Originalni naučni rad
DOI: 10.5937/gakv96-48068
UDC 34:004

Magdalena Primorac[*]
Pravni fakultet Univerziteta u Mostaru
ORCid: 0009-0002-6081-5300

PRAVNI SUSTAV PRED IZAZOVIMA TEHNOLOŠKOG NAPRETKA[**]

SAŽETAK: Moderno društvo svoje temelje za budućnost gradi na tehnologiji i znanosti. Ubrzani tehnološko-znanstveni napredak mijenja materiju koju pravni sustav regulira ili bi trebao regulirati. Razvoj novih tehnologija s posebnim naglaskom na razvoj i primjenu umjetne inteligencije na području prava otvara revolucionarna pitanja. Stoga će se u radu analizirati utjecaj tehnologije na područje kaznenog i građanskog prava te izazove zaštite ljudskih prava u digitalnom dobu primjenom znanstvenih metoda kako slijede: kompilacije, analize literature, sinteze i klasifikacije. Istraga i kazneni progon digitalnih zločina zahtijeva poštivanje pravičnih pravnih načela i zaštitu prava pojedinca. Nove tehnologije stavljaju pritisak na pravni sustav koji pod tim pritiskom krši temeljna pravna načela. Tehnološka dostignuća nude priliku njihove primjene u pravosuđu, a samo implementiranje istih otvara pitanje vladavine prava. Suvremeni pravni izazovi dovode do „tektonskih pomjeranja" na području prava. Pravni sustavi ne susreću se prvi put s reguliranjem neživog sustava koji nema svijest i sposobnost za krivnju. Ključno pitanje je jesmo li spremni na revolucionaran korak uvođenja trećeg pravnog subjekta – elektroničke osobe.

Ključne reči: pravo, nove tehnologije, krivnja, elektronička osoba

[*] e-mail: Primorac2020@outlook.com, studentkinja doktorskih studija.

[**] Rad je primljen 4. 12. 2023, izmenjen 21. 3. 2024, a prihvaćen je za objavljivanje 21. 10. 2024. godine.

Tekst je objavljen u izvornom obliku, bez lektorskih intervencija redakcije *Glasnika Advokatske komore Vojvodine*.

UVOD

Razvoj i primjena novih tehnologija dovode do promjena koje su prije desetak godina bile nezamislive. Razvojem ChatGPT i sličnih alata umjetna inteligencija ulazi u postepenu evoluciju i otvaraju se vrata implementacije iste u različita područja. Istovremeno ChatGPT popularizirao je umjetnu inteligenciju i naše društvo postalo je svjesno potencijala VI. Znanje na području tehnologije zatvara pitanje što možemo razvijati kao suvremeno društvo i više se ne čini tako nestvarno da bi se umjetna inteligencija u budućnosti mogla razviti kao autonomni sustav. Cilj rada je istražiti suvremena pravna pitanja te analizirati mogućnost priznavanja pravnog subjektiviteta umjetnoj inteligenciji. Svrha istraživanja je potvrditi ili odbaciti potrebu izmjene pravnog sustava u svrhu prilagodbe digitalnom dobu. Početne hipoteze su H1: područje tehnologije potrebno je pravno regulirati novim zakonima, H2: digitalni dokazi imat će sve veći značaj u sudskim sporovima. H3: pravni sporovi budućnosti sve više će se doticati novih tehnologija. Napredak na području tehnologije i razvoj VI pruža mogućnost primjene nove tehnologije u pravosudnom sustavu te možemo govoriti o razvoju pravne tehnike. Pravna tehnika odnosi se na bilo koju „tehnologiju temeljenu na algoritmima u pravnim stvarima“. Između ostalog to također obuhvaća mogućnost donošenja odluka temeljenih na algoritmima u provedbi zakona i pravosuđu, kao i raspravu o elektroničkoj osobnosti i utjecajima koje pametni ugovori i poslovni modeli temeljeni na algoritmima imaju na pravni sustav. Primjena tehnologije u pravosuđu nije budućnost već sadašnjost pojedinih pravnih sustava u svijetu. Tehnologija u SAD-u, Kini, Njemačkoj igra veliku ulogu u jurisdikciji. Preostaje nam vidjeti hoće li se pravo promatrano na globalnoj razini pred izazovima tehnologije pokazati kao živi sustav koji drži korak sa suvremenim društvom te je spreman na transformaciju ili će odabrati strogost i ne dopustiti značajne izmjene u području načela krivnje i pravnih subjekata. Najveći izazov je što se nove tehnologije aktivno primjenjuju bez pravne reguliranosti. Pravni sustav susreće se i susretat će se s pitanjima u praksi koja nisu obrađena nigdje u teoriji niti su obuhvaćena zakonskim regulativama. Kako tehnologija postaje sve autonomnija, definiranje odgovornosti postaje kompleksnije. Čovjek nije nepogrješiv, pa tako niti ono što stvara svojim vještinama i znanjem. Ako čovjek pogriješi snosi sankcije za posljedice do kojih je njegova pogreška dovela, no što kada pogriješi autonoman sustav kojeg je programirao čovjek, hoće li odgovarati „kreator“ ili „kreacija“?

KAZNENO PRAVO I TEHNOLOGIJA

Budućnost društva je digitalna, a izazovi koje ista nosi sa sobom odražavaju se i na kazneno pravo. U najširem smislu, kazneno pravo obuhvaća propise kojima se određuju sva kažnjiva ponašanja i sankcije za njihove počinitelje, odnosno sadržaj i opseg ovlasti države na kažnjavanje. Uži smisao, odnosi se na kaznena djela kao najteža kažnjiva ponašanja te kaznene sankcije i uvjete njihove primjene.[1] Na utjecaje novih tehnologija nije ostao imun niti kazneno-pravni sustav kojem je potrebna doza novih zakona da ispuni svoju temeljnu obvezu zaštite čovjeka. Kazneno pravo nalazi se na raskrižju na kojem treba odabrati podvlačenje novih kaznenih djela pod postojeće zakone ili transformaciju kazneno-pravnog sustava kroz formiranje novih zakona koji će direktno biti usmjereni na područje tehnologije. Kao posljedica zloupotrebe tehnologije područje ilegalnih aktivnosti postaje sve šire i nepoznatije. Uslijed digitalizacije ilegalnih aktivnosti potrebna su nam nova znanja koja ćemo koristiti prilikom pristupa novim kaznenim djelima, počiniteljima, dokazima i žrtvama. Stoga se danas razvija digitalna kriminologija koja se odnosi na znanstveno područje koje primjenjuje kriminološku, društvenu, kulturnu teoriju, teoriju tehničkih sustava i odgovarajućih istraživačkih metoda, u proučavanju zločina, delikventnog/devijantnog ponašanja i pravde u digitalnom društvu.[2] Kazneno-pravni sustav treba prepoznati kibernetički prostor kao prostor u kojem se odvija nasilje, prijetnje, prodaja droge… Pod okriljem kripto tržišta razvile su se kripto valute koje nam se prezentiraju kao novac budućnosti. Kripto valutama je nemoguće ući u trag, a upravo je anonimnost u virtualnom prostoru ono što otežava pronalaženje počinitelja kaznenih djela. Suvremena kaznena djela odvijaju se bez da se žrtva i počinitelj susretnu. U ulozi žrtve ili počinitelja može se pronaći svatko od nas u bilo kojem trenutku. Osim što cyber kriminal karakterizira teško pronalaženje počinioca „virtualnih" kaznenih dijela jednako tako karakterizira ga da pojedinci koji su bili žrtva kibernetičkog kriminala u većini slučajeva prekasno prijave isti. Suvremeni oblici kriminala i terorizma prate tehnološke „trendove" i prilagodljivi su modernom dobu. Tehnologija mijenja način na koji se zločini događaju, vrste dokaza dostupnih nakon počinjenja zločina, način na koji policija istražuje zločin i još mnogo toga.[3]

---

[1] Cvitanović, L., Derenčinović, D., Horvatić, Ž. (2016). *Kazneno pravo: Opći dio I.* Zagreb: Pravni fakultet Sveučilišta u Zagrebu, 7.

[2] Spyropoulos, F. (2009). *Technoethics, AI and Criminal Law.* Dostupno na: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Fourth_intersessional_consultation/Panel_3_Spyropoulos_Center_for_the_Study_of_C.pdf, pristupljeno 1. 10. 2023.

[3] Throckmorton, B. (2018). *Technology and criminal law.* Dostupno na: https://jolt.richmond.edu/2018/02/11/technology-and-criminal-law/, pristupljeno 1. 10. 2023.

KAZNENO-PRAVNA NAČELA PRED IZAZOVIMA NOVIH TEHNOLOGIJA

Područje tehnologije rapidno se mijenja i suvremeni pravni izazovi ne odražavaju se na zakone već na temeljna pravna načela. U ovom dijelu rada analizirat će se načelo zakonitosti i načelo krivnje kroz prizmu razvoja novih tehnologija. Načelo zakonitosti obično se izražava u latinskom obliku *nullum crimen sine lege, nulla poena sine lege*, što znači da nema kaznenog djela bez zakona i nema kazne bez zakona.[4] Postojanje kaznenog djela i kazneno-pravne sankcije unutar zakona prije počinjenja kaznenog djela imperativ je za ostvarivanje pravne sigurnosti. Načelo zakonitosti preuzeto je i kao ustavnopravno načelo većine suvremenih država, a svoje mjesto je pronašlo i u Europskoj konvenciji o zaštiti ljudskih prava i temeljnih sloboda (u daljnjem tekstu Konvencija). Navedeno je pokazatelj važnosti načela zakonitosti za zaštitu ljudskih prava. Načelo zakonitosti konkretizira se kroz četiri zahtjeva: zakon mora biti u pisanoj formi, zabrana retroaktivne primjene kaznenog zakona, precizna određenost ponašanja koje se predviđa kao kazneno djelo i zabrana prava analogijom.[5] Dinamika razvoja tehnologije i novih aplikacija, u ovom slučaju onih kriptiranih odrazila se na načelo zakonitosti. Pristupiti prema kriptiranim aplikacijama kao pravnom dokazu ili ga odbaciti postaje globalno pravno pitanje. Sud u Bosni i Hercegovini prihvaća dokaze prikupljene hakiranjem kriptiranih aplikacija kao valjan,[6] dok odvjetnici u Srbiji i Crnoj Gori dovode u pitanje legitimnost takvih dokaza.[7] Međutim autor neće analizirati dokaznu težinu navedenih aplikacija već njihovu legalnost. U Turskoj se dogodio slučaj hapšenja pojedinaca zbog posjedovanja kriptiranih aplikacija koje su se smatrale jedinim dokazom povezanosti pojedinaca sa terorističkom organizacijom. Zakoni koji izričito zabranjuju korištenje takvih aplikacija trenutno ne postoje i sama činjenica posjedovanja istih ne mora nužno značiti njihovo korištenje za ilegalne aktivnosti i povezanost sa kriminalnim ili terorističkim grupama. Kriptirane aplikacije, iako trenutno ne regulirane specifičnim zakonima,

[4] Horović, S. (2020). *Kazneno pravo – Opći dio.* Mostar: Sveučilište u Mostaru, 44.

[5] *Ibid.,* 45.

[6] Sud Bosne i Hercegovine potvrdio je prvu optužnicu u kojoj su korišteni dokazi iz SKY i ANOM aplikacija, što je potvrđeno je 16. 12. 2022. iz Tužiteljstva BiH. Optuženi su D. R., A. M., I. R., H. G., M. V., Ž. S., A. I. i G. G. Vidi više na: https://www.slobodnaevropa.org/a/sky-aplikacija-anom-bih-hapsenje-ubistvo-policajac/32179874.html, pristupljeno 13. 3. 2024. i https://www.tuzilastvobih.gov.ba/files/docs/Anonimizirana_optuznica_Dalibor_Railic_i_dr.-fin.pdf

[7] Jovanović, J., Mihajlović, D. (2022). *Advokati tvrde da Sky poruke ne mogu biti dokaz na sudu.* Dostupno na: https://www.vijesti.me/vijesti/crna-hronika/635617/advokati-tvrde-da-sky-poruke-ne-mogu-biti-dokaz-na-sudu, pristupljeno13. 3. 2024.

postavljaju zanimljiva pravna pitanja. Kako pravni sustav može reagirati na tehnološke inovacije koje nisu eksplicitno obuhvaćene postojećim zakonima i trebaju li se formirati zakoni koji navode određene tehnološke inovacije kao ilegalne? Europski sud za ljudska prava u predmetu *Üçdağ protiv Turske*[8] odlučio je da sama činjenica postojanja instalirane aplikacije ByLock nije dovoljna za osnovanu sumnju određivanja pritvora, već moraju postojati i drugi dokazi kako bi se mogla ustanoviti osnovana sumnja.[9] Nemamo zakon u pisanoj formi kojim je posjedovanje kriptiranih ili bilo kojih drugih aplikacija okarakterizirano kao ilegalno, stoga se pritvor ili bilo koja druga mjera ne može izreći samo na osnovu postojanja instaliranih kriptiranih aplikacija. Pretpostavka da će biti korištene za ostvarivanje komunikacije između kriminalnih skupina, kao što je to bio slučaj sa Sky i Anom aplikacijama, značio bi analogiju. Kriptirane aplikacije pokazale su nespremnost pravnog sustava na tehnološke novitete. S druge strane razvoj umjetne inteligencije označio je početak nove ere cyber kriminala i cyber terorizma. Istovremeno se otvorilo novo pitanje, može li umjetna inteligencija biti pravno odgovorna? Čovječanstvo je tisućljećima sanjalo o stvaranju umjetnog bića koje misli i djeluje ljudski, a ovaj san će se uskoro ostvariti.[10] Umjetna inteligencija rezultira nizom pravnih pitanja među kojima je i načelo krivnje. Načelo krivnje jedno je od najznačajnijih pravnih načela. Izraženo je maksimom „nema kazne bez krivnje[11]“. Krivnja predstavlja „subjektivni odnos počinitelja prema djelu zbog kojeg mu se može uputiti prijekor“[12]. Umjetna inteligencija kao neživi sustav nema razvijenu svijest i kao takva ne može se uklopiti u postojeće pravne okvire. Bez pravne regulacije umjetne inteligencije dovest ćemo se u situaciju da imamo oštećene, a nemamo odgovorne. Ako bi se svijet susreo sa zločinom iza kojega stoji umjetna inteligencija postavlja se pitanje koga bi kaznili? Isto pitanje javlja se i kada govorimo o pogrešci umjetne inteligencije. Međutim ne susreće se kazneno pravo po prvi put s izazovom reguliranja odgovornosti neživog sustava bez svijesti. U pravu se primjenjivalo načelo *societas delinquere non potest* koje pravne osobe ostavlja izvan kaznenog prava, pri čemu su izrečeni različiti argumenti, da pravne osobe ne mogu počiniti kazneno djelo, da im nedostaje volja, da je krivnja kao prijekor moguća samo kod fizičkih osoba, da kazna predstavlja individualnu kaznenu odgovornost pa se kažnjavanje tih

[8] *U. v. Turkey*, (App. no. 23314/19), 31. 8. 2021.

[9] AIRE Centar. (2023). Kriptirane aplikacije u fokusu evropskog pravosuđa. *Pravna hronika,* vol. 16.

[10] Karlsson, M. (2017). *Artificial Intelligence and the External Element of the Crime An Analysis of the Liability Problem.* Dostupno na: https://www.diva-portal.org/smash/get/diva 2:1115160/FULLTEXT01.pdf, pristupljeno 5. 10. 2023.

[11] Horović, S. (2020). *Kazneno pravo – Opći dio.* Mostar: Sveučilište u Mostaru, 97.

[12] Novoselec, P. (2016). *Opći dio kaznenog prava*. Osijek: Sveučilište u Osijeku, 101.

osoba protivi prirodi, smislu i funkciji kazne i suprotno ciljevima kažnjavanja. Postupno je ovo načelo napušteno i prihvaćeno je novo načelo *societas delinquere potest* koje se zasniva na realnoj teoriji. Ovim načelom pravna osoba dobiva sposobnost da odgovara za kazneno djelo. Vijeće Europe je 1988. donijelo preporuke o kažnjavanju pravnih osoba.[13] Autorica Horović navodi da je „kaznena odgovornost pravnih osoba u pravne sustave Švicarske, Češke i Hrvatske uvedena 2003, a u pravne sustave Srbije i Crne Gore 2006".[14]

Navedeno je pokazatelj da prepoznavanje kazneno-pravne odgovornosti pravnih osoba u kaznenim zakonima nije učinjeno toliko davno te iako trenutno izgleda nemoguće da umjetna inteligencija bude kaznenopravno odgovorna kao neživo biće takvo shvaćanje vremenom se može promijeniti. Daljnji tehnološkim napredak rezultirat će nizom pravnih, sigurnosnih i etičkih pitanja. Ključno je da pravni sustav prepozna potrebu pravne regulacije tehnologije i time spriječi mogućnost ugrožavanja temeljnih ljudskih prava. Nova kaznena djela zahtijevaju nove pristupe i spoznaje stoga je potrebno da stručnjaci s područja prava, tehnologije i sigurnosti razmjenjuju svoja znanja. Uslijed digitalnog razvoja mijenja se i domena kaznenog prava. Imperativ je da kazneni zakoni budu u korak s tehnološkim napretkom i razvojnim trendovima u digitalnom kriminalu. Uspostavljanje nedvosmislenih i učinkovitih protokola koji se odnose na kibernetički kriminal može pružiti snažan pravni okvir za provođenje zakona i omogućiti zaštitu stanovništvu.[15]

DIGITALNI DOKAZI

Razvojem tehnologije mijenjaju se i sredstva kojima se izvršavaju kaznena dijela i pojavljuju se novi oblici dokaza. Gotovo sve suvremene države prepoznaju digitalne dokaze i uređuju načine na koji se oni mogu koristiti kao dokazna sredstva. Koliko će ih teško ili lako biti pronaći ovisi i o tehnološkom znanju samog počinitelja. Prikupljanje i korištenje elektroničkih dokaza u istrazi i procesuiranju kaznenih djela često predstavlja izazov zbog potencijalnog sukoba između imperativa prikupljanja takvih dokaza i imperativa zaštite prava na privatnost pojedinaca.[16] Bavljenje kibernetičkim kriminalom

[13] Horović, S. (2020). *Kazneno pravo – Opći dio.* Mostar, Sveučilište u Mostaru, 98.

[14] *Ibid.,* 99.

[15] Silahi, J. (2023). *The Application of Criminal Law in the Digital Age: A Literature Review of Challenges and Opportunities.* Dostupno na: https://j-innovative.org/index.php / Innovative/ article/download/678/590, pristupljeno 20. 10. 2023.

[16] Kotecha, B. (2020). The International Criminal Court's Selectivity and Procedural Justice, *Journal of International Criminal Justice*, Vol. 18. Dostupno na: https://doi.org /10.1093/jicj/mqaa020, pristupljeno 13. 3. 2024.

zahtijeva stručnost stručnjaka za digitalnu forenziku koji posjeduju specijalizirana znanja i kompetencije u prikupljanju i ispitivanju digitalnih dokaza.[17] Samo korištenje digitalnih dokaza izazovno je zbog privatnosti elektroničkih podataka. Digitalni dokazi i digitalna forenzika imaju velik značaj za pravni sustav i samo kriminalističko istraživanje. Uzimajući u obzir da će razvoj tehnologije oblikovati počinjenje kaznenih djela i sam značaj digitalnih dokaza bit će veći. Stoga je ključno utvrditi razinu kvalitete digitalnog dokaza koji će biti upotrijebljen prije samog suđenja.[18] U suprotnom moglo bi se dovesti u pitanje pravičnost suđenja. Potrebno je uložiti napore znanja budućih tužitelja i sudaca o mogućnostima i izazovima digitalnih dokaza, te osposobljavati službenike za bolje prikupljanje i očuvanje digitalnih dokaza.[19] U svom istraživanju Kavazović i ostali ističu da

> „...kod prikupljanja digitalnih dokaza načelo zakonitosti predstavlja jedno od temeljnih načela, jer zakonitost u prikupljanju digitalnih dokaza ima ključan značaj za njihovu vrijednost u kaznenom postupku.“[20]

Također navode da se

> „...u domaćoj stručnoj literaturi koja se bavi pitanjem pribavljanja, odnosno postupanja sa ovom vrstom dokaza prilikom definiranja slijedi se pristup razvijen u stranoj stručnoj literaturi, prema kojem se digitalni dokaz poistovjećuje sa informacijom koja se pohranjuje ili prenosi u binarnoj, digitalnoj formi, a koja ima određenu dokaznu vrijednost u sudskom postupku.“

U svom istraživanju navedeni autori ističu

---

[17] Stoykova, R., Andersen, S., Franke, K., Axelsson, S. (2022). *Reliability assessment of digital forensic investigations in the Norwegian police. Forensic Science International: Digital Investigation,* (Vol. 40). Dostupno na: https://www.sciencedirect.com/science/article/pii/S0267364923000110, pristupljeno 14. 3. 2024.

[18] Stoykova, R. (2023). The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations. *Computer Law & Security Review,* Vol 49. Dostupno na: https://www.sciencedirect.com/science/article/pii/S0267364923000110, pristupljeno 14. 3. 2024.

[19] Goodison, E., Jackson, D. (2015). *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence.* Dostupno na: https://www.rand.org/pubs/research_reports/RR890.html, pristupljeno 11. 10. 2023.

[20] Kavazović, M., Bajraktarević Pajević, D., Lučić-Ćatić, M., Puharić, P. (2019). Kriminalističko postupanje sa digitalnim dokazima u praksi policijskih agencija u BiH. *Kriminalističke Teme,* Vol 5. Dostupno na: https://krimteme.fkn.unsa.ba/index.php /kt/article/view /231, pristupljeno13. 3. 2024.

> „...da međunarodna organizacija o kompjuterskim dokazima[21] na sličan način određuje digitalni dokaz kao informaciju pohranjenu ili prenesenu u binarnoj formi na koju se može osloniti pred sudom“[22]

kao i

> „...da se u procesnim zakonima Bosne i Hercegovine ne definira što se podrazumijeva pod zakonitim digitalnim dokazima, već se naprotiv fokusira na koncept nezakonitih dokaza“[23].

Pravna pitanja u vezi s digitalnim dokazima samo su djelomično riješena u većini jurisdikcija, no postoji tendencija reguliranja na načelnoj i nadnacionalnoj razini, s fokusom na suradnju u provedbi zakona.[24] Drugi dodatni Protokol uz Konvenciju o kibernetičkom kriminalu koji ima za cilj omogućiti prekogranični pristup i razmjenu digitalnih dokaza usvojen je na razini Vijeća Europe.[25] Potrebno je napomenuti da određenje pojma digitalnog dokaza otežava učestalo izjednačavanje pojmova „digitalni dokaz“ i „elektronski dokaz“ u teoriji i praksi, iako nisu u pitanju sinonimi.[26] Sve veći dio naše stvarnosti seli se u virtualni prostor i većina djelatnosti prolazi kroz procese digitalizacije samim time rasti će i stope kibernetičkih napada i kibernetičkog kriminala. Neprestani razvoj tehnologije rezultira novim i složenijim formama cyber kriminala. Javljaju se novi, suptilniji znatno opasniji oblici kriminalnog ponašanja, do sada nepoznati kriminalističkoj praksi.[27] Ključno je razvijati svijest i znanja o digitalnim dokazima i njihovom utjecaju na kazneno pravo, te samo vođenje sudskih postupaka. Najveći izazov je samo pravno definiranje pojmova kao što su cyber kriminal, cyber terorizam, digitalni dokaz, elektronički dokaz, umjetna inteligencija...

---

[21] *International Organization on Computer Evidence.*

[22] Kavazović, M., Bajraktarević Pajević, D., Lučić-Ćatić, M., Puharić, P. (2019). *Op. cit.*, 354.

[23] *Ibid.*

[24] United nations office on drugs and crime (2013). Comprehensive Study on Cybercrime, *Op. cit.*, 183. Dostupno na: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf, pristupljeno 15. 3. 2024.

[25] Council of Europe (2021). Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence. Dostupno na: https://www.coe.int/en/web/cybercrime/second-additional-protocol, pristupljeno 15. 3. 2024.

[26] Kavazović, M., Bajraktarević Pajević, D., Lučić-Ćatić, M., Puharić, P. (2019). Kriminalističko postupanje sa digitalnim dokazima u praksi policijskih agencija u BiH. *Kriminalističke teme*, vol. 5. Dostupno na: https://krimteme.fkn.unsa.ba/index.php /kt/article/view /231, pristupljeno 13. 3. 2024, 377.

[27] Bošković, M., Marković, M. (2015). *Kriminologija sa elementima viktimologije.* Novi Sad, 297.

TEHNOLOGIJA I GRAĐANSKO PRAVO

Razvoj tehnologije utječe na građansko pravo, a posebno razvoj umjetne inteligencije. Koncept „digitalnog društva" i digitalnih prava je relativno nov objekt građanskih prava. Znanost građanskog prava suočava se s teškim zadatkom razvijanja novih doktrinarnih pristupa pravnom uređenju društvenih odnosa povezanih s pojavama i uporabom novih tehnologija u gospodarstvu i drugim sferama života u suvremenom društvu.[28] Nedostatak normi koje reguliraju osobitosti pravnog režima za nositelje umjetne inteligencije, rezultate intelektualnog rada koje su oni stvorili, unosi nesigurnost u regulaciju nastalih odnosa i dolazi u sukob s trenutnim zakonodavstvom u sferi intelektualnog prava, kao i norme koje definiraju pravni položaj subjekata građanskog prava i osnove pravne odgovornosti.[29] Radnje umjetne inteligencije mogu uzrokovati štetu, a zakoni unutar građanskog prava koji se dotiču odgovornosti za štetu nastalu nečijom krivnjom ili rizikom formirani su prije razvoja VI i kao takvi neučinkoviti su za reguliranje ovih pitanja. Stoga se i na području građanskog prava otvaraju jednaka pitanja kao i na području kaznenog, trebaju li se postojeći propisi u potpunosti promijeniti ili primjereno prilagoditi. Građansko pravo odnosi se i na zaštitu ne materijalnih dobara te se otvara novo pitanje kako zaštititi ugled u digitalnom dobu? Ako čovjek ošteti ugled drugog ili pravne osobe pišući neistine koje plasira unutar virtualnog prostora, ali ispod takvih objava stavi da je tekst generirala umjetna inteligencija dovodi se u pitanje koga smatrati odgovornim? Unutar zakona nije regulirano tko je nositelj prava nad sadržajima koje generira umjetna inteligencija. ChatGPT postao je sinonim za umjetnu inteligenciju te iako je riječ o chatbotu kojeg pokreće umjetna inteligencija, isti je rezultirao nizom pravnih pitanja na koje nemamo pravnih odgovora. Razvoj generativne umjetne inteligencije otvara pitanja tko je nositelj autorskih prava i odgovornosti nad generiranim sadržajem. Pravni sustavi imaju različite pristupe u odgovoru na kompleksna pravna pitanje koja budi novi tehnološki fenomen. Kina[30] priznaje autorska prava umjetnoj inteligenciji navodeći da zadovoljava minimum originalnosti, dok Europa i SAD-e odbijaju priznati autorsko pravo umjetnoj inteligenciji kao neživom sustavu. Kada je umjetna inteligencija dobila glas otvara se pitanje potrebe pravne

[28] Kamyshanskiy, V., Stepanov, D., Mukhina, I., Kripakova, D. (2020). *Digital society, artificial intelligence and modern civil law: challenges and perspectives SHS Web of Conferences* (Vol. 109). Dostupno na: https://www.shsconferences.org/articles/shsconf/pdf/2021/20 /shsconf _lisid2021_01016.pdf, pristupljeno 16. 3. 2024.

[29] *Ibid.*

[30] Sud u Kini smatra da „odabir može zadovoljiti minimalni stupanj originalnosti" i zauzima pozitivan stav o zaštiti autorskih prava djela generiranih umjetnom inteligencijom (vidi slučaj *Shenzhen Tencent Computer System protiv Shanghai Yingxun Technology*).

zaštite glasa. Pomoću umjetne inteligencije moguće je tuđi glas bez pristanka te osobe koristiti u različite svrhe. Najjednostavniji primjer je predstavljanje dokumentarca iza kojeg stoji glas umjetne inteligencije koji je zapravo glas poznatog glumca. Automatski se otvara pitanje jeli moguće pokrenuti tužbu i na kraju krajeva prema kome je usmjeriti.

SUBJEKTI GRAĐANSKOG PRAVA

Subjekti građanskog prava su pravne i fizičke osobe koje imaju pravnu, poslovnu i deliktnu sposobnost. Pitanje ima li pravna osoba poslovnu sposobnost bilo je jedno od najspornijih pitanja na području teorije o pravnim osobama. Danas to pitanje pomalo gubi na važnosti, jer prevladava shvaćanje da pravna osoba može biti nositelj prava i obveza. Priznavanje poslovne sposobnosti pravne osobe bilo je polazna točka i za priznanje deliktne sposobnosti pravne osobe.[31] Umjetna inteligencija koliko god mogla oponašati čovjeka nije fizička osoba i teško da će se kao takva tretirati u pravu. Međutim nije niti skup fizičkih osoba kao što je to slučaj sa pravnim osobama. Ukoliko se pravna sposobnost prizna umjetnoj inteligenciji to će biti potrebno učiniti kroz razvoj nekog trećeg pravnog subjekta. Razvoj autonomne umjetne inteligencije doveo bi do potrebe priznavanja pravne osobnosti neživom sustavu. U studiji koju je naručio Europski parlament formuliran je stav prema kojem umjetna inteligencija može biti još jedan, novi pravni subjekt – elektronička osoba.[32] Elektronička osobnost pokazuje značajnu povezanost sa pravnom sposobnosti koju pravni sustav pripisuje pravnim osobama. Čovjek svoju pravnu sposobnost stječe rođenjem, pravna osoba osnivanjem, a sličan slučaj bio bi i sa formiranjem elektroničke osobe. U SAD se već (ili tek s obzirom na to da je pionir u razvoju VI) formiraju zakoni koji reguliraju primjenu umjetne inteligencije. Zakonodavna sjednica 2023. zabilježila je porast državnih zakona o umjetnoj inteligenciji predloženih diljem SAD, nadmašujući broj predloženih ili usvojenih zakona o umjetnoj inteligenciji na prošlim zakonodavnim sjednicama.[33] Ključni su zakoni koji navode svojevrstan registar korisnika umjetne inteligencije. Pravne osobe pravnu sposobnost dobivaju kroz zakonske regulative, a upravo na taj način pravnu sposobnost bi dobila i elektronička osoba.

[31] Vedriš, M., Klarić, P. (2014). *Građansko pravo*. Zagreb, 51.

[32] European Parliament, Directorate-General for Internal Policies of the Union, Nevejans, N. (2016). *European civil law rules in robotics*, Publications Office. Dostupno na: https://data.europa.eu/doi/10.2861/946158, pristupljeno 5. 11. 2023.

[33] Zhu, K. (2023). *The State of State AI Laws.* Dostupno na: https://epic.org/the-state-of-state-ai-laws-2023/, pristupljeno 16. 3. 2024.

Prirodu pravne osobnosti elektroničke osobe potrebno je detaljno razraditi zakonskom regulativom. Pravna osoba osnivanjem stječe poslovnu i deliktnu sposobnost. Elektronička osoba stekla bi ih upisivanjem u registar. Radnje koje bi poduzimala umjetna inteligencija tretirale bi se kao samostalne, ali i dalje bi jednim dijelom „opteretile" čovjeka kao što je to slučaj i kod pravnih osoba. Do koje mjere bi bili opterećeni vlasnici kompanija / programeri / korisnici odredilo bi se zakonskim propisima. Kakav će pristup biti potrebno razviti prema umjetnoj inteligenciji ovisi o tome koliko će biti „samostalna". Regulacija umjetne inteligencije također uvelike ovisi i o etičnosti pojedinaca koji je razvijaju. Pravni sustav teško da će zauzeti stav tretiranja umjetne inteligencije kao „fizičke" osobe u kojoj bi neživi sustav bio odgovoran za svoje (ne)činjenje. Radnje umjetne inteligencije su programirane stoga je teško odrediti gdje prestaje odgovornost čovjeka, a počinje odgovornost neživog sustava. U svakom slučaju čovjek će preuzeti dio odgovornosti za VI, a preostaje odrediti koji to u cijelom lancu ljudi koji stoje iza VI će imati najviše odgovornosti. Bez pravne regulacije umjetne inteligencije i rješavanja pitanja odgovornosti čovjek će izgubiti odgovornost za ono što se događa u njegovoj okolini. Unutar pravnog sustava fizičke osobe kao pravni subjekti dijele se u dvije kategorije: prema tome imaju li ili nemaju tzv. poslovnu sposobnost.[34] Pravni subjekti bez poslovne sposobnosti nisu odgovorni za svoje radnje zbog nemogućnosti shvaćanja istih. U tom kontekstu umjetna inteligencija nema svijest i sposobnost shvaćanja vlastitih radnji koje su programirane od strane čovjeka stoga fizička osoba ne može izbjeći odgovornost za štetu koju bi potencijalno prouzrokovala VI. Rezolucija Europskog parlamenta od 20. listopada 2020. s preporukama Komisiji o sustavu građanskopravne odgovornosti za umjetnu inteligenciju[35] navodi da sustavima umjetne inteligencije nije potrebno dati pravnu osobnost. Nadalje, ističe odgovornost operatera sustava umjetne inteligencije na temelju građanskopravne odgovornosti. Operateri imaju kontrolu nad rizikom povezanim sa sustavom, što je slično odgovornosti vlasnika automobila. U mnogim slučajevima, operateri će biti prva vidljiva kontaktna točka za oštećene osobe. Pravna regulacija umjetne inteligencije kao i potencijalne promjene do koje bi ista dovela na području prava možemo doživjeti kao pravnu revoluciju ili kao evoluciju prava koja ga prilagođava društvenim promjenama.

[34] Visković, N. (2001). *Teorija prava i države.* Zagreb: Impresum, 210.

[35] Europski parlament (2020). *Rezolucija s preporukama Komisiji o sustavu građanskopravne odgovornosti za umjetnu inteligenciju (2020/2014(INL)).* Dostupno na: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_HR.html. Pristupljeno 21. 3. 2024.

UTJECAJ TEHNOLOGIJE NA ZAŠTITU LJUDSKIH PRAVA

U svakom stoljeću susrećemo se s izazovima zaštite ljudskih prava, pa tako i u ovome. Ljudska prava nisu strog i apsolutan sustav, već se pod određenim uvjetima mogu ograničiti i ovisno o vremenu stavlja se naglasak na zaštitu pojedinih prava zajamčenih Konvencijom. Uslijed okruženosti čovjeka tehnologijom javlja se potreba zaštite čovjekove privatnosti za koju sve više gubimo osjećaj. Razvojem digitalnih medija koji imaju ogroman utjecaj na društvo sve češće se javlja potreba balansa između slobode izražavanja i prava na privatnost. Kažnjavanjem počinitelja „digitaliziranih" kaznenih djela bez zakonske regulative ugrožava čl. 7. Konvencije koji glasi nema kazne bez zakona. Upotreba digitalnih dokaza na neadekvatan način može se odraziti na vođenje pravičnog suđenja na koje svatko ima pravo prema čl. 6. Bez pravne regulacije tehnologije, pravni sustav ne može ispuniti jednu od svojih temeljnih vrijednosti, a to je sigurnost. Jednom kada pojedinac zakorači u virtualni prostor, ostavlja digitalni trag i izgrađuje svoj digitalni identitet. Ime, prezime, slika osobni su podaci koji u virtualnom prostoru postaju dostupni svima, a riječ je o podacima kojima se može ugroziti naša osobna sigurnost. Sve češće susrećemo se s potrebom prihvaćanja „kolačića" bez mogućnosti odbijanja na koje kliknemo pristajem bez da pročitamo na što pristajemo, kome pristajemo i zašto? Potrebu zaštite osobnih podataka prepoznala je EU te se nametnula kao lider zaštite osobnih podataka plasirajući Uredbu o zaštiti osobnih podataka.[36] Član 17. GDPR[37]-a navodi pravo na zaborav koje predstavlja potencijalno ljudsko pravo nove generacije ljudskih prava – digitalnih prava. U vremenu u kojem živimo ljudska i digitalna prava postaju ne odvojiva te ista prava koja vrijede *offline*, trebaju vrijediti i *online*. Sve ono što se dogodi u virtualnom prostoru ima ogroman utjecaj na naš stvarni život izvan ekrana. Razvoj ljudskih prava uvelike je povezan s prodorom pojedinca na područje međunarodnog prava. Jedna od najmarkantnijih karakteristika razvoja međunarodnog prava u periodu poslije Drugog svjetskog rata nesumnjivo je pojava pojedinca u sferi međunarodnog prava[38] te su se tijekom XX stoljeća dogodile značajne promjene u pogledu zaštite ljudskih prava. U XXI stoljeću znanstveni i tehnološki napredak novi su izazovi koji otvara pitanje jesu li instrumenti za zaštitu ljudskih prava razvijen prije postojanja novih dostignuća dovoljno „živi" da zaštite čovjeka u digitalnoj eri? Pravna pitanja koja se odnose na prava čovjeka mogu se kategorizirati u tri vrste pitanja: kršenja prava koja proizlaze

[36] European Union, (2016). *General Data Protection Regulation.* Dostupno na: https://gdpr-info.eu/, pristupljeno 21. 3. 2024.

[37] European Union, (2016). *Op. cit.,* pristupljeno 16. 3. 2024.

[38] Ćazim, S. (2003). *Europsko pravo ljudskih prava*. Sarajevo, 16.

iz (uporabe) novih tehnologija, sukobljena prava koja proizlaze iz (uporabe) novih tehnologija te nova pitanja koja proizlaze iz (uporabe) novih tehnologija, za koje još ne postoje zakoni.[39] Uzimajući u obzir da tehnologija prodire u sve sfere života suvremenog društva razumijevanje digitalnih prava ključno je za mogućnost zaštite temeljnih ljudskih prava. Pravnici će odigrati ključnu ulogu u prevenciji suvremenih oblika kršenja ljudskih prava i osiguravanju da tehnološke kompanije u razvoju novih tehnologija promiču prava. Zato su potrebni napori u smislu zagovaranja, primjene pravnih standarda na području tehnologije i izgradnje novih znanja koja će nam omogućiti shvaćanje transformacije našeg društva.

VLADAVINA PRAVA I TEHNOLOGIJA

Nakon izloženog očito je da postoji živa rasprava o tome kako regulirati umjetnu inteligenciju. Mnoge zemlje predložile su zakonske okvire za pravnu regulaciju umjetne inteligencije. Europska unija usvojila je prvi zakon o umjetnoj inteligenciji koji bi na snagu trebao stupiti 2026. godine.[40] Akt o umjetnoj inteligenciji, prvi je sveobuhvatni pravni VI okvir. Rasprava o regulaciji umjetne inteligencije često podcjenjuje da sama umjetna inteligencija ima regulatorne učinke na pravni sustav i time ugrožava vladavinu prava kao temelj mnogih suvremenih država. Utjecaj nove tehnologije na pravni sustav nešto je što bi se trebalo uzeti u obzir kada se raspravlja o bilo kakvim regulatornim pokušajima VI tehnologije.[41] U ovom dijelu rada analizirat će se utjecaj razvoja nove tehnologije na vladavinu prava. Vladavina prava je mehanizam, proces, institucija, praksa ili norma koja podupire jednakost svih građana pred zakonom, osigurava nearbitraran oblik vladavine i općenito sprječava proizvoljnu upotrebu moći.[42] Četvrta industrijska revolucija rezultirala je novim oblikom moći zvan tehnologija. Danas ne samo da čovjeka treba štititi od proizvoljne volje države koja posjeduje moć koja je normama ograničena

[39] Custers, B. (2022). New digital rights: Imagining additional fundamental rights for the digital era. *Computer Law & Security Review,* Vol 44. Dostupno na: https://www.sciencedirect.com/science/article/pii/S0267364921001096, pristupljeno 17. 3. 2024.

[40] Milovan, A. (2024). *Eurozastupnici usvojili zakon o umjetnoj inteligenciji: AI će se koristiti i za zaštitu granica i borbu protiv terorizma.* Dostupno na: https://euractiv.hr/tehnologija/a6854/Europski-parlament-usvojio-zakon-o-umjetnoj-inteligenciji.html, pristupljeno 17. 3. 2024.

[41] Rosengrün, S. (2022). *Why AI is a Threat to the Rule of Law.* Dostupno na: https://doi.org/10.1007/s44206-022-00011-5, pristupljeno 20. 11. 2023.

[42] Choi, N. (2023). Rule of Law. Dostupno na: https://www.britannica.com/topic/rule-of-law pristupljeno 20. 11. 2023.

na vlast, već i od proizvoljne moći onih koji monopoliziraju tehnologiju i tehnološka znanja. Tehnologija ima sve veći utjecaj kojeg nismo niti svjesni. Tehnološke korporacije poput Googlea i Amazona svojim algoritmima određuju što će se naći u razini naših očiju, a što će ostati van našeg vidnog polja. Ako Google ili Amazon promjenu svoje algoritme pretraživanja, automatski se mijenja tržište. Nekoliko redaka izvornog koda odlučuje koje će proizvode i trgovine pronaći milijarde ljudi i koliko će za to platiti.[43] Samo implementiranje novih tehnologija u pravosuđe (što je već slučaj u nekim državama u svijetu) otvara pitanje vladavine prava. Ovisno o tome koja je koncepcija vladavine prava, zamjena ljudskog prosuđivanja strojnim odlučivanjem može izazivati prigovore temeljene na transparentnosti, predvidljivosti, pristranosti i proceduralnoj pravednosti. Ljudski suci donose prosudbu prema potrebi, a ne prema izboru. Zamjena ljudskih sudaca VI tehnologijama vjerojatno će imati destabilizirajući učinak. Istovremeno se zaoštrava pitanje treba li apstraktni koncept vladavine prava realizirati kroz poseban institucionalni oblik i mogu li tehnološke promjene zahtijevati izmjene i dopune odnosa između koncepata i prakse vladavine prava.[44] Preostaje nam vidjeti koliko će onoga što nam je poznato vrijediti u uvjetima tehnoloških promjena i razvoja novih tehnologija. Unatoč tome što se vladavina prava može smatrati jednim od najvažnijih načela, definicije se razlikuje u različitim pravnim sustavima i kontekstima. Zapravo, sve ga je teže definirati jer se taj izraz koristi u mnogo različitih oblika. Fraza je postala kameleonska, poprimajući onu nijansu značenja koja najviše odgovara autorovoj svrsi. Bez jasne definicije, vladavina prava je u opasnosti da znači gotovo sve, a da zapravo može doći do toga da uopće ne znači ništa.[45]

ZAKLJUČAK

Znanost i tehnologija ubrzano napreduju dok pravna normativa „kasni" što otvara mogućnost zloupotrebe suvremenih dostignuća. Ključno je da u digitalnom dobu pravni sustav prepozna virtualni prostor kao novo mjesto počinjenja niza kaznenih djela. Digitalna transformacija našeg društva rezultira pojavom novih počinitelja, žrtava, dokaza koji ostaju nakon počinjenja

[43] Choi, N. (2023). Rule of Law. Dostupno na: https://www.britannica.com/topic/rule-of-law pristupljeno 20. 11. 2023.

[44] Huq, A. (2021). *Artificial Intelligence and the Rule of Law.* Dostupno na: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2194&context=public_law_and_legal_theory, pristupljeno 20. 11. 2023.

[45] Latušinskaja, S. G. (2023). *The rule of law and technology in public* secetor. Dostupno na: file:///C:/Users/Pc/Downloads/153862123.pdf, pristupljeno 21. 11. 2023.

kaznenih djela… Sve to zahtjeva drugačije pristupe u kažnjavanju suvremenih ilegalnih aktivnosti. Nakon analize aktualne literature potvrđuje se potreba izmjene pravnog sustava u svrhu prilagodbe digitalnom dobu. Početne hipoteze postavljene na početku rada potvrđene su kao i potreba transformacije pravnog sustava. Područje tehnologije nedovoljno je ograničeno zakonima te niti jedna tehnologija nije ilegalna i može se koristiti u sve svrhe (npr. zakoni ne brane primjenu umjetne inteligencije u vojne svrhe niti u proizvodnji oružja). Kako pravni sustav može reagirati na tehnološke inovacije koje nisu eksplicitno obuhvaćene postojećim zakonima ostaje otvoreno pitanje i time se potvrđuje hipoteza H1 koja glasi, područje tehnologije potrebno je pravno regulirati novim zakonima. Digitalizacija i daljnji tehnološki napredak dovest će do rasta suvremenih oblika kriminala, terorizma i kibernetičkih napada što potvrđuje hipotezu H2 koja glasi, digitalni dokazi imat će sve veći značaj u sudskim sporovima kao i hipotezu H3 koja glasi, pravni sporovi budućnosti sve više će se doticati novih tehnologija. Trenutno shvaćanje da umjetna inteligencija ne može biti pravni subjekt nužno ne znači da isto neće biti napušteno u budućnosti kao što je bio slučaj s pravnim osobama. Umjetna inteligencija i algoritmi imaju velik utjecaj na suvremeno društvo. Primjena novih tehnologija u pravosuđu odražava se na koncept vladavine prava. Hoće li VI biti najbolja ili najgora tehnologija ovisi o tome u čijim rukama se nalazi. U krivim rukama tehnologija postaje suvremeno oružje.

LITERATURA

AIRE Centar. (2023). Kriptirane aplikacije u fokusu evropskog pravosuđa. *Pravna hronika,* vol. 16.

Bošković, M., Marković, M. (2015). *Kriminologija sa elementima viktimologije.* Novi Sad.

Choi, N. (2023). *Rule of Law*. Dostupno na: https://www.britannica.com/topic/rule-of-law, pristupljeno 20. 11. 2023.

Custers, B. (2022). New digital rights: Imagining additional fundamental rights for the digital era. *Computer Law & Security Review,* vol 44. Dostupno na: https://www.sciencedirect.com/science/article/pii/S0267364921001096, pristupljeno 17. 3. 2024.

Cvitanović, L., Derenčinović, D., Horvatić, Ž. (2016). *Kazneno pravo: Opći dio I*. Zagreb: Pravni fakultet Sveučilišta u Zagrebu.

Ćazim, S. (2003). *Europsko pravo ljudskih prava*. Sarajevo

European Parliament, Directorate-General for Internal Policies of the Union, Nevejans, N. (2016). *European civil law rules in robotics*, Publications Office. Dostupno na: https://data.europa.eu/doi/10.2861/946158, pristupljeno 5. 11. 2023.

Goodison, E., Jackson, D. (2015). *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence.* Dostupno na: https://www.rand.org/pubs/research_reports/RR890.html, pristupljeno 11. 10. 2023.

Horović, S. (2020). *Kazneno pravo – Opći dio.* Mostar: Sveučilište u Mostaru.

Huq, A. (2021). *Artificial Intelligence and the Rule of Law.* Dostupno na: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2194&context=public_law_and_legal_theory, pristupljeno 20. 11. 2023.

Jovanović, J., Mihajlović, D. (2022). *Advokati tvrde da Sky poruke ne mogu biti dokaz na sudu.* Dostupno na: https://www.vijesti.me/vijesti/crna-hronika/635617/advokati-tvrde-da-sky-poruke-ne-mogu-biti-dokaz-na-sudu, pristupljeno13. 3. 2024.

Kamyshanskiy, V., Stepanov, D., Mukhina, I., Kripakova, D. (2020). *Digital society, artificial intelligence and modern civil law: challenges and perspectives SHS Web of Conferences* (Vol. 109). Dostupno na: https://www.shsconferences.org/articles/shsconf/pdf/2021/20 /shsconf _lisid2021_01016.pdf, pristupljeno 16. 3. 2024.

Karlsson, M. (2017). *Artificial Intelligence and the External Element of the Crime An Analysis of the Liability Problem.* Dostupno na: https://www.diva-portal.org/smash/get/diva 2:1115160/FULLTEXT01.pdf, pristupljeno 5. 10. 2023.

Kavazović, M., Bajraktarević Pajević, D., Lučić-Ćatić, M., Puharić, P. (2019). Kriminalističko postupanje sa digitalnim dokazima u praksi policijskih agencija u BiH. *Kriminalističke teme*, Vol 5. Dostupno na: https://krimteme.fkn.unsa.ba/index.php /kt/article/view /231, pristupljeno 13. 3. 2024.

Kotecha, B. (2020). The International Criminal Court's Selectivity and Procedural Justice. *Journal of International Criminal Justice*, (Vol. 18). Dostupno na: https://doi.org/10.1093/jicj/mqaa020, pristupljeno 13. 3. 2024.

Latušinskaja, S. G. (2023). *The rule of law and technology in public* secetor. Dostupno na: file:///C:/Users/Pc/Downloads/153862123.pdf, pristupljeno 21. 11. 2023.

Milovan, A. (2024). *Eurozastupnici usvojili zakon o umjetnoj inteligenciji: AI će se koristiti i za zaštitu granica i borbu protiv terorizma.* Dostupno na: https://euractiv.hr/tehnologija/a6854/Europski-parlament-usvojio-zakon-o-umjetnoj-inteligenciji.html, pristupljeno 17. 3. 2024.

Novoselec, P. (2016). *Opći dio kaznenog prava*. Osijek: Sveučilište u Osijeku

Rosengrün, S. (2022). *Why AI is a Threat to the Rule of Law.* Dostupno na: https://doi.org/10.1007/s44206-022-00011-5, pristupljeno 20. 11. 2023

Silahi, J. (2023). *The Application of Criminal Law in the Digital Age: A Literature Review of Challenges and Opportunities.* Dostupno na: https://j-innovative.org/index.php/Innovative/article/download/678/590, pristupljeno 20. 10. 2023.

Spyropoulos, F. (2009). *Technoethics, AI and Criminal Law.* Dostupno na: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Fourth_intersessional_consultation/Panel_3_Spyropoulos_Center_for_the_Study_of_C.pdf, pristupljeno 1. 10. 2023.

Stoykova, R. (2023). The Right to a Fair Trial as a Conceptual Framework for Digital Evidence Rules in Criminal Investigations. *Computer Law & Security Review,* Vol 49. Dostupno na: https://www.sciencedirect.com/science/article/pii/S0267364923000110, pristupljeno 14. 3. 2024.

Stoykova, R., Andersen, S., Franke, K., Axelsson, S. (2022). *Reliability assessment of digital forensic investigations in the Norwegian police. Forensic Science International: Digital Investigation,* (Vol. 40). Dostupno na: https://www.sciencedirect.com/science/article/pii/ S2666281722000208, pristupljeno 13. 3. 2024.

Throckmorton, B. (2018). Technology and criminal law. Dostupno na: https://jolt.richmond.edu/2018/02/11/technology-and-criminal-law/, pristupljeno 1. 10. 2023

United nations office on drugs and crime (2013). *Comprehensive Study on Cybercrime, Op. cit.,* 183. Dostupno na: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_ EG.4_2013/CYBERCRIME_STUDY_210213.pdf, pristupljeno 15. 3. 2024.

Vedriš, M., Klarić, P. (2014). *Građansko pravo*. Zagreb.

Visković, N. (2001). *Teorija prava i države.* Zagreb: Impresum.

Zhu, K. (2023). *The State of State AI Laws.* Dostupno na: https://epic.org/the-state-of-state-ai-laws-2023/, pristupljeno 16. 3. 2024.

Propisi i sudska praksa:

Council of Europe (2021). *Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence.* Dostupno na: https://www.coe.int/en/web/cybercrime/second-additional-protocol, pristupljeno 15. 3. 2024.

European Parliament (2019-2024) *Artificial Intelligence Act.* Dostupno na: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf, pristupljeno 20. 3. 2024.

European Union, (2016). *General Data Protection Regulation.* Dostupno na: https://gdpr-info.eu/art-17-gdpr/, pristupljeno 16. 3. 2024.

European Union, (2016). *General Data Protection Regulation.* Dostupno na: https://gdpr-info.eu/, pristupljeno 21. 3. 2024.

Europski parlament (2020). *Rezolucija s preporukama Komisiji o sustavu građansko-pravne odgovornosti za umjetnu inteligenciju (2020/2014(INL)).* Dostupno na: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_HR.html, pristupljeno 21. 3. 2024.

U. v. Turkey, (App. no. 23314/19). Pristupljeno 31. 8. 2021.