na osnovu sadašnjih i prošlih digitalnih informacija, te se u suštini čovek svodi na skup podataka odnosno stvar" (Signorato, 2020: 14).

Prvi korak za algoritamski potpomognuto donošenje odluka je objavljivanje sudskih odluka te formiranje značajne baze presuda koja će se analizirati i pronaći najsličniji slučaj odnosno slučajevi, u vidu sličnih činjeničnih obrazaca, u prošlosti rada sudova. Projekat automatizovanih presuda temelji se na sistemu prethodne aktivnosti veštačke inteligencije, analiziranja velikog broja sudskih odluka odnosno obrade sudske prakse algoritmima i presuđenja na osnovu „trendova" sudske prakse koje pokazuje statistika,

[15] Postavlja se pitanje da li se mašine, umesto sudija, mogu nazvati „sudijama" (vidi Ji, 2018: 525).

[16] Pojedini autori ukazuju da u najboljem slučaju, „postoji mnogo mogućih prednosti spajanja tehnološke tačnosti i ljudske empatije: takve odluke mogle bi biti mnogo tačnije i zasnovane na dobroj analizi faktora za prognoziranje" (Plesničar, Šugman Stubbs, 2018: 166).

te se pravilno zaključuje da je prirodno korišćenje predvidive pravde u državama precedentnog prava (Toskić Cvetinović, 2021). Odsustvo ljudske kontrole ogleda se najpre u postupku biranja modela sudskih odluka od strane algoritama.

Veštačka inteligencija ima mogućnost samostalnog donošenja odluka, tj. u preduzimanju radnji veštačka inteligencija nije nužno zavisna od onoga ko ga je projektovao ili ko njome upravlja. Nije pogrešno zaključiti da veštačka inteligencija, u manjoj ili većoj meri, ima elemente ljudskog mišljenja. Međutim, postupak zaključivanja i donošenja odluka kod AI ima efekat crne kutije. Preciznije, faze procesa donošenja odluke sakrivene su od ljudskog nadzora zbog tehnološke složenosti procesa (Završnik, 2020: 568).

Širenja upotrebe algoritama za odlučivanje, otkrivanje predrasuda AI i pretnje funkcionisanja algoritama po osnovna procesna prava doveli su do usvajanja Evropske etičke povelje o korišćenju veštačke inteligencije u pravosudnim sistemima i njihovom okruženju u okviru Saveta Evrope[17], od strane Evropske komisije za efikasnost pravosuđa (CEPEJ). Temelji Povelje su pet osnovnih načela: 1. načelo poštovanja osnovnih prava; 2. načelo nediskriminacije; 3. načelo kvaliteta i sigurnosti; 4. načelo transparentnosti, nepristrasnosti i pravičnosti; 5. načelo garantovanja kontrole korisnika.[18]

Načelno, automatizovane presude odnosno zasnivanje odluke samo na automatskom procesu je zabranjeno, ali ipak postoji pravni osnov za njihovu izuzetnu upotrebu. Zahteva se ispunjenje određenih uslova: 1. *pravo Evropske unije dopušta* ili *pravo države članice* čije je kontrolor subjekt; 2. *propisivanje odgovarajućih zaštitnih garancija* za prava i slobode lica na koje se podaci odnose, a najmanje prava na ljudsku intervenciju kontrolora.[19]

U Evropi je uspostavljeno pravo na informacije o osnovnoj logici odluka donetih korišćenjem algoritama. Pravo na informacije odnosno objašnjenje algoritamskog odlučivanja obuhvata pravo na informaciju o donošenju automatizovanih odluka uključujući i profilisanje i u tim slučajevima minimum značajne informacije o korišćenoj logici, kao i o značaju i predviđenim posledicama takve obrade za subjekta podataka (High-Level

[17] *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment*, Adopted at the 31st plenary meeting of the CEPEJ, Strasbourg, 3 – 4 December 2018

[18] U SAD pronalazimo primere zakonodavnih aktivnosti u domenu nadzora nad radom automatizovanih sistema za odlučivanje koje koriste agencije, transparentnosti odnosno širenja informacija o ovim sistemima i odgovornosti za štetu pričinjenu ljudima od strane ovih sistema (The New York City Council, 2022).

[19] Videti osnovna pravila o donošenju automatizovanih pojedinačnih odluka u članu 11 Direktive Evropskog parlamenta i Saveta od 27. aprila 2016. godine o zaštiti fizičkih lica u pogledu obrade ličnih podataka od strane nadležnih organa za potrebe prevencije, istrage, otkrivanje ili gonjenja krivičnih dela ili izvršenja krivičnih sankcija i o slobodnom kretanju tih podataka i stavljanju van snage Okvirne odluke Saveta 2008/977/JHA (*Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*; članu 22 Uredbe Evropskog parlamenta i Saveta od 27. aprila 2016. godine o zaštiti fizičkih lica u pogledu obrade ličnih podataka i slobodnog kretanja takvih podataka i o stavljanju van snage Direktive 95/46/EZ (*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation*).

Expert Group on Artificial Intelligence, 2018). Složenost rada algoritama bez preispitivanja njegove naučne validnosti, praktično bi dovela do toga da stručnjaci za veštačku inteligenciju donose odluke. Pojedini autori smatraju da se podsticanje tačnosti i transparentnosti tehnika veštačke inteligencije može postići ako sudija imenuje veštaka da proveri algoritamski proces ili neuronsku mrežu AI, kad god stranke u postupku ističu sumnju u ispravnost automatizovanih podataka (Pagallo i Quattrocolo, 2018: 398).

Upotreba veštačke inteligencije u krivičnom pravosuđu nužno proširuje i modifikuje tumačenje osnovnih pravnih dokumenata o ljudskim pravima i slobodama. Okrivljenom se mora obezbediti pravo da delotvorno osporava rezultat rada algoritma na kojem se zasniva odluka koja se na njega odnosi. Trend realnog proširivanja upotrebe AI u fazama procesa sudskog odlučivanja, vodi zaključku da pravo na unakrsno ispitivanje svedoka garantovano Evropskom konvencijom o ljudskim pravima i osnovnim slobodama treba tumačiti tako da obuhvata i „pravo na ispitivanje podataka i osnovna pravila metodologije ocenjivanja rizika" (Završnik, 2020: 577).

2. VEŠTAČKA INTELIGENCIJA I KRIVIČNA ODGOVORNOST

Odgovor na pitanje da li postoji *machina sapiens criminalis* zahteva da se vratimo filozofsko – sociološkom razumevanju svrhe krivičnog prava, kao i da otvorimo naš um, pa i maštu za nove pravne institute i drugačije poimanje tradicionalnih krivičnopravnih pojmova i instituta. Krivično pravo, najjednostavnije rečeno, predstavlja oruđe socijalne kontrole. Svrha krivičnog prava je kontrola socijalnog ponašanja u skladu sa prihvatljivim društvenim normama. Prihvatljivost društvene norma, odnosno pitanje koje društvene vrednosti treba da štitimo, zavisi i od moralnih vrednosti jednog društva. Kako se društvo menja, tako se menjaju i vrednosti koje to društvo štiti. Tehnološke promene vode ka promenama socijalnog ponašanja, jer tehnologija nije prosti medijator, već upravo mehanizam koji oblikuje naše ponašanje (Milivojević i Radulski, 2020: 265). Algoritmi, pametni uređaji i mašine su upravljači tehnoloških, socijalnih, političkih, pa nesumnjivo i pravnih promena (Milivojević, 2021: 120).

Međutim, tehnologija i pravo su često na suprotnim stranama spektra. Dok tehnologija stremi ka evoluciji inovacija, pravo ima konzervativni pravac. Ono što tehnologija smatra progresom, pravo može smatrati regresom (Hallevy, 2013: 14). Da bi krivično pravo moglo adekvatno da odgovori na nove tehnološke izazove, treba biti spremno da prepozna veštačku inteligenciju kao neizostavan deo savremenog društva, da prevaziđe društvene predrasude i strahove od veštačke inteligencije, kao i da prepozna i prihvati moralnu koncepciju na kojoj počiva društvo u kojem vlada tehnologija veštačke inteligencije. Sledeći korak u reakciji krivičnog prava na rastuću tehnologiju veštačke inteligencije jeste rešavanje dileme - da li tradicionalne kategorije krivičnog prava mogu biti primenjive na AI, odnosno, da li je došlo do njihove krize ili uskrsnuća (Ligeti, 2019: 3).

Da li postoji *machina sapiens criminalis*, odnosno, da li veštačka inteligencija može da bude pravni subjekat odgovoran u krivičnom pravu? Nesporno je da se krivično pravo

primenjuje samo na ljude i da primena krivičnog prava u odnosu na veštačku inteligenciju ne može da bude pravolinijska (Ligeti, 2019: 2).

Prilikom utvrđivanja razlike između mašina (veštačke inteligencije) i ljudi uočavamo par razlika. Prva je činjenica da se mašine, za razliku od ljudi, ne mogu smatrati moralnim subjektom (Milivojević, 2021: 44). Dakle, veštačka inteligencija može da zna šta je zakonito, a šta nezakonito, ali veštačka inteligencija ne može da zna šta je dobro, a šta nije dobro, u smislu morala.

Drugo, ponašanje ljudi podrazumeva volju i slobodu odlučivanja. Otuda je krivica element krivičnog dela i preduslov kažnjavanja. Veštačka inteligencija takođe može da ima volju i slobodu odlučivanja, ali ta volja i sloboda nije originerno njihova, već proizilazi iz one volje i slobode koja im je data i zadata algoritmom.[20] Međutim, činjenica je da veštačka inteligencija ima mogućnost da volju i slobodu neprestano razvija učeći kroz neuralne mreže. Kognitivna nauka upravo počiva na pretpostavci da je priroda ljudske inteligencije računska i da se stoga ljudski um može modelirati kao računarski program (Solum 1992: 1231).

Očigledno je da pitanje krivične odgovornosti veštačke inteligencije počiva na konceptualnoj mogućnosti mašina da postanu što sličniji ljudima, tako da neprestani zahtev za *machina sapiens* predstavlja ujedno zahtev i za *machina sapiens criminalis*, odnosno, za krivičnom odgovornošću veštačke inteligencije (Hallevy, 2013: 18).

Krivično delo podarazumeva objektivne i subjektivne elemente dela – radnju izvršenja, predviđenost u zakonu, protivpravnost i krivicu. Ova podela postoji kako u teoriji, tako i u drugim pravim sistemima.[21] U anglosaksonskom pravu ovi elementi objektivne i subjektivne prirode su *actus reus* i *mens rea*. Da li veštačka inteligencija može da ispuni oba uslova za postojanje krivičnog dela? Nesporno je da radnju izvršenja može da preduzme veštačka inteligencija, problem nastaje kod subjektivnih elemenata, odnosno kod pojma krivice. Uzrok ovog problema je u činjenici što veštačka inteligencija „i jeste i nije" samostalan subjekat. Naime, veštačka inteligencija nesumnjivo poseduje brojne odlike ljudske inteligencije – komunikativnost, interno znanje, eksterno znanje, ponašanje usmereno ka cilju i kreativnost (Hallevey, 2016: 175 – 177). Međutim, kod pojma krivice nailazimo na problem. Naime, osnovano se možemo zapitati da li entitet koji nema savest i koji ne može da učestvuje u dijalogu o etičkim pitanjima, niti da odgovori na prekor (Gless i dr. prema Ligeti, 2019: 3) može da ima slobodu i volju neophodnu za postojanje krivice.

Takođe, postavlja se pitanje da li kod veštačke inteligencije postoji uzročna veza između volje i radnje i da li je moguće dokazati tu vezu? Naime, u situaciji kada je veštačka inteligencija projektovana da izvrši krivično delo, nesporno je da postoji lanac

[20] Moguće je prigovoriti da ni ljudska volja i sloboda nisu neograničene, već da zavise od zadatog moralnog sistema pojedinca, koji nije ništa drugo već zadati algoritam, ali bojimo se da bi nas ovaj prigovor odveo dalje od naše teme.

[21] U Sjedinjenim Američkim Državama načelo zakonitosti ima „veoma izražene diferencijalne specifičnosti u odnosu na uobičajeno shvatanje i dejstvo tog vrhunskog krivičnopravnog načela u kontinentalnoj Evropi", a kada je reč o opštem pojmu krivičnog dela, kao posebno izražen element načela zakonitosti ispoljava se „neophodnost da određeni akt bude *propisan* odnosno *pravom određen* kao krivično delo" (Škulić,2022: 34).

uzročnosti između proizvođača, programera, korisnika koji koriste veštačku inteligenciju kao sredstvo izvršenja krivičnog dela i samog krivičnog dela. Međutim, šta se dešava ukoliko veštačka inteligencija nije projektovana da izvrši radnju koja se karakteriše kao krivično delo, a ona to ipak uradi. Tada se postavlja pitanje da li je lanac uzročnosti od proizvođača do radnje izvršenja negde prekinut i da li je veštačka inteligencija sama i svojevoljno taj lanac prekinula, kao i zašto je to učinila (Ligeti, 2019: 5).

Rasprava o krivičnoj odgovornosti nema nikakvog smisla ukoliko ne analiziramo pitanje sankcije. Naime, čak i ukoliko prihvatimo da je krivična odgovornost primenjiva na veštačku inteligenciju, tj. ukoliko veštačkoj inteligenciji dodelimo pravni subjektivitet u krivičnom pravu, postavlja se pitanje da li su krivične sankcije, kakve znamo, primenjive na veštačku inteligenciju (Hallevy, 2013: preface XVI), da li veštačka inteligencija može da razume njihov smisao i da li iz njih nešto može da nauči? Čini se da bi sankcionisanje veštačke inteligencije moralo da ima sasvim nove obrise i da bi ono što znamo o krivičnim sankcijama za ljude bilo slabo primenjivo na veštačku inteligenciju. Nužno se moramo zapitati, čemu krivična odgovornost, ako krivična sankcija nema smisla?

Uprkos jačini argumenata o nemogućnosti zasnivanja krivične odgovornosti veštačke inteligencije, neslućene mogućnosti učenja mašina i razvoja veštačke inteligencije nužno nas dovode do zaključka da je došlo vreme da razmišljamo o krivičnoj odgovornosti veštačke inteligencije koja nije, ili nije isključivo, vezana za ljude (Milivojević, 2021: 44).

Krivična odgovornost pravnih lica pojavljuje se kao jedna od ideja koja se čini realnom po pitanju kreiranja modela krivične odgovornosti za dela izvršena od strane veštačke inteligencije. Tako, pravna lica podležu krivičnoj odgovornosti, uprkos činjenici što nisu ljudska bića. Takođe, nesporno je da pravna lica nisu moralni subjekti koji mogu da zasluže i razumeju sankciju (Solum, 1992: 1248). Po ugledu na krivičnu odgovornost pravnih lica, krivična odgovornost veštačke inteligencije bi podrazumevala sankcionisanje njenih vlasnika, ali odgovornost kod veštačke inteligencije bi svakako morala da ima širi obuhvat odgovornih lica koja bi, pored vlasnika, obuhvatila i kreatora softvera, proizvođača i korisnika. Stoga, krivična odgovornost pravnih lica može da predstavlja samo osnov za dalji razvoj krivične odgovornosti veštačke inteligencije (Ligeti, 2019: 2).

2.1. Teorijski modeli krivične odgovornosti veštačke inteligencije

Proces donošenja odluke kod veštačke inteligencije ima efekat crne kutije (Završnik, 2020: 567 – 583). Naime, faze procesa donošenja odluke skrivene su duboko u neuronskim mrežama veštačke inteligencije i zbog tehnološke složenosti procesa nisu jasno vidljive i razumljive. Ukoliko se ovo ima na umu, jasno je da ne možemo uvek jasno da razlučimo zbog čega je veštačka inteligencija izvršila neko krivično delo – da li zbog lošeg softvera ili zbog toga što ciljevi tog softvera nisu u saglasnosti sa vrednostima koje štiti krivično pravo (Milivojević, 2021:44). U teoriji su poznata tri modela krivične odgovornosti veštačke inteligencije (Hallevy, 2016: 174).

Prvi model odgovornosti je „izvršenje putem drugog". Postoji kada čovek vrši krivično delo putem veštačke inteligencije. Dakle, kada čovek projektuje softver ili mašinu za

izvršenje krivičnog dela. U ovom modelu, veštačka inteligencija je nevini objekat, a krivica u celosti leži na onome ko je softver, odnosno mašinu naručio, projektovao, napisao softver, trenirao njegove neuralne mreže, odnosno na onome ko ga je koristio (Hallevy, 2016: 179).

Drugi model odgovornosti je tzv. model „prirodne i verovatne posledice". Ovaj model se primenjuje u slučaju kada je veštačka inteligencija projektovana da izvrši jednu radnju, ali ona preduzme sasvim drugu radnju koja joj nije zadata algoritmom. Tako, na primer, robot je programiran da izvrši tešku krađu, ali ne i da ubije, ali on prilikom izvršenja krađe preduzme i radnju lišenja života čuvara. Nama poznata koncepcija nehata čini se nedovoljnom za nivo opasnosti od delovanja veštačke inteligencije. Kreator veštačke inteligencije, odnosno programer treba da bude odgovoran ne samo za izdatu naredbu sadržanu u algoritmu, već i za svaku onu posledicu koja može da se predvidi kao prirodna i verovatna posledica zadatog algoritma. Ovaj oblik odgovornosti u mnogome podseća na treću kategoriju udruženog zločinačkog poduhvata definisanog u praksi ICTY[22]. Naime, ova koncepcija otvara mogućnost šireg opsega odgovornosti i ona postoji za sve učesnike u zajedničkom zločinačkom poduhvatu čak i u situaciji kada jedan od učesnika izvrši krivično delo koje nije bilo predviđeno zajedničkim ciljem poduhvata, ukoliko je izvršeno krivično delo predstavljalo prirodnu i predvidljivu posledicu realizacije zajedničkog cilja.[23]

Treći model podrazumeva direktnu odgovornost veštačke inteligencije, polazeći od toga da ne postoji nikakva zavisnost veštačke inteligencije od programera ili korisnika. Ovaj model priznaje veštačkoj inteligenciji mogućnost postojanja subjektivnih elemenata dela, budući da polazi od ideje da zahvaljujući senzornoj recepciji, neuralnoj mreži i sposobnosti učenja, veštačka inteligencija ima mogućnost spoznaje. Ovaj model je kritikovan iz razloga što se mogućnost spoznaje smatra nedovoljnom za postojanje *mens rea*, a sve iz razloga što veštačka inteligencija nema mogućnost prihvatanja morala, odnosno moralne spoznaje (Ligeti, 2019: 3).

Poslednja dva predstavljena modela mogu delovati kao modeli za daleku budućnost, a treći model kao idealan za budućnost distopije. Veštačka inteligencija, bar za sada, još uvek nije došla do tačke kada svojom voljom može da postupa mimo zadatog algoritma, odnosno da sama svojevoljno prekida lanac uzročnosti između algoritma i radnje. Do trenutka kada se pojavi takva mogućnost, čini se dovoljnim model objektivne odgovornosti proizvođača, programera, korisnika (Ligeti, 2019: 4) za svaku radnju koju preduzme veštačka inteligencija. Model objektivne odgovornosti odgovara savremenoj bezbednosnoj i preventivnoj orijentaciji krivičnog prava koje nastoji da reaguje već na prve znake opasnosti, jer sve više opasnost, a manje krivično delo postaju osnov za krivičnopravnu reakciju (Stojanović, 2011: 5). Strah od veštačke inteligencije, kao i nerazumevanje šta sve veštačka inteligencija može i koliko je slična čoveku, poziva na visok stepen opreza i preveniranje koje se u krivičnom pravu najbolje ostvaruje kroz model objektivne odgovornosti.

[22] Udruženi zločinački poduhvat je definisan kao Joint Criminal Enterprise (JCE) u presudi Tadic 1999, *Prosecutor v. Dusko Tadic*, ICTY, No. 94-1-A, Judgment, 15 July 1999.

[23] Videti više o konceptu odgovornosti kod udruženog zločinačkog poduhvata (Nenadić, 2021: 309).

Međutim, postojanje čiste objektivne odgovornosti bi kod proizvođača, programera i korisnika stvorilo snažan osećaj strepnje za svaki kreirani proizvod, što bi moglo da vodi ka zastoju u tehnološkom razvoju. U tom smislu, potrebno je ispitati da li je ovaj model u celosti prihvatljiv, a to podrazumeva postizanje društvenog kompromisa u pogledu prihvatljivog rizika – koliki rizik od upotrebe veštačke inteligencije je prihvatljiv društvu zarad benefita koji veštačka inteligencija sa sobom nosi (Ligeti, 2019: 4). Tako, može se reći da je jedini razlog zbog kog usporava tehnološki razvoj autonomnih vozila, nerešeno pitanje rizika od upotrebe ovih vozila koje je društvo spremno da prihvati (European Committee on crime problems (CDPC), 2019: 3).

2.2. Krivična dela veštačke inteligencije i pitanje dokazivanja

Od značaja je da se osvrnemo i na pitanje koja krivična dela može da vrši veštačka inteligencija i kako će se ta krivična dela dokazivati? Veštačka inteligencija može da bude čist softver, ali može da bude i mašina, odnosno robot u koji je ugrađen softver. Dakle, veštačka inteligencija može da deluje, kako u svetu softvera i interneta stvari, tako i u našem fizičkom svetu. Veštačka inteligencija može da preduzima softverske radnje, ali može da preduzima i fizičke radnje. U tom smislu, veštačka inteligencija može da preduzima radnje izvršenja većine propisanih krivičnih dela. Ona to može da čini na način kako to čine ljudi, ali može i da iznađe druge načine izvršenja tih krivičnih dela. Pored tzv. „tradicionalnih krivičnih dela", veštačka inteligencija može da preduzima radnje koje još nisu prepoznate kao krivična dela, odnosno koje nisu prepoznate kao dovoljno društveno opasne da budu propisane kao krivično delo. Ovo su najčešće one radnje koje se odvijaju u softverskom svetu i daleko su od naših očiju, a čovek sam ih ne može preduzeti. Primer navedenog je maliciozna upotreba blok čejna, nezakonito delovanje u sferi kriptovaluta, kao i drugi oblici društveno neprihvatljivog ponašanja koje će biti kriminalizovano u budućnosti (Ligeti, 2019: 6).

Dokazivanje krivice je pravni teren gde ćemo biti svedoci brojnih promena, kako po pitanju dokazivanja krivice ljudi, tako i po pitanju dokazivanja krivice za krivična dela izvršena od strane veštačke inteligencije. Pravilno je primećeno da će se u budućnosti uviđaj vršiti u „internetu stvari"[24], jer ćemo informacije o krivičnom delu da dobijamo od mašina koje nas prate i nadgledaju. Sa druge strane, u odnosu na krivična dela izvršena od strane veštačke inteligencije, osnovni zadatak će biti utvrđivanje čija volja je dovela do krivičnog dela – ljudska ili „volja" veštačke inteligencije. Stoga, dokazivanje krivice će podrazumevati istraživanje kompjuterskih kodova radi utvrđivanja iz kog razloga je veštačka inteligencija prekršila pravo (Goodman prema Milivojević, 2021: 44).

Kako bismo objasnili aktuelnost i značaj pitanja pravne regulacije odgovornosti za krivična dela izvršena od strane veštačke inteligencije, ilustracije radi, daćemo dva aktuelna primera. Prvi se tiče upotrebe autonomnih oružanih sistema (AWS – „*autonomous*

[24] Ovo zapažanje o prikupjanju dokaza u budućnosti sa pametnih uređaja u kući, Marka Stokesa, šefa odeljenja za digitalnu, sajber i komunikacijsku forenziku policije Metropolitena, izraženo u jednoj rečenici, originalno glasi: "*The crime scene of tomorrow is going to be the internet of things*" *(Stokes prema IDG Connect, 2017).*

weapon systems") u ratovanju, odnosno kršenja pravila ratovanja. Svedoci smo neslućenih tehnoloških inovacija u proizvodnji naoružanja. Ova grana privrede je u velikoj meri opredeljena ka razvoju veštačke inteligencije iz razloga što postoji uverenje da se na taj način štede vojni resursi (ljudski, vremenski i tehnološki), a unapređuje preciznost delovanja. Upotreba ovog oružja je postala interesantna istraživačima međunarodnog prava oružanih sukoba. Naime, upotreba veštačke inteligencije u kontekstu ratovanja podrazumeva da veštačka inteligencija može sama da bira i opredeljuje metu i da deluje nezavisno od ljudi. Sa stanovišta krivičnog prava i međunarodnog humanitarnog prava mogu se postaviti dva pitanja o delovanju autonomnih oružanih sistema (Ligeti, 2019: 13 – 15). Prvi se tiče sposobnosti veštačke inteligencije da pravilno proceni legitimnost mete, kao na primer, da pravilno proceni da li se radi o legitimnoj meti ili o civilima. Drugi se tiče sposobnosti veštačke inteligencije da primenjuje silu shodno načelu proporcionalnosti kao osnovnom načelu ratovanja definisanog dodatnim protokolima Ženevskih konvencija. Nezavisno od toga što nemamo odgovor na ova dva važna pitanja, razvoj autonomnih oružanih sistema je nezaustavljiv i neminovno je da će u bliskoj budućnosti ovi sistemi da preuzmu primat u ratovanju u odnosu na tradicionalne forme delovanja u oružanim sukobima.

Sa pažnjom treba pratiti buduće pravne regulacije na terenu upotrebe ovog oružja u oružanim sukobima, jer će upravo one pokazati budući smer pravne regulacije krivične odgovornosti veštačke inteligencije u nacionalnim zakonodavstvima. Postoje dva razloga za navedeno. Prvi se tiče činjenice da je međunarodna zajednica zainteresovana za pravno uobličavanje ovog tipa odgovornosti, što će se neminovno preslikati na nacionalne pravne sisteme. Drugi razlog leži u činjenici da se pojedinci, korporacije, pa i države, osećaju mnogo lagodnije da veštačku inteligenciju upotrebljavaju intenzivno u periodu rata, pre nego u periodu mira, u uređenom pravnom sistemu.

Drugi primer se tiče saobraćajnih nesreća izazvanih od strane *self drivig* vozila. Upotreba *self drivig* vozila donedavno je bila u sferi mašte. Danas takva vozila postoje, ona su pred nama i uistinu sama voze. Razlog zašto ih nema više na ulicama nije tehnološke, već pravne prirode. Naime, još uvek nije rešeno pitanje odgovornosti za štetu koju ova vozila mogu da nanesu. Preciznije, ne postoji pravna regulacija za pitanje krivične odgovornosti u slučaju saobraćajne nesreće. Ili, ne zna se ko je odgovoran ako *self drivig* vozilo nekoga ubije. Oba primera jasno pokazuju da je pitanje krivične odgovornosti za radnje izvršenja preduzete od strane veštačke inteligencije jedno od najznačajnijih pitanja savremenog krivičnog prava. Odbijanje teorije krivičnog prava da se bavi ovim pitanjem šire neće dovesti do nestanka veštačke inteligencije, već do njenog razvoja mimo pravila krivičnog prava što sve vodi još većim problemima u sferi krivičnog prava.

ZAKLJUČAK

Razvoj veštačke inteligencije neizostavno menja ljude, njihova ponašanja i vizuru društva. Na promene neće biti imuno ni krivično materijalno i krivično procesno pravo. Zaključak proističe iz početaka pravnog i etičkog regulisanja kreiranja i korišćenja veštačke inteligencije i razmatranja o krivičnoj odgovornosti veštačke inteligencije.

Upotreba veštačke inteligencije pospešuje ideju krivičnog prava orijentisanog ka budućnosti. Algoritmi za prognoziranje analiziraju verovatnoću ostvarivanja budućih krivičnih dela u cilju pravovremene i adekvatne reakcije policije usmerene ka sprečavanju krivičnih dela, verovatnoću recidivizma i bekstva okrivljenog radi odlučivanja suda o njegovoj slobodi.

Upotreba veštačke inteligencije u krivičnom pravosuđu poseduje potencijal da promeni ulogu suda i doživljaj suda o vlastitoj ulozi, te da uzdrma njegovu garanciju nezavisnosti. Bez adekvatnog odgovora prava na razvoj veštačke inteligencije, umesto da veštačka inteligencija poveća poverenje građana u sud i suzbije moguće sudijske predrasude, jer su odluke suda potpomognute objektivnom naukom i tehnikom, realnije je očekivati potpuno suprotan efekat. Smanjiće se poverenje u sudske odluke, donete bez razumljivog i adekvatnog obrazloženja i produbiti moguće predrasude. Neophodno je u izvesnoj meri modifikovati tumačenje određenih krivičnoprocesnih načela i osnovna prava u krivičnom postupku u cilju održavanja njihove suštine odnosno sprečavanja da ih veštačka inteligencija razori u potpunosti. Veštačka inteligencija ne sme da preoblikuje svoju ulogu ograničene, praktično tehničke, pomoći sudijama u radu, u zamenu sudije u krivičnom postupku. Njena pravno i etički neuređena pomoćna uloga razara načelo slobodne ocene dokaza i slobodnog sudijskog uverenja.

Ako se algoritmi upotrebljavaju tokom krivičnog postupka, neophodno je da se u potpunosti garantuje poštovanje načela jednakost „oružja" i pretpostavka nevinosti, čije poštovanje podrazumeva činjenje dostupnim uskladištenih podataka, podataka o kreiranju i funkcionisanju algoritma, odnosno metodama analiza koje se primenjuju da bi se došlo do tehničkog rezultata. Zahtev načela jednakosti „oružja" je pravo na informisanje o logici donošenja odluka i pravo na preispitivanje naučne validnosti algoritma.

Neophodno je da „prediktivni alati" budu predmet nezavisne i temeljne recenzije da li postoji pristrasnost u podacima koje generiše sistem krivičnog pravosuđa, pre nego što se upotrebe radi donošenja odluka.

U pogledu radnji dokazivanja, prognoze su da će se uviđaj budućnosti prevashodno sprovoditi na „internetu stvari", te da će se istražne radnje preduzimati na kompjuterskim kodovima.

Savremeno krivično pravo preokupirano je budućnošću, a veštačka inteligencija ima potencijalno veliki opseg primene, naročito kada je u pitanju sprečavanje pojedinih krivičnih dela. Promene u sferi tradicionalnog krivičnog prava mogu da se očekuju u tri osnovna pravca: 1. veća orijentisanost ka prognoziranju budućeg ponašanja umesto kažnjavanju za učinjeno krivično delo; 2. uvođenje novih inkriminacija, kao što su određeni oblici zloupotreba i nezakonitog delovanja u sferi kriptovaluta i blok čejna; 3. regulisanje odgovornosti proizvođača, programera i korisnika za radnje koje preduzima veštačka inteligencija.

LITERATURA

1. Anderson, M., Anderson, S., L. (2007) „Machine Ethics: Creating an Ethical Intelligent Agent", *AI Magazine*, Vol. 28, No. 4, 15-26.
2. Asimov, I. (1950) *I Robot,* Doubleday.
3. Basile, F. (2019), "Intelligenza artificiale e diritto penale: quattro possibili percorsi di indagine", *Diritto Penale e Uomo*, 1–33.
4. Bennett Moses, L., Chan, J. (2018) „Algorithmic prediction in policing: assumptions, evaluation, and accountability", *Policing and Society An International Journal of Research and Policy,* Vol. 28, No. 7, Routledge, 806–822.
5. Béranger, J. (2021) *The Algorithmic Code of Ethics. Ethics at the Bedside of the Digital Revolution,* Wiley. DOI:10.1002/9781119508632.
6. Béranger, J. (2021) *Societal Responsibility of Artificial Intelligence. Towards an Ethical and Eco-responsible AI,* Wiley.
7. Dewan, S. (2015) „Judges Replacing Conjecture With Formula for Bail", *The New York Times,* dostupno na *https://www.nytimes.com/2015/06/27/us/turning-the-granting-of-bail-into-a-science.html,* [15.8.2022.].
8. Forrest, B., K. (2021) *When Machines Can be Judge, Jury and Executioner - Justice in the Age of Artificial Intelligence*. Singapore: World Scientific Publishing.
9. Freeman, K. (2016) „Algorithmic Injustice: How the Wisconsin Supreme Court Failed to Protect Due Process Rights in State v. Loomis", *North Carolina Journal of Law & Technology*, Vol. 18, No. 5, 75 – 106.
10. Hallevy, G. (2013) *When Robots Kill, AI under Criminal Law*. Boston: Northeastern University Press.
11. Hallevy, G. (2016) „The Criminal Liability of Artificial Intelligence Entities – from Science Fiction to Legal Social Control", *Akron Intelectual Property Journal*, Vol. 4, No. 2, 171–201.
12. Isaac, S., W. (2018) „Hope, Hype, and Fear: The Promise and Potential Pitfalls of Artificial Intelligence in Criminal Justice", *Ohio State Journal of Criminal Law*, Vol. 15, 543-558.
13. Ji, W. (2020) „The Change of Jurisdiction in the Era of Artificial Intelligence", *Asian Journal of Law and Society*, No. 7, 515-530.
14. Milivojević, S., Radulski, M. E. (2020), "Internet budućnosti i kriminalitet - ka kriminologiji Interneta stvari", *Crimen*, Vol. 11, br. 3, 255-271.
15. Milivojevic, S. (2021) *Crime and Punishment in the Future Internet*. Routledge Taylor & Francis Group.
16. Nenadić, M., S. (2021) *Pretpostavka nevinosti sa posebnim osvrtom na praksu Evropskog suda za ljudska prava*. Beograd: Službeni glasnik.
17. Pagallo, U., Quattrocolo, S. (2018) The impact of AI on criminal law, and its twofold procedures. u: Barfield, W., Pagallo, U. (ur.) *Research Handbook on the Law of Artificial Intelligence*. Cheltenham: Edward Elgar Publishing, 385–410.

18. Peeters, R., Schuilenburg, M (2018) "Machine justice: Governing security through the bureaucracy of Algorithms", *Information Polity*, Vol. 23, 267–280.
19. Plesničar, M., M., Šugman Stubbs, K. (2018) „Subjectivity, algorithms and the courtroom" In: Završnik, A. (ur.) *Big Data, Crime and Social Control*. London: Routledge, Taylor & Francis Group, 154–176.
20. Re, M., R., Solow-Niederman, A. (2019) „Developing Artificially Intelligent Justice", *Stanford Technology Law Review*, Vol. 22, No. 2, 2019, 242 -289.
21. Savet Evrope – Komesar za ljudska prava (2019) *Veštačka inteligencija: Deset koraka za zaštitu ljudskih prava – Preporuke*. Strazbur: Savet Evrope.
22. Siau, K., Wang, W. (2020) „Artificial Intelligence (AI) Ethics: Ethics of AI and Ethical AI", *Journal of Database Management*, Vol. 31, No. 2, 74-87.
23. Signorato, S. (2020) „A New Right in Criminal Procedure Implied by Human Dignity: The right to Non-Automated Judicial Decision-Making", *Journal of Eastern-European Criminal Law*, No. 2, 9-16
24. Solum, B., L. (1992) "Legal Personhood for Atrificial Intelligences", *North Carolina Law Review,*Vol. 70, No. 4, 1231 – 1287.
25. Sourdin, T. (2018) „Judge v Robot?, Artificial Intelligence and Judicial Decision-Making", *UNSW Law Journal,* Vol. 41, No. 4, 1114–113.
26. Sourdin, T. (2021) *Judges, Technology and Artificial Intelligence – The Artificial Judge*. Cheltenham: Edwars – Elgar Publishing.
27. Stern, R., E. i dr. (2021) "Automating Fomating Fairness? Artificial Intelligence in the Chinese Court", *Columbia Journal of Transnational Law*, Vol. 59, 516–553.
28. Stojanović, Z. (2011) „Preventivna funkcija krivičnog prava", *Crimen* (II), 1/2011, 3–25.
29. Završnik, A. (2020) „Criminal justice, artificial inteligence systems, and human rights", *ERA Forum*, 567-583.
30. Završnik, A. (2019) „Algorithmic justice: Algorithms and big data in criminal justice settings", *European Journal of Criminology,* Vol. 18 (5), 623–642.
31. Škulić, M. (2020) *Krivično procesno pravo*. Beograd: Univerzitet u Beogradu – Pravni fakultet.
32. Škulić, M. (2022) *Osnovi krivičnog prava Sjedinjenih Američkih Država*. Beograd: edicija Crimen, Univerzitet u Beogradu – Pravni fakultet.

Internet izvori

1. Chou, J., Murillo, O., Ibars, R. (2017) "What the Kids' Game „Telephone" Taught Microsoft About Biased AI", Fast Company, dostupno na: *https://www.fastcompany.com/90146078/what-the-kids-game-telephone-taught-microsoft-about-biased-ai*, [31.8.2022.].
2. Cui, Y. (2017) "Artificial Intelligence" Makes the Court System More Just, Efficient and Authoritative", *Standford Law School*, dostupno na: https://law.stanford.edu/china-law-and-policy-association-clpa/articles/, [13.8.2022.].

3. Eckhouse, L. (2017) „Big data may be reinforcing racial bias in the criminal justice system", *The Washington Post*, dostupno na: *https://www.washingtonpost.com/opinions/big-data-may-be-reinforcing-racial-bias-in-the-criminal-justice-system/2017/02/10/d63de518-ee3a-11e6-9973-c5efb7ccfb0d_story.html*, [18.8.2022.].
4. European Commission for the Efficiency of Justice (CEPEJ), *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment*, Adopted at the 31st plenary meeting of the CEPEJ, Strasbourg, 3 – 4 December 2018, Council of Europe, 2019, https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c [13.8.2022.].
5. European Committee on crime problems (CDPC), Working Group of Experts on Artificial Intelligence and Criminal Law, REPORT 1st meeting, Paris, 27 March 2019, dostupno na: *https://rm.coe.int/cdpc-2019-11-report-1st-meeting-working-group-on-artificial-intelligen/168093fbc9*, [4.9.2022.].
6. High-Level Expert Group on Artificial Intelligence (AI HLEG) in June 2018, *European Commission, Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions*, dostupno na: *https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai,* [1.9.2022.].
7. IDG Connect (2017), Opinion - "The crime scene of tomorrow is going to be the internet of things.", dostupno na: *https://www.idgconnect.com/article/3576737/quotes-of-the-week-the-crime-scene-of-tomorrow-will-be-the-internet-of-things.html*, [1.9.2022.].
8. Independent Digital Ethics, Ethics Advisory Report for West Midlands Police, dostupno na: *https://www.turing.ac.uk/sites/default/files/201811/turing_idepp_ethics_advisory_report_to_wmp.pdf*, [19.7.2019.].
9. Ligeti, K. (2019) „Artificial Intelligence and Criminal Justice", *AIDP-IAPL International Congress of Penal Law*, dostupno na: *https://www.penal.org/sites/default/files/Concept%20Paper_AI%20and%20Criminal%20Justice_Ligeti.pdf*, [20.8.2022.].
10. ProPublica's report on 'Machine bias', dostupno na: *https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing,* [25.8.2022.].
11. Report of Open Society Justice Initiative`s Criminal Justice Program (2014) *Presumption of guilt. The Global Overuse of Pretrial Detention.* New York: Open Society Foundations.
12. Shi, C., Sourdin, T., Li, B. (2021) „The Smart Court – A New Pathway to Justice in China?", *International Association for Court Administration,* Vol. 12, No. 1, dostupno na: https://www.iacajournal.org/articles/10.36745/ijca.367/, stranici [29.7.2022.] 1 – 19.
13. The New York City Council, „A Local Law in relation to automated decision systems used by agencies", dostupno na: *https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0,* [24.8.2022.].

14. Toskić Cvetinović, A. (2021) „Da li je srpskom pravosuđu potrebna veštačka inteligencija", *Vreme*, broj 1580, 2021, dostupno na: *https://www.vreme.com/vreme/da-li-je-srpskom-pravosudju-potrebna-vestacka-inteligencija/,* [15.8.2022.].
15. Wakefield, J. (2016), „Microsoft chatbot is taught to swear on Twitter", reporter BBC, dostupno na: *https://www.bbc.com/news/technology-35890188*, [31.8.2022.].
16. Wu, X., Zhang, X. (2016) „Automated Inference on Criminality using Face Images", 1–9, dostupno na: *https://arxiv.org/abs/1611.04135v1*, [16.8.2022.].

Pravni akti

1. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Sudska praksa

1. *Prosecutor v. Dusko Tadic*, ICTY, No. 94-1-A, Judgment, 15 July 1999

CRIMINAL JUSTICE IN THE ERA OF ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI), as an extension of the digital transformation of society, is becoming an integral part of criminal justice. The paper analyzes the use of AI in criminal law, as well as the risks that its use poses for criminal law. AI is not only a simple tool of criminal justice but also a path to the transformation of criminal law. The first part of the paper analyze the concept of AI and its influence in the world of the Internet of Things (IoT) in the way of detection of criminal acts, prevention and assessment of the degree of risk of recidivism. As AI is prone to prejudice (AI bias), algorithms of "predictive justice" software can have a discriminatory effect, which needs to be identified. It is essential that algorithms are subject to independent and thorough review of whether there is bias in the data generated by the criminal justice system. In the judicial systems of technologically developed countries, AI also acquires the function of helping the judge to perform the judicial work faster and more efficiently. The application of "machine learning" technology to automatically generate judgments for judges leads to numerous risks, especially highlighted in criminal cases. Questions are raised about the reshaping of the role of the judge, and the right to be informed about the logic of decision-making and to challenge the scientific validity of the algorithm, which is an element of the principle of equality of arms. AI has the character of autonomy, so the question inevitably arises whether there is criminal responsibility for artificial intelligence, to what extent and in what way, and whether it is necessary to create new forms of responsibility and new subjects of responsibility in criminal law? In the sphere of substantive criminal law, theoretical considerations point to the potential regulation of the responsibility of producers, developers and users for actions taken by the AI.

KEYWORDS: *criminal justice; artificial intelligence (AI); Internet of Things (IoT); AI bias; subjects of criminal liability*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.22

PRIMENA VEŠTAČKE INTELIGENCIJE U PRAVOSUĐU – PERSPEKTIVE I IZAZOVI –

Ana Toskić Cvetinović*
Milica Tošić**

U ovom radu autori nastoje da ukažu na mogućnosti i izazove primene veštačke inteligencije u pravosuđu, kako u svrhu podrške radu pravosuđa, tako i kao eventualnu zamenu za rad sudija, uvođenjem tzv. „sudija robota." U tom cilju, u prvom delu rada daju pojašnjenja osnovnih pojmova relevantnih za razumevanje mogućnosti primene veštačke inteligencije u pravosuđu, kao i pregled relevantnog međunarodnog pravnog okvira, pre svega u kontekstu Saveta Evrope i Evropske unije. Poseban osvrt daje se na Nacrt Uredbe Evropskog parlamenta i Saveta o utvrđivanju usklađenih pravila o veštačkoj inteligenciji (Akt o veštačkoj inteligenciji) i izmeni određenih pravnih akata unije. Takođe, u radu su predstavljena uporedna iskustva u primeni veštačke inteligencije u pravosuđu, kao i izazovi koji su prilikom njene primene do sada uočeni, pre svega u pogledu rizika po ljudska prava i slobode – pravo na zaštitu podataka o ličnosti, zaštitu od diskriminacije i pravo na pravično suđenje. U nastavku rada autori analiziraju relevantan pravni i strateški okvir Republike Srbije za uvođenje veštačke inteligencije, uključujući Zakon o zaštiti podataka o ličnosti, Strategiju razvoja veštačke inteligencije za period od 2020-2025, i prateći Akcioni plan za period 2020-2022. godine. Konačno, u radu se ukazuje na rizike specifične za Republiku Srbiju u pogledu primene veštačke inteligencije u pravosuđu, te daju preporuke za smanjenje ovih rizika, kako na regulatornom, tako i na praktičnom nivou.

KLJUČNE REČI: *nauka o podacima, veštačka inteligencija, upravljanje predmetima, zaštita podataka o ličnosti, automatsko donošenje odluka.*

* Master prava, izvršna direktorka organizacije Partneri za demokratske promene Srbija.
E-mail: *ana.toskic@partners-serbia.org*

** Istraživač u organizaciji Partneri za demokratske promene Srbija.
E-mail: *milica.tosic@partners-serbia.org*

UVOD

Sredinom 20. veka, američki pisac naučne fantastike Filip K. Dik u svojoj noveli Suvišni izveštaj (Dick, 1956), opisao je društvo u kome se čitav krivično-pravni sistem bazira na predikcijama različitih verzija budućnosti. Policija hapsi potencijalne „učinioce" krivičnih dela pre nego što su stigli da izvrše zločin, često i pre nego što su na njega i pomislili, a presude se izriču odmah, bez potrebe za suđenjem. Na taj način je stvoreno „savršeno" društvo u kom ne postoji kriminal, ali ni pravna sigurnost i pretpostavka nevinosti. Razvoj veštačke inteligencije (u daljem tekstu: „VI") omogućio je da danas tzv. predvidiva pravda postoji i izvan domena naučne fantastike. Razvijanje, testiranje, ali i upotreba ovih softvera je svakodnevnica u mnogim državama – u nekima kao rešenje za upravljanje predmetima, u nekima kao podrška za donošenje sudskih odluka, a negde (još uvek samo u uskom krugu predmeta) i kao zamena za sudiju.

Najave zvaničnika o mogućem uvođenju veštačke inteligencije u pravosuđe Republike Srbije sa jedne strane ne iznenađuje – Srbija je usvojila Strategiju razvoja veštačke inteligencije za period od 2020-2025. godine[1] u kojoj je jedna od predviđenih mera i unapređenje usluga javnog sektora primenom veštačke inteligencije. Kako se pravosuđe Srbije već decenijama bori sa velikim brojem predmeta i nedovoljnom efikasnošću (a uz to se često ističe i neujednačenost sudske prakse), upotreba VI može biti dodatni mehanizam za rešavanje ovih problema. Međutim, primena veštačke inteligencije sa sobom donosi i niz rizika, koji se u pravosuđu, imajući u vidu posledice sudskih postupaka po građane i njihova prava, dodatno ističu.

Stoga, ovaj rad ima za cilj da ispita perspektive i izazove primene veštačke inteligencije u pravosuđu, uopšte, sa fokusom na uslove za primenu VI u Republici Srbiji. Rad daje pregled razvoja koncepta predvidive pravde, međunarodnog pravnog okvira u ovoj oblasti, a predstavlja i pravni okvir Republike Srbije koji je relevantan za primenu veštačke inteligencije, i koji bi trebalo uzeti u obzir pri razvoju sistema VI. Konačno, u tekstu su predstavljeni i neki od rizika po ljudska prava koje donosi primena VI u pravosuđu, i dat je niz preporuka sa predlozima aktivnosti koje bi trebalo sprovesti prilikom razmatranja uvođenja veštačke inteligencije u pravosuđe naše zemlje.[2]

1. POJAM I METODE FUNKCIONISANJA PREDVIDIVE PRAVDE

Veza tehnologije i prava, kao i primena informacionih tehnologija u pravosuđu, nisu nastali u 21. veku. Još 1963. godine američki pravnik Li Levinger predložio je uvođenje nove naučne discipline pod nazivom „jurimetrika" (eng. „*jurimetrics*"), koja bi trebalo da se bavi pitanjima poput „kvantitativne analize ponašanja sudija, primene teorije komunikacije i informacija na pravno izražavanje, upotrebe matematičke logike u

[1] *Službeni glasnik RS,* broj 96/2019.

[2] Rad se ne bavi tehničkim aspektima uvođenja veštačke inteligencije, u smislu procene kapaciteta pravosuđa za uspostvljanje veštačke interligencije, a što može biti predmet posebne analize.

pravu, preuzimanja pravnih podataka elektronskim i mehaničkim sredstvima i formulisanja proračuna pravne predvidivosti"[3] (Myltseva, 2019: 1). Pojam predvidive pravde (eng. *Predictive Justice*) je novijeg datuma, s obzirom da je razvoj ovog koncepta zapravo podstaknut ubrzanim razvojem informacionih tehnologija krajem 20. i početkom 21. veka, pre svega razvojem računarskih metoda obrade velikog obima podataka.

Predvidiva pravda podrazumeva mogućnost predviđanja ishoda sudskog postupka ili neke njegove faze primenom matematičkih algoritama zasnovanih na obradi velikog obima dostupnih podataka, odnosno prethodnih odluka. Rezultati u vidu predviđanja ishoda dobijaju se kroz statističko modeliranje prethodnih odluka, i to primenom dva metoda računarskih nauka: obradom prirodnog jezika (eng: Natural Language Processing – NLP) i mašinskog učenja (eng: Machine Learning).[4] Radi se o metodama koje spadaju u pojam veštačke inteligencije (eng: Artificial Intelligence), koja u najširem smislu predstavlja disciplinu koja kombinuje računarske nauke i velike skupove podataka za potrebe rešavanja problema.[5]

Još uvek ne postoji jedinstvena definicija veštačke inteligencije. Prema jednoj od češće citiranih, koju je dao američki matemaričar Ričarda Belmana (Russel & Norvig, 1995: 2), veštačka inteligencija podrazumeva automatizovanje aktivnosti koje povezujemo sa ljudskim razmišljanjem, poput donošenja odluka, rešavanja problema, učenja.[6] Nešto novija definicija, na koju se poziva i Savet Evrope, navodi da je VI krovni termin koji se koristi da označi set nauka, teorija i tehnika posvećenih unapređenju sposobnosti mašina da obavljaju radnje koje traže inteligenciju. Sa druge strane, pojam sistema veštačke inteligencije podrazumeva „mašinski sistem koji izrađuje preporuke, predviđanja ili odluke za određeni set ciljeva, i to tako što: (a) koristi mašinsko i/ili ljudsko učešće da sagleda stvarna i/ili virtuelna okruženja; (b) takve percepcije pretvara u modele; i (v) iz tih modela izvodi ishode, bilo preko čoveka ili automatizovanim putem, u formi preporuka, predviđanja ili odluka."[7][8]

U kontekstu predvidive pravde, primena veštačke inteligencije podrazumeva unošenje u računarski program velikog obima podataka – zakona, podzakonskih akata, presuda, dokumentacije iz spisa velikog broja sudskih predmeta. Program potom analizira konkretan sudski postupak, tako što izdvaja ključne elemente, ali ga i povezuje sa različitim leksičkim grupama koje sačinjavaju sudske odluke, a koje se odnose na tzv. ulazne (činjenice i obrazloženje) i izlazne elemente (izreka odluke). Konkretan predmet povezuje se sa odlukama koje su donete u predmetima koji su imali iste ili slične materijalne i procesne karakteristike. Na taj način program „predviđa" ishod čitavog spora ili faze postupka, a pouzdanost modela zavisi od kvaliteta unetih podataka i izbora tehnike

[3] Tekst je dostupan na: https://journals.indexcopernicus.com/api/file/viewByFileId/924850.pdf, [28.08.2022.].

[4] European Commissioner for the Efficiency of Justice (CEPEJ), European Ethical Charter for the use of Artificial Intelligence in judicial systems and their environment, dostupno na: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c, 29, [28.08.2022.].

[5] https://www.ibm.com/cloud/learn/what-is-artificial-intelligence#toc-what-is-ar-DhYPPT4m, [5.12.2022.].

[6] Dostupno na: https://zoo.cs.yale.edu/classes/cs470/materials/aima2010.pdf, [28.08.2022.].

[7] Veštačka inteligencija: Deset koraka za zaštitu ljudskih prava, Savet Evrope, Komesar za ljudska prava, 5. Dostupno na: https://rm.coe.int/-/1680997222, [28.08.2022.].

[8] U nastavku teksta, pod pojmom veštačka inteligencija podrazumevaće se i sistemi veštačke inteligencije.

mašinskog učenja.[9] Međutim, za razliku od ranijih modela veštačke inteligencije (tzv. ekspertski modeli) koji su „kopirali" ljudski način razmišljanja i donošenja odluka, savremeni sistemi omogućavaju da računari sami identifikuju postojeće statističke modele u podacima i upare ih sa specifičnim rezultatima.

Upravo zbog te karakteristike, kao i činjenice da se ovi sistemi zasnivaju na obradi velikog broja podataka (tj. setova podataka), postoji rizik da sistem pogreši pri povezivanju tj. prepoznavanju sličnih slučajeva.[10] Uz to, neki od uzroka pogrešnih rezultata sistema veštačke inteligencije leže i u činjenici da se sistem zasniva na elementima verovatnoće, kao i da je kvalitet, odnosno tačnost i relevantnost podataka koji se koriste neretko upitna. Konačno, nerealna očekivanja od tehnologije mogu dovesti do situacije u kojoj se ona primenjuje u kontekstu u kome ne može da dovede do željenih rezultata.[11]

1.1. Pregled pravnog okvira relevantnog za primenu veštačke inteligencije u pravosuđu

Primena sistema mašinskog učenja i veštačke inteligencije u pravosuđu, odnosno predvidive pravde, novijeg je datuma,[12] pa je tako i pravni okvir koji uređuju ovu oblast, kako na nacionalnim tako i na međunarodnom nivou, još uvek u razvoju. To svakako ne znači da je primena ovih sistema u potpunosti van pravnog okvira, posebno u pogledu garancija prava učesnika postupaka u kojima se primenjuje mašinsko učenje ili veštačka inteligencija, dok međunarodne organizacije u fokus uglavnom stavljaju razvoj tzv. mekog prava u ovoj oblasti, u vidu etičkih smernica ili principa.

1.2. Međunarodni pravni okvir relevantan za primenu veštačke inteligencije u pravosuđu

U okviru Ujedinjenih nacija (u daljem tekstu "UN") još uvek nije došlo do usvajanja instrumenta koji bi uređivao primenu veštačke inteligencije, uopšte, pa ni i u kontekstu pravosuđa. Iako je verovatno da će UN usvojiti konvenciju o veštačkoj inteligenciji (Fournier-Tombs, 2021: 1)[13], dok se to ne desi relevantne su odredbe Univerzalne deklaracije o ljudskim pravima[14] i Međunarodnog pakta o građanskim i političkim pravima,[15]

[9] European Commission for the Efficiency of Justice (CEPEJ), European Ethical Charter for the use of Artificial Intelligence in judicial systems and their environment, 31. Dostupno na: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c, [28.08.2022.].

[10] *Ibid,* 35.

[11] The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights, 13. septembar, 2021, 5. Dostupno na: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf?OpenElement, [28.08.2022.].

[12]

[13] Dostupno na: https://journals.sagepub.com/doi/pdf/10.1177/20539517211039493, 1, [28.08.2022.].

[14] Univerzalna deklaracija o ljudskim pravima, Generalna skupština UN, 1948.

[15] Zakon o ratifikaciji Međunarodnog pakta o građanskim i političkim pravima, (*Službeni list SFRJ*, br. 7/71).

koje garantuju pravo na pravično suđenje,[16] pravo na delotvoran pravni lek,[17] pravo na zaštitu o diskriminacije,[18], kao i zaštitu od proizvoljnog mešanja u privatni život.[19] Poslednjih godina, tela UN-a adresirala su pitanja uticaja primene veštačke inteligencije kroz posebne tematske izveštaje. Tako se u Izveštaju Specijalnog izvestioca UN-a za slobodu mišljenja i izražavanja[20] ukazuje na rizike koje primena veštačke inteligencije donosi za slobodu mišljenja, slobodu izražavanja, pravo na privatnost, zaštitu od diskriminacije, pravo na delotvoran pravni lek. Takođe, poseban izveštaj Specijalnog izvestioca za prava osoba sa invaliditetom[21] bavi se pitanjima prava ove kategorije lica u kontekstu primene veštačke inteligencije, posebno ukazujući na moguću diskriminaciju ovih lica.[22] U Izveštaju Visokog komesara UN za ljudska prava o pravu na privatnost u digitalnom dobu,[23] posebno se ukazuje na rizike primene veštačke inteligencije u oblasti sprovođenja zakona (eng: *law enforcement*[24]), nacionalne bezbednosti, krivičnih postupaka i upravljanja granicama.[25] U Izveštaju se poziva da ova oblast bude među prvima koju bi trebalo regulisati, i to strožim pravilima za primenu veštačke inteligencije.[26]

U okviru Saveta Evrope poslednjih godina intenzivno se radi na razvoju "mekog" prava koje se odnosi na primenu VI, ali su za ovu oblast svakako relevantne i odredbe Evropske konvencije o ljudskim pravima (u daljem tekstu: „EKLJP")[27] kojima se garantuje pravo na pravično suđenje,[28] pravo na poštovanje privatnog i porodičnog života,[29] pravo na delotvorni pravni lek[30] i zabrana diskriminacije.[31]

---

[16] Član 10. Univerzalne deklaracije o ljudskim pravima i član 14. Međunarodnog pakta o građanskim i političkim pravima.

[17] Član 8. Univerzalne deklaracije o ljudskim pravima.

[18] Član 7. Univerzalne deklaracije o ljudskim pravima i član 26. Međunarodnog pakta o građanskim i političkim pravima.

[19] Član 12. Univerzalne deklaracije o ljudskim pravima i član 17. Međunarodnog pakta o građanskim i političkim pravima.

[20] Izveštaj Specijalnog izvestioca UN-a za slobodu mišljenja i izražavanja od 29. avgusta 2018

[21] Izveštaj Specijalnog izvestioca UN-a za prava lica sa invaliditetom, od 28. decembra 2021, dostupno na engleskom jeziku na: https://digitallibrary.un.org/record/3956054, [5.12.2022.].

[22] Videti: *Ibid*. 15-17.

[23] The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights, 13 September 2021, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf?OpenElement, [5.12.2022.].

[24] U terminologiji engleskog jezika, „law enforcement" označava policiju, sudove i ustanove za izvršenje sankcija.

[25] The right to privacy in the digital age, 6-8.

[26] *Ibid*. strana 11.

[27] Konvencija o zaštiti ljudskih prava i osnovnih sloboda, dostupno na: European Convention on Human Rights (coe.int), [5.12.2022.].

[28] *Ibid*. čl. 6.

[29] *Ibid*. čl. 8.

[30] *Ibid*. čl 13.

[31] *Ibid*. čl. 14.

Najznačajniji međunarodni instrument za oblast automatske obrade podataka je Konvencija o zaštiti lica u odnosu na automatsku obradu ličnih podataka sa Dodatnim Protokolima (u daljem tekstu: "Konvencija 108"),[32] koja je direktno uticala na razvoj niza nacionalnih zakona[33] u oblasti zaštite podataka o ličnosti, kao i na praksu Evropskog suda za ljudska prava. Konvencija 108 ima za cilj da obezbedi poštovanje prava i osnovnih sloboda, a posebno prava na privatnost, svakog lica na teritoriji svake od država ugovornica u pogledu automatske obrade ličnih podataka. Prema članu 2. Konvencije, automatska obrada, ako se sprovodi u celini ili delimično automatizovanim sredstvima, obuhvata: čuvanje podataka, izvođenje logičkih i/ili aritmetičkih operacija nad tim podacima, njihovu izmenu, brisanje, pronalaženje ili širenje. Delokrug Konvencije 108 obuhvata i obradu ličnih podataka u javnom i privatnom sektoru (član 3. (1)).

Imajući u vidu razvoj tehnologije, kao i pravnog okvira u Evropskoj uniji u oblasti zaštite podataka o ličnosti, 2018. godine Savet Evrope usvaja Modernizovanu konvenciju o zaštiti lica u odnosu na automatsku obradu ličnih podataka („Konvencija 108+").[34] U kontekstu primene veštačke inteligencije, Konvencija 108+ predviđa pravo lica da ne podležu odluci koja značajno utiče na njih, a koja je doneta samo na osnovu automatizovane obrade podataka bez uzimanja u obzir stavova lica na koja se podaci odnose (član 9, stav 1, tačka a), kao i pravo da na zahtev dobiju informacije o obrazloženju osnova obrade kada se rezultati takve obrade primenju na njih (član 9, stav 1, tačka c). Republika Srbija 2020. godine ratifikovala je i Konvenciju 108+.[35]

Evropska komisija za efikasnost pravosuđa (SEPEŽ – "CEPEJ") usvojila je u decembru 2018. godine Evropsku etičku povelju o korišćenju veštačke inteligencije u pravosuđu (u daljem tekstu: "Evropska etička povelja"), u kojoj je formulisano pet osnovnih načela za subjekte iz javnog i privatnog sektora koji razvijaju i primenjuju alate zasnovane na veštačkoj inteligencije, a koji uključuju obradu sudskih odluka i podataka. Takođe, načela Evropske etičke povelje odnose se i na donosioce odluka koji bi trebalo da rade na usvajanju regulatornog okvira za razvoj, upotrebu, ali i reviziju nad primenom alata i usluga veštačke inteligencije.[36] Tako, prema Evropskoj etičkoj povelji, primena veštačke inteligencije u pravosuđu treba da se zasniva na sledećim načelima:

- Načelo poštovanja ljudskih prava podrazumeva da razvoj i primena veštačke inteligencije moraju biti u skladu sa osnovnim ljudskim pravima, garantovanih EKLJP i Konvencijom 108+. Ukoliko se ovi sistemi koriste kao podrška u sudijskom

[32] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, 1981, https://rm.coe.int/1680078b37, [5.12.2022.].

[33] Republika Srbija ratifikovala je Konvenciju 2006. godine, što je za rezultat imalo i usvajanje Zakona o zaštiti podataka o ličnosti 2008. godine. Zakoni o potvrđivanju Konvencije i Dodatnih protokola dostupni su na stranici: https://www.poverenik.rs/sr/међународни-документи6/савет-европе.html, [5.12.2022.].

[34] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Savet Evrope, 2018, https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf, [5.12.2022.].

[35]

[36] Evropska etička povelja, 5.

odlučivanju ili za potrebe davanja smernica javnosti, ne smeju se podrivati garancije prava na pristup sudiji i prava na pravično suđenje. Konačno, treba dati prednost pristupu "etika po dizajnu" ili "ljudska prava po dizajnu", koji podrazumevaju da se pri samom dizajniranju (razvoju) sistema moraju integrisati pravila o zabrani direktne ili posredne povrede vrednosti zaštićenih konvencijama.[37]

- Načelo nediskriminacije podrazumeva da primena sistema VI ne sme razvijati ili uvećavati već postojeću diskriminaciju među pojedincima ili grupama pojedinaca. Sa druge strane, ohrabruje se primena algoritama za suzbijanje ovakve diskriminacije.[38]
- Načelo kvaliteta i bezbednosti podrazumeva da se prilikom obrade sudskih odluka i podataka u njima, moraju koristiti sertifikovani (sigurni) izvori podataka, kao i da podaci treba da budu zaštićeni. Takođe, razvoj sistema VI u pravosuđu treba da se zasniva na multi-disciplinarnom pristupu, sa timovima koji, pored stručnjaka za razvoj sistema VI, okupljaju stručnjake iz različitih naučnih disciplina i profesija Podaci koji se unose u sistem moraju biti u integralnom obliku i ne smeju se modifikovati, a modeli i algoritmi se moraju pohranjivati i primenjivati u bezbednom okruženju.[39]
- Načelo transparentnosti, nepristrasnosti i pravičnosti podrazumeva da metodi obrade podataka treba da budu pristupačni i razumljivi, kao i da treba omogućiti njihovu eksternu reviziju. Ovo načelo uzima u obzir zaštitu intelektualne svojine nad sistemima VI, tj metodama obrade podataka, ali ukazuje da je neophodno pronaći balans između potrebe za zaštitom ovog prava i zahteva za transparentnošću sistema, njegove nepristrasnosti, pravičnosti i intelektualnog integriteta (koji se ogleda u tome da se u prvi plan stavljaju interesi pravde). Jedan od načina da se ovo postigne jeste potpuna tehnička transparentnost sistema (na primer, kroz tzv "open source code" i dokumentaciju koji su dostupni svima). Druga opcija je pojašnjavanje sistema na razumljiv i prijemčiv način. Konačno, potrebno je uvesti sistem sertifikacije i revizije metoda obrade podataka.[40]
- Načelo "pod kontrolom korisnika" podrazumeva da su korisnici sistema adekvatno informisani i da imaju kontrolu nad izborima koje prave. To znači da primena sistema VI u pravosuđu treba da doprinese povećanju integriteta korisnika, a ne njegovom smanjenju, kao i da zaposleni u pravosuđu u svakom momentu treba da imaju mogućnost da razmotre odluku donetu primenom VI, i da tom odlukom nisu nužno obavezani. Korisnici treba da budu informisani na jasan i razumljiv način o tome da li su rešenja koja daje VI obavezujuća, da li postoje i druge opcije, kao i o svojim pravima na pravni savet i na pristup sudu. Takođe, ukoliko bi u nekoj prethodnoj fazi postupka za obradu konkretnog predmeta bila korišćena VI, lice o tome mora biti obavešteno i mora mu se dati mogućnost da praktikuje svoje

[37] *Ibid.* 8.

[38] Evropska etička povelja, 9.

[39] *Ibid,* 10.

[40] *Ibid,* 11.

pravo na prigovor, kao i pravo na pristup sudu u smislu člana 6. EKLJP. Konačno, primenu sistema VI treba da prate i program edukacije u oblasti digitalne pismenosti, kao i debata u koju bi bili uključeni zaposleni u pravosuđu.[41]

Studija o primeni VI u pravosuđu, odnosno o primenama VI na obradu sudskih odluka i podataka, izrađenoj za potrebe Evropske etičke povelje, ukazuje i na potencijalne opasnosti različitih načina upotrebe VI, na osnovu čega ih svrstava u nekoliko kategorija. Tako, među onim oblastima u kojima treba podsticati razvoj i primenu VI su i unapređenje upravljanja predmetima i pristupa pravu (na primer, kroz razvoj tzv. čet botova), dok se za upotrebu VI u rešavanju sporova u *online* sferi, ili kao podrške alternativnom rešavanju pojedinih građanskih sporova, moraju preduzeti dodatne metodološke mere. Sa druge strane, za razmatranje upotrebe VI za potrebe profilisanja sudija, odnosno njihovog ponašanja tokom suđenja, ili za predviđanje sudskih odluka, potrebno je sačekati i uzeti u obzir dodatna naučna istraživanja. Upotrebu VI u slučajevima poput profilisanja pojedinaca u krivičnim stvarima, treba uzeti sa najvećom mogućom rezervom.[42]

Savet Evrope je u martu 2018. godine objavio i Studiju o dimenzijama ljudskih prava u tehnikama obrade podataka i mogućim regulatornim implikacijama[43] u kojoj ističu da javne institucije moraju biti odgovorne za odluke koje donose na osnovu algoritamskih procesa, kao i da razvoj ovih tehnologija mora biti pod konstantnim nadzorom kako bi se sprečili negativni uticaji. Svi propisi koji regulišu ovakve algoritme moraju biti u saglasnosti sa međunarodnim standardima iz oblasti ljudskih prava.

U januaru 2019. godine, Savet Evrope je objavio Smernice o veštačkoj inteligenciji i zaštiti podataka o ličnosti[44], sa ciljem da se usmere tvorci sistema VI i pružaoci ovih usluga da prilikom implementacije novih tehnologija ne ugroze pravo na privatnost građana. Smernice nastoje da obezbede zaštitu personalne autonomije zasnovane na pravu građana da imaju kontrolu nad dostupnosti i obradom svojih ličnih podataka.

Mesec dana kasnije, Savet Evrope je objavio još jedan dokument koji je izradio Komitet Ministara – Deklaraciju o manipulativnim mogućnostima algoritamskih procesa,[45] u kome je upozoreno na rizik od koriščenja algoritamskih procesa u svrhe

[41] *Ibid*, 12.

[42] *Ibid*, 63-67.

[43] Originalan naziv dokumenta: Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, Council of Europe Study, DGI(2017)12. Dostupno na: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5, [5.12.2022.].

[44] Originalan naziv dokumenta: New Guidelines on Artificial Intelligence and Data Protection, Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of Personal Data, https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8, [5.12.2022.].

[45] Originalan naziv dokumenta: Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, Decl(13/02/2019), Council of Europe, Committee of Ministers, 13 February 2019. Dostupno na: https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b [5.12.2022.].

manipulisanja socijalnog i političkog ponašanja građana. Komitet ministara ovim dokumentom apeluje na države članice da razmotre potrebu za kreiranjem dodatne zakonske regulative koja štiti podatke građana od potencijalnih zloupotreba nastalih korišćenjem naprednih tehnologija.

Evropska unija ostvarila je veliki napredak u pogledu razvoja pravnog okvira u oblasti veštačke inteligencije, iako je i on dalje u procesu razvoja. Među važećim propisima svakako je najznačajnija Opšta uredba o zaštiti podataka EU (engl. General Data Protection Regulation – GDPR, u daljem tekstu „Uredba"),[46] koja je, uz tzv. Policijsku direktivu, [47] poslužila i kao uzor za usvajanje novog Zakona o zaštiti podataka o ličnosti Republike Srbije (iz kog razloga će u nastavku biti predstavljene njene odredbe od značaja za primenu VI). Uredba vrši unifikaciju prava i neposredno se primenjuje u državama članicama EU, a relevantan je izvor prava kako za automatsku, tako i za neautomatsku obradu podataka. Uredba, između ostalog propisuje načela obrade podataka o ličnosti, prava lica na koja se podaci odnose, pravila međunarodnog transfera podataka, ali ne i posebna pravila koja se odnose na zaštitu podataka o ličnosti primenom VI. Međutim, u članu 4. Uredba daje definicije nekih pojmova koji su relevantni za ovu oblast.

Tako, prema Uredbi, obrada podataka je svaka radnja ili skup radnji koje se vrše automatizovano ili neautomatizovano sa podacima o ličnosti ili njihovim skupovima, kao što su prikupljanje, beleženje, razvrstavanje, grupisanje, odnosno strukturiranje, pohranjivanje, prilagođavanje ili menjanje, otkrivanje, uvid, upotreba, obelodanjivanje prenosom, odnosno dostavljanjem, umnožavanjem, širenjem ili činjenjem dostupnim na drugi način, uređenje, ograničavanje, brisanje ili uništavanje. Dakle, svaki vid korišćenja, čuvanja podataka ili manipulisanja podacima smatra se obradom, čak i u slučajevima kada se podaci ne koriste „aktivno", već su jednostavno pohranjeni na određenoj lokaciji (Toskić, Stojanović, Kerić & Jang, 2020: 27). [48]

Profilisanje podrazumeva obradu podataka o ličnosti koju karakteriše sledeće: 1) da se radi o automatizovanom obliku obrade podataka; 2) da se izvodi nad podacima o ličnosti; 3) da za ishod ima procenu određenih aspekata fizičkog lica kako bi se predvidelo njegovo ponašanje i donela određena odluka u vezi sa tim. Primena VI neretko podrazumeva i profilisanje.[49]

Uredba predviđa obavezu rukovaoca da primeni određene tehničke i organizacione mere za potrebe poslovnog sprovođenja načela zaštite podataka. Ovaj koncept zapravo podrazumeva da je rukovalac dužan da inkorporira zaštitu podataka u svoje radnje

[46] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[47] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[48] Dostupno na: http://www.skgo.org/publications/download/495, [5.12.2022.].

[49] *Ibid*, 27.

obrade i poslovne procese, od njihovog dizajna do realizacije. Ta se obaveza primenjuje u odnosu na broj prikupljenih podataka, obim njihove obrade, rok njihovog pohranjivanja i njihovu dostupnost.[50]

U skladu sa načelima integrisane i pretpostavljene privatnosti, Uredba predviđa novu obavezu rukovaoca, a to je da, pre započinjanja nove obrade podataka, izvrši procenu uticaja te radnje obrade na zaštitu podataka o ličnosti. Prema članu 35. Uredbe, ova obaveza postoji ukoliko je verovatno da će neka vrsta obrade, posebno upotrebom novih tehnologija i s obzirom na prirodu, obim, okolnosti i svrhu obrade, prouzrokovati visok rizik za prava i slobode fizičkih lica.[51]

Kako bi se podstakao razvoj sistema VI, uz adresiranje rizika koje primena VI podrazumeva, na nivou EU započet je rad na propisu koji bi trebalo da unifikuje pravo država članica u ovoj oblasti. U aprilu 2021. objavljen je nacrt Uredbe Evropskog parlamenta i Saveta o utvrđivanju usklađenih pravila o veštačkoj inteligenciji (Akt o veštačkoj inteligenciji) i izmeni određenih pravnih akata unije,[52] a konsultacije o konačnoj verziji ovog dokumenta još uvek traju. Akt o veštačkoj inteligenciji ima za cilj da pruži onima koji razvijaju, implementiraju i koriste VI jasne zahteve i obaveze u vezi sa specifičnom upotrebom VI. Istovremeno, predlog nastoji da smanji administrativna i finansijska opterećenja za preduzeća, posebno za mala i srednja preduzeća.

Akt bi trebalo da uspostavi pristup zasnovan na proceni rizika, pa tako Nacrt daje listu onih sistema za koje je procenjeno da nose neprihvatljive rizike, i njihova upotreba je zabranjena. U najširem smislu, u ove sisteme spadaju:

- Sistemi VI koji primenjuju podsvesne tehnike izvan čovekove svesti kako bi materijalno izobličio ponašanje osobe na način koji uzrokuje ili bi mogao da izazove fizičku ili psihičku povredu te ili druge osobe (na primer, igračke sa govorom/glasovima koji podstiču na nasilno ponašanje);
- Sistem VI koji iskorišćava bilo koju od ranjivosti određene grupe osoba zbog njihovog uzrasta, fizičkog ili mentalnog invaliditeta, kako bi narušio ponašanje osobe u na način koji uzrokuje ili može da izazove fizičku ili psihičku štetu toj osobi ili drugoj osobi;
- Sistemi VI koji vrše tzv društveno bodovanje/ocenjivanje od strane javne vlasti
- Sistemi VI za daljinsku biometrijsku identifikaciju lica u javno dostupnim prostorima, u realnom vremenu za svrhe sprovođenja zakona, uz određene izuzetke.

Sa druge strane, Nacrt prepoznaje i one sisteme koji imaju potencijalno veći uticaj na prava pojedinaca, ali u meri u kojoj ih nije nužno zabraniti, već se njihovim proizvo-

[50] *Ibid,* 35-36.

[51] *Ibid,* 39.

[52] European Comission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and Amending certain Union Legislative acts, Brussels, 21.4.2021, COM(2021)206 final, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF, [5.12.2022.].

đačima i korisnicima propisuju posebne obaveze. U takve sisteme svrstavaju se, između ostalog i:

- sistemi VI koji su namenjeni da ih koriste organi za sprovođenje zakona za izradu pojedinačnih procena rizika fizičkog lica od krivičnog dela ili ponavljanja dela ili rizika po potencijalne žrtve krivičnih dela;
- sistemi VI namenjene da ih organi za sprovođenje zakona koriste kao poligrafe i slična sredstva ili da otkriju emocionalno stanje fizičkog lica;
- sistemi VI koji su namenjeni da ih koriste organi za sprovođenje zakona za otkrivanje tzv. „deepfake" (lažiranje slike, snimka ili ponašanja stvarnog lica);
- sistemi VI koji su namenjeni da ih koriste organi za sprovođenje zakona za procenu pouzdanosti dokaza u toku istrage ili krivičnog gonjenja;
- sistemi VI koji su namenjeni da ih koriste organi za sprovođenje zakona za predviđanje pojave ili ponavljanja stvarnog ili potencijalnog krivičnog dela na osnovu profilisanja fizičkih lica ili ocenjivanje osobina i karakteristika ličnosti ili ranijeg kriminalnog ponašanja fizičkih lica ili grupa;
- sistemi VI koji su namenjeni da ih organi za sprovođenje zakona koriste za profilisanje fizičkih lica u toku otkrivanja, istrage ili krivičnog gonjenja krivičnih dela;
- sistemi Vi namenjeni da se koriste za analitiku kriminala u vezi sa fizičkim licima, omogućavajući organima za sprovođenje zakona da pretražuju složene povezane i nepovezane velike skupove podataka koji su dostupni u različitim izvorima podataka ili u različitim formatima podataka kako bi identifikovali nepoznate obrasce ili otkrili skrivene odnose u podacima.[53]

Takođe, u ovu kategoriju svrstavaju se i sistemi koji bi se koristili u pravosuđu, i to za potrebe podrške sudijama (tj drugom sudskom organu) u istraživanju i tumačenju činjenica i prava, i u primeni prava na konkretno činjenično stanje.[54]

Iako je još uvek rano govoriti o konačnoj sadržini Akta, njegove odredbe svakako će uticati na dalji razvoj pravnog okvira u oblasti veštačke inteligencije u Srbiji.

2. PRAVNI OKVIR REPUBLIKE SRBIJE RELEVANTAN ZA PRIMENU VEŠTAČKE INTELIGENCIJE U PRAVOSUĐU

Pravni sistem Republike Srbije još uvek nije dobio propis koji bi regulisao primenu veštačke inteligencije, uopšte, pa tako ni u sistemu pravosuđa. Međutim, u važećim propisima, ali i strateškim dokumentima, nalaze se odredbe koje se primenjuju na sisteme VI, odnosno koje bi trebalo uzeti u obzir i prilikom razmatranja uvođenja VI u pravosuđe.

To su, pre svega, odredbe Zakona o zaštiti podataka o ličnosti (u daljem tekstu: „ZZPL"),[55] koji uređuje sve aspekte prava na zaštitu fizičkih lica u vezi sa obradom po-

[53] Aneks III Nacrta Akta o veštačkoj inteligenciji, član 1.

[54] *Ibid*. član 2.

[55] *Službeni glasnik RS,* br. 87/2018.

dataka o ličnosti. Kao krovni zakon ove oblasti, primenjuje se i na sve situacije vezane za obradu podataka o ličnosti u pravosuđu, sa izuzetkom nadležnosti nezavisnog organa, Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti (u daljem tekstu: „Poverenik"), koja se ne odnosi na obradu podataka o ličnosti od strane sudova u vršenju njihovih sudskih ovlašćenja.

Takođe, kao što je već napomenuto, ZZPL usvojen je u skladu sa Opštom uredbom EU o zaštiti podataka i Policijskom direktivom, preuzimajući tako odredbe koje uređuju tzv. opšti i posebni režim obrade podataka. Poseban režim obrade podataka zapravo podrazumeva obradu podataka o ličnosti koju vrše nadležni organi u svrhe sprečavanja, istrage i otkrivanja krivičnih dela, gonjenja učinilaca krivičnih dela ili izvršenja krivičnih sankcija, uključujući sprečavanje i zaštitu od pretnji javnoj i nacionalnoj bezbednosti, kao i slobodni protok takvih podataka (član 1, stav 2). Međutim, kako je Policijska direktiva dokument koji harmonizuje pravo država članica EU, te je na njima da u skladu sa svojim pravnim sistemima preziciraju koji krug organa se smatra "nadležnim organima", naš zakonodavac propustio je da ovu odredbu precizira. Tako, nije jasno da li sudovi u krivičnim postupcima primenjuju opšti ili poseban režim obrade podataka, što je značajno za utvrđivanje prava lica, ali i obaveza rukovalaca podacima.

Zakon izričito uređuje koja se sve načela moraju poštovati prilikom obrade podataka o ličnosti[56] i za njihovo nepoštovanje propisuje i prekršajnu odgovornost. Obrada mora biti zakonita, poštena i transparentna. Podaci se moraju prikupljati u konkretno određene svrhe, koje su izričite, opravdane i zakonite. Podaci moraju biti primereni, bitni i ograničeni na ono što je neophodno u odnosu na svrhu obrade (minimizacija podataka), a bitno je i da budu tačni, i ako je to neophodno, ažurirani. Čuvanju podataka se mora pristupiti sa posebnim oprezom, a trajanje čuvanja mora biti ograničeno na rok koji je neophodan za ostvarivanje svrhe obrade. Podaci moraju biti zaštićeni od neovlašćene ili nezakonite obrade, kao i od slučajnog gubitka, uništenja ili oštećenja.

Zakon reguliše i automatizovano donošenje odluka i profilisanje i propisuje kao posebnu obavezu rukovalaca da informišu lica o postojanju automatizovanog donošenja odluka, uključujući profilisanje, i pruže informacije o logici koja se pri tome koristi, kao i o značaju i očekivanim posledicama te obrade na lice na koje se podaci odnose.[57]

ZZPL posebno izdvaja i obaveze rukovalaca prilikom obrade podataka koji se odnose na krivične presude, kažnjiva dela i mere bezbednosti (član 19), i propisuje da se obrada ovih podataka može vršiti samo pod nadzorom nadležnog organa ili, ako je obrada dopuštena zakonom, uz primenu odgovarajućih posebnih mera zaštite prava i sloboda lica na koje se podaci odnose.

Naročito značajan za potencijalno uvođenje VI u pravosuđe je član 38 stav 1, koji licu na koje se podaci odnose daje pravo da se na njega ne primenjuje odluka doneta isključivo na osnovu automatizovane obrade, odnosno profilisanja, ako se tom odlukom proizvode pravne posledice po to lice, ili ta odluka značajno utiče na njegov položaj. Zakon propisuje i da se navedeni član ne primenjuje ako je odluka zasnovana na

[56] Član 5.

[57] Član 23.

zakonu, ako su tim zakonom propisane odgovarajuće mere zaštite prava, sloboda i legitimnih interesa lica na koje se podaci odnose.[58] Dakle, od vrste i sadržine pravnog osnova koji uvodi veštačku inteligenciju u naše pravosuđe zavisiće i potencijalno pravo na izbor lica iz člana 38 stav 1 ZZPL.

Međutim, ukoliko obradu vrše tzv. nadležni organi u posebne svrhe, član 39 ZZPL zabranjuje donošenje odluke isključivo na osnovu automatizovane obrade, uključujući i profilisanje, ako takva odluka može da proizvede štetne pravne posledice po lice na koje se podaci odnose ili značajno utiče na položaj tog lica, osim ako je donošenje te odluke zasnovano na zakonu i ako su tim zakonom propisane odgovarajuće mere zaštite prava i sloboda lica na koje se podaci odnose, a najmanje pravo da se obezbedi učešće fizičkog lica pod kontrolom rukovaoca u donošenju odluke. To bi značilo da bi ovakve garancije trebalo obezbediti prilikom automatskog donošenja odluka u krivičnim postupcima.

Lice na koje se podaci odnose ima pravo da u svakom trenutku podnese rukovaocu prigovor[59] na obradu njegovih podataka o ličnosti, uključujući profilisanje. Rukovalac podacima je u tom slučaju dužan da prekine sa obradom, osim ako je predočio da postoje zakonski razlozi za obradu koji pretežu nad interesima, pravima ili slobodama lica na koje se podaci odnose. Rukovalac je dužan da prilikom uspostavljanja prve komunikacije sa licem na koje se podaci odnose informiše to lice o njegovom pravu na prigovor.

U kontekstu primene VI, posebno treba ukazati na član 54. ZZPL, koji propisuje obaveznu izradu procene uticaja radnji obrade na prava građana, ako je verovatno da će neka vrsta upotrebe, posebno upotrebom nove tehnologije, prozrokovati visok rizik za prava i slobode fizičkih lica,[60] (a za upotrebu sistema veštačke inteligencije je to izvesno). U stavu 6. člana 54. ZZPL određuje se i minimum sadržine procene uticaja koji obuhvata:

1. sveobuhvatan opis predviđenih radnji obrade i svrhu obrade, uključujući i opis legitimnog interesa rukovaoca, ako on postoji;
2. procenu neophodnosti i srazmernosti vršenja radnji obrade u odnosu na svrhe obrade;
3. procenu rizika za prava i slobode lica na koje se podaci odnose;
4. opis mera koje se nameravaju preduzeti u odnosu na postojanje rizika, uključujući mehanizme zaštite, kao i tehničke, organizacione i kadrovske mere u cilju zaštite podatka o ličnosti i obezbeđivanja dokaza o poštovanju odredbi ovog zakona, uzimajući u obzir prava i legitimne interese lica na koje se podaci odnose i drugih lica.

U pogledu radnji obrade podataka o ličnosti povodom kojih je obavezno izvršiti procenu uticaja, Zakon predviđa da su to:

1. sistematska i sveobuhvatna procena stanja i osobina fizičkog lica koja se vrši pomoću automatizovane obrade podataka o ličnosti, uključujući i profilisanje, na

[58] Član 38. stav 2, tačka 2.

[59] Član 37.

[60] Član 54. stav 1 i član 54. stav 4, tačke 1 i 2.

osnovu koje se donose odluke od značaja za pravni položaj pojedinca ili na sličan način značajno utiču na njega;
2. obrada posebnih vrsta podataka o ličnosti ili podataka o ličnosti u vezi sa krivičnim presudama i kažnjivim delima, u velikom obimu;
3. sistematski nadzor nad javno dostupnim površinama u velikoj meri.

Na osnovu člana 54. ZZPL, Poverenik je doneo i podzakonski akt (Odluku[61]) kojim se određuje lista vrsta radnji obrade podataka o ličnosti za koje se mora izvršiti procena uticaja i tražiti mišljenje Poverenika. Odlukom Poverenika predviđeno je devet različitih vrsta radnji obrade u pogledu kojih je, pre početka obrade podataka, obavezno izvršiti procenu uticaja i tražiti mišljenje Poverenika. Između ostalih, na ovoj listi su i „upotreba novih tehnologija ili tehnoloških rešenja za obradu podataka o ličnosti ili sa mogućnošću obrade podataka o ličnosti koji služe za analizu ili predviđanje ekonomske situacije, zdravlja, sklonosti ili interesovanja, pouzdanosti ili ponašanja, lokacije ili kretanja fizičkih lica“,[62] kao i obrada podataka o ličnosti ukrštanjem, povezivanjem ili proverom podudarnosti iz više izvora.”[63]

Imajući u vidu obim obrade, kao i vrste podataka koje bi se obrađivale, primena VI u pravosuđu bi zahtevala sprovođenje procene uticaja. Dalje, stav 11. člana 54. ZZPL dodatno predviđa da, ukoliko su radnje obrade podataka propisane posebnim zakonom, a radi se o obradi podataka koja je neophodna u cilju poštovanja pravnih obaveza rukovaoca, odnosno u cilju obavljanja poslova u javnom interesu ili izvršenja zakonom propisanih ovlašćenja rukovaoca, nije potrebno vršiti procenu uticaja pod uslovom da je ona već izvršena u okviru procene uticaja prilikom donošenja zakona. Kako se obrada podataka u pravosuđu zasniva na zakonu kao pravnom osnovu, bilo bi neophodno usvojiti propis koji bi regulisao i primenu VI u pravosuđu, i tom prilikom i sprovesti procenu uticaja na zaštitu podataka.

2.1. Strategija razvoja pravouđa za period 2020-2025. godine[64]

Ova Strategija predstavlja šest ciljeva koje propoznaje kao ključne za unapređenje pravosuđa u našoj zemlji i kao poseban (peti) cilj izdvaja razvoj e-pravosuđa.

Iako ne govori direktno o uvođenju veštačke inteligencije, Strategija najavljuje primenu informacionih i komunikacionih tehnologija koji će omogućiti uspostavljanje elektronske platforme pravosuđa. Ova platforma omogućila bi građanima da sve kontakte sa sudovima mogu da obave elektronskim putem (osim onih koji zahtevaju fizičko prisustvo), da predstavnici Visokog saveta sudstva i Državnog veća tužilaštva efikasnije

[61] Odluka o listi vrsta radnji obrade podataka o ličnosti za koje se mora izvršiti procena uticaja na zaštitu podataka o ličnosti i tražiti mišljenje Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti.

[62] *Ibid,* član 2, stav. 5

[63] *Ibid.,* član 2, stav 8.

[64] Tekst Strategije dostupan na linku: Стратегија развоја преавосуђа 2020-2025.pdf (sud.rs), [12.09.2022.].

vode evidencije o nosiocima pravosudnih funkcija, da raspodela predmeta bude automatska i nepristrasna, da prikupljanje podataka za pisanje izveštaja bude olakšano.

Pravosudne institucije u Srbiji već su započele uvođenje sistema elekronskog upravljanja predmetima. U prekršajnim sudovima je u upotrebi softver SIPRES[65], koji omogućava elektronsko podnošenje prekršajnih naloga. Za privredne sudove je dizajniran softver SIPRIS[66], čija je uvođenje još uvek u toku. Kada su u pitanju tužilaštva, u toku je implementacija SAPO[67] softvera, kao i SAPA[68] sistema u svim zavodima za izvršenje krivičnih sankcija. Još uvek nije poznato kada će ovi sistemi biti potpuno spremni za upotrebu od strane svih institucija kojima su namenjeni.

Ministarstvo pravde takođe razvija i aplikacije koje će omogućiti elektronsku razmenu podataka među pravosudnim institucijama, kao i aplikacije za sudsku praksu i centralnu statistiku.

Iako se veštačka inteligecija ne pominje implicitno u ovom delu strategije, jasno je da bi uspostavljanje ovih sistema i elektronskih baza podataka ubrzalo i olakšalo upotrebu sistema veštačke inteligencije u pravosuđu, ukoliko do toga dođe.

2.2. Strategija razvoja veštačke inteligencije u Republici Srbiji za period 2020-2025[69], sa Akcionim planom za prve dve godine važenja Strategije

Iako se Strategija ne bavi direktno veštačkom inteligencijom u pravosuđu, kao poseban cilj (broj 5) ističe se etična i bezbedna primena veštačke inteligencije, u svim sferama. Strategija se u ovom delu posebno fokusira na zaštitu ličnih podataka, zaštitu od diskriminacije, kao i odgovoran razvoj veštačke inteligencije u skladu sa međunarodnim etičkim standardima.

Kada je u pitanju zaštita ličnih podataka, sve predviđene mere su usmerene na to da građani mogu da imaju poverenje da su njihovi podaci bezbedni i da su određena rešenja zasnovana na veštačkoj inteligenciji u skladu sa zakonom i međunarodnim standardima. Automatizacija odlučivanja pomoću veštačke inteligencije uvek sa sobom nosi rizik diskriminacije, jer sami podaci koji se koriste za treniranje algoritama mogu biti zasnovani na prošlim diskriminatornim praksama. Iz tog razloga Strategija posebno apeluje na neophodan oprez pri korišćenju ovih tehnoligija, kako bi se uspostavila prevencija socijalne isključenosti osetljivih društvenih grupa s obzirom na njihovo lično svojstvo. Kao metode koje bi ovo omogućile izdvojene su poštovanje etičkih smernica iz ove oblasti, edukacija lica koja rade na razvoju novih tehnologija, organizovanje takmičenja u kojima će se razvijati sistemi kontrole, razvijanje precizne zakonske regulative za diskriminaciju i sankcionisanje diskriminacije, kao i uspostavljanje obaveze kreiranja transparentnih i obrazloženih odluka koje donosi veštačka inteligencija. Strategija

[65] Sajt portala: Регистар неплаћених новчаних казни и других новчаних износа (sud.rs), [12.09.2022.].

[66] Sistem pravosudnih sudova.

[67] Standard Application for Prosecution Offices.

[68] Standard Application for Prison Administration.

[69] Tekst strategije dostupan na linku: Стратегија развоја вештачке интелигенције у Републици Србији за период 2020–2025. године (srbija.gov.rs) [12.09.2022.].

takođe ističe i neophodnost poštovanja principa transparentnosti elemenata relevantnih za veštačku inteligenciju – podataka, sistema i primenjenih poslovnih modela.

Kao poseban i veoma značajan metod za adekvatnu primenu ovih novih tehnologija ističe se javni dijalog, organizovanje radionica, predavanja, seminara namenjenih široj javnosti sa ciljem približavanja prednosti i izazova koji su sastavni deo primene veštačke inteligencije, ali i sa ciljem kreiranja jače društvene odgovornosti javnog i privatnog sektora pri uvođenju veštačke inteligencije.

3. UTICAJ PRIMENE VEŠTAČKE INTELIGENCIJE U PRAVOSUĐU NA LJUDSKA PRAVA

U zavisnosti od toga u kojoj meri, na koji način i u kojim fazama postupka se veštačka inteligencija koristi u pravosuđu, menjaju se i potencijalni rizici upotrebe ovakvih tehnologija, kao i njihov potencijalni uticaj na ljudska prava. Na primer, uticaj na privatnost građana, ali i na ljudska prava uopšte, ne bi bio isti ukoliko bi sud koristio sisteme VI za upravljanje predmetima i ukoliko bi ta upotreba imala oblik najnaprednije primene predvidive pravde (uvođenje „sudija robota"). Isto tako, potencijalne posledice primene veštačke inteligencije nisu iste ako govorimo o korišćenju veštačke inteligencije u upravnim postupcima, u odnosu na, na primer, njenu primenu u medijaciji ili parničnim postupcima, ili ukoliko bi ih koristili advokati za procenu uspeha u sporu. I krivični postupci nose svoje specifičnosti, a može se reći i da su po pitanju rizika najosetljiviji, jer zbog potencijalnog lišenja slobode imaju direktan uticaj na osnovna prava građana. Konačno, primena sistema veštačke inteligencije u pravosuđu nema uticaj samo na prava stranaka i drugih učesnika u sudskim postupcima, već i na druga lica čiji se podaci obrađuju za potrebe „učenja" algoritma, kao i učesnike nekih budućih postupaka na koje će se odnositi odluke zasnovane na podacima koji se u sistem unose u sadašnjem vremenu.

Bez obzira na stepen i način korišćenja veštačke inteligencije u pravosudnim sistemima, upotreba ovih sistema zahteva visok stepen opreza. Za potrebe ovog teksta, proći ćemo kroz neke od izazova i pretnji po ljudska prava koje bi donelo uvođenje veštačke inteligencije u pravosuđe Srbije.

4. PRAVO NA PRAVIČNO SUĐENJE

Članom 32 Ustava Republike Srbije garantuje se pravo na pravično suđenje, a u skladu sa članom 6 Evropske konvencije o ljudskim pravima. Da bi građani mogli u celosti da uživaju u pravu na pravično suđenje, potrebno je da bude ispunjen niz garancija, kao što su nezavisno pravosuđe, nepristrasne i nezavisne sudije, i jednako pravo na pristup sudu za sve.

Nepristrasnost podrazumeva analizu nezavisnosti suda u odnosu na stranke u nekom konkretnom postupku. Ona takođe predstavlja odsustvo predrasuda ili unapred

utvrđenog stava prema strankama[70] (Vitakauskas, Dikov, 2017: 56). Nepristrasnost je jedan od osnovnih elemenata koje je potrebno obezbediti kako bi sudska odluka bila pravična u najširem smislu te reči, a presude koje donose "sudije roboti" sa sobom nose posebne specifičnosti povodom ovoga.

Tako, u presudi Vernes protiv Francuske[71], Evropski sud za ljudska prava utvrdio je povredu načela nepristrasnosti zbog nemogućnosti identifikacije članova sudskog veća koje je donelo odluku. Sud je naveo da je identifikovanje sudije koji donosi odluku ključno kako bi se ispunili i subjektivni i objektivni kriterijumi za određivanje stepena pristrasnosti suda, te da u odsustvu ove garancije sudsku odluku ne možemo sa sigurnošću okarakterisati kao nepristrasnu. Ako kriterijum odsustva predrasuda ili unapred utvrđenog stava prema strankama posmatramo u kontekstu problema vezanih za diskriminaciju koje sistemi predvidive pravde nose sa sobom, postavlja se pitanje da li odluka iza koje stoji ova vrsta veštačke inteligencije i "sudije roboti" ikada može biti nepristrasna.

Član 1. Zakona o sudijama[72] propisuje da je sudija nezavisan u postupanju i donošenju odluke. Zakon takođe određuje da sudija sudi i presuđuje na osnovu Ustava, zakona i drugih opštih akata, potvrđenih međunarodnih ugovora, opšteprihvaćenih pravila međunarodnog prava. Postavlja se pitanje da li je nezavisan i onaj sudija koji sudi i presuđuje na osnovu preporuke algoritma.

Ukoliko posmatramo situaciju u kojoj algoritam zasnovan na veštačkoj inteligenciji sudijama predlaže sadržinu sudskih odluka koje treba da donesu, nameće se pitanje da li su te sudije potpuno nezavisne, ili osećaju pritisak da svoje postupanje i odlučivanje usklade sa obrascem ponašanja koji algoritam prepoznaje kao adekvatan.

Ukoliko kao primer uzmemo praksu Kine, gde sudije moraju da opravdaju algoritmu razlog zbog kog žele da postupe drugačije od predloženog rešenja, jasno je da takvi sistemi ne ostavljaju puno prostora za nepristrasnost sudija.

I najzad, čiju nezavisnost utvrđujemo onda kada ne sude žive sudije, već odluke donose "sudije roboti"?

5. JEDNAKOST STRANAKA

Korišćenje bilo kog stepena veštačke inteligencije ne bi smelo da ugrozi jednakost stranaka pred sudom, niti da stavi u nepovoljniji položaj građane koji nisu u dovoljnoj meri upoznati sa radom računara i korišćenjem interneta. Međutim, nesporno je da bi uvođenje elektronskih platformi za pravosuđe izazvalo poteškoće za veliki broj građana, a verovatno uticalo i na to da građani koji su manje upućeni u korišćenje tehnologija

[70] Definicija preuzeta iz priručnika Saveta Evrope Zaštita prava na pravično suđenje po Evropskoj konvenciji o ljudskim pravima, dostupno na linku: Zaštita prava na pravično suđenje po Evropskoj konvenciji o ljudskim pravima (coe.int), [13.09.2022.].

[71] Vernes v. France, 30183/06, W+ECHR, 20.01.2011.

[72] *Sl. glasnik RS,* br. 116/2008, 58/2009 - odluka US, 104/2009, 101/2010, 8/2012 - odluka US, 121/2012, 124/2012 - odluka US, 101/2013, 111/2014 - odluka US, 117/2014, 40/2015, 63/2015 - odluka US, 106/2015, 63/2016 - odluka US, 47/2017 i 76/2021

izbegavaju da pokreću sudske postupke kako bi zaštitili svoj pravni položaj. Kao jedan od ključnih preduslova je svakako pristup građana internetu. U 2021. godini, penetracija interneta među pojedincima u Srbiji iznosila je 81,5% (Topić, Milivojević, 2022).[73] Jasno je da bi to automatski stavilo u nepovoljniji položaj, ali i onemogućilo preostalih 18,5% stanovništva da pristupe sudu i imaju aktivnu ulogu u zaštiti svojih prava.

Veoma je važno kreirati sistem u kom građani nisu prepušteni sami sebi onda kada treba da ostvare svoja osnovna prava vezana za pravnu zaštitu. Potrebno je da budu u dovoljnoj meri edukovani i informisani kome mogu da se obrate za pomoć, kao i da im u svakom momentu budu na raspolaganju korisnički servisi za sva pitanja i nedoumice koje imaju. Imajući u vidu dosadašnje probleme koje su građani imali pri pokušaju digitalizacije drugih sfera javnih usluga[74] teško je imati dovoljno poverenja da bi pravosudne platforme i sistemi korisničke podrške funkcionisali na zadovoljavajućem nivou i da bi uvek bili jednako dostupni svim građanima, čak i pod pretpostavkom da svi građani umeju jednako efikasno da ih koriste.

6. DISKRIMINACIJA

Početku upotrebe ovih algoritama prethodile su tvrdnje da je veštačka inteligencija u ovim situacijama preciznija od ljudi, ali i da se ovim otklanja svaka mogućnost za diskriminaciju i pristrasnost. Međutim, iskustva iz SAD-a su pokazala potpuno suprotne rezultate. Šansa da vam algoritam da lažno negativnu ocenu (predvidi da ćete ponovo izvršiti krivično delo, a to se ne dogodi) iznosila je 44,9% ako ste crnci, a 23,5% ako ste belci. Šansa da algoritam da lažno pozitivnu ocenu (predvidi da nećete ponovo izvršiti krivično delo, a to se dogodi) iznosila je 28,1 procenat ako ste crnci, a 47,7% ako ste belci[75] (Angwin, Larson, Mattu, Kirchner, 2016). Imajući u vidu da se prilikom unošenja podataka o okrivljenom nije navodila i njegova rasa, niti je postojao drugi način da veštačka inteligencija to utvrdi, postavilo se pitanje kako je moguće da su ovi sistemi diskriminatorni.

Istraživanja su dala veoma jednostavan odgovor na ovo pitanje – algoritmi su diskriminatorni, jer su takvi i podaci o ranijoj praksi koji su u njih uneti. Uprkos izjavi da će diskriminacija biti potpuno izbegnuta, ovi sistemi samo su potvrdili i nastavili lošu praksu koju su sudije i policajci godinama pokazivali tako što su za ista krivična dela češće hapsili crnce nego belce, češće vodili postupke protiv njih, ali im davali i strože kazne. Algoritmi nisu ispravili grešku ljudi, već su je pravili jačim intenzitetom, jer se u ovim slučajevima diskriminacija krila iza kompleksnih procesa veštačke inteligencije,

[73] Dostupno na linku: Report_on_implementation_of_the_Digital_Agenda_in_Serbia_2022.pdf (partners-serbia.org), [15.09.2022.].

[74] Na primer, prestanak rada svih službi katastra zbog hakerskog napada na sistem. Više o ovome može se pročitati u sledećem teksu: RTS :: Katastar do daljeg ne radi zbog hakerskih napada [12.09.2022.].

[75] Više o samom istraživanju može se naći u sledećem članku: Machine Bias — ProPublica, a objašnjenje načina na kojih su dobijeni ovi procenti mogu se naći ovde: How We Analyzed the COMPAS Recidivism Algorithm — ProPublica, [12.09.2022.].

mašinskog učenja, predvidivih algoritama, stvarajući privid da oni mogu doneti precizniju i sofisticiraniju odluku od čoveka.

Svako društvo nosi svoje specifičnosti kada je u pitanju diskriminacija, i iako savremene demokratske tendencije vode ka tome da se diskriminisanje grupa građana u odnosu na njihova svojstva iskoreni, loša praksa i dalje postoji kada su u pitanju određene kategorije lica, poput žena, migranata, ili ranije osuđivanih lica. Imajući u vidu da sistemi veštačke inteligencije crpe podatke iz prethodnog postupanja, postoji veliki rizik da raniji primeri loše prakse postanu stalni obrazac po kom se odluke donose.

7. PRAVO NA PRAVNU POMOĆ

Članom 67. Ustava RS propisano je da je pravo na pravnu pomoć zagarantovano svima i da pravnu pomoć, između ostalog, pruža advokatura.

U nekim zemljama se algoritmi predvidive pravde ne koriste samo u javnim insitucijama, već i u advokaturi. Na taj način advokati imaju na raspolaganju baze podataka koje sadrže ogromnu količinu dosadašnje sudske prakse, i koriste softvere kako bi dobili predikciju ishoda spora. Ovo advokatima svakako može pomoći da efikasnije savetuju i zastupaju klijenta onda kada algoritam predviđa da će spor biti uspešno rešen u njegovu korist, ali su po stranke moguće i negativne posledice, pre svega u situaciji kada su ove predikcije negativne, ili pokazuju jako male šanse za uspeh stranke u sporu. U takvim situacijama, postavlja se pitanje da li bi advokat koji zastupa stranku sa malim šansama za uspeh u sporu uložio potreban stepen truda i energije ako zbog predikcije algoritma smatra da je spor unapred izgubljen, odnosno da li bi ovakva primena VI ostavila neke građane u potpunosti bez raspoloživog pravnog savetovanja.

8. PRIVATNOST, ZAŠTITA I BEZBEDNOST PODATAKA

Bez obzira na to da li se veštačka inteligencija u pravosuđu koristi za upravljanje predmetima, ili se upotrebljavaju sistemi predvidive pravde, nesporno je da ovi sistemi mogu da funkcionišu samo ako su u njih unete ogromne količine podataka. Spisi sudskog predmeta mogu sadržati veoma veliki broj podataka o ličnosti, od osnovnih identifikacionih informacija, pa do podataka o zdravstvenom stanju osobe (i drugim podacima koji spadaju u tzv. posebne vrste podataka o ličnosti iz člana 17. ZZPL), porodičnim prilikama, informacija o zaradi i troškovima, podataka o korišćenju psihoaktivnih supstanci i slično. Imajući to u vidu, rizici po povrede prava građana su visoki, počev od povrede načela obrade podataka propisanih Zakonom o zaštiti podataka o ličnosti, odredbi o automatizovanoj obradi podataka o ličnosti i profilisanju, do bezbednosti podataka i sistema u kojima se oni nalaze.

U tom smislu, sudovi (kao rukovaoci podacima o ličnosti) imali bi posebne obaveze u pogledu informisanja lica o svim aspektima obrade podataka, u skladu sa Zakonom

o zaštiti podataka o ličnosti, i to na sažet, transparentan, razumljiv i lako dostupan način, korišćenjem jasnih i jednostavnih reči. Ova obaveza posebno je značajna u pogledu informisanja lica o postojanju automatizovanog donošenja odluke, s obzirom da ona podrazumeva i obavezu davanja svrsishodne informacije o logici koja se za ove potrebe koristi, kao i o značaju i očekivanim posledicama obrade podataka po lice na koje se podaci odnose (član 23. stav 2, tačka 6). Ovo bi predstavljao poseban izazov za rukovaoce podacima, imajući u vidu kompleksnost sistema VI, i različite nivoe informisanosti, obrazovanja i digitalne pismenosti učesnika sudskih postupaka.

Imajući u vidu obim, ali i vrste podataka koji se nalaze u sudskim bazama, rizici za bezbednost podataka su izuzetno visoki, i dolaze kako spolja, tako i iz samih sistema. Lako je uočiti i da bi ovi softveri i baze podataka mogli biti veoma primamljiva meta za hakerske napade, a imajući u vidu niz slučajeva upada u informacione sisteme kojima upravljaju organi vlasti, otvoreno je i pitanje poverenja građana u sistem bezbednosti podataka. Takođe, iako vesti o "curenju" informacija o građanima, neovlašćenom odavanju poverljivih informacija i neregularnom postupanju predstavnika javnih institucija kada su u pitanju podaci o ličnosti neretko završavaju u medijima,[76] jako retko smo svedoci sudskih epiloga u ovim situacijama (ako se postupak uopšte i pokrene) i sankcionisanja lica u okviru organa vlasti koji su postupali suprotno odredbama Zakona o zaštiti podataka o ličnosti.

Stoga je pre uvođenja bilo kog vida VI u naše pravosuđe potrebno preduzeti sistemske izmene kako bi se rukovaoci podacima obučili da postupaju u skladu sa zakonskom regulativom i međunarodnim standardima iz ove oblasti, kako bi softveri bili dovoljno otporni na eksterne uticaje i kako bi građani uvek bili adekvatno informisani o načinima obrade i bezbednosti svojih podataka.

Konačno, postavlja se i pitanje ovlašćenja za vršenje nadzora u oblasti zaštite podataka o ličnosti ukoliko bi se sistemi veštačke inteligencije primenjivali kao zamena za sudiju, ili podrška za donošenje sudske odluke. Imajući u vidu da Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti nije nadležan da vrši nadzor nad obradom podataka o ličnosti od strane sudova u vršenju njihovih sudskih ovlašćenja, pitanje je koji organ bi bio nadležan u slučaju povrede prava na zaštitu podataka o ličnosti prilikom primene algoritma za donošenje odluke u sudskom predmetu, odnosno da li bi sama primena algoritma bila smatrana vršenjem sudskih ovlašćenja.

9. PREPORUKE U POGLEDU UVOĐENJA SISTEMA VEŠTAČKE INTELIGENCIJE U PRAVOSUĐE REPUBLIKE SRBIJE

Imajući u vidu navedene rizike primene veštačke inteligencije u pravosuđu uopšte, ali i specifičan kontekst u kome funkcioniše pravosuđe u Republici Srbiji (pre svega, u vidu izazova digitalizacije javne uprave i usluga, te problema sa bezbednošću podataka),

[76] Primer: Poverenik pokreće postupak nadzora povodom objavljivanja podataka o maloletnom licu, sadržanih u krivičnoj prijavi - Poverenik za informacije od javnog značaja i zaštitu podataka o ličnosti [12.09.2022.].

u nastavku dajemo niz preporuka u pogledu aktivnosti koje bi trebalo sprovesti pre uvođenja jednog ovakvog sistema:

- Odluka o uvođenju sistema VI u pravosuđe u Republici Srbiji mora biti predmet široke debate stručne i druge zainteresovane javnosti (pravosuđa, akademske zajednice, civilnog i privatnog sektora), kako bi se u obzir uzeli širi društveni aspekti ovakve inicijative.
- Uvođenje sistema VI u pravosuđe u Republici Srbiji mora imati adekvatan pravni osnov, tj zakon koji bi regulisao primenu VI u pravosuđu koji bi, između ostalog, trebalo da propiše odgovarajuće mere zaštite prava, sloboda i legitimnih interesa lica na koje se podaci odnose.
- U fazi izrade propisa koji bi uređivao primenu VI u pravosuđu, neophodno je sprovesti procenu potrebe za jednim ovakvim sistemom, procenu uticaja na ljudska prava, moguće rizike u tom pogledu, i izraditi plan upravljanja rizicima.
- Za razvoj sistema VI u pravosuđu neophodno je obezbediti pristup sudskim odlukama u mašinski čitljivom formatu, tj u formi otvorenih podataka, uz poštovanje pravila o anonimizaciji podataka, kako bi sistem dobio dovoljan obim informacija za kreiranje što je moguće preciznijih modela.
- Podaci koji se unose u sisteme veštačke inteligencije moraju biti i formatu otvorenih podataka (open data format).
- Pre uvođenja sistema u pravosudni sistem, potrebno je obezbediti dovoljno vremena za njegovo testiranje, kako bi se postigao najveći mogući nivo preciznosti.
- Pre uvođenja sistema, tokom faze dizajna, potrebno je sprovesti procenu uticaja na zaštitu podataka, a u skladu sa Zakonom o zaštiti podataka o ličnosti.
- Potrebno je obezbediti najveći mogući nivo transparentnosti algoritma, kao i stalno praćenje njegovog funkcionisanja. Potrebno je izraditi posebne standarde transparentnosti ovih sistema, koji bi bili merljivi i podobni za praćenje i dalju analizu.
- Potrebno je obezbediti nezavisan i efikasan nadzor nad primenom algoritma, uključujući i praćenje primene etičkih standarda u ovoj oblasti.
- Neophodno je adekvatno, na jasan i razumljiv način, informisati građane o primeni VI i njihovim pravima u tom pogledu.
- Neophodno je obučiti zaposlene u pravosuđu o veštačkoj inteligenciji i njenom uticaju na ljudska prava, čak i ukoliko se ne razmatra uvođenje ovih sistema u naše pravosuđe, posebno za odlučivanje u postupcima o povredi prava usled primene VI.
- Neophodno je obučiti zaposlene u pravosuđu o bezbednosti podataka, i uopšte unaprediti nivo informacione bezbednosti u sistemu.
- Potrebno je stalno pratiti uporedna iskustva primene VI u pravosuđu, kako u pogledu razvoja regulatornog okvira, tako i u pogledu praktične primene.
- Pre uvođenja sistema VI u pravosuđe u vidu podrške ili zamene za sudsko odlučivanje, treba razmotriti automatizacija drugih radnih procesa kao prethodni korak ka unapređenju efikasnosti pravosuđa.

ZAKLJUČAK

Primena veštačke inteligencije u pravosuđu nesumnjivo predstavlja jedan od globalnih trendova, te, iako VI još uvek ni u jednom sistemu nije zamenila sudije, polje njene primene je sve šire. Uporedo sa razvojem tehnologije, razvija se i pravni okvir koji ima za cilj da uredi primenu veštačke inteligencije, uopšte, pa tako i u pravosuđu.

Međutim, napredak tehnologije nije uspeo da u potpunosti eliminiše probleme koje primena VI podrazumeva. Upitna neutralnost algoritama, njihova pravičnost, preciznost, kao i uticaj VI na pristup pravdi i prava na pravično suđenje, pravo na zaštitu podataka o ličnosti, i niz drugih prava građana, samo su neki od problema koje bi trebalo adresirati pri razmatranju uvođenja veštačke inteligencije u pravosuđe.

U Srbiji se problemi koje VI donosi mogu dodatno produbiti, zbog i inače nedovoljno efikasnih mehanizama zaštite ljudskih prava, te nedovoljne spremnosti našeg sistema da obezbedi resurse (u vidu informacione infrastrukture, ali i dovoljno velikog obima odluka dostupnih za "treniranje" algoritama) za razvoj sistema veštačke inteligencije. Imajući to u vidu, od izuzetnog je značaja da se uvođenju VI u naše pravosuđe pristupa sa velikim oprezom, uz poštovanje najviših etičkih, tehničkih i standarda zaštite ljudskih prava. Tačnije, pri razmatranju uvođenja jednog ovakvog sistema u Srbiji, neophodno je preduzeti niz regulatornih, edukativnih, i tehničkih intervencija koje bi postavile osnove za adekvatnu i svrsishodnu primenu VI. Prva, a možda i najvažnija od predloženih intervencija je i započinjanje široke društvene debate o potrebi, mogućnostima i izazovima primene veštačke inteligencije.

U fokusu prava i pravde ne bi trebalo da bude tehnologija, već pojedinci na koje se upotreba tehnologije odnosi. U tom smislu, i u konceptu predvidive pravde prioritet treba da budu građani i njihova prava, a ne nužno efikasnost pravosuđa. Stoga bi pri dizajniranju, razvoju i primeni sistema veštačke inteligencije u pravosuđu, bez obzira u kom obliku i za koje namene, trebalo imati u vidu najviše etičke standarde i pristup zasnovan na ljudskim pravima.

LITERATURA

1. Dick, K.F. (1956) *The Minority Report*.
2. Myltseva, V. The legal nature and principles of the predictive justice, Recht der Osteuropäischen staaten; REOS 03/19, 59-62.
3. Russel, S., Norvig, P. (2010) *Artificial Intelligence – A Modern Approach*, New Jersey: Prentice Hall.
4. Topić, P. i Milivojević, M. (2022) *Digitalna agenda u Srbiji*, Izveštaj za 2021. godinu, Beograd: Partneri Srbija.
5. Toskić, A., Stojavnović Kerić, M. i Jang, D. (2020) Analiza uticaja procesa evropskih integracija na lokalnu samoupravu u Srbiji u oblasti zaštite podataka o ličnosti i pristupa informacijama od javnog značaja (deo pregovaračkog poglavlja 23 – pravosuđe i osnovna prava), Beograd: Stalna konferencija gradova i opština-Savez gradova i opština Srbije.

6. Tournier-Tombs, E. (2021) „Towards a United Nations Internal Regulation for Artificial Intelligence" *Big Data & Society, dostupno na:* https://journals.sagepub.com/doi/pdf/10.1177/20539517211039493, [28.08.2022.].
7. Turing, A. (1950) „Computer Machinery and Intelligence", *Mind,* Volume LIX, Issue 236, https://doi.org/10.1093/mind/LIX.236.433, 433-460.
8. Vitkauskas, D., Dikov, G. (2018) *Zaštita prava na pravično suđenje po Evropskoj konvenciji o ljudskim pravima, Priručnik za pravnike praktičare*, Beograd: Savet Evrope, Kancelarija u Beogradu.

Pravni akti

1. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, 1981. https://rm.coe.int/1680078b37, [5.12.2022.].
2. Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes, Council of Europe, 2019. https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b [5.12.2022.].
3. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
4. Ethics guidelines for trustworthy AI, Council of Europe, 2018.
5. European Ethical Charter for the use of Artificial Intelligence in judicial systems and their environment, European Commissioner for the Efficiency of Justice (CEPEJ), 2018.
6. Izveštaj Specijalnog izvestioca UN-a za prava lica sa invaliditetom, od 28. decembra 2021.
7. Izveštaj Specijalnog izvestioca UN-a za slobodu mišljenja i izražavanja od 29. avgusta 2018.
8. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Savet Evrope, 2018.
9. New Guidelines on Artificial Intelligence and Data Protection, Council of Europe, 2019.
10. Odluka o listi vrsta radnji obrade podataka o ličnosti za koje se mora izvršiti procena uticaja na zaštitu podataka o ličnosti i tražiti mišljenje Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti (*Službeni glasnik RS*, broj 45/2019).
11. Opšta uredba o zaštiti podataka o ličnosti (GDPR), Evropska Unija, 2018.
12. Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and Amending certain Union Legislative acts. European Commission, 21.4.2021,

COM(2021)206 final https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF, [5.12.2022.].
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
14. Strategija za razvoj pravosuđa u Republici Srbiji za period 2020-2025. godine (*Službeni glasnik RS*, broj 101/2020).
15. Strategija za razvoj veštačke inteligencije u Republici Srbiji za period 2020-2025. godine (*Službeni glasnik RS*, broj 96/2019).
16. Study on the human rights dimensions of automated data processing techniques (in particular algorithms) and possible regulatory implications, Council of Europe, DGI(2017)12. Dostupno na: https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5, [5.12.2022.].
17. The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights, 13. septembar, 2021, 5. Dostupno na: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/21/PDF/G2124921.pdf?OpenElement, [28.08.2022.].
18. Univerzalna deklaracija o ljudskim pravima, Generalna skupština UN, 1948.
19. Veštačka inteligencija: Deset koraka za zaštitu ljudskih prava, Savet Evrope, Komesar za ljudska prava, 5. Dostupno na: https://rm.coe.int/-/1680997222, [28.08.2022.].
20. Zakon o ratifikaciji Međunarodnog pakta o građanskim i političkim pravima, (*Službeni list SFRJ*, broj 7/71).
21. Zakon o zaštiti podataka o ličnosti (*Službeni glasnik RS*, broj 87/2018).
22. Zakon o sudijama (*Službeni glasnik RS*, broj 116/2008, 58/2009 - odluka US, 104/2009, 101/2010, 8/2012 - odluka US, 121/2012, 124/2012 - odluka US, 101/2013, 111/2014 - odluka US, 117/2014, 40/2015, 63/2015 - odluka US, 106/2015, 63/2016 - odluka US, 47/2017 i 76/2021).

Internet adrese

1. https://www.ibm.com/cloud/learn/what-is-artificial-intelligence#toc-what-is-ar-DhYPPT4m [15.09.2022.].
2. Angwin, J., Larson, J., Mattu, S. and Kirchner, L. "Machine Bias", *ProPublica,* May 23, 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [15.09.2022.].
3. Larson, J., Mattu, S., Kirchner, L. and Angwin, J. *How we analyzed the COMPAS recidivism algorithm,* May 23, 2016, https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm [15.09.2022.].
4. https://data.gov.rs/sr/discover/ [15.09.2022.].
5. Mlađenović, A., Miljković, N., *Katastar do daljeg ne radi zbog hakerskih napada,* 16. jun 2022. https://www.rts.rs/page/stories/sr/story/125/drustvo/4851419/katastar-hakerski-napadi.html [15.09.2022.].

APPLICATION OF ARTIFICIAL INTELLIGENCE IN JUDICIARY – PERSPECTIVES AND CHALLENGES –

In this paper, the authors try to point out the possibilities and challenges of applying artificial intelligence in the judiciary, both for the purpose of supporting the work of the judiciary, and as a possible replacement for the work of judges, by introducing the so-called "robot judge." To that end, in the first part of the paper, they explain the basic terms relevant to understanding the possibility of applying artificial intelligence in the judiciary, as well as an overview of the relevant international legal framework, primarily in the context of the Council of Europe and the European Union. A special review is given to the Draft Regulation of the European Parliament and the Council on establishing harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain legal acts of the Union. Also, the paper presents comparative experiences in the application of artificial intelligence in the judiciary, as well as the challenges that have been observed during its application so far. primarily in terms of risks to human rights and freedoms - the right to protection of personal data, protection from discrimination and the right to a fair trial. In the continuation of the work, the authors analyze the relevant legal and strategic framework of the Republic of Serbia for the introduction of artificial intelligence, including the Law on the Protection of Personal Data, the Strategy for the Development of Artificial Intelligence for the period from 2020-2025, and the accompanying Action Plan for the period from 2020-2022. years. Finally, the paper points out the risks specific to the Republic of Serbia regarding the application of artificial intelligence in the judiciary, and gives recommendations for reducing these risks, both at the regulatory and practical levels.

KEYWORDS: *data science, artificial intelligence, case management, personal data protection, automatic decision making.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.23

ULOGA VEŠTAČKE INTELIGENCIJE U KONTROLI KRIMINALITETA

Aleksandar Stevanović*

U nastojanju da analizira ulogu veštačke inteligencije u kontroli kriminaliteta, autor polazi od terminoloških objašnjenja budući da je reč o složenim fenomenima što zahteva jasno i precizno definisanje relevantnih pojmova. U tom smislu, dat je istorijski prikaz razvoja pojma veštačke inteligencije, a ukazano je na ubrzani razvoj visoke tehnologije koja sve više veštački poprima osobine intelektualnosti i autonomnosti, što u velikoj meri utiče i na koncept kontrole kriminaliteta u instrumentalnom smislu. Zato su u radu predstavljeni osnovni oblici upotrebe veštačke inteligencije u kontroli kriminaliteta bez detaljnijeg zalaženja u objašnjenja sadržine i načina funkcionisanja budući da bi taj poduhvat iziskivao značajna multidisciplinarna znanja. Pored toga, razmotren je i krimi-nalno-politički aspekt pri čemu su u kontekstu kontrole kriminaliteta posmatrani društveno-ekonomski činioci koji su doprineli stvaranju aktuarijalnog modela kontrole koji nameće princip efikasne zaštite „po svaku cenu" bez naročitog osvrta na pojedinca i pitanja povezana sa njegovim tretmanom ili reintegracijom. Korišćenje intruzivnih i još uvek nedovoljno zakonski normiranih metoda isleđivanja koje se baziraju na veštačkoj inteligenciji, odnosna njihova upotreba u sudskom, dokaznom postupku, dovelo je u pitanje načela krivičnog prava, ali i ugrozilo značajan broj zajemčenih ljudskih prava, o čemu je detaljnije izlagano u delu rada u kojem se analizira argumentacija kojom se osporava upotreba veštačke inteligencije u kontroli kriminaliteta. Analitički koraci pri razmatranju uloge veštačke inteligencije u kontroli kriminaliteta preduzeti su sa ciljem da se ispita njena uloga u okviru aktuelne paradigme kontrole kriminaliteta, dok su analiza i komparacija uticajnih sudskih odluka iz ove oblasti imale cilj da pokažu (ne)kompatibilnost pragmatičnog krivičnog mehanizma i postojećeg normativnog okvira u kontekstu zaštite osnovnih ljudskih prava i poštovanja procesnih garantija.

KLJUČNE REČI: *veštačka inteligencija, tehnologija, kriminalitet, kontrola kriminaliteta.*

* Istraživač saradnik, Institut za kriminološka i sociološka istraživanja.
E-mail: *aleksandar.stevanovic993@gmail.com*

UVOD

Sa prvim nastojanjima da se država na organizovan i sistemski način suprotstavi aktivnostima koje je označila kao štetne i inkriminisala ih, borba protiv njih je u permanentnom sukobu sa uživanjem zajemčenih ljudskih prava. Kada je reč o primeni veštačke inteligencije u okviru kontrole kriminaliteta, taj sukob dodatno dobija na intenzitetu otvarajući pri tom mnoga pitanja među kojima naročitu pažnju zaslužuju ona koja se tiču zaštite privatnosti građana, kao i opravdanog cilja, odnosno srazmernosti metoda koje primenjuju organi formalne socijalne kontrole prilikom isleđivanja.

Težnja ka konstantnoj kontroli svih rizika karakterišu današnje društvo, koje je sve više sklono nepoverenju u državnu vlast i institucionalne oblike zaštite bezbednosti. Veštačka inteligencija u smislu najnovijeg vida visoke tehnologije kao nikada ranije uključuje i privatni sektor u procese kontrole kriminaliteta[1] oduzimajući pri tom tradicionalnoj policiji ekskluzivnost ekspertizma u oblasti kaznene reakcije. Na taj način se zadovoljava potreba za stalnim osećajem sigurnosti koja je u modernom društvu intenzivno izražena, a prevazilazi se i oslanjanje na sporu i pre svega tehnološki ograničenu zaštitu bezbednosti od strane institucionalnih sistema, pa se zato proučavanje uloge veštačke inteligencije u kontroli kriminaliteta nameće kao važno kriminalno-političko i kriminološko pitanje.

Sve veća uloga veštačke inteligencije u ljudskim životima predstavlja važan praktičan i konceptualni izazov za čitav pravni sistem, što proizlazi iz činjenice da tehnološke inovacije vremenom menjaju svakodnevnicu i postaju neizostavni element savremenog načina života.[2] Po prirodi stvari se tu nameće i potreba za normativnom intervencijom koja bi uzela u obzir sve relevantne okolnosti koje se odnose na razvoj i upotrebu veštačke inteligencije na različitim poljima. Kontrola kriminaliteta je u tom smislu izrazito osetljiva oblast s obzirom da podrazumeva korišćenje legalne prinude, odnosno ograničenje ili ukidanje određenih ljudskih prava kada se za to steknu zakonski uslovi, dok veštačka inteligencija shodno svojim osobenostima, dodatno proširuje jaz između zaštite bezbednosti i drugih zajemčenih prava.

Imajući u vidu da su „veštačka inteligencija" i „kontrola kirminaliteta" dva složena pojma, a kakao bi se stekao valjan uvid u njihove glavne karakteristike, u radu su najpre razmotrene osnovne tačke koje se tiču strukture, prirode i sadržine dva pojma.

U radu se polazi od opšte pretpostavke da veštačka inteligencija, iako prema svojim osobinama odgovara aktuelnoj tendenciji kontrole kriminaliteta, odnosno predstavlja nezaobilazan sadržaj političkog diskursa koji se tiče kontrole kriminaliteta, najvećim delom ne odgovara postignutom nivou zajemčenih ljudskih prava odnosno tzv. „*due process*" garantijama koje čine konstitucionalnu osnovu gotovo svih današnjih država. Iz nje logičkim sledom stvari proizlazi i konkretnije određena pretpostavke prema kojoj upotreba veštačke

[1] Mnoge kompanije se kada je reč o njihovoj korporativnoj bezbednosti danas više oslanjaju na znanje svojih informatičara nego u policiju, odnosno druge državne organe u čijoj je nadležnosti borba protiv kriminaliteta.

[2] Tako su danas, naročito u razvijenim zemljama u široj upotrebi automobili koji se kreću sami bez upravljanja čoveka (eng. *unmanned vehicels*), roboti – hirurzi, algoritimi koji se koriste u trgovini i dr.

inteligencije sa kojom se najpre otpočelo u komercijalnom sektoru, nije u značajnijoj meri, na legalnoj osnovi moguća u oblasti kontrole kriminaliteta imajući u vidu osnovne institute i načela materijalnog krivičnog prava, odnosno krivičnog postupka.

Provera tačnosti pretpostavki od kojih se pošlo u radu izvršena je pre svega oslanjanjem na istorijsko-komparativni metod. U tom smislu, praćen je razvoj koncepta kontrole kriminaliteta sve do onog koji se naziva aktuarijalnim i danas predstavlja dominantan skup tendencija i ideja o tome kako treba reagovati na kriminalitet. To je učinjeno kako bi se stekao uvid u funkciju koju „pametne mašine" u tom kontekstu mogu imati. Pored toga, izvršena je komparacija izabranih sudskih odluka, kako onih koje su donete pred sudovima u Sjedinjenim Američkim Državama (dalje: SAD), tako i onih koje je doneo Evropski sud za ljudska prava (dalje: ESLJP) u predmetima koji se odnose na povredu ljudskih, odnosno važnih procesnih prava upotrebom veštačke inteligencije u kontroli kriminaliteta, a imajući u vidu činjenicu da upravo SAD i evropske zemlje imaju najviše praktičnog iskustva u tom smislu. Na taj način smo nastojali da ispitamo legalnost primene veštačke inteligencije u postojećim normativnim okvirima datih jurisdikcija. Budući da efikasnost i objektivizacija kao glavne prednosti upotrebe veštačke inteligencije u aktivnostima kontrole kriminaliteta načelno nisu sporne, jezgro analitičkog osvrta dato je u delu rada u kojem se detaljnije analiziraju razlozi koji tu upotrebu osporavaju.

1. GLAVNE KARAKTERISTIKE POJMA „VEŠTAČKA INTELIGENCIJA"

Čuveni francuski filozof, Rene Dekart (*René Descartes*), je još u 17. veku problematizovao navodnu mogućnost mašina da razmišljaju i zaključuju poput ljudi (Solum 1992, 1234). On nalazi da mašine, tada iz jedne hipotetičke perspektive koja se vremenom pokazala kao tačna, zaista mogu biti konstruisane nalik ljudskim bićima, da mogu upotrebljavati reči, davati odgovore na određena pitanja i tome slično. U nastavku ipak navodi da mašine nikada neće moći da odgovore na svako pitanje ili situaciju koja ih može zadesiti (Wilson 1969, 138), što je nesporno odlika svakog ljudskog bića, bez obzira na kvalitet odgovora ili adekvatnost reakcije na datu okolnost. Ovakav Dekartov zaključak je i do danas ostao u središtu rasprava o veštačkoj inteligenciji i njenoj ulozi u društvu (Solum,1992: 1235).

Inteligencija se u relevantnoj literaturi označava kao sposobnost razumevanja pojava i odnosa, donošenja pravih odluka i adekvatnog postupanja u datim okolnostima (Jones, 2009: 1). Termin „veštačka inteligencija" ušao je u naučni i opšti diskurs sredinom pedesetih godina 20. veka (Scherer, 2016: 360) i tada se odnosio na inženjerski proces stvaranja inteligentnih mašina, što je bilo polazište za dalja razmatranja i potpunija objašnjenja. Prema jednoj kasnijoj definiciji veće kognitivne upotrebljivosti, veštačka inteligencija je deo nauke o računarima, koja se bavi kreiranjem takvih računarskih sistema koji su sposobni da poseduju karakteristike koje asociraju na ljudsko ponašanje (Russel & Norvig, 2010: 1034).

U početku je oponašanje ljudskih radnji (eng. *acting humanly approach*) primarno određivalo veštačku inteligenciju što je u radovima pionira ove nauke, Alana Turinga (*Alan Turing)* isticano kao njena glavna karakteristika (Scherer, 2016: 360). Isti autor veštačku inteligenciju poredi sa „igrom imitacije" navodeći da tu zapravo nije fokus na tome da se veštački kreira sam proces ljudskog razmišljanja, već njegove spoljašnje manifestacije na način da se sagovornika ili posmatrač ubede da su u određenoj interakciji sa čovekom, a ne sa mašinom (Scherer, 2016: 360).

Sa druge strane, ljudsko ponašanje nije uvek rezultat logike i pravilnosti koja se može ustanoviti, zapisati i predstaviti pomoću matematičkih izraza. Neizostavne determinante ne samo ljudskog ponašanja, već i ličnosti uopšte su i identitet, iskustvo, integritet, stav, moral, kreativnost, motivacija, emocije, navike, opsesije i dr. Sve ove čovekove karakteristike prema sadašnjem stanju nauke nije moguće programirati i predvideti. Tu se svakako postavlja i pitanje mogućnosti programiranih mašina da prodiru u suštinu semantičkih simbola, odnosno da „čitaju između redova". Tako pojedini autori primećuju da moderne, „pametne mašine" rade tačno ono što im se naredi i kaže, ali često ne i ono što se zapravo time htelo reći (Kemeny, 1972: 10). U tom smislu proizlazi da veštačka inteligencija predstavlja samo delimičnu humanizaciju robota i mašina i to u pogledu onih karakteristika čoveka koje se primenom induktivnih i deduktivnih metoda mogu jasnije odrediti i predviđati, a koje se zasnivaju na racionalnoj osnovi.

Kao eventualna relativizacija prethodno iznete teze o ponašanju mašina na osnovu precizno programiranih matematičkih i logičkih modela moglo bi se istaći sve veće podizanje stepena „intelektualnosti" kod mašina nove generacije. Naime, već je ušla u širu upotrebu sintagma „mašine koje uče" (eng. *learning machine*), a koja se koristi da označi mašine koje imaju sposobnost učenja bez posebnog programiranja (Kamarinou *et al.* 2016: 3) oslanjajući se na iskustvo i interakciju sa ljudima.[3] Važnu napomenu u pogledu procesa mašinskog učenja daje Ralf Hajrbrih (*Ralf Herbrich*), direktor sektora za učenje mašina u nemačkom ogranku Amazona, kada ukazuje da se mašinsko učenje sastoji od niza algoritama čiji je cilj da identifikuju glavne varijable i frekvenciju unetih podataka i tako predvide karakteristike novih podataka (Kamarinou *et al.* 2016: 6). Problem koji se tu javlja odnosi se na činjenicu da mašine na taj način ne spoznaju nužno stvarnost, već onu verziju nje koja nastaje u procesu obrade u zavisnosti od sadržine i kvaliteta kako algoritma tako i unetog podatka. Slično je i sa kognitivnim procesom kod čoveka, s tim da on raspolaže daleko složenijim i savršenijim „algoritmom" koji uzima u obzir i emocije, prethodno iskustvo, intuiciju, kreativnost, analogiju, imaginaciju, predrasude i

[3] Najbolji primer ove nove tendencije u svetu nauke o veštačkoj inteligenciji jeste Guglov prevodilac (eng. *Google translate*). U početku je delovalo da je zamisao automatskog prevođenja sadržaja neodrživa i neostvariva usled brojnih različitosti u svetskim jezicima, ali i dijalektima istog jezika, kao i postojanja mnoštva skraćenica i žargona. Ovaj problem prevaziđen je upravo interakcijom sa korisnicima Guglovog programa („molimo Vas ocenite prevod ili poboljšajte prevod") i iskustva u smislu pamćenja novih stvari i učenja na prethodnim greškama. Otuda se u literaturi ističe da je iako sličnog korena i jezičke morfologije, automatsko prevođenje na engleski jezik sa ruskog u odnosu na srpski jezik daleko uspešnije. To se objašnjava činjenicom da u Rusiji živi bar dvadeset puta više ljudi nego u Srbiji, što znači i da je statistički posmatrano, opcija „molimo Vas ocenite prevod ili poboljšajte prevod" tamo daleko korišćenija, a time i program intenzivnije razvijan (Branković, 2017: 7-8).

mnoge druge elemente koji nisu karakteristični za proces mašinskog učenja, a značajan su deo spoljne manifestacije svakog sadržaja. Valja imati u vidu i činjenicu da način razmišljanja i zaključivanja kod čoveka može da varira u zavisnosti od različitih društvenih i organskih faktora, dok se kod mašina to postiže isključivo pisanjem novog algoritma.

2. KONTROLA KRIMINALITETA – POJAM I TENDENCIJE

2.1. Određivanje pojma i njegov kriminološki aspekt

U savremenom političkom i krivičnopravnom diskursu u upotrebi je više različitih termina koji označavaju reagovanje na kriminalitet poput rata, borbe, suprotstavljanja, suzbijanja i sprečavanja. Smatramo da je kontrola kriminaliteta genusni pojam koji obuhvata najrazličitije načine društvenog reagovanja na kriminalitet u cilju njegovog redukovanja. One mogu podrazumevati mehanizme različitog intenziteta i karaktera, ali je važno imati u vidu da „kontrola" u osnovi obuhvata dve vrste reagovanja, a to su profilaksa (prevencija) i represija.[4] Bez obzira na prihvaćeni koncept kontrole kriminaliteta, reč je o skupu aktivnosti koje preduzimaju nadležni državni organi (formalne aktivnosti) ili civilno društvo (porodica, škola, mediji i dr.) sa ciljem da se kriminalitet suzbija, odnosno da se njegova stopa održava na društveno prihvatljivom nivou.

Društva su od najranijih oblika organizovanja i uspostavljanja zajednice kontinuiranog zajedničkog života na različite načine reagovala na ponašanja koja su ugrožavala osnovne vrednosti na kojima su zasnovana. U početku se radilo o gotovo instiktivnim reakcijama na kriminalitet koje su često bile praćene simboličkim obeležjima bez bilo kakvih ograničenja predviđenih u pravnim propisima. Takve reakcije su svoje uporište uglavnom imale u moralnim načelima i preovlađujućim društvenim shvatanjima određene zajednice (Ignjatović 2003, 1). Glavnu ulogu u kontroli kriminaliteta su najpre imale društvene institucije, a naročito porodica, crkva i neposredno socijalno okruženje. Međutim, sa nastankom države i njenim institucionalnim razvojem, reagovanje na kriminalitet postaje formalizovano[5] u smislu uspostavljanja pravnih pravila koja u osnovi određuju koje radnje će se smatrati dovoljno štetnim da ugrožavaju osnovne vrednosti društva, na koji način će se na njih reagovati, kao i ko je nadležan da odgovori na takve radnje u svakom konkretnom slučaju.

Od stvaranja prvih država, značaj neformalne socijalne kontrole opadao je na račun formalne kontrole, tj. organa državne vlasti koji su personalizovali i operacionalizovali njeno *ius puniendi*, čime je pitanje kontrole kriminaliteta ušlo u političku sferu, a u kasnijim periodima, sve do danas, ostalo neodvojivo povezano sa najvišom državnom politikom. Potrebno je prepoznati činjenicu da je krivično zakonodavstvo koncipirano

[4] U prvom slučaju, reč je o preventivnom delovanju, tj. reagovanju pre nego što je delo izvršeno, dok se u drugom slučaju radi o antikriminalnom delovanju od strane nadležnih državnih organa, onda kad je norma prekršena (Ignjatović, 2003: 2).

[5] Navedena konstatacija ne isključuje uticaje vanpravnih faktora ne samo na krivičnopravni progon, već uopšte na donošenje i primenu pravnih pravila.

tako da uspostavljenim krivičnopravnim mehanizmom predviđa reagovanje na one radnje koje imaju kapacitet da ugroze osnovne vrednosti jedne društvene zajednice, a koje se danas označavaju kao krivična dela. Bez obzira na oprečna tumačenja kada je reč o funkciji države, nesporno je da je obezbeđivanje opšte bezbednosti zajednice jedna od njenih osnovnih uloga koja ujedno i opravdava prerogative koje poseduje.[6]

Valja imati u vidu i uticaj straha koji kriminalitet generiše kod ljudi. Dosadašnje iskustvo je pokazalo da su mnoge vlasti nastojale da upravo kontrolom straha kod građana uspostave kontrolu i nad političkom situacijom, a sebi obezbede privilegovane pozicije u društvu. Otuda su i manipulacije kontrolom kriminaliteta čest *modus operandi* u cilju stvaranja i održavanja političke moći, primera radi, obezbeđivanjem više sredstava iz budžeta ili prikazivanjem stvarne i percipirane sile spoljašnjem i unutrašnjem „neprijatelju". Takvu tendenciju politizacije kontrole kriminaliteta slikovito opisuje Džonatan Simon (*Jonathan Simon*) nazivajući je „vladavinom preko zločina" (Simon, 2007).

Politika kontrole kriminaliteta ne može se posmatrati izvan relevantnog ekonomskog i sociološkog okvira (Soković, 2011: 213), a moglo bi se reći da pristup kriminalitetu i njegovoj kontroli nastaje i menja se upravo u skladu sa društveno-istorijskim osobenostima određenog društva i vremena. S tim u vezi, treba imati u vidu da aktuelni trendovi opšte društvene globalizacije i liberalnog modela ostvaruju svoje efekte i na kontrolu kriminaliteta. U novijim akademskim publikacijama na ovu temu pretežno je naglašen negativan uticaj aktuelnog društveno-ekonomskog okvira uz isticanje slabljenja efekata primarne, neformalne socijalne reakcije na zločin (Soković, 2011: 213). Pored toga, ukazuje se i na činjenicu da aktuelni model političke ekonomije ohrabruje ekspanziju krivičnopravnog reagovanja (Stuntz 2001, 510) i to na način da ono biva instrumentalizovano za potrebe prilagođavanja modernim uslovima društvenog života (Simović-Hiber. 2016: 239).

Povećana fluktuacija ljudi, robe i informacija i njihovo slobodno kretanje, pored nesumnjivo pozitivnih tržišnih i kulturoloških posledica, utiče i na osećaj socijalne nesigurnosti kod ljudi. U takvim uslovima, „moralni individualizam" imanentan liberalno-kapitalističkom modelu uzrokuje ponekad i nekontrolisani strah usled čega je sa stanovišta političkog oportunizma poželjno kreirati agendu „kaznenog populizma" koja bi bila u skladu sa strahom od kriminaliteta koji je u savremenom društvu naročito izražen i definisan kroz koncept „društva rizika"[7] koji u osnovi predstavlja stanje permanentnog straha u kojem se društvo nalazi usled opasnosti koje sa sobom nosi moderan način života, odnosno reakciju društva na njih.

2.2. Tendencije u oblasti kontrole kriminaliteta

Stav da je koncept kontrole kriminaliteta u protekle četiri decenije pretrpeo suštinske promene u potpunosti je akademski afirmisan i to naročito kada se radi o zapadnim liberalnim demokratijama (Marks *et al.* 2015: 4; Hudson, 2002: 246). Te promene

[6] Postoje i zanimljiva mišljenja prema kojima bi se formiranje države kao normativno uređene zajednice moglo posmatrati kao obezbeđivanje sigurnosti i zaštite u zamenu za plaćanje „poreza" (Karstedt, 2014: 306).

[7] Reč je o konceptu koji su kroz svoj rad razvila dvojica uticajnih sociologa, Urlih Bek (*Ulrich Beck*) i Entoni Gidens (*Anthony Giddens*).

su, kako se to navodi u literaturi, stvorile državu koja „upravlja na daljinu" pa shodno tome i „kažnjava na daljinu" (Rose & Miller, 1992: 181) unoseći komercijalni etos u javno (državno) delovanje (Marks *et al*. 2015: 4). Posledica takvog stanja stvari je težnja da se sa minimalno uloženih napora i sredstava ostvari najveći mogući rezultat. Upotreba veštačke inteligencije se upravo u tom kontekstu pokazuje kao otelotvorenje efikasne i ekonomične kontrole.

Aktuarijalna paradigma uloge i cilja krivičnog prava se sve više nameće kao dominantna, a njena suština ogleda se u okretanju ka najefikasnijim metodama kontrole kriminaliteta (Feeley & Simon, 1992: 457). Primarni cilj je da se zaštiti društvo od svih mogućih rizika, dok se manje pažnje posvećuje pojedincu, odnosno pitanjima „krivice", „dijagnoze", „tretmana" i tome slično (Ignjatović, 2018: 762). Na taj način se pravi distanca od tradicionalnog individualističkog modela krivičnog pravosuđa što otvara pitanje uloge i cilja krivičnog prava uopšte. Jedna od značajnijih posledica promene u koncepciji pristupa kontroli kriminaliteta je davanje prednosti praksi preventivnog postupanja. To znači da je sve do sedamdesetih godina 20. veka uspešna antikriminalna reakcija podrazumevala da se bude prisutan i učinkovit na „licu mesta" (Sherman 2013, 399), dok je danas fokus na tome da do izvršenja krivičnog dela uopšte i ne dođe. Ovakvo stanovište je potvrđeno i u odluci Vrhovnog suda SAD u predmetu *US. v. Salerno*[8] kada je sud odlučivao o ustavnosti odredbi tzv. *Bail Reform Act* iz 1984. godine, nalazeći da pritvor u fazi istrage ne povređuje „*due process*" garantije ističući u prvi plan bezbednost zajednice. Danas je istražni pritvor opšte prisutna mera krivičnog postupka sa naglašenim preventivnim dejstvom.

U cilju pojačane sekuritizacije društva odgovornost za kontrolu kriminaliteta ponovo je prebačena i na privatni sektor, odnosno i na činioce neformalne socijalne kontrole. Tako se recimo sa uvođenjem video nadzora otpočelo šezdesetih godina prošlog veka u Velikoj Britaniji i SAD i to u privatnim entitetima kao što su banke i prodavnice, pretežno radi zaštite kapitala, ekonomskih i političkih interesa, te radi smanjenja straha od kriminaliteta kod građana (Kovačević-Lepojević & Žunić-Pavlović, 2012: 327). U kriminološkoj nauci je ubrzo koncipiran pojam „odbranjivog mesta" (*eng. defensible space*) koji je ilustrativno opisala američka novinarka Džejn Džejkobs (*Jane Jacobs*) navodeći da zločin ima manje šanse da uspe u urbanim područjima sa velikim brojem ljudi i prodavnica onda kada je „mnogo očiju uprto u izvršioce" (Rock, 2002: 63). U tom smislu se primena veštačke inteligencije pokazuje kao „savršeno" (dokazno) sredstvo za pribavljanje podataka, jer nije podložno podmitljivosti, strahu, zaboravu i drugim faktorima dokaznih deficita.

Paralelno sa procesom sekuritizacije društva odigravala se i svojevrsna privatizacija kontrole kriminaliteta, čemu je u značajnoj meri doprinela i upotreba veštačke inteligencije. Naime, tradicionalno ustrojeni organi krivičnog gonjenja gubili su korak sa tehnološkim uzletom i sve više im je bila potrebna pomoć eksperata koji poseduju sofisticirana znanja iz oblasti visoke tehnologije. Otuda su vremenom razvijane privatne kompanije koje policiji na lokalu nude svoje usluge pre svega u vidu specijalizovanih

[8] 107 S. Ct. 2045, 2101-2 (1987).

softvera za predikciju kriminaliteta, praćenje rizika, obradu velike količine podataka i tome slično.[9]

Moguće je uočiti razliku u konceptu kontrole kriminaliteta u odnosu na politički. Vlasti koje pripadaju desno orijentisanom političkom spektru svoju politiku kontrole kriminaliteta po pravilu zasnivaju na strogom represivnom mehanizmu (smrtne kazne, doživotni zatvor, dugogodišnje zatvorske kazne) pa je takva borba simbolički svedena na „borbu dobra protiv zla" (Simon, 2002: 1039). Sa druge strane, politička levica češće polazi od profilaktičkog delovanja, a strah od kriminaliteta vidi kao pretnju po bezbednost u porodici, u školi, na javnim mestima, na radnom mestu, odnosno u svakom polju i aspektu društvenog angažovanja (Simon, 2002: 1039). Otuda se insistira na merama prevencije koje podrazumevaju video nadzor lica i objekata, praćenje kretanja i drugih aktivnosti, kontrolu komunikacije, procene bezbednosnih rizika zasnovane na algoritmima i dr. Ipak, čini se da je bez obzira na ideološko ustrojstvo, težnja svake vlasti da ostvari potpunu kontrolu nad svim društvenim aktivnostima, pa tako i nad kriminalitetom u čemu upotreba veštačke inteligencije daje nemerljive rezultate. Najzad, u modernom „društvu rizika" moralnim načelima potkrepljena borba „dobrog protiv zla" stavljena je u drugi plan, a korišćenje preventivnih tehnika i uopšte pokretanje krivičnog mehanizma vođeno je strahom i anticipiranjem različitih opasnosti.

Vlade gotovo svih država utrkuju se da predstave svoje odgovore na kriminalitet u vidu implementacije veštačke inteligencije u sistem formalne reakcije na društveno štetna ponašanja.[10] [11] Takvo stanje stvari ipak ne bi trebalo da čudi ukoliko se ima u vidu da je tehnologija još od antičkih vremena bila smatrana multiplikatorom političke moći (Damnjanović, 2012: 343) koja se ogleda u kapacitetu države (političke elite) da sprovodi svoje odluke, a bez ikakve dileme i da kontroliše sve aktivnosti kojima se krše važeći propisi, odnosno njeni interesi.

Pod uticajem društveno-ekonomskih činilaca izmenjena je i fenomenologija kriminaliteta, pa je tako sa većim prisustvom visoke tehnologije u svakodnevnom životu došlo i do transformacije kriminalnih prilika i ponašanja. Kriminalne aktivnosti su postale globalne, distributivne i informacionalizovane (Wall 2015, 86). Zločini efikasno mogu biti vršeni „na daljinu", a automatizacija tehnologije doprinosi tome da sve veći broj potencijalnih izvršilaca može zloupotrebiti mogućnosti koje ona pruža, uz povećane šanse da ostanu neotkriveni.

[9] Vidi primera radi internet prezentaciju italijanske kompanije KeyCrime na: https://www.keycrime.com/about-us, [20.5.2022].

[10] Tako je ruski predsednik, Vladimir Putin, svojevremeno izjavio da će lider u oblasti veštačke inteligencije biti i lider sveta (prema: Tilovska – Kechedji *et al.* 2018: 14).

[11] Kina je primera radi još 2006. godine implementirala program upotrebe veštačke inteligencije u cilju ostvarivanja nacionalne bezbednosti koji je kasnije iznova redefinisala i inovirala. Plan Rusije je da do 2025. godine ima 30 odsto robotizovane vojne opreme, dok su SAD prema dostupnim podacima u okviru jednog od vladinih programa upotrebe veštačke inteligencije u vojne svrhe uložile blizu 500 milijardi američkih dolara (Navedeno prema: Tilovska – Kechedji *et al.* 2018: 11-14).

3. UPOTREBA VEŠTAČKE INTELIGENCIJE U KONTROLI KRIMINALITETA

Upotreba jedinica veštačke inteligencije moguća je na svim nivoima kontrole kriminaliteta bez obzira na to da li se radi o policijskim organima koji vrše isleđivanje ili drugim državnim organima koji imaju nadležnost u prikupljanju podataka i identifikovanju dela i učinioca, tužilaštvima koja vode istrage, sudovima koji donose odluke, te kaznenim zavodima i drugim ustanovama koje te odluke treba da sprovode. Uopšte, primena tehnoloških dostignuća je odavno sveprisutna u savremenim politikama kontrole kriminaliteta (Grabosky, 1998: 58).

Korišćenje veštačke inteligencije u radu organa formalne socijalne kontrole se po pravilu vezuje za isleđivanje najtežih krivičnih dela.[12] Upravo se iz suzbijanja takvih dela koja u najvećoj meri ugrožavaju osnovne vrednosti društva crpi opravdanost za upotrebu veštačke inteligencije uz veći stepen tolerancije na njenu intruzivnost. Međutim, čini se da je u modernom „društvu rizika" koje teži da eliminiše svaku bezbednosnu pretnju bez obzira na druge okolnosti, primena visoke tehnologije postala nekontrolisana i preobimna, šireći svoj domašaj čak i na suprotstavljanje kaznenim deliktima koji imajući u vidu značaj i težinu neprava, spadaju u prekršaje ili druge povrede zakona koje ne zahtevaju kaznenu rekaciju.

Radikalni zaokreti u kontroli zločina se po pravilu dešavaju nakon događaja koji u najvećoj meri predstavljaju opasnost po bezbednost zajednice. Tako primera radi počev od „11. septembra" i čuvenog terorističkog napada u SAD na scenu stupa pojačana militarizacija u sprovođenju zakona kao i šira upotrebe tehnologije nadzora koja se koristi u javnom i privatnom sektoru kako bi se istovremeno sa uspehom vodila borba kako protiv „domaćih uličnih zločina" tako i protiv međunarodnog kiber kriminaliteta ili terorizma.[13] U periodima povećane opasnosti po bezbednost, menja se i bezbednosno-politički diskurs, te posezanje za upotrebom svih raspoloživih sredstava, a naročito za visokom tehnologijom i jedinicama veštačke inteligencije kako bi se lakše „pobedio" neprijatelj, potiskuje sva pitanja koja se tiču poštovanja *due process* garantija i drugih zajemčenih prava. Osvajanje novih tehnologija i njihova upotreba danas jeste način da se promptno smanji strah od svih bezbednosnih pretnji, ali je ujedno značajan i stav pojedinih autora koji tvrde da postoji nadmetanje u pogledu ne samo postizanja nivoa bezbednosne kontrole, već i u pogledu ovladavanja bezbednosnim diskursom, budući da sposobnost kontrole nad njim određuje „ko odlučuje šta bezbednost predstavlja, koja pitanja ulaze u bezbednosnu agendu i kako uopšte ta pitanja treba da se rešavaju. (Barak, 2020: 132).

Iako je korišćenje veštačke inteligencije u kontroli kriminaliteta odveć postalo opšte mesto, moguće je klasifikovati polja njene primene u cilju boljeg razumevanja materije. U osnovi, situaciona prevencija kriminaliteta zahteva od organa socijalne kontrole

[12] Pod tim bismo mogli smatrati krivična dela za koja je zaprećena kazna od četiri godine ili teža kazna, ili ona dela kod koji postoji mogućnost primene posebnih dokaznih radnji.

[13] Velika Britanija je više od dve trećina svog budžeta potrošila na uvođenje video nadzora na ulicama i javnim površinama nakon pogibije dva dečaka usled napada terorističke organizacije IRA 1993. godine (prema: Kovačević-Lepojević & Žunić-Pavlović, 2012: 88).

da budu „korak ispred" što znači da moraju posedovati i lako manipulisati velikom količinom informacija. Posmatrano sa sociološkog aspekta, mreža informacija predstavlja centralnu tačku socijalne strukture u „Informatičko doba" (Castells 2000, 5), dok je u literaturi zastupljen stav da je primarna upotreba visoke tehnologije upravo u oblasti prikupljanja informacija i komunikacija (Bowling *et al.* 2008: 59).

Da bi se kriminalitet mogao kontrolisati neophodno je da organi formalne, ali i subjekti neformalne socijalne kontrole raspolažu informacijama. Uloga veštačke inteligencije se tu posebno nameće kao značajna u situaciji kada prema relevantnim istraživanjima, količina raznorodnih informacija na svetu godišnje raste po stopi od 40 odsto (Branković, 2017: 7). Prema tome, svi karakteristični vidovi upotrebe veštačke inteligencije u kontroli kriminaliteta imaju cilj da prikupe podatke, sortiraju ih i obrade. Razlika postoji samo u pogledu načina na koji se do podatka dolazi i na koji se on obrađuje. Shodno navedenom, možemo razlikovati *prikupljanje i obradu podataka*, *video nadzor* i *biometrijske tehnologije*. Radi se o sada već tradicionalnim metodama za pribavljanje neophodnih podataka budući da su softverski pretraživači, evidencije i video nadzor u upotrebi nekoliko decenija unazad. Razvoj tehnologije i „intelektualnosti" mašina doveo je do toga da danas umesto o klasičnim programima za pretragu govorimo o tzv. „*big data*" pretraživačima, DNK profilisanje dobija konkurenciju u vidu forenzičkih metoda druge generacije, dok „novi nadzor" kako se u literaturi naziva, višestruko prevazilazi mogućnosti ranijih sistema za video nadzor.[14]

Prikupljanje podataka, vođenje evidencija i obrada smatraju se tradicionalnom funkcijom jedinica veštačke inteligencije. Tako su osnovne funkcije „inteligentnih agenata" da šetajući Web-om prikupe za korisnika što više podataka (*Web crawler*), da se infiltriraju u druge Web stranice i tamo pronađene podatke indeksiraju i čuvaju u sopstvenoj bazi podataka koju korisnik može jednostavno pretraživati (*Web spider*), kao i to da autonomno izvršavaju kompleksne zadatke koje im je poverio korisnik, što podrazumeva i obradu radnih podataka (*Web robot*) (Kuk, 2015: 133).

Specijalizovani roboti mogu biti od naročite koristi organima formalne kontrole, ukoliko se njihova uloga zadrži na pružanju pomoći. Tako je policija jednog okruga u Velikoj Britaniji u okviru pilot projekta, u svoje redove sredinom 2016. godine uvela robota-policajca po imenu HART (*eng. Harm Assesment Risk Tool).* Njegov glavni zadatak je da pomaže pri donošenju odluka o zadržavanju ili puštanju osumnjičenih lica iz pritvora. Broj neophodnih informacija koje treba uzeti u obzir je ogroman, a kada se to pomnoži sa nekoliko hiljada predmeta koliko je potrebno obraditi na godišnjem nivou, angažovanje veštačke inteligencije se nameće kao racionalno rešenje u cilju postizanja efikasnosti. HART koristeći svoju bazu podataka i specijalizovani algoritam deli osumnjičene u grupe formirane prema riziku od ponavljanja kažnjive radnje.[15] Odluku ipak

[14] Tako je nekada bilo uobičajeno da jedno lice dugotrajno posmatra više ekrana pokušavajući da uoči eventualne opasnosti, što je sa stanovišta fizičkih i bioloških karakteristika čoveka, izuzetno težak poduhvat.

[15] Vidi više u dokumentu: „European Commission for the Efficiency of Justice (CEPEJ) - European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment" koji je usvojen u decembru 2018. godine na plenarnoj sednici.

donosi čovek – nadležno lice, oslanjajući se na „mišljenje" HART-a, ne prepuštajući mu ulogu donosioca konačne odluke, što treba smatrati odgovarajućim rešenjem.[16]

Pametne sisteme za upravljanje podacima koriste i sudovi pojedinih zemalja. U naučnoj i opštoj javnosti je ukorenjeno mišljenje prema kojem je nekonzistentnost sudske prakse u donošenju odluka jedan od glavnih uzroka neuspeha u pokušajima da se potencijalni izvršioci krivičnih dela odvrate od svojih namera, odnosno da se uspešno rehabilituju (Berman & Hafner, 1989: 933). Zato je u jednoj od kanadskih provincija, Britanskoj Kolumbiji, kreiran sistem koji sadrži preko 40.000 sudskih odluka iz proteklih nekoliko godina. Interaktivni interfejs zahteva od sudije da u odgovarajuća polja unese podatke o delu koje je u pitanju, godinama okrivljenog, polu, bračnom statusu i ranijoj osuđivanosti, te da svoju odluku uskladi sa dobijenim rezultatima (Berman & Hafner, 1989: 933).

Video nadzor se smatra važnim mehanizmom situacione prevencije[17] i korelira sa aktuarijalnom paradigmom kontrole kriminaliteta zasnovanoj na praćenju rizika (Lyon, 2003: 8). Prvobitno su sigurnosne kamere postavljane kako bi se osigurao privatni kapital, najpre u bankama i prodajnim objektima, pa potom i na drugim mestima gde je postojala potreba za ovim vidom zaštite. Vremenom se video nadzor preneo i na javni prostor gde čini gotovo neizostavni sadržaj urbane infrastrukture (Žunić-Pavlović & Kovačević-Lepojević, 2010: 35). Video nadzor je u svom osnovnom obliku oličen u sistemu CCTV (*eng. closed circuit television*) koji se sastoji od kamera kojima se posmatra određeno područje, tehnologije koja omogućava prenos slike na monitore koji prenose sliku, snimanje i čuvanje digitalnih zapisa, uz učešće operatera koji prate prenos slike (po pravilu policajci ili pripadnici privatnog obezbeđenja) (Žunić-Pavlović & Kovačević-Lepojević, 2010: 35).[18]

Biometrijske tehnologije koje omogućavaju automatsku identifikaciju lica na osnovu njihovih individualnih bioloških karakteristika danas su u masovnoj upotrebi prilikom isleđivanja različitih zločina, pri čemu DNK profilisanje, usled svoje izražene preciznosti zauzima posebno mesto (Kovačević-Lepojević & Žunić-Pavlović, 2012: 89). Vremenom su mnoge države razvile nacionalne baze biološkog (najčešće DNK) materijala.

3.1. Razlozi osporavanja upotrebe veštačke inteligencije u kontroli kriminaliteta

Razlozi koji govore u prilog upotrebe veštačke inteligencije u aktivnostima organa formalne reakcije na zločin nisu upitni i prevashodno se odnose na *efikasnost* i *širi domašaj kontrole*. Oni predstavljaju odraz pragmatskog pristupa ne samo kada je reč o

[16] Imao i autora koji opisanom „pametnom sistemu" zameraju to što kao faktore rizika razmatra i one koji po opštem shvatanju ne bi trebalo da imaju preteranog uticaja na kriminalitet kao što je poštanski broj (Sushina & Sobenin, 2019: 435).

[17] To naročito važi za kriminološko-akademski prostor Velike Britanije (Kovačević-Lepojević & Žunić-Pavlović, 2012: 88).

[18] Reč je o osnovnim postavkama sistema, dok razvoj tehnologije pruža ogromne mogućnosti u pogledu načina unapređenja i automatizacije rada sistema.

kontroli kriminaliteta, već i kada se radi o širem društvenom kontekstu. Teško bi se racionalno moglo braniti stanovište da mogućnost pribavljanja i obrade velikog broja podataka ili primena CCTV sistema ne olakšavaju posao organima krivičnog gonjenja. Međutim, osnovano bi se moglo postaviti pitanje dozvoljene mere masovne i invanzivne upotrebe visoke tehnologije u smislu ostvarivanja negativnog uticaja na svakodnevni život ljudi. Kako je jedan od važnijih ciljeva krivičnog prava da zaštiti osnovne društvene vrednosti, predmet akademskog sporenja u vezi sa primenom veštačke inteligencije u kontroli kriminaliteta je kontradiktornost koja se ogleda u činjenici da se sa tom primenom po pravilu ugrožavaju upravo one vrednosti koje krivičnopravni mehanizam nastoji da zaštiti.

3.1.1. Normativno (ne)regulisanje „pametnih mašina"

Normativni problem koji se ogleda u nedostajućoj, nepotpunoj i nepreciznoj pravnoj regulativi predstavlja osnov svih daljih relativizacija i osporavanja. Kada je reč o pravnom regulisanju veštačke inteligencije, primetno je da je ona uglavnom *ad hoc* karaktera bez sistemskog sagledavanja svih pozicija. To možemo zaključiti iz činjenice da postoje brojni propisi koji segmentarno normiraju primenu različitih oblika veštačke inteligencije,[19] dok primera radi i dalje ne postoji jasan stav o deliktnoj odgovornosti „pametnih mašina"[20] odnosno o načinu na koji se osnovni instituti krivičnog prava na njih primenjuju.

Upravo krivično pravo podrazumeva i najmoćniju legalnu (formalnu) socijalnu kontrolu koju moderna civilizacija poznaje (Clark & Marshall, 1967: 23). Kako tvrde pojedini autori, ljudi u najvećem broju slučajeva osećaju strah od veštačke inteligencije iz razloga što ona nije subjekt krivičnog prava, odnosno krivičnopravne odgovornosti (Solum, 1992: 1231). Otuda usklađivanje kreiranja i funkcionisanja jedinica veštačke inteligencije sa normama krivičnog prava i postupka treba razumeti kao važan korak u njenom pravnom regulisanju. U osnovi bi tu trebalo razmotriti njihovu deliktnu sposobnost i osvrnuti se na pitanje da li je rastući stepen inteligencije mašina dovoljan osnov da ih učini subjektima koji su podložni krivičnoj odgovornosti (Hallevy, 2013: 174). Odgovor na prethodno postavljeno pitanje nužno otvara i raspravu na temu pravnog subjektiviteta „pametnih mašina" što višestruko prevazilazi domašaj krivičnog prava. Funkcionisanje veštačke inteligencije i dalje nije predmet zakonskog regulisanja kako u materijalnom[21] tako i u procesnom delu što sa jedne strane ostavlja veliku pravnu

[19] Trenutno je u formi predloga koji čeka da bude usvojen, tzv. Artificial Inteligence Act, koji će ako bude usvojen biti prvi propis na nivou EU koji na sveobuvatan način reguliše važne aspekte veštačke inteligencije.

[20] Istini za volju, u literaturi se mogu pronaći predlozi o tome kako odrediti deliktnu odgovornost jedinica veštačke inteligencije. Više o tome u: Hallevy, Gabriel. 2013. *When Robots Kill: Artificial Intelligence under criminal Law.* London: Northeastern Univerity Press of New England.

[21] Retke su zemlje koje su zakonom regulisale veštačku inteligenciju u masovnoj primeni kao što je to recimo slučaj sa auto industrijom. Nakon skandala koji je u SAD izazvala saobraćajna nezgoda u kojoj je poginuo vozač automobila dok je ono bilo u samovozećem režimu, tamošnja Uprava za državni autoput, transport i bezbednost (*National Highway Transportation and Safety Administration)*dala je tumačenje federalnog zakona prema kojem se sistem koji kontroliše vožnju može smatrati vozačem poput

prazninu u domenu koji *de facto* iziskuje zakonsku „pokrivenost" dok sa druge strane omogućava brojne zloupotrebe. Tako se recimo u literaturi navodi primer administracije bivšeg predsednika SAD, Džordža Buša (*George W. Bush*) koja je prva počela sa upotrebom bespilotnih letelica sa raketnim naoružanjem za izvršenja ubistava kako bi se izbegla krivičnopravna odgovornost (Barak, 2020: 64).[22]

3.1.2. Pitanje povrede zajemčenih ljudskih prava i pitanje etičnosti

Priroda upotrebe veštačke inteligencije je takva da *dehumanizuje* jednu od centralnih aktivnosti svake države, kontrolu kriminaliteta, na način da je suprotstavlja gotovo svim zajemčenim ljudskim pravima čija bi zaštita trebalo da predstavlja „kičmu" modernog sveta. Kod takvog stanja stvari, razumljiv je i očekivan skepticizam usmeren ka mašinama koje preuzimaju ulogu čoveka i „odlučuju" o pravima i obavezama koje su ljudi predvideli kako bi sebi uredili život u zajednici. Tu se naročito nameće pitanje ugroženosti prava na privatnost, pa je grupa autora članka sa ilustrativnim nazivom „Što je mnogo, mnogo je" (*eng. When enough is enough*) sa punim pravom upozorila na strahovite mogućnosti „mašina koje uče" da sa velikom preciznošću procenjuju starost, pol, zanimanje, interesovanja, emotivni status, pa čak i da predviđaju buduće kretanje u geografskom smislu, samo na osnovu podataka iz mobilnog telefona.[23]

ESLJP je u više navrata odlučivao o povredama prava na privatnost podnosilaca predstavki usled tajnog nadzora njihove komunikacije. U odluci donetoj u predmetu *S. and Marper v United Kingdom*[24] iz 2008. godine, navedeno je da je potrebno naročito osigurati poštovanje zajemčenih prava u vezi sa prikupljanjem i obradom ličnih podataka kada je u proces uključen automatizovani program, a da ta potreba nije ništa manja ni u slučaju kada se podaci koriste u „policijske svrhe". Dalje se ističe da nacionalna zakonodavstva moraju to pitanje pravno urediti na način da prikupljeni podaci budu relevantni, odnsono da budu u skladu sa ciljem zbog kojeg se prikupljaju i obrađuju. Smatramo da je ovom odlukom, kao jednom od prvih, koja se bavila pitanjem automatizovanih „pametnih programa" za prikupljanje i obradu podataka, postavljen dobra temelj za dalju sudsku praksu, kako kada je reč o ESLJP, tako i kada se radi o nacionalnim sudovima.

Polazeći od stava koji je zauzet u odluci *S. and Marper v United Kingdom,* ESLJP je u predmetu *Roman Zakharov v Russia*[25] iz 2015. godine, našao da postoji povreda prava na privatnost u slučaju kada je telefonski operater instalirao takvu opremu na osnovu koje bezbednosna služba države, bez prethodnog naloga suda, može pristupiti kominikaciji određenog lica u bilo kom trenutku. Vodeći se istim principima, ESLJP nalazi

čoveka. Vidi o tome više na: https://fortune.com/2016/02/10/google-self-driving-cars-artificial-intelligence/, [20.5.2022].

[22] Takva ubistva nazivaju se *extrajudical killing* upravo iz razloga što ih je teško procesuirati imajući u vidu nerešeno pitanje deliktne sposobnosti jedinica veštačke inteligencije.

[23] Navedeno prema: (Stanila, 2018: 24).

[24] S. and Marper v United Kingdom App no 30562/04 (ECtHR 4 December 2008.

[25] Roman Zakharov v Russia, App no 47143/06 (ECtHR 4 December 2015).

povredu prava na privatnost u predmetima *Szabó and Vissy v. Hungary*[26] iz 2016. godine i *Gaughran v. the United Kingdom*[27] iz 2020. godine, u slučaju kada se vrši tajni nadzor komunikacije posredstvom „pametnih programa" odnsono kada se na neograničeni period čuva biometrijski sadržaj kako bi on u eventualnom kasnijem krivičnom postupku bio upoređen sa prikupljenim dokaznim materijalom.

U osnovi, kada razmatra povrede konvencijskih prava, ESLJP, bez izuzetka primenjuje test kontrole poznat kao „tripartitni test." Da bi u skladu sa tim testom određena restrikcija prava bila opravdana, potrebno je da ona kumulativno bude *predviđena zakonom*, *propisana radi zaštite nekog legitimnog cilja* i *neophodna u demokratskom društvu*. Imajući to u vidu, teško je očekivati da mere poput prepoznavanja lica svih prolaznika, bez postojanja osnova ili osnovane sumnje da su učinioci kaznenog dela ili neograničenog čuvanja biometrijskih podataka kako bi ih eventualno kasnije „pametni" programi poredili sa prikupljenim materijalom i tome slično, mogu uspešno proći navedeni test.

Federalni biro za istrage (*eng. Federal Bureau of Investigation*) – FBI, u svom operativnom radu koristi sistem NGI (*eng. Next Generation Identification)* koji sadrži višemilionsku bazu podataka o otiscima prstiju koje povezuje sa konkretnim licima. Kako su to u jednoj prilici objasnili nadležni iz FBI, sistem ne pruža tačnu identifikaciju osoba za kojima se traga, već je njegova uloga da obezbedi listu kandidata, potencijalnih osumnjičenih, navodeći da ako „pravi kandidat" postoji u sistemu, on će se pojaviti u prvih 50 koje je sistem označio. Upotreba opisanog sistema koji se zasniva na veštačkoj inteligenciji izazvao je reakcije javnosti koja je sa pravom problematizovala način obrade i čuvanje podataka onih „kandidata" za koje se ispostavi da nisu traženi. (Prlja *et al.* 2021: 83).

Praksa korišćenja algoritama za procenu rizika od ponavljanja dela ukazala je i na tendenciju diskriminišućeg postupanja prema određenim grupama, konkretno pripadnicima Afroameričke populacije u pojedinim federalnim državama SAD gde je u obaveznoj primeni softver COMPAS (*eng. Correctional Offender Management Profiling for Alternative Sanctions*). Naime, iako je za pripadnike navedene rasno-etičke grupe stepen rizika od ponavljanja dela na osnovu upitnika koji čini sastavni deo algoritma, po pravilu bio višestruko veći nego kod ostalih, dvogodišnja praksa je pokazala da su zapravo Afroamerikanci proporcionalno manje ponavljali krivična dela u odnosu na druge.[28]

Diskriminatorno postupanje primetno je i u bezbednosnom diskursu koji je vremenom formiran upravo na osnovu unetih podataka za kreiranje algoritama. Tako je na primer, nakon „11. septembra" nemački zakonodavac vođen strahom od potencijalnih terorističkih napada usvojio paket anti-terorističkih zakona uvodeći kroz njih u zakonodavstvo pojam „spavajućeg teroriste" koji je koncipiran tako da sadrži karakteristike prosečnog pripadnika islamske veroispovesti. Uz pomoć posebno kreiranih algoritama mnogi Muslimani koji su živeli u Nemačkoj bili su praćeni i podaci o njima bili su korišćeni za preventivno reagovanje nadležnih organa na „terorističku pretnju" (Završnik, 2019: 627).

[26] Szabó and Vissy v. Hungary App no 37138/14 (ECtHR 6 June 2016).

[27] Gaughran v. the United Kingdom App no 45245/15 (ECtHR 13 June 2020).

[28] Vidi više o tome na: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c [20.5.2022].

Pitanje etičnosti pri korišćenju veštačke inteligencije važno je tema naročito kada se radi o oblasti kaznene reakcije. Tako je primera radi Evropska komisija u jednom od svojih dokumenata koji je posvećen njenoj upotrebi u pravosuđu definisala pet osnovnih principa za obezbeđivanje etičnosti. Prvi se odnosi upravo na poštovanje fundamentalnih ljudskih prava, dok preostala četiri podrazumevaju zabranu diskriminatornog postupanja, obezbeđivanje kvaliteta i sigurnosti, odnosno transparentnosti.[29]

3.1.3. Uticaj na sudski (dokazni) postupak i „due process" garantije

Upotreba tehnoloških inovacija utiče i na krivični postupak na način da po prirodi stvari, podriva civilizacijsku tekovinu tzv. *due process* garantija.[30] Nepoverenje u tužioce i sudije i sporost tradicionalnog krivičnog postupka u kojem se presuda zasniva samo na činjenicama u koje je sud uveren iako je javnost već „presudila" okrivljenom, polako su u središte dokaznog postupka postavili prirodne nauke zato što se rezultati bioloških, mašinskih i drugih forenzičkih ispitivanja smatraju „objektivnom istinom." Vremenom je primećeno da se čak i sudovi sve više oslanjaju i pozivaju na tu „istinu" pri donošenju odluka zanemarujući osnovne procesne principe što je nazvano „CSI efektom"[31] (Stephens, 2006: 591). U literaturi se ističe još jedan sindrom, tzv. „crne kutije" (Završnik, 2020: 568) koji ukazuje na netransparentnost u donošenju odluka koje bi trebalo da se donose u ime naroda, upravo iz razloga tehnološke kompleksnosti veštačkih sistema koji prete da preuzmu ulogu sudija.

Težnja ka objektivizaciji i ubrzanju postupka komplementarna je akturijalnoj kontroli kriminaliteta kojoj procesne garantije predstavljaju svojevrsni balast. Posledica nekritičkog uzdizanja značaja pomoćnih instrumenata suda za donošenje odluka je da se proces odlučivanja premešta izvan klasičnog, pravilima uređenog krivičnog postupka, pa se kako to piše Mirjan Damaška, nominalni sluga suda preobraća u njegovog gospodara (Damaška, 1997: 151). Da stvar nije čisto teorijske prirode pokazuje i odluka Vrhovnog suda države Viskonsin (*eng. Wisconsin*) koja je doneta u predmetu *State v Loomis*[32] 2016. godine. Sistem zasnovan na veštačkoj inteligenciji, COMPAS, je okrivljenog prepoznao kao osobu visokog rizika po bezbednost zajednice, te je njegov zahtev za uslovnim otpustom u prvom stepenu bio odbijen. Odlučujući po žalbi, sud najviše instance u Viskonsinu je potvrdio odluku prvostepenog suda navodeći da preporuka sistema COMPAS nije jedini razlog za odbijanje zahteva za puštanje na uslovni otpust i da se imajući to u vidu ne može tvrditi da su osuđenom povređena bilo kakva procesna prava. Sa

[29] Reč je o dokumentu Evropske komisije pod nazivom „European Commission for the Efficiency of Justice (CEPEJ) - European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment" koji je usvojen u decembru 2018. godine na plenarnoj sednici.

[30] Pod tim naročito podrazumevamo presumpciju nevinosti, jednakost procesnih instrumenata i određeni stepen sumnje za preduzimanje formalnih radnji u postupku.

[31] U literaturi se navodi kako su nazivu doprineli mnogobrojni detektivski filmovi koji tzv. „rešavanje slučajeva" zasnivaju na volšebnim forenzičkim dokazima, glorifikujući pri tom njihovu ulogu (Chin & Workewych 2016).

[32] State v Loomis 881 N.W.2d 749 (Wis. 2016).

druge strane, sasvim drugačiji pristup zauzima Apelacioni sud u Kanzasu (*eng. Kansas*) kada je usvojio žalbu osuđenog u predmetu *State v Walls*[33] iz 2017. Godine, zbog povrede osnovnih prava u krivičnom postupku, budući da mu sud odlučujući o uslovima određivanja probacije, nije omogućio pristup softveru koji na osnovu određenih parametra sudu predlaže uslove probacije, jer iz tog razloga nije bio u prilici da eventualno ospori informacije do koji je došao „pametni sistem".

3.1.4. „Moravecov Paradoks"

Iako na prvi pogled to može delovati začuđujuće, „pametne mašine" često nisu u stanju da uspešno obavljaju aktivnosti koje se kada je čovek u pitanju smatraju rutinskim. Hans Peter Moravec (*Hans Peter Moravec*) ponudio je jedinstveno objašnjenje ovog fenomena, te je on kako to obično biva i nazvan po njemu. Ovaj austrijski autor svoje objašnjenje suštinski zasniva na Teoriji evolucije i navodi da je za obavljanje radnji koje ljudima deluju rutinski poput prepoznavanja lica, glasova, orijentacije u prostoru i vremenu, razlikovanje prostih objekata, potreban ogroman broj resursa i ulaznih podataka ne bi li se na osnovu njih formirao algoritam, a onda i program pomoću kojeg bi te aktivnosti kao rutinske obavljala i mašina. Kada je čovek u pitanju, intelektualne i motoričke sposobnosti neophodne za automatsko vršenje takvih aktivnosti razvijane su stotinama hiljada godina, što nije slučaj sa robotima i mašinama pa je potrebno mnogo vremena kako bi i jedinice veštačke inteligencije povećale nivo automatizacije prilikom obavljanja takvih radnji (Rotenberg, 2013: 108).

U praksi kontrole kriminaliteta se upravo najčešće obavljaju rutinske aktivnosti i to naročito kada je reč o prevenciji zločina. U tom smislu je važna napomena o tzv. „Moravecovom Paradoksu" koja na konkretnom planu ukazuje da roboti i mašine sa veštačkom inteligencijom ne mogu istisnuti čoveka kao nosioca svih analitičkih i operativnih aktivnosti. Naprotiv, njihova uloga trebalo bi da se iscrpi obavljanjem specifičnih zadataka koji prevazilaze prosečne psiho-fizičke osobine čoveka u cilju efikasnosti, kada to nije u suprotnosti sa zakonom.[34]

ZAKLJUČAK

Da bi aktivnosti i postupci u okviru kontrole kriminaliteta mogli da budu efikasni neophodno je da budu adaptirani na društvenu realnost. Tehnološke inovacije su svojevrsna konstanta društvenog života, pa je usled toga potrebno i da se organi krivičnog gonjenja prilagode takvoj situaciji. Načelno se može reći da je odgovarajuća reakcija na nove vidove kriminaliteta, naročito one koji se pripremaju i izvršavaju na mreži (*eng. online crimes*), gotovo nezamisliva bez korišćenja novih tehnologija.

[33] State of Kansas v. John Keith Walls, 116,027, The Court of Appeals of the State of Kansas (2017).

[34] Tu primera radi, mislimo na obradu velikog broja podataka u kratkom vremenskom periodu, tačno prepoznavanje određenih karakteristika lica i stvari iz velikog broja uporednih karakteristika i tome slično.

Društveno-ekonomski činioci formatirani u okvirima procesa globalizacije i liberalnog modela inicirali su, između ostalog, i osećaj straha i nesigurnosti kod ljudi, što je dalje vodilo ka etabliranju „kaznenog populizma" kao poželjne političke agende kada je reč o formalnoj kaznenoj reakciji na kriminalitet. Paralelno je razvijan i koncept aktuarijalne kontrole koji podrazumeva najekonomičnije i najefikasnije metoda otklanjanja rizika od inkriminisanih radnji. U tom smislu, „pametne mašine" su se nametnule kao efikasan odgovor na izazove koje donosi tzv. „izmenjena fenomenologija kriminaliteta", odnosno današnje „globalizovano društvo".

U kontekstu reakcije na kriminalitet, primena veštačke inteligencije je čini se, u značajnoj meri uticala na prirodu kaznenog mehanizma na način da su tradicionalne osnove i ciljevi krivičnog prava izloženi redefinisanju. Aktuelni društveno-ekonomski činioci doprineli su razvoju takve tendencije u krivičnom pravu koja ide ka tome da uklanjanje svake vrste opasnosti bez obzira na posledice, nameće kao osnovnu vrednost i funkciju krivičnog prava. Tu po prirodi stvari, pitanja koja se tiču resocijalizacije, reintegracije, tretmana i uopšte korektivne uloge krivičnog prava ostaju u drugom planu, pri čemu bi se kod takvog stanja stvari mogla očekivati progresija različitih devijantnih ponašanja, a što bi problem postojanja različitih oblika kriminaliteta samo multiplikovalo.

Matematička tačnost i objektivnost koja je svojstvena prirodnim naukama pominju se kao prednosti primene visoke tehnologije, između ostalog i u borbi protiv različitih oblika kriminaliteta. Ipak, imajući u vidu sve okolnosti te primene, koje se u osnovi tiču i kreiranja algoritama, interpretacije dobijenih rezultata i tehnološke nesavršenosti „pametnih mašina", čini se da mogućnosti koje veštačka inteligencija pruža nikako ne bi trebalo da budu odbačene bez analize stvarnih koristi po efikasnost krivičnog postupka imajući u vidu aktuelno stanje tehnike i normativne uređenosti društva.

Upotreba veštačke inteligencije se zbog svoje osobenosti uklapa u danas dominantan sistem ideja o reagovanju na kriminalitet. Međutim, analiza sudske prakse dva najuticajnija suda za Evropu i SAD, pojedinih ključnih odluka iz ove oblasti pokazuje da normativni okvir ne podržava apsolutni pragmatizam krivičnog mehanizma koji bi bio oličen u upotrebi „pametnih mašina". Problem po pravilu nastaje na polju zaštite prava na privatnost (kada govorimo o implementiranju algoritama za prepoznavanje lica, zvuka, glasa i slično), odnosno na polju mogućnosti pre svega okrivljenog, da ospori sadržaj koji algoritam pretvara u svojevrsni rezultat, a na koji se sud oslanja pri donošenju odluka. Na taj način se, na prvom mestu, grubo zadire u pravo okrivljenog na odbranu, što bi trebalo tretirati kao njegovo osnovno pravo. Imajući uz to u vidu i da gotovo nijedno zakonodavstvo nije do kraja rešilo pitanje deliktne sposobnosti jedinica veštačke inteligencije, možemo opštu polaznu pretpostavku od koje se pošlo prilikom pisanja ovog rada pretvoriti u zaključak. Efikasnost i objektivizacija koji karakterišu veštačku inteligenciju savršeno odgovaraju akturaijalnoj paradigmi kontrole kriminaliteta, dok za sada, normativni okvir (primena materijalnog prava, procesnih pravila, osnovnih načela krivičnog prava i postupka, zaštita zajemčenih ljudskih prava) ne daju previše prostora za njenu upotrebu na legalnoj osnovi. U svakom slučaju, nakon analiziranih osnovnih elemenata uloge veštačke inteligencije u kontroli kriminaliteta, zaključak je da njena

upotreba može imati značajan doprinos u pružanju pomoći organima formalne socijalne kontrole (prikupljanje i obrada velikog broja informacija u kratkim rokovima i sl.), s tim da se donošenje odluka bez izuzetaka treba ostaviti u isključivu nadležnost ljudi.

LITERATURA

1. Barak, G. (2020) *Nekontrolisana moć korporacija - Zašto su zločini multinacionalnih korporacija rutinizovani i šta sa tim u vezi možemo učiniti*. Beograd: Pravni fakultet Univerziteta u Beogradu.
2. Berman, D., Hafner, C. (1989) „The potential of artificial intelligence to help solve the crisis in our legal system", *Communications of the ACM*. 32: 928-938.
3. Bowling, B., Marks, A., Murphy, C. C. (2008) „Crime Control Technologies: Towards an Analytical Framework and Research Agenda" *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes,* (Roger Brownsword, Karen Yeung. ed.) Oxford: Hart Publishing. 51-78.
4. Branković, S. (2017) „Veštačka inteligencija i društvo". *Srpska politička misao. No. 2,* 56: 13-32.
5. Castells, M. (2000) Materials for an explorator y theory of the network society. *British Journal of Sociolog.* No. 1, 51, 5-24.
6. Chin, J., Workewych, L. (2016) „The CSI Effect", *The Oxford Handbook Online,* (Marcus Dubber ed.) Oxford: Oxford University Press. 1-39.
7. Clark, W., Marshall, W. (1967) *A Treatise on the Law on Crimes*. 7 ed. Callaghan: Mundelein III.
8. Damaška, M. (1997) *Evidence Law Adrift*. New Haven: Yale University Press.
9. Damnjanović, I. (2012) „Terorizam i tehnologija", *Terorizam kao globalna pretnja*. Beograd: Centar za bezbednosne studije, 340-352.
10. Feeley, M., Simon, J. (1992) „The New Penology: Notes on the Emerging Strategy of Corrections and Its Implications" *Criminology*. 30: 449-474.
11. Grabosky, P. (1998) „Technology and Crime Control", *Trends and Issues in Crime and Criminal Justice*. 58: 2-6.
12. Hallevy, G. (2013) *When Robots Kill: Artificial Intelligence under criminal Law*. London: Northeastern Univerity Press of New England.
13. Hudson, B. (2002) „Punishment and Control" *The Oxford Handbook of Criminology*, (Mike Maguire, Rod Morgan, Robert Reiner (ed.) Oxford: Oxford University Press. 233-263.
14. Ignjatović, Đ. (2003) „Kriminalitet i reagovanje države", *Bezbednost*, No. 4, 1-14.
15. Ignjatović, Đ. (2018) „Kontroverze kazne zatvora i njeno izvršenje", *Sociologija*, No. 4, 60: 750-768.
16. Jones, T. (2009) *Artificial Intelligence: A System Approach*. Burlington: Jones & Bartlett Publishers.

17. Kamarinou, D., Millard, C., Singh, J. (2016) „Machine Learning with Personal Data", *Legal Studies Research Paper* 247: 2-23.
18. Karstedt, S. (2014) „Organizing Crime-The State as Agent", *The Oxford Handbook of Organized Crime,* (Letizia Paoli. (ed.)), Oxford: Oxford University Press. 303-321.
19. Kemeny, G. (1972) *Man and the Computr.* New York: CharlesScribner's Sons.
20. Kuk, K. (2015) Veštačka inteligencija u prikupljanju i analizi podataka u policiji. *Nauka, bezbednost, policija*. No. 3, 20: 131-148.
21. Lyon, D. (2003) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination.* London: Routledge.
22. Marks, A., Bowling, B., Keenan, C. (2015) „Automatic Justice? Technology, Crime and Social Control" *The Oxford Handbook of the Law and Regulation of Technology,* (Roger Brownsword, Eloise Scotford, Karen Yeung eds.), Oxford: Oxford University Press. 1-34.
23. Prlja, D., Gasmi, G., Korać, V. (2021) *Veštačka inteligencija u pravnom sistemu EU*. Beograd: Institut za uporedno pravo.
24. Rock, P. (2002) Sociological Theories of Crime. *The Oxford Handbook of Criminology*, (Mike Maguire, Rod Morgan, Robert Reiner. (ed.)) Oxford: Oxford University Press. 51-83.
25. Rose, N., Miller, P. (1992) „Political Power beyond the State: Problematics of Government", *British Journal of Sociology*, 43: 173-205.
26. Rotenberg, S. V. (2013) „Moravec's Paradox: Consideration in the Context of Two Brain Hemisphere Functions", *Activitas Nervosa Superior.* No. 3, 55: 108-111.
27. Russel, S., Norvig, P. (2010) *Artificial Intelligence: A Modern Approach*. 2 ed. N.J: Prentice Hall.
28. Scherer, M. (2016) „Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies", *Harvard Journal of Law & Technology.* No. 2, 29: 354-398.
29. Sherman, L. W., (2013) „The Rise of Evidence-based Policing: Targeting, Testing, and Tracking", *Crime and Justice*. 42: 377-451.
30. Simon, J. (2002) „Governing Through Crime Metaphors", *Brooklyn Law Review. 67*: *1035-1070.*
31. Simon, J. (2007) *Governing Through Crime.* Oxford: Oxford University Press.
32. Simović-Hiber, I. (2016) „Ogled o krivičnom pravu i vladavini prava na primeru načela zakonitosti – retrospektiva i perspektive", *CRIMEN*. No. 3. 237-257.
33. Soković, S. (2011) „Savremene globalne tendencije u kontroli kriminaliteta" *CRIMEN*, No. 2, 212-226.
34. Solum, L. (1992) „Legal Personhood for Artificial Intelligences", *North Carolina Law Review*, 1231-1287.
35. Stanila, L. (2018) „Artificial Inteligence and Human Rights. A Challenging Approach on the Issue of Equality", *Journal of Eastern-European Criminal Law.* No. 2, 19-31.

36. Stephens, S. L. (2007) „The "CSI effect" on real crime labs", *New England Law Review*, 41: 591-608.
37. Stuntz, J. W. (2001) „The Pathological Politics of Criminal Law", *Michigan Law Review*. No. 3, 100: 506-598.
38. Sushina, T., Sobenin, A. (2020) „Artificial Inteligence in the Criminal Justice System: Leading Trends and Possibilities", *Proceedings of the 6th International Conference on Social, economic, and academic leadership*. Atlantis Press. 432-437.
39. Tilovska-Kechedji, E., Kolaković Bojović, M., Čvorović, D. (2018) Artificial Inteligence influencing foreign Policy and Security. *Journal of Eastern-European Criminal Law*. No. 2, 7-19.
40. Wall, S. D. (2015) „Dis-Organised Crime: Towards a Distributed Model of the Organization of Cybercrime" *The European Review of Organised Crime*. No. 2, 71-90.
41. Wilson, M. (1969) *The essential Descartes*, New York : New American library.
42. Završnik, A. (2019) „Algorithmic justice: Algorithms and big data in criminal justice settings", *European Journal of Criminology*. 18(5): 623-642.
43. Završnik, A. (2020) Criminal justice, artificial inteligence systems, and human rights. *ERA Forum* 20: 567–583.
44. Žunić-Pavlović, V,, Kovačević-Lepojević, M. (2010) „Mere javnog nadzora u službi prevencije kriminala", *Zbornik Instituta za kriminološka i sociološka istraživanja*. No. 1-2, 29: 31-51.
45. Žunić-Pavlović, V., Kovačević-Lepojević, M. (2012) „Primena video-nadzora u kontroli kriminala", *Zbornik Instituta za kriminološka i sociološka istraživanja*. No. 2, 11: 325-345.

Internet izvori

1. https://www.keycrime.com/about-us, [20.5.2022].
2. https://fortune.com/2016/02/10/google-self-driving-cars-artificial-intelligence/, [20.5.2022].
3. https://rs.n1info.com/vesti/a584070-odrzana-prva-skajp-sudjenja-struka-upozorava-krse-se-prava-okrivljenih/, [20.5.2022].
4. https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c, [20.5.2022].

Legislativa

1. „European Commission for the Efficiency of Justice (CEPEJ) - European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment" usvojen u decembru 2018. godine na plenarnoj sednici.

ARTIFICIAL INTELLIGENCE AND ITS ROLE IN CRIME CONTROL

This Article is focused upon a artificial intelligence and its potential impact on legal practice when it comes to the crime control issues. In the light of this, the author has attempted to analyze a conceptual framework for the law and regulation in the context of artificial intelligence and crime control through a criminological prism. Recent technological innovations have exacerbated tensions in the traditional model of criminal justice to the point that basic principles of criminal justice were subjected to redefining. For instace, a departure from the individually oriented doctrine with an increasingly intense acceptance of the actuarial paradigm supports the previously stated thesis. Regardless of the efficiency of the application of artificial intelligence in the field of crime control, the threat of certain basic human rights as well as due process guarantees is increasingly noticeable. This derives from the fact that artificial entity could not be equalized to the human beings. Smart machines, apart from a high degree of intelligence, do not have other human features such as identity, experience, integrity, attitudes, morals, creativity, motivation, emotions, habits, obsessions etc. Mirroring the normative and regulatory aspects of this rapidly developing field we have found that the application of science and technology to the crime control raises more debatable issues. In our view, we need to think more carefully about the broader social impact of 'crime control technologies' in order to ensure human rights respect.

KEYWORDS: *artificial intelligence, technology, crime, crime control.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.24

ALGORITHMIZING CRIMINAL LAW: WHAT IS LEFT TO HUMAN JUDGMENT

Yannis Naziris*

Algorithms have been used in criminal cases, while their use is expected to expand over the coming years. A case in point is sentencing, which will exceedingly rely on risk-assessment tools. There have been certain downsides, of course: aside from what many term as an 'inhuman' way of meting out justice, flaws also emerge in terms of the efficiency of such systems, especially taking into account the biases that are embedded therein.

Digital systems are put together to facilitate judicial cooperation in cases featuring cross-border elements. Setting aside security issues, these systems are mostly effective in those fields, but human intervention will still be required in the foreseeable future. There simply appear to be matters where human intervention is indispensable.

Reducing sets of rules to algorithms proves to be an effective way of teaching law (among other disciplines). Yet there are certain perils to this approach: for instance, it may lead to rote memorization of processes as opposed to cultivating the ability to delve into the system's logic.

These areas appear only superficially related. However, there may be a common reason underlying the limits of algorithms. Explaining why algorithms fall short presupposes a fundamental understanding of key areas which should be left to human judgment, at least for the time being. This paper will draw on some experience working with those systems in research projects and in teaching to outline these areas. Although the themes underlying this subject affect various fields of law, the emphasis will be on criminal law.

KEYWORDS: *human weaknesses, machine strengths, drafting the algorithm, substantive and procedural law as a "continuum", "feeding" the algorithm, types of "judgments".*

* PhD, Ass. Professor of Substantive & Procedural Criminal Law, Aristotle University Law School, Thessaloniki. E-mail: *jnaziris@law.auth.gr*

INTRODUCTION

Artificial Intelligence is expected to radically change a whole host of domains, including law. The legal profession will no doubt be affected by improvements in AI, although it may be premature to declare the 'end of lawyers' yet (Susskind, 2010)[1] More modest approaches, however, are already making headway in various legal fields. Our focus in this piece will be on criminal law, but the implications of the pertinent discussion are equally relevant to other fields.

Algorithms have been used in criminal cases, while their use is expected to expand over the coming years. A case in point is sentencing, which will exceedingly rely on risk-assessment tools Ryberg & Roberts: 2022; Chohlas-Wood: 2022) There have been certain downsides, of course: aside from what many term as an 'inhuman' way of meting out justice, flaws also emerge in terms of the efficiency of such systems, especially taking into account the biases that are embedded therein (Bagaric, Hunter, Stobbs, 2020;,] (Shi, 2022: 121).[2]

Digital systems are put together to facilitate judicial cooperation in cases featuring cross-border elements.[3] Setting aside security issues, these systems are mostly effective in those fields, but human involvement will still be required in the foreseeable future. There simply appear to be matters where human intervention is indispensable.

Reducing sets of rules to algorithms has proved to be an effective way of teaching law (. Johnson, Shen, 2021) (among other disciplines). Yet there are certain perils to this approach: for instance, it may lead to rote memorization of processes as opposed to cultivating the ability to delve into the system's logic. Besides, if sets of rules are reduced to algorithms, there would be little point in training future lawyers, since the bulk of their tasks would be performed with limited human intervention (or none whatsoever).

These areas appear only superficially related. However, there may be a common reason underlying the limits of algorithms. Explaining why algorithms fall short presupposes a fundamental understanding of key areas which should be left to human judgment, at least for the time being.

A relatively moderate approach involving the application of algorithms in criminal law would entail the creation of decision trees, incorporating sets of rules with the accompanying case-law. Even an approach as simple as this might go a long way towards simplifying the application of legal rules, while making them more accessible to the average layperson.

---

[1] That is not to say, of course, that adjustments of the legal profession to, among other things, technological disruptions are not called for.

[2] ., D. Kehl et al 'Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing', Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School, available online at: https://dash.harvard.edu/handle/1/33746041 [31.10.2022].

[3] Artificial Intelligence supporting Cross-Border Cooperation in Criminal Justice, Joint Report prepared by eu-LISA and Eurojust, 2022, available online at: https://www.eurojust.europa.eu/sites/default/files/assets/artificial-intelligence-cross-border-cooperation-criminal-justice-report.pdf [31.10.2022].

The paper will begin with a discussion of human weaknesses, which may be overcome with the help of machine learning. Subsequently, word will be made of modes of legal reasoning, persisting problems, and differing approaches as to drafting an algorithm, as well as 'feeding' it with data. A case in point which will be used is the extent of criminal jurisdiction (which features an international law as well as a criminal law prong), coupled with the rules governing the competence of courts *ratione loci* (which is a body of law belonging to domestic criminal procedure). This will enable us to present substantive and procedural rules as a continuum, in contrast to the traditional view treating these disciplines as related but distinct from each other. Lastly, we will ponder about possible weaknesses inherent in machine learning, which may be offset by the human intellect. This will allow us to at least sketch the areas that will be left (at least for the foreseeable future) to human judgment (albeit a judgment augmented by AI 'prosthetics'). This is the modest ambition of this contribution.

1. HUMAN WEAKNESSES, MACHINE STRENGTHS

If intelligence is understood as the ability to collect and classify knowledge, with a view to solving problems of varying complexity,[4] then Artificial Intelligence (AI) is already on its way to at least matching – if not surpassing – human intelligence. Even in its classical, symbolic form (Boden, Frankish, Ramsey, 2014),[5] AI has been able to tackle problems with increasing ease compared to humans. Adding to the picture, novel approaches have made it possible for AI applications to infiltrate virtually all areas of human intellectual effort. AI is no longer confined to ensuring the integrity of information systems [as, for instance, in network intrusion detection] but is actively involved in, among other areas, medicine, finances, statistical analysis, and so forth (Friedrich *et al.* 2021: 424; Nichols, Chan, Baker, 2019: 111; Sarker, 2022: 158). Its successes are owed to developments in areas such as language [especially semantic information processing], perception [enabling pattern recognition], modeling [based on internal representations], and so forth (Minsky (ed.) 1968). Even though the 'singularity' is still not at sight, all types of AI envisaged (Bostrom, 2014: 64). appear to be on the rise: whether based on speed [i.e. the ability to do everything a human does, only much faster]; collective thinking [i.e. being able to amass all the knowledge available to individuals, within the grasp of one entity]; or quality [i.e. being able to perform novel tasks, beyond the reach of the human brain]. Truth be told, even the so-called 'weak AI'[6] that is available today is much stronger than humans in certain activities,

[4] This would not be too far from the standard definition of intelligence: see, e.g., the definition of 'intelligence' provided by the Cambridge Dictionary "the ability to learn, understand, and make judgments or have opinions that are based on reason".

[5] The symbolic form of AI is sometimes referred to as 'good old-fashioned AI' or GOFAI, for short. This term (and the type of AI it denotes) should not be identified with AI in general, which would also include a number of other approaches, such as connectionism (with its variations), evolutionary programming, etc.

[6] 'Weak AI' (also known as 'narrow AI') is limited to a specific area, as opposed to 'strong AI', which will amount to 'human-level' or 'general intelligence'.

including computation, swift research in vast databases, cataloguing data retrieved, recognizing correlations between pieces of data,[7] and many others.

As things currently stand in the legal profession(s), there are certain areas which appear to be dominated by AI. These include (but are not limited to, certainly not with a view to the proximate future) (Susskind, 2019).

- Legal research: AI significantly reduces the time needed to survey voluminous data consisting in statutory law, decided cases, briefs, and other sources of information. In addition, it classifies the data retrieved in a manner that is useful, as opposed to merely listing entries.
- Case outcome prediction: it has already become possible (within certain boundaries) to trace patterns in the text of court decisions with a relatively high degree of precision.[8] One interesting finding arising from similar projects is that the language employed and the circumstances involved were more reliable factors in predicting the outcome of given case compared to the legal rule invoked.[9]
- Analytics: Dissecting data derived from millions of cases is already providing lawyers valuable insights, even short of predicting case outcomes. Relying on this data is helpful in putting together arguments, drafting legal documents, etc.
- Contract AI: The lack of uniformity in terms of drafting contracts is a perennial issue for lawyers and law firms. The use of drafting tools helps eliminate ambiguity, while machine learning enables users to visualize the risks involved, with the goal of minimizing them, and significantly expedite the review process.
- Practice management: Even though it may be somewhat premature to declare the end of lawyers, AI tools will soon make redundant human paralegal services. The activities in this domain are already being automated, and it will not be long before one software specialist supervising a machine will have replaced armies of paralegals (Kauffman & Soares, 2020: 223).[10]

Whether in academia, in the courtroom, or in everyday legal chores, AI comes with obvious benefits, that cannot easily be outweighed by human capabilities. Regardless of what one may think of the possible dangers inherent in AI infiltrating various domains, it may not be placed in doubt that it will benefit the legal domain by virtue of, inter alia:

---

[7] Which would enable correlation between rule with data / comparative presentation between outcomes of cases / correlation with other fields [medicine, economics], eliminating the need for an expert opinion.

[8] Artificial Intelligence and the Legal Profession [horizon scanning], p. 6. A.D. Reiling, 'Courts and Artificial Intelligence', International Journal for Court Administration, available online at: https://www.iacajournal.org/article/10.36745/ijca.343/ [31.10.2022].

[9] N. Aletras / D. Tsarapatsanis / D. Preoţiuc-Pietro / V. Lampos, 'Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective', PeerJ Computer Science 2:e93, available online at: https://peerj.com/articles/cs-93/ [31.10.2022].

[10] B. Alarie / A. Niblett / A. Yoon, 'How Artificial Intelligence Will Affect the Practice of Law', available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3066816 [31.10.2022].

- Enhancing speed through the automation of multiple activities, either of auxiliary or principal import.
- Improving accuracy, at least in terms of activities involving calculation [which, one might argue, are the only ones where accuracy may validly be expected].
- Releasing humans from the toil of mundane and/or repetitive tasks.
- Ensuring uniformity by algorithmizing (thereby standardizing) a number of processes relating to legal practice.
- Broadening the audience to which legal norms and their application are accessible. In a sense, algorithmizing a process is more 'democratic', in that it helps even those unfamiliar with key concepts apply basic legal rules [that the same route may lead to lawyers becoming obsolete is an unfortunate side effect (or fortunate, depending on one's point of view)].

2. LEGAL RASONING IN THE AI AREA/TOP-DOWN [RULE-BASED] OR BOTTOM-UP [FACT-BASED] APPROACH

Problem-solving in the legal domain is among the ideal areas for the development of AI applications. Indeed, legal reasoning appears to be quite receptive to machine learning technologies, given that it is formal and multi-modal (Rissland, 1990: 1957) at the same time, however, it encompasses a human element that eludes mere computation. Thus, merely improving computational ability will not be enough to achieve helpful results in terms of legal problems; rather, the solutions are expected to radically improve as AI approaches (or exceeds) human-level intelligence.

Since its inception, AI has been developed based on various modes of reasoning (or combinations thereof) (Buchanan & Headrick, 1970: 40). Several of these modes are also employed in legal reasoning, though with necessary adjustments (Koenig & Mandell, 2022: 559).

Accordingly, one may allude to deductive, inductive, or abductive reasoning; reasoning by analogy, contradiction, or generalization; conditional, modal, or deontic reasoning; and several others, without even mentioning rhetorical structures, which quite often function as a supplement to (or substitute for) modes of reasoning (Bibel, 1993, *passim*; Engle, 2003; Sunstein, 2001: 29; Weinreb, 2012, *passim*.).[11]

Of course, the perennial desideratum that these modes of reasoning aspire to attain is to solve real-life problems by means of legal rules. The two (primary) forms of legal reasoning which have been put to work in the legal domain are deductive reasoning and analogical reasoning.

Deductive reasoning is essentially a top-down approach which starts with a general premise, which is applied to a set of given facts in order to arrive at secure conclusions. In the legal domain, one starts with a rule, which it applies to the facts of the case,

[11] See indicatively M. Aikenhead, *Legal analogical reasoning – the interplay between legal theory and artificial intelligence*, 1997, available at Durham E-Theses Online: http://etheses.dur.ac.uk/5462/ [31.10.2022].

arriving at a (legal) conclusion that enjoys broad acceptance, since it is the product of a robust syllogism. Deductive reasoning gained traction in Europe alongside the scientific revolution, especially among those subscribing to rationalism (Aune, 1970). This is not surprising, since it combined general presuppositions about society with an ostensibly scientific method leading to (at least the illusion of) legal certainty.

Analogical reasoning, on its part, essentially consists in reasoning by example, aspiring to ensure equal treatment of similar cases. Reasoning by analogy entails three stages (given an actual problem): firstly, one starts (not with a rule but rather) with a 'base' situation from which to reason further; secondly, one must identify the factual similarities (as well as the differences) between the 'base' situation and the 'problem' situation; thirdly, one must assess the importance of the similarities between the two situations, and decide whether they outweigh the differences, in which case the 'base' situation shall be held to control in the problem situation. Reasoning in this way does not begin with general presuppositions about the world at large or about society. Rather, it is highly situational, in that its application almost entirely hinges on the context of each particular situation. From the outside, this may appear to run contrary to legal certainty, which to some extent is true, but is counterbalanced by this mode's adaptive force. It is no wonder, then, that this form of reasoning has gained prevalence in common law jurisdictions, in which pragmatism trumps scientific or ideological preconceptions (Lamond, 2014: 567).

Experience shows that, regardless of the mode of reasoning, certain issues remain open. One might classify those issues in two categories: first, there are 'definitional' issues, whose resolution is a prerequisite to problem-solving; second, there are 'executive' issues, whose resolution is a prerequisite to a functioning system (whether based on human or artificial intelligence).[12] The latter will be discussed in the following chapter, while the former are discussed here:

Much discussion has been devoted to the question of what exactly is a 'rule'. Aside from providing a self-sufficient definition (Burton, 185: 13),[13] interesting issues arise when attempting to juxtapose the notion of a 'rule' to similar – but distinct – concepts, such as that of a 'principle'. To be sure, not everybody agrees that there is any meaningful distinction to be made between these two notions (Braithwaite, 2002) since many consider principles (to the extent that they bear normative content[14]) to constitute a subset of rules. Yet the prevailing view is that some difference does exist, and the development of AI will most likely make it more pronounced. According to one widely embraced account (Dworkin, 1967: esp. at 22 *et seq*) a rule (if it is valid) "dictates a particular result",[15] while a principle "states a reason that argues in one direction, but does not necessitate a particular decision" (*Ibidem.*). The difference may be salient in explaining why AI is not

[12] These issues have been around even before AI, but the advent of AI has made tackling them imperative.

[13] According to one view, "a rule is an abstract or general statement of what the law permits or requires of classes of persons in classes of circumstances".

[14] If they did not bear normative content, they would not be worthy of attention.

[15] Much like the rules of a game, such as chess.

yet able to provide persuasive solutions to legal problems, which may be due to its inability to apply principles (or standards, or policies, or other precepts requiring human judgment). Question remains, of course, as to whether this is merely a difference of degree, especially if one were to subscribe to the position that there is no such thing as a rule which inexorably leads to preordained outcomes (meaning that human intervention will always remain of crucial significance).

This leads to a second question: is a 'rule' different from its application? The question may sound paradoxical at first; yet one might consider a simple rule, such as the one declaring that any act committed within the territory[16] of a given State fall within the scope of that State's domestic criminal law. This rule is present in every criminal code.[17] What is that 'thing' that we call a 'rule' in this regard? Is it the letter of the pertinent provision? Is it the overarching 'principle' of territoriality that it reflects (whether in its concrete form as a 'rule' of international law or as an abstract concept)? Is it its every application in real-life situations (or an abstraction of all these applications)? Further: are we talking about the same 'rule' worldwide or 'n' different (though similar) rules, equal to the number of jurisdictions?[18] It may be a truism that a rule is as good as its application, but in an AI environment the distinction will not be as straightforward as one may desire.

More often than not, rules operate in groups, which begs the question: is a set of rules different from 'a rule'? A set of rules in that regard would consist not just of the letter of each rule but also of the relationships between them [hierarchically and otherwise[19]], as well as the structure binding them [meaning their 'ordering'[20]]. You can break up a single 'rule' into itemized parts (mostly in the form of conditions for the rule's application), each of which might be regarded as a rule in its own right. A series of rules leading to a single outcome, however, may be seen as a single 'rule'. On at least some occasions, the level of generalization appears to be somewhat arbitrary. The development of AI transforms these questions into their digital 'analogues'. Thus, one may wonder: is a 'rule' different from a computer command? Is a set of rules different from a program? Is the act of legislating the equivalent of writing code? Regardless of how one approaches these questions, a realistic possibility is that, once a legal rule has been converted into an algorithm, the algorithm will itself become the rule for all practical purposes.[21] We will no longer have a code or a statute, but in fact an oracle.[22]

Falling back on analogical reasoning does not solve these problems, at least not all of them. To begin with, it would be illusory to think that reasoning by example is all but free of the concept of 'rules'. Such rules still lurk between the lines of each useful

[16] Or in *loci* equated to such territory.

[17] See, e.g., art. 5 of the Greek Criminal Code.

[18] This question is not important if you are trying to solve a problem from the perspective of (a specified) domestic law.

[19] E.g. whether one functions as an exception to another.

[20] More on this *infra*.

[21] Once the algorithm is put to work, the outcomes will shape reality, substituting the rule.

[22] People ask questions, and it provides answers.

precedent (Burton, 59 et seq.) More crucially, it is unclear exactly what the notion of a 'case' or 'precedent' actually consists of. Is it the bare facts, is it the holding, is it the underlying 'rule' or guiding 'principle', or all of these combined? What would a programmer have to provide as input to an algorithm to make it 'reason' by analogy based on previous cases? Is it even possible for machine learning to follow all steps of analogical reasoning without human intervention?[23]

Of course, nothing precludes the combination of both the deductive and the analogical approach to solve legal problems. In fact, such 'dual' approach had already been suggested even prior to the advent of AI, based on the difficulty of each case. According to such an approach, 'easy' cases can be solved by means of deductive reasoning, given that most would agree on at least the rules evoked. However, rules are by their very nature drafted to address situations envisaged (with some degree of precision) at the time of drafting. Because reality tends to exceed the drafters' imagination, one is sooner faced with unprecedented situations (aka 'hard' cases) than is able to describe them on paper. Inevitably, then, rules are exhausted, and another approach is called for. This is when analogical reasoning comes into play. Of course, one may attempt to employ deductive and analogical reasoning in the same case, the former to resolve 'easy' aspects of it, while the latter to address its 'harder' parts.[24]

The so-called 'hard' cases are characterized by indeterminate predicates that are embedded therein. Such 'open-textured' concepts are found in other disciplines, yet the unique feature in the legal realm is that the law is supposed to provide a single answer where in fact there may be more than one possible solutions (Rissland, 1988: 46-47). Admittedly, pretending that one among several solutions is legitimate *par excellence* is a uniquely human ability that would leave any AI dumbstruck.

3. THREE PROBLEMS

Any attempt to algorithmize any branch of law would run against three problems whose solution would appear to require a human 'touch', namely (i) importance; (ii) ordering; and (iii) evaluation.

The problem of importance has perplexed jurists for quite some time (Burton, 31, 50 and 83). While it is as such unrelated to AI, its resolution would be a prerequisite to machine learning applications. Interestingly, the problem of importance arises both in deductive and in analogical reasoning, though on slightly different terms. In deductive reasoning, the problem arises in selecting important facts (or aspects thereof) so as to align the minor premise with the major premise. Actual facts obviously do not come tagged with the terms which are used in the text of the applicable rules. Thus, a legal syllogism only

[23] On the evaluative judgments required to arrive at a conclusion see *infra*.

[24] K. Atkinson / T. Bench-Capon, 'Reasoning with Legal Cases: Analogy or Rule Application?', in 17th International Conference on Artificial Intelligence and Law (ICAIL '19), June 17–21, 2019, Montreal, QC, Canada. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3322640.3326695.

becomes valid if it can arrange the facts in such a way as to make them fit to the rule. In order to perform this function, someone needs to assign relative importance to the facts at hand (or to particular aspects thereof). For instance, article 312 of the Greek Criminal Code (proscribing domestic violence) extends its scope to, among other persons, those who are "unable to defend themselves". In order to apply the provision to its intended victim group, one has to decide – in each particular case – which facts are important so as to classify someone as 'defenseless': will it matter whether the individual is disabled, young or old, male or female? Will the answer lie in some combination of these traits? Legal terms are often deliberately designed to be vague, and are sometimes arranged in ambiguous sentences, but at some point they have to be applied in concrete situations, and merely reciting their definitions will not suffice to do the trick.

In analogical reasoning, the same problem arises in choosing which facts of the 'problem' situation are more important, prior to seeking out their counterparts in a 'base' case.[25] Which facts count as 'important' in that regard is largely a matter of debate, and can rarely be determined beforehand (at least in cases that are not straightforward). Accordingly, one point of criticism to the analogical form of legal reasoning is that it provides hardly any insight into selecting the pertinent facts (Hart, 1961: 155). To an outside observer, this process appears like performing a magic trick; at any rate, human intervention seems irreplaceable to perform this task.

The problem of ordering essentially consists in deciding which questions to ask first when examining a case, in order to arrive at a proper conclusion. Were one to depict decision points as nodes where pathways branch, ordering would essentially consist in placing the nodes in their proper places. This might at first appear a task better left to AI; yet placing decision points in order requires more than merely computation. This is better explained with examples, but three observations can be made at this point: first, even when a particular 'order' is preordained by law, as for example in the sequence admissibility → merits, there may be exceptions;[26] second, some questions may come first not because of a logical relationship but because of policy considerations: for instance, statutory limitation is treated as grounds expunging criminal liability (thereby doctrinally following the ascertainment of a crime) in several jurisdictions, but it is still examined prior to any discussion on the merits of the case; third, sometimes a question precedes another not based on a legal or logical relationship but simply for convenience (i.e. because the underlying facts are more easily provable). These considerations are not easily pre-programmable, and are thus better handled by humans.

The problem of evaluation is what renders judges necessary, and its resolution may prove to be the stepping stone for attaining human-level intelligence. When dealing with a specific case, answering certain questions will merely consist in inputting measurable factual data into the algorithm. This can easily be automated. Yet there will inevitably be

[25] One would have to first identify crucial facts in the 'problem' situation, so as to look for an appropriate precedent to judge it by. On the other hand, prominent 'base' situations (or precedents) will come with a pre-determined list of crucial facts, which enables their proper use.

[26] For instance, when addressing an admissibility question hinges on a subsequent determination, the decision on admissibility will be delayed until the merits stage.

questions that can only be answered by means of an evaluative judgment. One might set about eliminating such evaluations by assigning numerical values to facts and then only use rules that rely on measurable facts. But then three questions arise:

a. Is this feasible?

In theory, it would be possible to substitute concrete concepts for vague notions to avoid evaluative judgments. A case in point would be crimes against property, which are aggravated based on the net worth of the object of the offense. Under one approach, the aggravating circumstance consists in a specified amount.[27] A different approach employs a vague term, such as 'significant value', which calls for an evaluation in concreto. The former approach offers legal certainty, but poses proportionality and equality issues. The latter creates ambiguity, but also provides flexibility,[28] avoiding the pitfalls of specified amounts. In addition, statistical analysis could yield uniform results based on analogical reasoning, which would mitigate the usefulness of employing fixed amounts. One might indeed argue that the easier it is to quantify a concept, the less useful such quantification will be in actual practice.

b. Is this 'fair'?

Another way to put the question would be: Will it lead to better results?[29] Several jurisdictions have attempted to remove subjectivity from the conditions of criminal law provisions. This often leads to the use of more words to describe the same notion, sometimes less successfully. One victim is dispositive terms,[30] which do not tend to survive long in jurisdictions which are suspicious of judicial discretion. Greek law used to criminally proscribe sexual offenses with the use of the term 'lewd and lascivious act', which in turn was interpreted so as to denote an act combined with the perpetrator's underlying intent. As of 2019, the new Criminal Code employs the term 'sexual act', which the explanatory report confines to certain (graphic) examples. Such new configuration is presumably more descriptive, therefore more 'accurate', while the former was more evaluative. Yet in actual practice courts are not absolved of the need to proceed to an evaluation, as evidenced in case-law; where such evaluation failed to take place, the outcome was problematic, as in cases where defendants were acquitted of rape because their act did not fall within the enumeration of 'sexual acts'.

[27] For example, most offenses against property are classified as felonies under Greek law if the damage caused or the benefit gained or intended exceeds the amount of 120,000 €.

[28] Such flexibility is accorded to the judge, and, truth be told, it takes some level of trust in the Judiciary to use such terms.

[29] From a strictly legal perspective, that is.

[30] '*Dispositionsbegriffe*' in the German language.

c. Is this desirable?[31]

Asking whether something is desirable may sound redundant following a question on fairness. Yet one may decide that, even though something is objectively fairer, it does not lead to positive societal outcomes because it disturbs some equilibrium (thus being 'fair' but undesirable nonetheless). A case in point would be the notion of 'pornographic'[32] material [as opposed to art or other lawful depictions]. Even if this notion could be quantified (which is doubtful) and even if such quantification led to more accurate results, removing human evaluation from pertinent judgments would reduce them to 'cold', artificial dicta. In addition, it would lead to static judgments, not adjustable based on evolving social mores, artistic movements, etc. That is actually the good scenario: in a worst-case scenario, it would hinder progress, since AI would punish any deviation, leaving us in perpetual immobility (this is generally a theme to look out for in the AI-era).[33] Assessing this sort of concepts[34] will be one of the last conquests of AI: one might indeed surmise that it will require human-level intelligence of the sort required to solve "I'm not a robot" puzzles such as 'click all squares containing a cat', etc.

These issues point to the difficulty of handling legal concepts. But easier legal problems may be automated, and a more modest approach may work better, at least in the short run.

4. A MORE MODEST APPROACH TO ALGORITHMIZE SETS OF RULES

The aforementioned problems (alongside other, more technical, issues), have thus far prevented AI solutions to even ordinary legal problems. However, more modest approaches might go a long way towards facilitating the legal process. To perform this function, an application has to be able to furnish solutions to actual problems. In the particular domain of criminal law, a typical problem would consist in identifying whether a given act or omission falls within the scope of a provision proscribing a particular criminal offense. Of course, there are other issues that will have to be resolved, such as the application of provisions *ratione temporis* (in the event of an amendment), participation in the offense (depending on the system adopted), assessing the penalty/ies to be imposed,

[31] Note that an ordering question arises here: should 'feasible' precede 'desirable' or vice versa? The answer may very well depend on whether you are a pragmatist or an idealist [if something is very desirable, it may become feasible]. Will an AI even have an ideology? Will it be an optimist or a pessimist pragmatist?

[32] Depending on the jurisdiction, publishing and/or viewing 'indecent' or 'pornographic' material may be punishable only when it involves minors or in other situations. Yet an evaluation as to the content of the material will invariably be called for.

[33] Consider the following point: divergent behavior is sometimes 'tolerated' either because it is not caught or because it is left unpunished by courts. This leads to some kind of 'evolution' in societal practices (much like gene mutations leads to evolution in biology). Such process will not be allowed in the AI-era (for better or for worse).

[34] These concepts generally fall within the aphorism "I know it when I see it but I cannot put it into words".

and many others, not to mention procedural matters that have to be resolved in order to apply substantive law rules.

When you try to solve a problem [based on a real situation], starting from the rule would be like choosing a cellphone case without knowing what type of cellphone it is intended for.[35] On the other hand, cellphone cases are already available prior to needing them, as are rules (at least that is the norm). In some areas of the law (more than in others), the enactment of laws predating the situation envisaged by them is mandatory, a typical example being (substantive) criminal law, at least in terms of provisions proscribing an offense or aggravating the penalty threatened. Therefore, digitizing criminal would have to proceed on two parallel paths: on the one hand, arrange existing rules in such a manner as to be receptive to pertinent facts; on the other, ensure the 'routing' of facts into this streamlined set of rules, so that legal conclusions can safely be derived. These parallel functions can be performed by creating simple algorithms in the form of decision trees.

The usefulness of decision trees has been well documented even before machine learning (Strauss & Topping, 1970). The technique embedded in decision trees entails breaking down the applicable provisions into their constituent elements, ordering these elements in a series of consecutive steps, and presenting each step in the form of a legal question, which will usually be answered with a 'yes' or a 'no' (Mingay, Hendricusdottir, Ceross, Bergmann, 2022.

Depending on the answer given at each node, the diagram leads the to a subsequent question, which shall be answered in turn; as long as the inputted information is accurate, and the questions are answered in their predetermined order, the conclusion will have to be accepted as valid (Strauss & Topping, 448).

The particular rapport between reality and law, i.e. between the facts of a given case and the applicable rules, makes criminal law an ideal candidate for digitization in the above sense.[36] Creating decision trees, of course, would presuppose proffering solutions to at least the problems of importance[37] and ordering;[38] problems of evaluation, on their part, will have to be addressed while applying the algorithm.[39] An example is given in the diagram below, which relates to the extension of criminal jurisdiction to cases (including – but not limited to – those featuring a cross-border element).

This diagram can be supplemented with further nodes, ushering in answers concerning the application (or non-application) of the *ne bis in idem* principle (should a case have been dispensed with by a foreign court of law), accounting for sentences served abroad, etc.

---

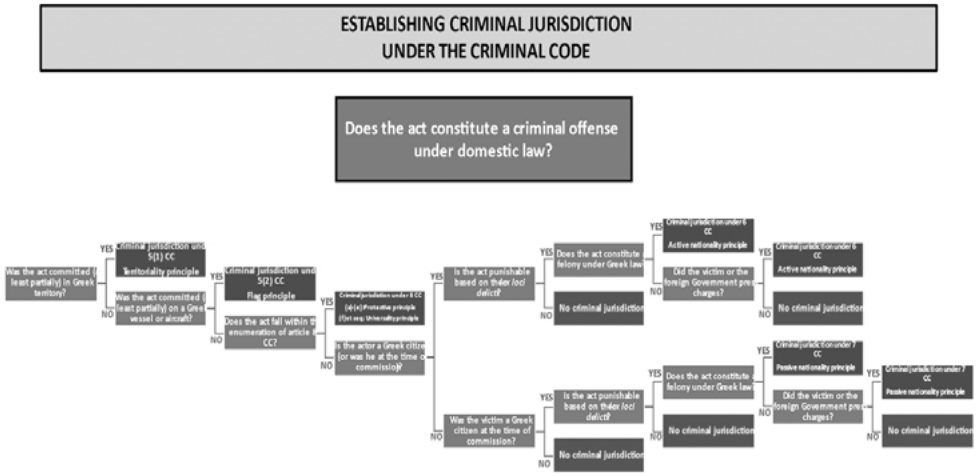
[35] In many ways, this is equally true even if the problem is how to draft the rule itself.

[36] With proper doses of fact-finding and evaluative judgments.

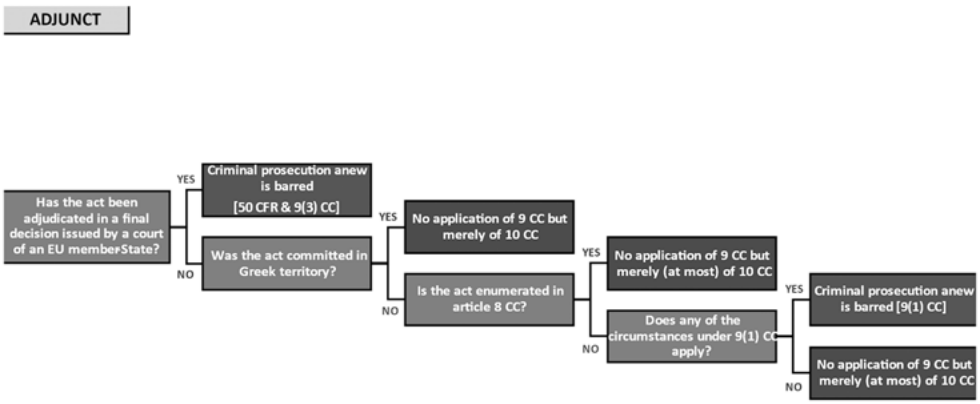
[37] Because one needs to select the crucial traits to look for in each particular case.

[38] Because misplacing even one node could compromise the final outcome of the syllogism, leading to a non-valid answer.

[39] How this will be done is among the tough issues that will be left to human judges.



The second diagram may be joined with the former diagram, following every green box [which will become a node in itself].[40]



Aside from a robust problem-solving tool, drafting algorithms in the form of decision trees provides useful insights into the relationship between legal rules which are normally thought to belong to different domains. Thus, substantive and procedural law rules may be ordered uninterruptedly, in the form of a 'continuum'. This might easily be done by joining two (initially independent) decision trees [one incorporating substantive and the other procedural rules] one after the other. But there may be combinations: admissibility questions would be placed in the beginning,[41] while other procedural issues may intervene.[42] Drafting decision trees, especially in the beginning, will create the impression

[40] In the context of such a configuration, the question concerning where the act was committed [second blue node in the second diagram] would be omitted.

[41] Preceding not only other procedural issues but also substantive law questions.

[42] Certain areas belong to different domains depending on the jurisdiction: for instance, statutory limitations are treated as a substantive law issue in several jurisdictions, but as a procedural matter in others.

that the underlying sets of rules form 'closed systems', independent of one another. This is no more than a 'convention' that will be relied upon as a starting point. Truth be told, however, there is no such thing as a 'closed' system of rules. The entirety of rules which are included in a Criminal Code form a system that could be ordered in a single decision tree, if the appropriate level of abstraction is used. By further 'zooming out', one would also extend the tree's branches to contain procedural rules. In point of fact, one might order rules from different domains (civil law, administrative law, and so forth) into a single tree. It follows that, although we can work on the hypothesis that 'closed' systems of rules exist in order to solve particular problems,[43] practice will reveal which configurations are workable.

Once the algorithm is put into place, activating it will presuppose input based on the particularities of each case. One would thus have to 'feed' the algorithm either 'by hand' (where the user would input factual data depending on the case at hand) or automatically, by means of linking the various algorithms with databases properly configured to play this role. In time, each node will function as a portal to case-law and other authorities, assisting future users, as well as researchers.

5. IMPACT ON THE LEGAL PROCESS

The widespread use of AI applications in the proximate future will have a dramatic impact on the criminal justice system. Yet even a modest approach (as the one described above) would bring with it serious ramifications, aside from rendering human participation auxiliary or even redundant.

One may think of a number of upshots resulting from the expansion of AI into the criminal justice system (not just from a purely legal perspective but also on a societal level). Here we list a few which are pertinent to our subject:

- The Judiciary will effectively merge into the Legislature. Creating the rule and then converting it into an algorithm[44] will essentially be all that matters. It is not just that human judges will be 'out of business' (or be confined to menial tasks). In essence, there will be but one Power, exercised by the Regulator [who may well be a machine]. One might counter that creating the algorithm is a mere 'technicality' entrusted with the AI, and that humans will still be calling the shots [or pulling the strings, or what have you]. Yet no one can be sure about that, as the improvement of machine learning is quite likely to enable AI to even define final goals, amend the algorithms as it sees fit, etc.
- Regardless of the previous comment, algorithmizing legislation will probably improve the legislative process as such. The day-to-day oversight of the application of the rules, the easy amassing of statistical data (including such data as the frequency of invoking a certain exception) will assist in bringing about targeted amendments. It will also

[43] Besides, this is usually what happens in the actual practice of courts of law.

[44] Pretty soon, the act of legislating itself will consist in drafting the algorithm.

help achieve uniformity in the applicable law across different jurisdictions [since it will make plain both the similarities and the differences, greatly facilitating comparative analysis].

- The lawyers' role will be radically different, confined to the stage of inputting data into the algorithm (and, to a lesser degree, questioning the algorithm's operation). One may indeed envisage a future where an ordinary citizen, trained in AI, will be in a better position to exercise the role of 'counsel' in criminal law cases as opposed to those having a legal education.
- The distinction between interpretation and application of the rule will be blurred. The 'handler' will 'insert' the facts (input) into the machine and wait for the answer [much like one who places a light bulb in its position and awaits light]. Questions pertaining to the application of the rules will still be present, but they will be invisible to the naked eye, much like the code hidden deep below the user-friendly interface of various apps.
- The algorithm will dispense with the need for a detailed reasoning of a judgment (at least in relation to the legal aspects of a case).[45] All that matters will be that certain steps were followed in their proper turn. The outcome will then be 'self-explanatory', and it will have to be accepted by everyone *perforce*.
- The algorithm will abolish the need for an appeal (at least with respect to legal matters).[46] Indeed, everybody will be 'running' the same algorithm, hence there will be no point in repeating the same process before a higher court.[47] Some leeway will be allowed: a. for an appeal where new evidence may be presented [to change the 'factual input'] and b. for a process of review of proper 'functioning' of the algorithms [perhaps leading to annulment of the decision and repetition]. Other than that, a judgment delivered by the algorithm will be as good as final.
- There will be no need for human involvement in assessing risks, checking the effectiveness of the system, and so forth. These tasks will be performed based on metrics handled by machines (drawing on data from various sources).
- The criminal process quite frequently relies on predictive judgments involving, *inter alia*, the assessment of personality traits. Cases in point would include the decision whether to provisionally detain the defendant or impose other restrictions [which hinges on the possibility of the defendant committing other offenses if released or the risk of flight] or the decision whether to release a convict on parole [which depends on an assessment of the degree of rehabilitation, and the possibility of committing future offenses]. This kind of decisions will gradually be made by means of algorithms.[48]

[45] In many jurisdictions, the requirement for a detailed reasoning of judicial decisions (particularly those issued by criminal tribunals) is constitutionally enshrined.

[46] The jurisdiction of a typical Supreme Court may be confined to technicalities or violations of the 'algorithmic process'.

[47] There will not be a question of added expertise or experience, since these attributes will be equally present in all machines placed in the service of the criminal justice system.

[48] Tools of this sort are already being put to use in certain jurisdictions, although reservations have been expressed, especially concerning the bias inherent in these systems [see *supra* n. 3].

6. CONCLUDING THOUGHTS: MACHINE WEAKNESSES, HUMAN STRENGHTS

Intimidating or not, AI is bound to dominate many aspects of social life, including the criminal justice system, limiting the role of human intervention. Question, then, remains as to what role – if any – will be reserved for humans in such an environment.

Interestingly enough, today's 'problematic' areas will be tomorrow's human havens. The three current 'problems' discussed above[49] will be addressed (at least for the foreseeable future) by humans. To briefly recapitulate:

- Choosing which facets are important either in terms of a minor premise or in analogical reasoning will be based on human judgment [the problem of 'importance'].
- Arranging rules in a particular configuration, so as to be able to apply their conditions in due turn, requires decisions not exclusively of a computational nature, especially when questions of 'convenience' come into play [the problem of 'ordering'].
- Perhaps most important of all, applying vague terms requires uniquely human abilities, and is especially predicated on a set of values, which cannot simply be 'uploaded' so as to function absent human intervention[50] [the problem of 'evaluation'].

Accordingly, there are types of 'judgments' that cannot be outsourced to machines, and are thus best left to humans. In addition, certain human skills are expected to remain useful for the foreseeable future. These would include:

- The uniquely human ability to generate information from limited data or even from none whatsoever [by generalizing from scant information or first principles].[51]
- Conversational skills, which are by definition exercised in the legal profession. As longa as the legal process remains adversarial (at least to a certain extent), humans will have a role to play.[52]
- It should not be overlooked that the human presence begets attention and creates a sense of security. The example of self-driving cars indicates that machine errors will (initially at least) be less tolerable compared to human mistakes (even if the latter outnumber the former).[53] The same is true of justice (Grewal, Guha, Satornino, Schweiger, 2021). perversely, parties to a case as well as the general public will need to personify those responsible for the outcome of a dispute. Such need

[49] *Supra*, under [4].

[50] Although a number of techniques have been contemplated to 'infuse' AI with values, none is sure to work in actual practice. See N. Bostrom, *op. cit*.

[51] It will probably take human-level intelligence to match this human ability.

[52] It remains an open issue whether legal argumentation is a subset of generic argumentation or whether it can be construed as a superset: see L. Eliot, 'AI and Legal Argumentation: Aligning the Autonomous Levels of AI Legal Reasoning', available online at: https://arxiv.org/ftp/arxiv/papers/2009/2009.11180.pdf [31.10.2022].

[53] This is due to psychological reasons: people need *someone* to blame, which appears to defuse unrest.

is especially pronounced in criminal justice, which is why the participation of humans will create trust in the system even after algorithms have trickled therein.[54]

Some may hope that the singularity is fast approaching, while others are apprehensive of what they see as a grim future. For the time being, however, it would be wise to start educating the next generation of jurists to conceive of rules differently. Moreover, creating legal databases, though useful as such, is not enough unless they are linked to ordered systems of rules in every jurisdiction. This process will be faster and more effective if carried out based on synergies between jurists and programmers. Besides, a jurist and a programmer will become indistinguishable. Until that happens, lawyer and judge 'prosthetics'[55] are as realistic a prospect as one may expect.

REFERENCES

1. Alarie, B., Niblett, A., Yoon, A (2018) "How Artificial Intelligence Will Affect the Practice of Law", *University of Toronto Law Journal,* 68(1), 106-124, https://utpjournals.press/doi/10.3138/utlj.2017-0052, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3066816 [31.10.2022].
2. Aletras, N., Tsarapatsanis, D., Preoţiuc-Pietro, D., Lampos, V. "Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective", *PeerJ Computer Science* 2:e93, https://doi.org/10.7717/peerj-cs.932-19 Available at: https://peerj.com/articles/cs-93/ [31.10.2022].
3. Aikenhead, M. (1997) *Legal analogical reasoning – the interplay between legal theory and artificial intelligence*. Master thesis, Available at Durham E-Theses Online: http://etheses.dur.ac.uk/5462/ [31.10.2022].
4. Artificial Intelligence supporting Cross-Border Cooperation in Criminal Justice, Joint Report prepared by eu-LISA and Eurojust, (2022), Available online at: https://www.eurojust.europa.eu/sites/default/files/assets/artificial-intelligence-cross-border-cooperation-criminal-justice-report.pdf [31.10.2022].
5. Atkinson, K. Bench-Capon, T. (2019) "Reasoning with Legal Cases: Analogy or Rule Application?", *In Proceedings of the 17th International Conference on Artificial Intelligence and Law (ICAIL '19)*, June 17–21, 2019, Montreal, QC, Canada. 12-21, Available at: https://doi.org/10.1145/3322640.3326695 [31.10.2022].
6. Aune, B. (1970) *Rationalism, Empiricism, and Pragmatism: An Introduction*, New York: Random House.
7. Bagaric, M., Hunter, D., Stobbs, N. (2020) "Erasing the Bias Against Using Artificial Intelligence to Predict Future Criminality: Algorithms are Color Blind and Never Tire", *University of Cincinnati Law Review,* Vol. 88, Issue 4, 1037-1088.

[54] Acceptance by the public (or lack thereof) will be a key issue in the success of AI. This is more so the case in high context societies, like Greece.

[55] These tools already exist, and are expected to both multiply and improve in the proximate future.

8. Bibel, W. (1993) *Deduction: Automated Logic*, San Diego: Academic Press.
9. Boden, A. M. (2014) "GOFAI", In: *The Cambridge Handbook of Artificial Intelligence*, (Frankish, K. Ramsey, W. eds.), Cambridge University Press. 89-107.
10. Bostrom, N. (2014) *Superintelligence: Paths, Dangers, Strategies*, Oxford: Oxford University Press.
11. Braithwaite, J. (2002) "Rules and Principles: A Theory of Legal Certainty", 27 *Australasian Journal of Legal Philosophy* Vol 27, 47-82.
12. Buchanan, B., Headrick, T. (1970) "Some Speculation About Artificial Intelligence and Legal Reasoning", *Stanford Law Review.* Vol. 23, 40-62.
13. Burton, S. (1985) *An Introduction to Law and Legal Reasoning*, Little, Brown and Company.
14. Chohlas-Wood, A. (2020) *Understanding risk assessment instruments in criminal justice, Report from The Brookings Institution's Artificial Intelligence and Emerging Technology (AIET)* Initiative, available online at: https://www.brookings.edu/research/understanding-risk-assessment-instruments-in-criminal-justice/ [31.10.2022].
15. Dworkin, R. (1967) "The Model of Rules", 35 *The University of Chicago Law Review,* Vol 35, No. 1, 14-46.
16. Eliot, L. (2009) "AI and Legal Argumentation: Aligning the Autonomous Levels of AI Legal Reasoning", Arxiv:2009:11180, Available online at: https://arxiv.org/ftp/arxiv/papers/2009/2009.11180.pdf [31.10.2022].
17. Engle, E. (2003) "Smoke and Mirrors or Science? Teaching Law with Computers – A Reply to Cass Sunstein of Artificial Intelligence and Legal Science, *Richmond Journal of Law and Technology,* Vol. 9, Issue 2, Available at: https://scholarship.richmond.edu/jolt/vol9/iss2/4, [31.10.2022].
18. Friedrich, S. *et al*. (2021) "Applications of artificial intelligence/machine learning approaches in cardiovascular medicine: a systematic review with recommendations", 2 *European Heart Journal – Digital Health*, Vol. 3, Issue 1, 424-436.
19. Grewal, D., Guha, A., Satornino, C., Schweiger, E. (2021) "Artificial intelligence: The light and the darkness", *Journal of Business Research*, Vol. 136, 229-236.
20. Hart, H. L. A. (1961) *The Concept of Law*, Oxford: Oxford University Press.
21. Johnson, B., Shen, F. (2021) "Teaching Law and Artificial Intelligence", Minnesota Journal of Law, Science & Technology, Vol. 22, Issue 2, Available at: https://scholarship.law.umn.edu/mjlst/vol22/iss2/4, 23-42.
22. Kauffman, M., Soares, M. (2020) "AI in legal services: new trends in AI-enabled legal services", *Service Oriented Computing and Applications,* Volume 223, No. 14, 223-226, https://doi.org/10.1007/s11761-020-00305-x.
23. Kehl D. *et al*. (2017) "Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing", *Responsive Communities Initiative*, Berkman Klein Center for Internet & Society, Harvard Law School, Available online at: https://dash.harvard.edu/handle/1/33746041 [31.10.2022];

24. Koenig Love M.E., Mandell. C. (2022) "A New Metaphor: How Artificial Intelligence Links Legal Reasoning and Mathematical Thinking", *Marquette Law Review,* Vol. 105, Issue 3, 559-601. 559.
25. Lamond, G. (2014) "Analogical Reasoning in the Common Law", *Oxford Journal of Legal Studies*, Vol. 34, No. 3, 567-588.
26. Mingay H., Hendricusdottir, R., Ceross, A., Bergmann, J. (2022) "Using Rule-Based Decision Trees to Digitize Legislation", *Prosthesis* 4(1), 113-124, 10.3390/prosthesis4010012.
27. Minsky, M. (ed.) (1968) *Semantic Information Processing*, The MIT Press.
28. Nichols, J., Chan, H., Baker, M. (2019) "Machine learning: applications of artificial intelligence to imaging and diagnosis", *Biophysical Review,* 11(15), 111-118, DOI:10.1007/s12551-018-0449-9.
29. Reiling, A.D. *Courts and Artificial Intelligence', International Journal for Court Administration*. Vol. 11, Issue 2, Available online at: https://www.iacajournal.org/article/10.36745/ijca.343/ [31.10.2022].
30. Rissland, E. (1988) "Artificial Intelligence and Legal Reasoning: A Discussion of the Field & Gardner's Book", *AI Magazine* 9(3), 45-55, https://doi.org/10.1609/aimag.v9i3.942.
31. Rissland, E. (1990) "Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning", *The Yale Law Journal*, Vol. 99, No. 8, 1957-1981.
32. Ryberg, J., Roberts, J. (eds.) (2022) *Sentencing and Artificial Intelligence*, Oxford: Oxford University Press.
33. Sarker, I. (2022) "AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems", *SN Comput Science,* 3, 158 https://doi.org/10.1007/s42979-022-01043-x.
34. Shi, J. (2022) Artifcial Intelligence, Algorithms and Sentencing in Chinese Criminal Justice: Problems and Solutions. Criminal Law Forum 33, 121–148, https://doi.org/10.1007/s10609-022-09437-5.
35. Strauss, P., Topping, M. (1970) "Decision Trees", 7 *Journal of Ethiopian Law,* 447-461. Available at: https://core.ac.uk/download/pdf/230175298.pdf, [31.10.2022].
36. Susskind, R. (2010) *The End of Lawyers? Rethinking the Nature of Legal Services*, Oxford: Oxford University Press.
37. Sunstein, C. (2001) "Of Artificial Intelligence and Legal Reasoning", *Law School Roundtable* 8(1) University of Chicago, 29-25. Available at: http://heinonline.org/HOL/Page?handle=hein.journals/ucroun8&start_page=29&collection=journals&id=37, [31.10.2022].
38. Susskind, R. (2019) *Online Courts and the Future of Justice*, Oxford: Oxford University Press.
39. Weinreb, L. (2012), *The Use of Analogy in Legal Argument*, Cambridge University Press.

UVOĐENJE ALGORITMA U KRIVIČNO PRAVOSUĐE: ŠTA OSTAJE LJUDSKOJ PRIRODI?

Algoritmi su već korišćeni u krivičnim predmetima, a očekuje se da će se njihova upotreba povećati u narednim godinama. Primer za to je njihovo korišćenje prilikom izricanja krivičnih sankcija, a koje će se u velikoj meri oslanjati na alate za procenu rizika. Bilo je, naravno, i ukazivanja na druge nedostatke korišćenja algoritama osim onoga što mnogi nazivaju "nehumanim" načinom zadovoljenja pravde. Ti nedostaci se odnose na efikasnost digitalnih sistema, a posebno pristrasnost koja je prisutna u takvim odlukama.

Digitalni sistemi se primenjuju da bi se olakšala pravosudna saradnja u predmetima koji sadrže prekogranične elemente. Ako ostavimo po strani bezbednosna pitanja, ovi sistemi su uglavnom efikasni u toj oblasti, ali će ljudska intervencija i dalje biti neophodna u doglednoj budućnosti. Jednostavno se čini da postoje situacije u kojima je ona neizostavna.

Svođenje skupova pravila na algoritme pokazuje se kao efikasan način proučavanja prava (između ostalih disciplina). Ipak, postoje određene opasnosti u takvom pristupu. Na primer to može dovesti do mehaničkog pamćenja procesa za razliku od kultivisanja sposobnosti da se udubi u logiku sistema.

Moguće je da postoji zajednički razlog koji leži u osnovi ograničenja algoritama. Objašnjenje zašto algoritmi ne uspevaju pretpostavlja fundamentalno razumevanje ključnih oblasti koje bi trebalo prepustiti ljudskoj proceni, bar za sada. Ovaj rad se oslanja i na određeno iskustvo autora u radu sa tim sistemima u istraživačkim projektima i u nastavi. Iako je u osnovi ova tema značajna za različite oblasti prava, naglasak u ovom radu će biti na krivičnom pravu.

KLJUČNE REČI: *ljudske slabosti, snaga mašina, izrada algoritma, materijalno i procesno pravo kao "continuum", "hranjenje" algoritma, vrste presuda.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.25

THE NIS DIRECTIVE AND THE CRIMINAL RESPONSIBILITY OF THE NIS OFFICER

Cristina Nicorici*

The NIS Directive (Directive number 2016/1148) has imposed a higher standard for cyber security in seven main domains considered to be of public interest, all across the European Union, with the main goal to unify the protection of sensible data and the provision of essential services against cybersecurity attacks. Given aside the technical requirements, which are not few, and which do imply an investment of costs and human resources, this directive regulates several technical and procedural items that all essential operators must comply with, and which state what procedure should be followed in case of cyberattack. Of particular interest for the criminal law is the figure of the NIS officer – the employee of an essential operator that has the responsibility to keep under surveillance the security alerts that the national authorities send periodically. However, what if this responsibility is not fulfilled? How should the criminal responsibility of this person should be analyzed? In this article I will present the general framework set by the NIS Directive and the Romanian regulations in this matter, and I will try to answer to the questions above.

KEYWORDS: *The NIS Directive, cyber security, the NIS officer, responsibility*

* PhD, Research assistant Faculty of Law, West University of Timisoara, Romania.
E-mail: *cristina.nicorici@e-uvt.ro*

INTRODUCTION

Our lives are more and more digitalized, and therefore, the number and types of cyber risks threatening the security of our data have increased. The NIS Directive (Directive number 2016/1148) is a mandatory act adopted by the European Commission, regarding measures for a high common level of security of network and information systems across the Union, and came as a response in what concerns these risks. This Directive lays down measures with the aim of achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.

The introduction of the NIS Directive underlines the importance of cyber security: "(…) Network and information systems and services play a vital role in society. Their reliability and security are essential to economic and societal activities, and in particular to the functioning of the internal market. The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union. Network and information systems, and primarily the internet, play an essential role in facilitating the cross - border movement of goods, services and people. (…) To achieve and maintain a high level of security of network and information systems, each Member State should have a national strategy on the security of network and information systems defining the strategic objectives and concrete policy actions to be implemented".

Article 14 of the Directive underlines that "Member States shall ensure that operators of essential services take appropriate and proportionate technical and organizational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed". In appliance of this Directive, Romania has adopted, firstly, the Law number 362/2018, and also secondary acts, such as Order 1323/2020, that contains the technical and minimum conditions that must be respected in order to be compliant with the NIS regulations.

In order to fully understand the concepts of article 14, we must first define a few key notions. Some of the definitions are given by the Directive, some are given by the Romanian Law nr. 362/2018:

- "security of network and information systems" is defined by the Directive as the "ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems";

- "incident" is defined by the Directive as "any event having an actual adverse effect on the security of network and information systems";
- "essential operator" could be defined as an economic agent that acts in the field of energy (electricity, oil, gas), transport (air, rail transport, water transport, road transport), banking, financial – market institutions, health sector, drinking water supply and distribution, digital infrastructure. An economic agent operating in one of these fields, if meets some national criteria regarding the number of users, is an essential operator. A legal strict definition is not provided by the Directive or by the national Romanian law.

1.THE GENERAL FRAMEWORK IMPOSED BY THE NIS DIRECTIVE

As shown before, the goal of the NIS Directive is, first of all, to establish a minimum level of cyber security that all operators must comply, if they pass certain criteria in the seven essential domains: energy (electricity, oil, gas), transport (air, rail transport, water transport, road transport), banking, financial – market institutions, health sector, drinking water supply and distribution, digital infrastructure.

This directive imposes certain technical standards that have as a goal to set this level of cyber security. Of course, these provisions are not the subject of this article, but, however, there are some main technical elements that deserve to be mentioned:

- the essential operator must implement different programs that allow to make penetration testing – testing the network in order to see if the system is vulnerable to attacks;
- the essential operator must make annual and biannual internal and external technical audits botch of the network and of the enforcement of the procedures;
- the essential operator must implement technical programs for backup of data;
- the operator must implement technical programs that allow the recovery of data in case of disaster;
- the operator must implement technical programs able to identify security threats and to deal with them.

This directive also imposes certain procedural standards, and the operator has to develop the following procedures: rules regarding cybersecurity, the manner of action in case of cyber security crises, the audit regulations, the responsibilities of the technical team in case of incident of cyber security, the schedule of education of the employees of the operators in the matter of secure use of the network components, rules regarding the interconnection with the national authorities in the cybersecurity domain.

One of the main requirements that each operator has to respect is to nominate a NIS officer, this being an employee with specific attributions, and of particular importance, as it will be detailed in the following lines.

2. THE "NIS OFFICER"

Although the Directive speaks generally of the NIS officer, national legislators were under duty to determine the responsibilities correspondent to this position. Articles 31 - 33 of Romanian Order 1323/2020 establish the attributions of this employee. In essence, the NIS officer is an employee of the operator that has as main attribute the responsibility to follow up any alerts emitted or communicated by the national authority of cyber security and to disseminate this information inside the company.

This responsibility is extremely important, because, in the NIS Directive perspective, notification and permanent inter-connectivity between essential operators and the authorities is of maximum importance. All operators have to be in a permanent connection with the national authorities, and they have to inform them in case an incident of cyber security of a certain importance has taken place. Also, every operator must have designated NIS officers that supervise in permanence the notifications sent by the authorities, and to take the necessary measures imposed by the event.

Given this framework of interconnectivity and the responsibilities of the NIS officer, several questions can be formulated: what if the NIS officer does not comply with his responsibility, and he/she does not analyses with attention the notifications sent by the national authorities? What if the operator should have taken some measures after this notification, and these measures are not taken, or are taken with delay, and data is compromised or the essential service is not available for a period of time? Sure, the disciplinary responsibility of the officer could be discussed, but can we or should and could we talk of a criminal responsibility based on an inaction of this person? To these questions I will try to formulate an answer below.

3. CRIMINAL RSPONSIBILITY OF THE NIS OFFICER – PERSPECTIVES

The Directive, of course, does not regulates any crimes, as the European Union does not have this attribution; criminal law is a field of national perspective. Romanian Law nr. 368/2016 does not contain any specific regulations. In this context, it could be said that the NIS officer is not criminally liable if he or she does not comply with their duties imposed by the NIS Directive. However, such a conclusion would be false, as it will be presented in the following lines.

First of all, what should be underlined from the begging is that the law imposes to this officer some duties to act, to do, to comply with some actions. Therefore, we are talking about norms that impose a certain way to act to the subject. If the agent does not fulfill these duties, their responsibility, even from a criminal point of view, will be held considering their passivity, their inaction. However, it must be said from the beginning that not all inactions are relevant – since in every moment of our existence each and every one of us omits to comply an infinity of possible actions, and, therefore, commits an infinity of omissions. Relevance can have only those inactions that suppose that the

agent did not do something that the law imposed to do, therefore they did not comply with a duty imposed by the law.

In this paradigm, in the Romanian legal system, as in some European legal systems (German, Italian, Spanish, to give just a few examples), two are the types of crime that sanction the inaction of the agent, and these are generally known as follows: the proper omission and the improper omission, also known as commission by omission.

The proper omission is the type of crime where the legislator has defined the dangerous conduct as an inaction. In other words, by it's the definition, the offence sanctions the passivity of the agent. Generally, in this type of crime, the duty to act is implicit and it can be deduced from the incrimination. The NIS Legislation, however, does not contain any regulations of this type regarding the NIS officer.

The second type of omissive crime is the improper omission or the commission by omission. This type of crime has a general definition, described in article 17 in Romanian Criminal Code, as follows:

"*The commissive crime that consists in the production of a result can be committed also by omission when:*

a) *There is a legal or contractual duty to act, or*

b) *When the agent has created, by a previous action or inaction, a state of danger for the social value that has eased the production of the dangerous result*".

Therefore, regarding this type of crime, the following can be mentioned: it is not a crime specifically regulated by the Criminal code in the special part of Criminal code, but it has a general definition. For every crime that has as a consequence a material result (therefore, a concrete modification of reality, and not a state of danger – something abstract), through interpretation, given the definition of article 17, it can be said that it can be committed also by omission, resulting the crime of commission by omission. However, although at first sight it may seem that, given the large definition provided by article 17 of Romanian Criminal Code, every crime could also be committed by omission, in the modality of commission by omission, several observations must be made.

As explained in a previous article (Nicorici, 2022: 347), the improper omission crime has a particular structure that be analyzed when analyzing criminal responsibility for omission. The main elements of the commission by omission are as following:

- The existence of the duty to act;
- The capacity of the agent to comply with this duty;
- The non-compliance of the duty;
- The dangerous result;
- The causality connection.

We will analyze each of these elements in particular.

3.1. The duty to act

The existence of the duty act is the main element, and traditionally, it is considered that the source of the duty to act can be found in a law, a contract or from the previous conduct of the agent.

This might seem simple in the begging, but, in reality, all these sources are largely debated in the legal literature. Regarding the law as source of the duty to act, many authors ask whether law should be understood as a normative act in general (Luzón Peña, 2017: 198; Ordeig, 1997: 13; Aráuz Ulloa, 2000: 36) or as an act emitted by the legislative authority only. Regarding the contract as the source of the duty to act, should we understand a contract in the civil form? Because in this case, any cause of nullity or invalidation of the contract will affect the duty to act, thus being inexistent. The majority of authors sustain that the answer is negative, and that by „contract" we should understand a voluntary assumption of the duty to act, that should not be affected by the causes that from a civil point of view invalidate the contract (Zaffaroni, Slokar, Alagia, 2002: 578; Mir Puig, 2006: 323).

Thirdly, the previous conduct as the source of the duty to act generates numerous discussions. If the conduct is illicit, it can be argued that it could fundament a duty to act, but if the conduct is licit, or justified by a justification cause, then, some argue, it is not normal to fundament criminal responsibility.

All the discussion above is valid mainly if we analyze from a formal point of view the sources of the duty to act, position criticized for its rigidity (Roxin, 2014: 848; Jescheck, 1993: 18; Crespo, 2009: 9). However, other authors, beginning with Armin Kaufmann, sustain that instead of formalizing the duties to act, facing all types of problems, we should fundament them on the functions of the agent. Armin Kaufmann identifies three functions: the function to protect the social value, the function to supervise a source of danger, and the function to control the source of danger (Kaufman, 2006: 289).

This interpretation avoids the formality problems, but makes other to arise. Regarding the function of protection, this comes from a special relationship with the owner of the social value, but could we say that any form of special relationship fundaments a function of protection? Or, to put it in other words, what are the characteristics of a relationship that fundament this function? Parents for children (but at any age of the children?), children for parent (in any case, or only in special conditions?), spouses between them, brothers and sisters, friend for a long time, neighbours? And the list may continue. Regarding the function to supervise or to control a source of danger, the things are not clear either. Should there be an absolute function? What if the victim „provokes" the source of danger (especially when the source of danger is an animal), so the victim increases the risk of the danger? What about the responsibility to control a person who cannot control his or her acts? Can this responsibility be equalized to the function of control? What about owning certain goods, such as buildings or spaces used by other to commit crimes?

As I have shown before (Nicorici, 2022: 350), all these questions show that the problem of the sources of the duty to act is still to be solved.

In the matter of the NIS officer, the duty to act is foreseen in the contract that the employee concludes with the essential operator. Although it may seem, at first sight, that it comes from the law, in reality, the law stipulates with general character what a NIS officers should do. It is only by contract that a specific person accepts to be a NIS officer, and, therefore, is under the obligation to comply the specific duties.

3.2. The existence of a typical situation

The duty to act activates only when there is a situation that threatens the social value (Zaffaroni, Slokar, Alagia, 573; Kaufmann, 2006: 114; Roxin, 814). Only in this case it might be said that the duty to act of the agent was activated and that he or she must act in order to save the social value.

In the case of the NIS officer, the duty to act is activated once a notification from the authorities is emitted, notification regarding an incident of cybersecurity.

4. THE CAPACITY TO ACT

The third element of great importance is the capacity to act, meaning that the agents must be able to perform an action that would avoid the result (Hurtado: 1987: 175; Gullock: 2008: 157). For example, if the mother does nothing while her child is drowning, she will not be held criminally liable if she did not know how to swim and did not have any possibility to call for help.

The literature identifies two faces of the capacity to act: the intellectual element (Nicorici, 2022: 350; Zaffaroni, Slokar, Alagia, 573; Kaufman, 114; Roxin, 814), meaning that the agent must have the representation of the action that can be performed. For instance, in the example above, the mother might have used a lifebuoy to save her son, but she does not notice it. In this case, it is obvious that she will not be held liable for a crime committed with intent, however negligence might be identified. The second element is the physical possibility to act (Bacigalupo, 2006: 151; Zaffaroni, Slokar, Alagia, 574), meaning that the guarantor must have the physical ability to perform the saving action. For example, if the father is paralyzed and, being in a room alone with his new born child notices that the child is suffocating, he will not be held liable for not acting, given the fact that he was physically unable to act.

Of course, in the case of the NIS officer, I the moment when a notification is emitted, they should be able to act, by this understanding that they are during the working hours as stipulated by the contract, have all the electronic means (computer, internet etc.), and are not stopped by an external cause (drugs, faint etc.).

5. THE OMISSION TO ACT

If the agent has a duty to act and has the capacity to perform the action, of course he or she must not act (Bacigalupo, 128; Zaffaroni, Slokar, Alagia, 573), in order to talk about a relevant omission. If there is an attempt to act and to save the social value, then criminal liability might not be held. However, it should be carefully analyzed on the grounds of causality why the attempt did not succeed.

6. THE CAUSALITY CONNECTION

Not every omission is criminally relevant, but only the one that is in causal connection with the dangerous result. This means, in the opinion of some authors, that there has to be certified probability that is close to certitude that, if the imposed action would have been committed, the dangerous result would not have been provoked or it would have been avoided.

CONCLUSION

It is clear that the NIS Directive, and the national laws that translate this Directive, have raised new challenges, both technical and legal, for the essential operators.

One of the first things that must be kept in mind regarding the commission by omission is the following: the omission must have, as a consequence, a material result. Therefore, the state of danger that the data of the essential services operator or administrated by it could be compromised is not a material result. Data must be blocked, deleted, lost, or the essential service must be blocked or suspended, and prejudice must be created.

Secondly, an important attention must be paid to the causality connection. Since not every omission, not even of a duty imposed by the law is relevant. Given that a technical field is involved, it should be demonstrated that, if the NIS officer would have complied with his duty, the result (consisting in data loss, or suspension of the essential service, to give just a few examples), would not have appeared. This is not something that can be easily proved, since, as we remember, the main duty of the NIS officer is only to inform of the security incident.

REFERENCES

1. Aráuz Ulloa, M. (2000) "La comisión por omission y la posición de garante", *Encuentro,* No. 54, 32-41.
2. Bacigualupo, E. (2006) *Delitos impropios de omission,* Madrid: Dykinson.
3. Crespo, E. D. (2009) "Sobre la posición de garante del empresario por la no evitación de delitos cometidos por sus empleados", *Derecho Penal Contemporáneo*: *Revista Internacional,* No. 28, 195-225.
4. Gullock, V. R. (2008) *Fundamentos teóricos básicos del delito de omisión su aplicación en el derecho penal costarricense*, Heredia, San Juaquín de Flores: Escuela Judicial.
5. Jascheck, H.H. (1993) "Problemas del delito impropio de omission desde la perspectiva del derecho penal comparado", *Nuevo Foro Penal*, No. 56, 9-23.
6. Kaufmann, A. (2006) "Dogmática de los delitos de omission, Madrid: Marcial Pons.
7. Luzón Peña, D.M. (2017) "Omisión impropria o comisión. Cuestiones nucleares: Imputación objectiva sin causalidad, posiciones de garante, equivalencia (concreción del criterio normativo de la creación o aumento de peligro o riesgo) y autoría o participación, *Libertas – Revista de la Fundación Internacional de Ciencias Penales,* No. 6, 145-272.
8. Mir Puig, S. (2006) *Derecho penal, Parte general,* Barcelona: Editorial Reppertor.
9. Nicorici, C. (2022) "Commission by Omission", in: *New Legal Reality: Challenges and Perspectives II",* Collection of research papers in conjunction with the 8th International Scientific Conference of the Faculty of Law of the University of Latvia, Riga: University of Latvia, 347-353.
10. Odeig, E.G. (1997) "La omission en la dogmática penal alemana", *Anuario de Derecho Penal y Ciencias Penales*, Vol. L, 5-112.
11. Pozo, J. H. (1987) *Manual de derecho penal*, Lima: Eddili.
12. Roxin, C. (2014) Derecho Penal, Parte General, Tomo II, Especiales formas de aparición del delito. (Traducción y notas de Diego Manuel Luzón Peña (Director) *et al.* Madrid: Civitas-Thomson Reuters.
13. Zaffaroni, E.R., Slokar, A., Alagia, A. (2002), *Derecho penal: parte general,* Buenos Aires: Editar Sociedad, Anónima Editora, Comercial, Industrial y Financiera.

NIS DIREKTIVA
I KRIVIČNA ODGOVORNOST NIS SLUŽBENIKA

NIS Direktiva (Direktiva broj 2016/1148) nametnula je viši standard u oblasti sajber bezbednosti u osam glavnih domena za koje se smatra na nivou Evropske unije da su od javnog interesa. Glavni cilj njihovog uspostavljanja bio je objedinjavanje sistema zaštite osetljivih podatka i obezbeđivanje efikasne zaštite protiv ugrožavanja sajber bezbednosti. Pored uspostavljanja adekvatnog nivoa tehničkih uslova koji podrazumevaju ulaganje materijalnih sredstava i ljudskih resursa, ova Direktiva uređuje i proceduralne aspekte kojih moraju da se pridržavaju svi relevantni operateri, a što podrazumeva primenu adekvatnih mera u slučaju sajber napada. Za krivično pravo posebno je zanimljiva uloga NIS službenika, a čija je dužnost da vrši nadzor nad bezbednosnim upozorenjima koja državni organi povremeno šalju. Međutim, postavlja se pitanje šta se dešava u situacijama ukoliko to lice ne ispunjava svoju dužnost, kao i da li to podrazumeva njegovu krivičnu odgovornost?U ovom radu se najpre osvrćemo na opšti okvir uspostavljen NIS Direktivom, kao i rumunske propise u toj oblasti, a zatim ćemo pokušati da damo odgovor na postavljena pitanja.

KLJUČNE REČI: *NIS Direktiva, sajber bezbednost, NIS službenik, odgovornost.*

DOI: https://doi.org/10.56461/ZR_22.DUKPP.26

ZAŠTITA RAČUNARSKIH PODATAKA OD KOMPJUTERSKIH VIRUSA – KRIVIČNOPRAVNI ASPEKT –

Filip Mirić*

Računarski virusi predstavljaju posebne programe koji su napravljeni da nanose štetu računarima i velikim računarskim sistemima, menjajući način njihovog funkcionisanja. U radu će nakon određivanja pojma računarskog virusa biti analizirani elementi bića krivičnog dela pravljenje i unošenje računarskih virusa iz člana 300. Krivičnog zakonika Republike Srbije (Službeni glasnik Republike Srbije, br. 85/2005...35/2019). U vezi sa ovim krivičnim delom posebno su interesantna pitanja određivanja mesta i vremena izvršenja, kao i otkrivanja izvršilaca u slučajevima kada je ono izvršeno upotrebom javno dostupnih računara i računarskih sistema.

Imajući u vidu štetu koja može nastati upotrebom kompjuterskih virusa, u radu će biti prikazani i neki slučajevi iz prakse, uz praktične savete za zaštitu od kompjuterskih virusa. U svetu prepunom digitalnih pretnji, krivično pravo mora da stvara nove inkriminacije i unapređuje postojeće, radi očuvanja bezbednosti računarskih sistema i podataka. Ovaj proces je neprekidan i dovodi do svojevrsne "digitalizacije" krivičnog prava.

KLJUČNE REČI: *računari, računarski virusi, digitalizacija, krivično pravo.*

* Autor je naučni saradnik i samostalni stručno-tehnički saradnik za studije i studentska pitanja III stepena, Pravnog fakulteta Univerziteta u Nišu. E-mail: *filip@prafak.ni.ac.rs* • *filip.miric@gmail.com*

UVOD

Ako postoji nešto što simbolizuje današnji novi svet i nove tehnologije, ako postoji nešto što nam pokazuje koliko je današnji svet mali, onda je to internet (Prlja, Ivanović, Reljanović, 2011: 5). Razvoj informacionih tehnologija doneo je mnogo toga pozitivnog čovečanstvu. Velika dostupnost informacija nesumnjivo stvara nesagledive mogućnost za napredak na svim poljima. Računarske mreže su predstavljale prekretnicu u informatičkoj revoluciji. One su se razvile kao posledica potrebe različitih vojnih i vladinih institucija u SAD (Nikolić Komlen, Gvozdenović, Radulović i dr., 2010: 10). Međutim, i ova pojava ima svoju negativnu stranu. Na internetu svi korisnici nemaju dobre namere, Mnogi od njih teže da svoje kriminalne aktivnosti ostvare u virtualnom svetu i tako dođu najčešće do protivpravne imovinske koristi. To se najčešće postiže kreiranjem posebnih programa (malware) , sa ciljem da se ovlada kompjuterima ili računarskim sistemima i od njih preuzmu određeni podaci. Reč je o kompjuterskim virusima. Računarski virusi predstavljaju posebne programe koji su napravljeni da nanose štetu računarima i velikim računarskim sistemima, menjajući način njihovog funkcionisanja. U radu će nakon određivanja pojma računarskog virusa biti analizirani elementi bića krivičnog dela pravljenje i unošenje računarskih virusa iz člana 300. Krivičnog zakonika Republike Srbije (*Službeni glasnik Republike Srbije,* br. 85/2005...35/2019, u daljem tekstu: KZ). U vezi sa ovim krivičnim delom, posebno su interesantna pitanja određivanja mesta i vremena izvršenja, kao i otkrivanja izvršilaca u slučajevima kada je ono izvršeno upotrebom javno dostupnih računara i računarskih sistema.

Imajući u vidu štetu koja može nastati upotrebom kompjuterskih virusa, u radu će biti prikazani i neki slučajevi iz prakse, uz praktične savete za zaštitu od kompjuterskih virusa. U svetu prepunom digitalnih pretnji, krivično pravo mora da stvara nove inkriminacije i unapređuje postojeće, radi očuvanja bezbednosti računarskih sistema i podataka. Ovaj proces je neprekidan i dovodi do svojevrsne "digitalizacije" krivičnog prava.

U prvom delu rada biće definisan pojam kompjuterskog virusa u krivičnom zakonodavstvu i informacionoj tehnologiji kao i osnovna podela kompjuterskih virusa prema vrsti moguće infekcije, da bi se zatim izložile osnovne karakteristike a krivičnog dela pravljenje i unošenje računarskih virusa iz člana 300. Krivičnog zakonika Republike Srbije. U ovom delu rada biće reći, o istina skromnoj, sudskoj praksi u Republici Srbiji kada je reč o ovom krivičnom delu. Ukazujući na značaj očuvanja bezbednosti računara i računarskih podataka, autor će svoju pažnju usmeriti i na praktične savete korisnicima kompjuterskih mreža i računara, uzimajući u obzir relevantnu i dostupnu literaturu iz oblasti informacionih tehnologija i bezbednosti računara na internetu. U eri lako dostupnih informacija različite vrste, očuvanje njihove bezbednosti zahteva multidisciplinarni pristup i bar osnovna znanja o kompjuterskim virusima I drugim štetnim programima svih korisnika računarskih mreža.

1. POJAM RAČUNARSKOG VIRUSA

Postoji nekoliko pojmovnih određenja računarskog virusa. U krivičnom pravu računarski virus je računarski program ili neki drugi skup naredbi unet u računar ili računarsku mrežu koji je napravljen da sam sebe umnožava i deluje na druge programe ili podatke u računaru ili računarskoj mreži dodavanjem tog programa ili skupa naredbi jednom ili više računarskih programa ili podataka (čl.112. st. 20. KZ).

Sa druge, strane prema zvaničnom sajtu kompanije Microsoft, „računarski virus je mali softverski program koji se širi sa jednog računara na drugi i ometa operaciju računara. Računarski virus može da ošteti ili izbriše podatke na računaru, koristi program za e-poštu da bi preneo virus na druge računare ili čak izbrisao sve na čvrstom disku. Računarski virusi često šire priloge u e-porukama ili razmenom trenutnih poruka. Stoga prilog e-pošte nikada ne morate da otvorite, osim ako ne znate ko je poslao poruku ili očekujete prilog e-poruke. Virusi mogu da se maskiraju kao prilozi zanimljivih slika, čestitki ili audio i video datoteka. Računarski virusi se šire i putem preuzimanja na internetu. Oni mogu da se sakriju u piranom softveru ili u drugim datotekama ili programima koje možete preuzeti."[1] Upravo ove karakteristike omogućavaju kompjuterskim virusima lako ubacivanje u različite kompjuterske sisteme i individualne računare, čime mogu da nanesu nesagledivu štetu. Računarski virusi se šire sa računara na računar slično širenju virusa između ljudi (Kephart, Sorkin, Chess, *et al*. 1997). Načini prenošenja kompjuterskih virusa su različiti; pokretanje inficiranih datoteka, korišćenje spoljnih memorija koje sadrže inficirane datoteke itd (Spafford, E. H., 1990). Razvojem društvenih mreža, i one postaju moćno sredstvo za širenje kompjuterskih virusa koji postaju ozbiljna pretnja po informacionu bezbednost svake države, što im daje i veliki krivičnopravni značaj. O krivičnom delu pravljenje i unošenje računarskih virusa iz člana 300. Krivičnog zakonika Republike Srbije, biće više reči u nastavku rada.

2. PODELA KOMPJUTERSKIH VIRUSA PREMA VRSTI INFEKCIJE

Razvojem informatike kao nauke i interneta, kao globalne računarske mreže višestruko se uvećao broj kompjuterskih virusa i ostalih kompjuterskih pretnji, tako da savremeni antivirusni programi nisu uvek u mogućnosti da ih navreme detektuju i uklone. U skladu sa tim postoje brojne podele računarskih virusa, a u okviru ovog rada će biti prikazana samo podela prema vrsti infekcije iz koje se može sagledati i način funkcionisanja pojedinih virusa. Metode infekcije se odnose na tehnike koje se koriste kako bi se virus ubacio u neki određeni fajl. Ovde govorimo o sledećim metodama infekcije:

- prepisivanje preko postojećeg fajla
- parazitiranje
- praćenje
- linkovanje

[1] *Kako se sprečavaju i uklanjaju virusi i drugi malver,* https://support.microsoft.com/sr-latn-rs/topic/kako-se-spre%C4%8Davaju-i-uklanjaju-virusi-i-drugi-malver-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5, [1.5.2022.].

- prevođenje (kompajliranje) foldera
- izmene izvornog koda aplikacije.

Prepisivanje znači da virus zamenjuje programski kod zaraženog fajla sopstvenim (briše originalni kod). Ovakav virus čini određeni fajl neupotrebljivim, javlja se greška u radu operativnog sistema ili aplikacije i virus se brzo otkriva.

Parazitiranje je proces kada virus samo delimično promeni kod fajla. Fajl i dalje ostaje operativan ali je virus ipak prisutan.

Link virusi ne menjaju host fajlove ali primoravaju operativni sistem da izvrši virusni kod i to na način što će promeniti određene sistemske fajlove.

Virusi pratioci ne menjaju kod fajla u kome se nalaze. Kada se pokrene zaraženi fajl oni će se prvi izvršiti, pa tek fajl u kome se nalaze.

Određena vrsta virusa (kompajliranje) se ne vezuje za izvršne fajlove (.exe) već se jednostavno kopira u neki od foldera na kompjuteru i čeka trenutak kada će ga korisnik pokrenuti. Postoje i one vrste virusa koji imaju imena izvršnih fajlova (install.exe) i koji mogu da svojim imenom zavaraju korisnika da ih pokrene u određenom trenutku.[2] Heterogenost računarskih virusa uslovljava posedovanje specifičnih znanja za njihovo suzbijanje, uglavnom iz oblasti informacionih tehnolog uja, čime se u okviru ovog rada nećemo detaljnije baviti. U skladu sa već definisanim predmetom i ciljem rada, u nastavku biće više reči o krivičnopravnim aspektima zaštite računarskih podataka od kompjuterskih virusa.

3. KRIVIČNO DELO PRAVLJENJE I UNOŠENJE RAČUNARSKIH VIRUSA U KRIVIČNOPRAVNOJ TEORIJI I ZAKONODAVSTVU

Krivični zakonik Republike Srbije sadrži materijalne odredbe kojima se propisuju krivična dela u vezi sa informaciono-komunikacionim tehnologijama. Ova krivična dela su uvedena u krivičnopravni sistem Republike Srbije Zakonom o izmenama i dopunama Krivičnog zakona iz 2003. godine (Zirojević & Ivanović, 2002: 229). Kao što je u teoriji krivičnog prava poznato, biće krivičnog dela obuhvata skup obeležja koje čine posebne pojmove pojedinih krivičnih dela (Stojanović & Perić, 2000: 16). U skladu sa iznetim, biće analizirano i biće krivičnog dela pravljenje i unošenje računarskih virusa. Ovo krivično delo vrši onaj ko napravi računarski virus u nameri njegovog unošenja u tuđ računar ili računarsku mrežu. Za osnovni oblik ovog krivičnog dela propisana je novčana kazna ili kazna zatvora u trajanju do 6 meseci. Kvalifikovani (teži) oblak ovog krivičnog dela vrši onaj ko unese računarski virus u tuđ računar ili računarsku mrežu i time prouzrokuje štetu, u kom slučaju je propisana novčana kazna ili kazna zatvora do dve godine. Uređaji i sredstva kojima je izvršeno ovo krivično delo se oduzimaju, što, ustvari, predstavlja obavezno izricanje mere bezbednosti oduzimanje predmeta (čl.300. KZ). Kao što se može zaključiti inkriminisano je samo pravljenje (stvaranje) računarskog virusa kao i

[2] *Kako da se zaštitite od kompjuterskih virusa?,* https://svezakomp.rs/kako-da-se-zastitite-od-kompjuterskih-virusa/, pristup [2.5.2022.].

njegovo unošenje u tuđi računar ili računarsku mrežu i prouzrokovanje štete. U pogledu vinosti potreban je direktan umišljaj, koji obuhvata svest o stvaranju kompjuterskog virusa ili njegovom unošenju u tuđi računar ili računarsku mrežu. Iako iz zakonske definicije proizilazi da izvršilac ovog krivičnog dela može svako lice, ipak kao izvršioci mogu da se u praktično jave lica koja poseduju specifična znanja za rad na računaru (Lazarević, 2006: 747-748). U tom smislu, ovo krivično delo se može svrstati u *delicta propria*.

Sa praktičnog stanovništva, zanimljivo je pitanje pravne kvalifikacije ukoliko učinilac napravi računarski virus, ubaci ga u tuđi računar ili računarsku mrežu i time prouzrokuje štetu. U opisanom slučaju, prema našem mišljenju, učinilac može biti oglašen krivim za izvršenje krivičnog dela pravljenje i unošenje računarskih virusa iz čl. 300 st. 2, u vezi st.1. KZ jer radnje u opisane u stavu 1 predstavljaju samo pripremne radnje koje ostaju van zone kažnjivosti ako se pređe na izvršenje pripremanog krivičnog dela. Ovakav stav je podržan od strane pojedinih autora u krivičnopravnoj teoriji.[3]

Poseban praktičan problem prilikom dokazivanja ovog krivičnog dela i određivanja nadležnosti sudova za vođenje krivičnih postupaka zbog izvršenja ovog i sličnih krivičnih dela predstavlja određivanja mesta i vremena njegovog izvršenja. Naime, prema teoriji jedinstva (ubikviteta) kao mesto izvršenja krivičnog dela smatra se mesto gde je učinilac preduzeo, odnosno propustio činjenje, kao i mesto gde jenastupila posledica (Jovašević, 2006: 69-70). Slično je i sa određivanjem vremena izvršenja krivičnog dela iz čl. 300. KZ. U ovom slučaju, kao i kod ostalih krivičnih dela primenjuje se teorija delatnosti, prema kojoj je krivično delo izvršeno u vreme kada je učinilac radio ili bio dužan da radi bez obzira kada je posledica nastupila (Jovašević, 2006: 70). Iako se čini da je opisan teorijski pristup dovoljno precizan za pdređivanje mesta i vremena izvršenja krivičnih dela u svakom konkretnom slučaju, to uvek nije moguće iz razloga što savremene informaciono-komunikacione tehnologije omogućavaju učiniocima krivičnih dela protiv bezbednosti računarskih podataka da ostanu anonimni, uprkos naporima nadležnih državnih organa. Odeljenje za borbu protiv visokotehnološkog kriminaliteta u Republici Srbiji za sada postoji pri Ministarstvu unutrašnjih poslova Višem sudu i Višem javnom tužilaštvu u Beogradu, što je, prema našem mišljenju, nedovoljno za suzbijanje ovog oblika kriminaliteta. Smatramo da bi ovakva odeljenja trebalo oformiti i u Nišu. Kragujevcu i Novom Sadu, u kojima se nalaze sedišta apelacionih sudova. Ovaj predlog bi, bilo korisno razmotriti prilikom nekog od narednih noveliranja zakonodavstva u ovoj oblasti.

4. KRIVIČNO DELO PRAVLJENJE I UNOŠENJE RAČUNARSKIH VIRUSA U SUDSKOJ PRAKSI

U nastavku rada biće prikazani malobrojni primeri iz prakse u vezi sa izvršenjem ovog krivičnog dela korišćenjem podataka iz pravno-informacione baze *Paragraf Lex*.

Što se tiče distribucije kompjuterskih virusa u Srbiji, 2010. godine je po prvi put podneta krivična prijava za pravljenje i unošenje računarskog virusa od kako je ovo

[3] Videti više u: Lazarević, 2006:748.

delo propisano u KZ. Krivična prijava je podneta protiv osobe iz Beograda, kome se na teret stavljalo i krivično delo prevare, a sprečeno je dalje širenje virusa na kompjutere, kao i nastajanje velike materijalne štete koju je taj računarski virus mogao da izazove. Osoba je u periodu od 2006. do februara 2010. godine koristeći svoj računar napravila «virus» tipa «IRC trojanac» pod nazivom «OMEA» koji je imao funkcije slikanja aktivnog monitora zaraženog računara, snimanja kucanja karaktera na tastaturi, kao i funkcije postavljanja sadržaja na «zaraženi» računar i skidanja sadržaja sa računara preko IRC kanala. Predstavljajući se pod lažnim imenima, osumnjičeni je slao virus kao priloge poruka putem elektronske pošte većem broju korisnika (pojedinaca, preduzeća, fakulteta, državnih ustanova) a zarazio je i računare tri nemačka državljanina. Prema navodima MUP-a, osoba je podatke koje je pribavila sa zaraženog računara nemačkog državljanina, klijenta jedne nemačke banke, iskoristila da preko internet sajta banke unese podatke u predviđena polja za tu svrhu, kako bi lažno prikazala da je korisnik i vlasnik računa i pritom je dovela u zabludu službenike da na račun jedne banke u Beogradu uplate iznos od 2.600 evra, sa lažnom svrhom «pomoć prijatelju».

Takođe, poznat je slučaj hakera iz Subotice, koji je 2011. godine uhapšen zbog sumnje da je počinio krivična dela protiv bezbednosti računarskih podataka, u saopštenju MUP-a se navodi da je osumnjičen za dela koja se odnose na pravljenje i unošenje računarskih virusa, računarske prevare i pranje novca. Osumnjičeni je u junu 2010. godine kupio računarski virus, potom ga sačuvao na zakupljenom serveru, a zatim ga je putem interneta uneo u više od 1.000 računara širom sveta, stvarajući takozvanu "botnet" mrežu kojom je upravljao sa svog servera. Koristeći zaražene računare, osumnjičeni se registrovao na torent sajtovima i postavljao fajlove sa nazivima filmova, koji nisu sadržavali film već reklamu koja je upućivala na internet sajt koji je kreirao, kako bi se preko njega preuzimali softverski sadržaj, lažno prikazujući da je sadržaj postavljenog fajla film. Ovako neregistrovanu uslugu, lice je naplaćivalo od jedne kanadske kompanije koju je dovelo u zabludu i od nje za devet meseci naplatilo preko svog deviznog računa više od 70.000 američkih dolara. Osumnjičeni je, uz krivičnu prijavu, priveden nadležnom istražnom sudiji Višeg suda u Beogradu.[4] Prikazani ukazuju na to da se krivično delo iz člana 30. KZ nedovoljno procesuira u pravosudnom sistemu Republike Srbije i da njegovi učinioci najčešće ostaju neotkriveni i nesankcionisani.

5. PREVENCIJA ŠIRENJA KOMPJUTERSKIH VIRUSA

Iako internet i posebno za to dizajniran softver daje mogućnost da se virusi anonimno šalju korisnicima, ipak postoje odrežene mere prevencije koje svaki korisnik interneta može da preduzme kako bi se zaštitio od kompjuterskih virusa i štete koju oni mogu prouzrokovati. Reč je o merama primarne prevencije usmerene ka suzbijanju računarskog kriminaliteta.

[4] *Krivična dela protiv bezbednosti računarskim podataka*-stručni komentar, Paragraf Lex, [29.4.2022.].

Preventivni koraci koji se mogu preduzeti su najbolji način da se zaštite od kompjuterskih virusa Najvažniji su sledeći:

- aktiviranje "zaštitnog zida" (Firewall);
- proveravanje sumnjivih email poruka;
- korišćenje antimalver aplikacija;
- blokiranje reklama tokom korišćenja interneta;
- redovno ažuriranje operativnog sistema;
- brisanje istorije pregledanja i keš memorije internet pregledača;
- skeniranje USB, DVD i CD;
- zaštita datoteka lozinkom i zabranom pristupa;
- korišćenje Dual But (Dual boot).

Kako bi se obezbedila adekvatna zaštita od različitih računarskih virusa, važno je napomenuti i mogućnost korišćenja *Dual Booot-a*. Naime, kompjuter poseduje mogućnost da se na njemu u isto vreme nalaze dva operativna sistema, npr. Windows i Linux. Prilikom uključivanja računara mogu se odabrati jedan od ova dva sistema i nastaviti rad u odabranom operativnom sistemu. Ukoliko kompjuterski virus zarazi vaš operativni sistem, npr. Windows bude zaražen, podacima je moguće pristupiti preko Linux operativnog sistema. Ovo je samo jedan od vidova bezbednog korišćenja računara i sprečavanja eventualne štete koja može biti naneta ličnim podacima.

Sve eksterne medije treba skenirati. Ovi mediji mogu sadržavati viruse i zlonamerni softver koji može zaraziti kompjuter. Pre korišćenja samog USB uređaja potrebno je da ga se skenira i utvrdi da li je sadržaj koji se nalazi na njemu bezbedan. Prilikom korišćenja interneta, sve informacije o posećenim sajtovima se skladište interntet pregledaču. Ovi podaci mogu biti i osetljive prirode. Iz ovih razloga je potrebno ove podatke s vremena na vreme izbrisati iz internet pregledača (istorija pregledanja i keš memorija).

Redovno ažuriranje operativnog sistema i antivirusnog programa od izuzetnog su značaja za očuvanje bezbednosti računara. Periodično objavljivanje bezbednosnih ispravki od strane Microsofta je redovna aktivnost koja služi da korisnici Windows operativnog sistema imaju najbolju moguću zaštitu. Ovakve vrste ispravki sprečavaju napade od strane virusa kojima je operativni sistem izložen. Ovde govorimo o zatvaranju bezbednosnih rupa koje Microsoft programeri nalaze. Najbolje bi bilo da uvek imate uključenu Windows update opciju kako bi se proces instaliranja ispravki.[5]

Kompjuterski virusi mogu biti korišćeni i za različite prevare koji se mogu vršiti putem računara. Kako bi se smanjila mogućnost da ovakva protivpravna i štetna delatnost bude izvršena, važno je preduzeti neke preventivne mere. Važno je učiniti sledeće:

- nikada ne otvarati elektronsku poštu koja dolazi od nepoznatih pošiljalaca;
- ne posećivati sajtove sumnjivog sadržaja;
- kod internet kupovine uveriti se da firma koja vrši prodaju zaista postoji i posluje u skladu sa pozitivnim pravnim propisima (obavezna provera u APR);

[5] *Kako da se zaštitite od kompjuterskih virusa?,* https://svezakomp.rs/kako-da-se-zastitite-od-kompjuterskih-virusa/, pristup [2.5.2022.].

- plaćanje vršiti sopstvenom platnom karticom, što olakšava dokazivanje daje plaćanje izvršeno, ako dođedo prevare) i
- kod aukcijske prodaje robe proveriti ko je sprovodi i da li to pravno ili fizičko lice legalno posluje (Mirić, 2018: 539).

Pojava interneta je dovela do neslućenih mogućnosti za prenos i obradu informacija. Živimo u eri informcija. Gotovo da se ne može zamisliti svakodnevni život bez upotrebe različitih internet i drugih informacionih servisa koji se koriste u poslovne obrazovne ili informacione slike, I upravo to virtuelno okruženje, sa mnoštvom informacija stvara pogodne uslove za različite protivpravne delatnosti. Po svojoj društvenoj opsnosti posebno se izdvajaju internet prevare. Njihova pogubnost se ogleda pre svega u nanošenju velike imovinske štete žrtvama na koju se nadovezuju i teškoće dokazivanja i otkrivanja, što je nažalost, karakteristično i za ostale oblike kompjuterskog kriminaliteta (Mirić, 2018: 539-540).

ZAKLJUČAK

Kompjuterski virusi u mnogome ugrožavaju bezbedno korišćenje interneta, a mogu dovesti i do velike materijalne štete. Osim problema otkrivanja učinlaca krivičnog dela iz člana 300. KZ nameće se i problem određivanja mesta i vremena izvršenja ovog krivičnog dela. Skromna sudska praksa u ovoj oblasti nije od pomoći prilikom rešavanja ovog praktičnog problema. Teorija ubikviteta i teorija delatnosti, kao što smo videli predstavljaju samo delimično rešenje ovog problema jer ne može uvek lako odrediti mesto i vreme izvršenja ovog krivičnog dela.

Sa ciljem poboljšanja krivičnoprocesnih uslova za efikasnije otkrivanje i procesuiranje učinilaca krivičnih dela iz oblasti računarskog kriminaliteta, valjalo bi istaći da Odeljenje za borbu protiv visokotehnološkog kriminaliteta u Republici Srbiji za sada postoji pri Ministarstvu unutrašnjih poslova Višem sudu i Višem javnom tužilaštvu u Beogradu, što je, prema našem mišljenju nedovoljno za suzbijanje ovog oblika kriminaliteta. Smatramo da bi ovakva odeljenja trebalo oformiti i u Nišu. Kragujevcu i Novom Sadu, u kojima se nalaze sedišta apelacionih sudova. Ovaj predlog bi, bilo korisno razmotriti prilikom nekog od narednih noveliranja zakonodavstva u ovoj oblasti.

Sa praktičnog stanovišta zanimljivo je i pitanje pravne kvalifikacije ukoliko učinilac napravi računarski virus, ubaci ga u tuđi računar ili računarsku mrežu i time prouzrokuje štetu. U opisanom slučaju, prema našem mišljenju, učinilac može biti oglašen krivim za izvršenje krivičnog dela pravljenje i unošenje računarskih virusa iz čl. 300 st. 2, u vezi st.1. KZ jer radnje u opisane u stavu 1. predstavljaju samo pripremne radnje koje ostaju van zone kažnjivosti ako se pređe na izvršenje pripremanog krivičnog dela.

Kako bi se sprečilo širenje računarskih virusa, od posebnog ke značaja primena preventivnih mera i zaštita ličnih podataka posebnim programima za enkripciju. Sofisticirano informatičko znanje svih onih koji prave i šire različite kompjutweske viruse, nužno je suprostaviti znanje, umeće itehniku nadležnih državnih organa kako bi virtualni svet računara postao zaista bezbedan.

LITERATURA

1. Jovašević, D. (2006) *Krivično pravo - opšti deo*, Beograd: Nomos.
2. Kephart, J. O., Sorkin, G. B., Chess, D. M., White, S. R. (1997) "Fighting Computer Viruses", *Scientific American*, *277*(5), 88–93.
3. Krivični zakonik Republike Srbije (*Službeni glasnik Republike Srbije,* br. 85/2005...35/2019).
4. Lazarević, L. (2006) *Komentar Krivičnog zakonika Republike Srbije*, Beograd: Savremena administracija.
5. Mirić, F. (2018) "Internet prevara kao oblik kompjuterskog kriminaliteta", *Zbornik radova Pravnog fakulteta u Nišu*, vol. 80, 531-542.
6. Nikolić Komlen, L., Gvozdenović, R., Radulović, S., Milosavljević, A., Jerković, R., Živković, V., Živanović, S., Reljanović, M., Aleksić, I. (2010) *Suzbijanje visokotehnološkog kriminala*, Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije.
7. Prlja, D., Ivanović, Z., Reljanović, M. (2011) *Krivična dela visokotehnološkog kriminala*, Beograd: Institut za uporedno pravo.
8. Stojanović, Z., Perić, O. (2000) *Krivično pravo- posebni deo*, Beograd: Službenik glasnik.
9. Zirojević, M., Ivanović, Z. (2002) *Cyber law - Serbia*, Belgrade: Institute of Comparative Law.

Internet izvori

1. *Kako da se zaštitite od kompjuterskih virusa?,* https://svezakomp.rs/kako-da-se-zastitite-od-kompjuterskih-virusa/, [2.5.2022.].
2. *Kako se sprečavaju i uklanjaju virusi i drugi malver,* https://support.microsoft.com/sr-latn-rs/topic/kako-se-spre%C4%8Davaju-i-uklanjaju-virusi-i-drugi-malver-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5, [1.5.2022.].
3. *Krivična dela protiv bezbednosti računarskim podataka*-stručni komentar, Paragraf Lex, [29.4.2022.].
4. Spafford, E. H. (1990). Computer Viruses-A Form of Artificial Life?, https://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1836&context=cstech, [1.5.2022.].

PROTECTION OF COMPUTER DATA FROM COMPUTER VIRUSES – CRIMINAL LAW ASPECT –

Computer viruses are special programs designed to harm computers and large computersystems by changing the way they work. After defining the term computer virus, author in the paper will analyze the elements of the criminal offense of Creating and Introducing of Computer Viruses from Article 300 of the Criminal Code of the Republic of Serbia (Official Gazette of the Republic of Serbia, No. 85/2005...35/2019). In connection with this criminal offense, the issues of determining the place and time of execution, as well as the detection of perpetrators in cases when it was committed using publicly available computers and computer systems, are particularly interesting.

Having in that mind the damage can occur with the use of computer viruses, the paper will present some practical cases, along with practical tips for protection against computer viruses. In a world full of digital threats, criminal law must create new incriminations and improve existing ones, in order to preserve the security of computer systems and data. This process is continuous and leads to a kind of "digitalization" of the criminal law.

KEYWORDS: *computers, computer viruses, digitization, criminal law.*

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

343.533::004(082)
343:004.7(082)

МЕЂУНАРОДНИ научни скуп дигитализација у казненом праву и правосуђу (7 ; 2022 ; Београд)

Tematski zbornik radova međunarodnog značaja / VII međunarodni naučni skup digitalizacija u kaznenom pravu i pravosuđu, Beograd, novembar 2022. = Thematic Conference Proceedings of International Significance / VII International Scientific Thematic Conference Digitalization in Penal Law and Judiciary, Belgrade, november 2022 ; urednici, editors Jelena Kostić, Marina Matić Bošković. - Beograd : Institut za uporedno pravo : Institut za kriminološka i sociološka istraživanja = Institute of Comparative Law : Institute of Criminological and Sociological Research, 2022 (Aranđelovac : Tri O). - X, 404 str. ; 24 cm

Tiraž 200. - Reč urednika = A Word from the Editors: str. VII-X. - Napomene i bibliografske reference uz tekst. - Bibliografija uz svaki rad. - [Rezimei ; abstracts].

ISBN 978-86-80186-92-4 (IUP)

ISBN 978-86-80756-52-3 (IKSI)

а) Рачунарска технологија -- Злоупотреба -- Зборници б) Кривично право -- Дигиталне технологије -- Зборници

COBISS.SR-ID 84081161

ISBN 978-86-80186-92-4 (IUP)
ISBN 978-86-80756-52-3 (IKSI)