IZAZOVI POSEBNOG DIJELA KAZNENOG PRAVA ZBOG RAZVOJA UMJETNE INTELIGENCIJE UZ POSEBAN OSVRT NA HRVATSKO KAZNENO PRAVO

*Prof. dr. sc. Igor Vuletić**
*Izv. prof. dr. sc. Ante Novokmet***
*Izv. prof. dr. sc. Zvonimir Tomičić****

UDK: 343.3/.7:004.3/.7
343.346:004.3/.7.01
DOI: 10.3935/zpfz.74.1.01
Izvorni znanstveni rad
Primljeno: prosinac 2023.

Umjetna inteligencija ostvaruje sve snažniji prodor u različite aspekte svakodnevnog života. Prednosti umjetne inteligencije u smislu povećanja učinkovitosti i isplativosti mnogih poslova čine je nezaobilaznim čimbenikom razvoja društva. Iako je taj razvoj još uvijek izraženiji u SAD-u i pojedinim razvijenijim azijskim zemljama, neupitno je da će ovaj trend u bližoj budućnosti prevladati i u Europi. S obzirom na to da primjena umjetne inteligencije donosi i različite vrste rizika, od kojih neki izravno ugrožavaju najviša pravna dobra poput života i tijela ili imovine, postavlja se pitanje kako postići odgovarajući stupanj kaznenopravne zaštite u ovom području. Tradicionalno kazneno pravo zasniva se na načelima koja su prilagođena čovjeku kao počinitelju kaznenog djela pa novi trendovi otvaraju potrebu preispitivanja temeljnih postavki kaznenog prava. Ovaj rad promatra spomenutu problematiku iz perspektive posebnog dijela kaznenog prava. Najprije se utvrđuju

* Dr. sc. Igor Vuletić, profesor Pravnog fakulteta Sveučilišta Josipa Jurja Strossmayera u Osijeku, S. Radića 13, 31000 Osijek; ivuletic@pravos.hr;
ORCID ID: orcid.org/0000-0001-5472-5478

** Dr. sc. Ante Novokmet, izvanredni profesor Pravnog fakulteta Sveučilišta Josipa Jurja Strossmayera u Osijeku, S. Radića 13, 31000 Osijek; ante.novokmet@pravos.hr;
ORCID ID: orcid.org/0000-0001-8833-9751

*** Dr. sc. Zvonimir Tomičić, izvanredni profesor Pravnog fakulteta Sveučilišta Josipa Jurja Strossmayera u Osijeku, S. Radića 13, 31000 Osijek; tomicic.zvonimir@pravos.hr;
ORCID ID: orcid.org/0000-0001-6159-6475

područja od primarnog interesa kaznenopravne zaštite, kada je u pitanju kriminalitet umjetne inteligencije. Potom se analizira i preispituje hrvatsko zakonodavstvo, s ciljem da se utvrdi jesu li postojeće odredbe posebnog dijela Kaznenog zakona u promatranim područjima dovoljne da osiguraju adekvatnu kaznenopravnu reakciju. Dolazi se do zaključka da je to samo djelomično, tako da i u tom pogledu postoje pravne praznine. Autori ujedno predlažu određene promjene de lege ferenda, na mjestima gdje se to pokazuje svrhovitim i potrebnim.

Ključne riječi: umjetna inteligencija, posebni dio, kriminalitet, promet, sigurnost, kaznena odgovornost

1. UVOD

Jedna od najvažnijih značajki suvremenog doba jest intenzivni razvoj modernih tehnologija. Tehnološki napredak brži je nego ikad, a njegov utjecaj na svakodnevni život izraženiji nego u prošlosti. Suvremena tehnologija postala je dostupna svima te je na taj način postala sastavni dio svakodnevice. Posljednjih nekoliko godina sve se više razvija i oblikuje tehnologija zasnovana na pojmu umjetne inteligencije, odnosno samostalne (autonomne) umjetne inteligencije (dalje: UI). Za sada ne postoji suglasnost oko definiranja tog pojma pa će se, za potrebe ovog rada, prihvatiti definicija prema kojoj on obuhvaća sve one tehnološke sustave koji su osmišljeni tako da djeluju na različitim razinama neovisnosti o čovjeku.[1] Drugim riječima, radi se o softverskim (a prema nekima i o hardverskim[2]) sustavima koji su sposobni donositi samostalne odluke na temelju podataka koji su im dani ili koje su prikupili iz okoline. Tehnologija na takvom stupnju razvoja u stanju je preuzeti znatan broj zadataka koje su prethodno obavljali ljudi pa je posve jasno da ona može uvelike povećati kvalitetu života, pridonijeti povećanju ekonomičnosti i učinkovitosti rada te imati mnoge druge pozitivne učinke. No, isto tako, ovakva tehnologija može uzrokovati nemale pravne (pa time i kaznenopravne) poteškoće kada dovede do pogrešaka i nanese štetu pravnim dobrima. S druge strane, postavlja se i pitanje možebitnog nastajanja i oblikovanja novih kategorija pravnih dobara koje trebaju

[1] OECD, Recommendations of the Council on Artificial Intelligence, OECD/LEGAL/0449, 2019., str. 7; dostupno na https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (4. srpnja 2023.).

[2] Usp. The European Commission`s High Level Expert Group on Artificial Intelligence, *A Definition of AI: Main Capabilities and Scientific Disciplines*, 2018., str. 8; dostupno na https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines (4. srpnja 2023.).

uživati kaznenopravnu zaštitu.[3] Zato je problematika umjetne inteligencije u kontekstu (kaznenog) pravosuđa posljednjih godina sve češće u fokusu ponajprije doktrinarnih rasprava.

Utjecaj UI-ja na svakodnevni život u okvirima Europe i EU-a nije toliko prodoran kao u SAD-u ili razvijenim azijskim zemljama (npr. Južnoj Koreji, Japanu ili Kini). Unatoč tomu realno je očekivati kako će i Europa, u želji da zadrži korak u razvoju sa spomenutim dijelovima svijeta i njihovim tržištima, u bližoj budućnosti sve više prihvaćati takvu vrstu tehnologije. Zato je i EU posljednjih godina pokrenuo inicijativu za uspostavljanje minimalnih etičkih i pravnih standarda sa svrhom osmišljavanja odgovarajućih okvira za odgovornu i sigurnu uporabu UI-ja.[4] U europskom pravnom krugu će najveći izazov u tom smislu biti kako pomiriti težnju za tehnološkim napretkom s potrebom očuvanja postojećeg standarda ljudskih prava, kategorije koja je u Europi izraženija nego bilo gdje drugdje u svijetu.[5]

U kontekstu kaznenog materijalnog prava, ovu je problematiku, prije svega, moguće sagledati iz perspektive općeg dijela, koja podrazumijeva redefiniciju temeljnih kaznenopravnih načela i ocjenu primjenjivosti tradicionalnih kaznenopravnih instituta na situacije koje uključuju neki oblik djelovanja UI-ja.[6] Jednako tako, moguć je i osvrt iz kuta posebnog dijela, koji podrazumijeva preispitivanje primjenjivosti konkretnih kaznenih djela na situacije vezane uz UI, odnosno razmatranje potrebe uvođenja posve novih inkriminacija. Ovaj tekst bit će posvećen drugospomenutom kutu gledanja.

Najprije će se razmotriti područja posebnog dijela koja su od primarnog interesa za uređenje u bližoj budućnosti, uzimajući u obzir trenutačne trendove u razvoju UI-ja. Ujedno će se opisati određena poredbenopravna iskustva onih sustava koji već imaju razvijenu kaznenopravnu praksu u području UI-ja. Za-

---

3 O tome vidi npr. Rodrigues, R., *Legal and human rights issues of AI: Gaps, challenges and vulnerabilities*, Journal of Responsible Technology, *vol.* 4, 2020., str. 1 – 12.

4 Vidi: https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines (5. srpnja 2023.).

5 Mantelero, A., *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, Computer Law & Security Review, *vol.* 34, br. 4, 2018., str. 754 – 772.

6 Problematika općeg dijela u kontekstu UI-ja zaokuplja pozornost mnogih autora u poredbenoj literaturi u posljednjih nekoliko godina. Dobar prikaz problema i najvažnijih stajališta za anglo-američko pravno područje može se naći u Lagioia, F.; Sartor, G., *AI Systems Under Criminal Law: a Legal Analysis and a Regulatory Perspective*, Philosophy & Technology, *vol.* 33, br. 3, 2020., str. 433 – 465. Iz europske kontinentalne perspektive, kvalitetan prikaz problema u zemljama germanskog pravnog kruga nude Gleβ, S.; Weigend, T., *Intelligente Agenten und das Strafrecht*, Zeitschrift für die gesamte Strafrechtswissenschaft, *vol.* 126, br. 3, 2014., str. 561.

tim će se analizirati postojeće hrvatsko materijalno kazneno zakonodavstvo u promatranim područjima posebnog dijela sa svrhom odgovora na pitanje. Cilj je utvrditi pruža li domaće uređenje odgovarajući pravni okvir za izazove koje otvara UI. Na temelju takve analize predložit će se i određene smjernice hrvatskom zakonodavcu *de lege ferenda*.

Svrha ovog rada je dvojaka. S jedne se strane želi pružiti pregled globalnih i poredbenih kaznenopravnih trendova iz posebnog dijela kaznenog prava te opisati zanimljive slučajeve iz poredbene prakse. Naime, iz hrvatske perspektive još je uvijek riječ o razmjerno apstraktnoj materiji jer ne postoji odgovarajuća sudska praksa. Zato su poredbena iskustva osobito važna za buduća razmatranja ove problematike u hrvatskom kaznenopravnom kontekstu. S druge je strane cilj i preispitati pozitivno hrvatsko kazneno pravo i utvrditi je li ono spremno nositi se s izazovima koje otvara razvoj UI-ja.

2. PODRUČJA OD PRIMARNOG ZAŠTITNOG INTERESA

Kazneno pravo uvijek mora pratiti potrebe društvenog razvoja, nastojeći postići ravnotežu između potrebe za učinkovitom zaštitom društva i potrebe za njegovim razvojem i napretkom. To znači da će primarna područja razvoja posebnog dijela nužno morati pratiti ona područja razvoja UI tehnologije koja su u određenom trenutku najzastupljenija u stvarnom (svakodnevnom) životu. U ovom trenutku, UI ostvaruje najintenzivniji prodor u području automobilske industrije i prometa, naoružanja i vojnog sektora, određenih područja zdravstva i medicine, financijskog sektora te korištenja internetom.[7] U skladu s tim, aktualna kriminološka literatura prepoznaje različita područja potencijalnih rizika, među kojima neka imaju veći stupanj vjerojatnosti ostvarenja i visok stupanj pogibeljnosti pa se u tom smislu govori i o područjima visokog rizika.[8]

Kao područja s višim stupnjem rizika, kada je riječ o korištenju umjetne inteligencije, najčešće se navodi kaznenopravna zaštita najviših osobnih dobara, sigurnosti prometa, vojne industrije i uporabe samostalnog oružja, financijskog sektora i burze, zaštite osobnih podataka (posebice u kontekstu biometrijske

[7] West, D. M.; Allen, J. R., *How artificial intelligence is transforming the world*, dostupno na: https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/ (11. srpnja 2023.).

[8] Tako npr. Bikeev, I.; Kabanov, P.; Begishev, I.; Khisamova, Z., *Criminological Risks and Legal Aspects of Artificial Intelligence Implementation*, AIIPCC '19: Proceedings of the International Conference on Artificial Intelligence, Information Processing and Cloud Computing, December 2019, Article No. 20, str. 1 – 7, dostupno na: https://dl.acm.org/doi/pdf/10.1145/3371425.3371476 (17. listopada 2023.).

identifikacije i prepoznavanja obilježja lica i glasa) te interneta i sigurne komunikacije u virtualnom svijetu (koja podrazumijeva i zaštitu od uznemiravanja i seksualnog ugrožavanja putem društvenih mreža).[9]

Polazeći od iznesenoga, pregled područja od (trenutačno) primarnog interesa promotrit će se u nastavku teksta kroz prizmu kaznenopravne zaštite najviših dobara osobe, zatim sigurnosti prometa, pravila i običaja ratovanja, zaštite zdravlja, zaštite gospodarstva te zaštite privatnosti i kibernetičke sigurnosti.

2.1. Ugrožavanje i povređivanje najviših osobnih dobara

Kada je riječ o kaznenim djelima kojima se ugrožavaju ili povređuju najviša osobna dobra, poput života, tijela, slobode kretanja ili spolne slobode, važno je istaknuti kako se autori uglavnom slažu da u ovom području rizik ne proizlazi iz UI-ja kao takvog, nego iz zlonamjerne interakcije UI-ja i čovjeka.[10] Zato se u kontekstu ovih kaznenih djela UI promatra ponajprije kao sredstvo (s većim ili manjim stupnjem samostalnosti) u rukama čovjeka. U skladu s tim, na situacije korištenja UI-ja radi napada na najviša osobna dobra primjenjivat će se u pravilu opća kaznena djela protiv osobnih sloboda, a počinitelj će uvijek biti fizička osoba koja se takvim alatima koristi.[11]

Osim počinitelja fizičke osobe, u pojedinim europskim državama pravni okvir dopušta i kaznenu odgovornost fizičkih i pravnih osoba koje se javljaju kao proizvođači ili prodavači ovakvih proizvoda. Vrijedi navesti primjere Italije i Nizozemske, zakonodavstva kojih propisuju kaznena djela apstraktnog ugrožavanja, kojima se inkriminira već samo stavljanje u promet proizvoda koji mogu biti opasni za život i tijelo.[12] Ostaje, međutim, dvojba treba li korištenje UI tehnologije kod ovakvih kaznenih djela tretirati kao posebnu kvalifikatornu okolnost, s obzirom na to da je riječ o zlouporabi te tehnologije i da takva zlouporaba može imati dalekosežne posljedice.[13] U pojedinim sustavima razmatra se pitanje da se proizvodnja UI-ja za svrhe nezakonitih aktivnosti, poput ilegalne trgovine i transporta droga, trgovine ljudi i slično propiše kao posebno,

---

9 Usp. King, T. C.; Aggarwal, N.; Taddeo, M.; Floridi, L., *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, Science and Engineering Ethics, *vol.* 26, br. 1, 2020., str. 89 – 120.

10 *Ibid*., str. 101; isto i Miró-Llinares, F., *Association International de Droit* Pénal – International *Association of Penal Law XXI International Congres of Penal Law: "Artificial Intelligence and Criminal Justice", International Colloquium of Section II (Criminal Law-specific offences in the Criminal code)*, 2023., str. 26.

11 Miró-Llinares, *op. cit.* u bilj. 10, str. 26 – 27.

12 *Ibid*., str. 26.

13 *Ibid.*

teško kazneno djelo (po uzoru na kaznena djela koja se sastoje u organiziranju zločinačkih udruženja).[14]

Najveći kaznenopravni rizik u ovoj domeni trenutačno predstavlja uporaba posebnih programa (engl. *social bot*) koji se mogu zlorabiti za različite oblike uznemiravanja, uhođenja ili čak seksualnog zlostavljanja, odnosno seksualne objektivizacije. Tako se, primjerice, *social bot* može rabiti za distribuciju ili podupiranje govora mržnje putem interneta. Moguće su i sofisticirane metode oponašanja nečijeg glasa, manipulacije fotografijama, dodavanja seksualnog sadržaja i sl.[15] Može se navesti primjer softvera koji proizvodi tzv. sintetske videozapise. Ti videozapisi temelje se na stvarnom videu s nekom osobom ali softver pritom zamjenjuje lice te osobe licem neke druge osobe. Lice te druge osobe nije samo kopirano i zalijepljeno iz fotografija. Naprotiv, tzv. generativna neuronska mreža sintetizira lice te druge osobe nakon što je uvježbana na videima koji prikazuju tu drugu osobu.[16] Vrlo često takvi su sadržaji pornografske naravi, što onda ozbiljno zadire u sferu spolnih sloboda.

Osim opisanoga, jedan od potencijalno opasnih rizika uključuje korištenje UI-jem u svrhe ispitivanja i mučenja. Ostvarenje tog rizika postaje vjerojatno ako se nastavi razvijati UI tehnologija poput automatizirane detekcije prijevare u prototipu robotskog čuvara za kontrolu granice SAD-a. Uporaba UI-ja u svrhe ispitivanja ljudi temelji se na shvaćanju o većoj učinkovitosti u otkrivanju ponašanja poput prijevare, ali i manipuliranja ispitivanom osobom. No, UI s ovim navodnim sposobnostima može isto tako naučiti mučiti žrtvu. Za ispitivanu osobu rizik je da bi takav UI mogao biti iskorišten kako bi primijenio različite psihološke ili fizičke tehnike mučenja. Pritom je važno istaknuti da UI može djelovati bez bilo kakve prisutnosti i nadzora čovjeka pa su u tom smislu moguće poteškoće kod dokazivanja pojedinih subjektivnih i objektivnih elemenata konkretnog kaznenog djela.[17]

2.2. Sigurnost prometa i odgovornost za prometnu nesreću

Ugrožavanje prometa i kaznena odgovornost za prometne nesreće predstavljaju trenutačno najaktualnije područje ovdje obrađivane problematike. Prema našem mišljenju, najizglednije je da će se prvi izazovi kaznenog prava i UI-ja u Europi pojaviti upravo u području kaznene odgovornosti za prometne nesreće.

14 *Ibid.*, str. 30.

15 Vidi: https://www.linkedin.com/pulse/cloning-human-voices-has-created-new-type-crime-ai-for-real-drw8f?trk=public_post (22. veljače 2024.).

16 King *et al.*, *op. cit.* u bilj. 9, str. 101.

17 *Ibid.*, str. 102.

To proizlazi iz činjenice da se automobilska industrija sve više okreće tehnologijama zasnovanima na UI-ju[18] te da su u pojedinim dijelovima svijeta (osobito u SAD-u) već zaživjeli pilot-projekti puštanja posve samostalnih UI vozila u opći promet.[19] Kao i u drugim područjima u kojima se uvodi UI, ovdje se također navode višestruke prednosti, od kojih je najvažnija ona koja se odnosi na smanjenje broja prometnih nezgoda i ljudskih žrtava.

Iz kaznenopravne perspektive, međutim, uvođenje autonomnih vozila u opći promet otvara pitanje kaznene odgovornosti za prometnu nesreću s teškim posljedicama koje takvo vozilo prouzroči. Iako je ovakav tip vozila zamišljen da bi smanjio rizik od prometnih nesreća, praksa pokazuje da je moguć i drukčiji ishod. Kao primjer može se navesti događaj iz 2018. godine, kada je u američkoj saveznoj državi Arizoni autonomni automobil tvrtke *Uber*, kojim je upravljao UI, usmrtio pješakinju jer nije prepoznao da se približava i nije prilagodio svoju brzinu. U automobilu je tada bila vozačica zadužena da reagira ako UI pogriješi (engl. *test-driver*), ali je ona u tom trenutku gledala film na mobilnom uređaju pa nije pravodobna reagirala. Vozačica je priznala krivnju za kazneno djelo ugrožavanja i nagodila se za uvjetnu kaznu, dok nitko od odgovornih osoba iz tvrtke *Uber*, kao ni iz tvrtke koja je proizvela vozilo nije odgovarao.[20]

Iako je u ovom primjeru testna vozačica proglašena kazneno odgovornom i razmjerno blago kažnjena, ako se uzme u obzir činjenica da je nastupila smrtna posljedica, taj slučaj otvara ozbiljne dvojbe u vezi s tim tko će biti odgovoran kada se počnu rabiti automobili u kojima neće biti pričuvnog test-vozača.[21] Situacija će biti dodatno složena ako korporacije koje budu stajale iza takvih vozila poduzmu sve prethodne mjere testiranja i osiguranja od opasnosti, a štetni događaj nastupi usprkos tomu. To će osobito doći do izražaja u sustavima koji ne poznaju kaznenu odgovornost pravnih osoba.[22] Moguće je da će se

---

18 Antonialli, F.; Martinesco, A.; Mira-Bonnardel, S., *Artificial intelligence as a determinant for reshaping the automotive industry and urban mobility services*, International Journal of Automotive Technology and Managment, *vol.* 22, br. 3, 2022., str. 324 – 351.

19 Vidi više na: https://fortune.com/2023/08/18/san-francisco-launching-driverless-bus-service-beep-california-robotaxi-expansion/ (17. listopada 2023.).

20 Vidi više na: https://edition.cnn.com/2023/07/29/business/uber-self-driving-car-death-guilty (17. listopada 2023.). Također vidi Mrčela, M.; Vuletić, I., *Kazneno pravo pred izazovima robotike: tko je odgovoran za prometnu nesreću koju je prouzročilo neovisno vozilo?*, Zbornik Pravnog fakulteta u Zagrebu, *vol.* 68, br. 3-4, 2018., str. 467.

21 https://www.nbcnews.com/business/business-news/can-driverless-cars-get-tickets-california-law-rcna131538 (23. veljače 2024.).

22 Iscrpan poredbenopravni osvrt o tome može se naći u Gless, S.; Silverman, E.; Weigend, T., *If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability*, New Criminal Law Review, *vol.* 19, br. 3, 2016., str. 412 – 436.

javiti problemi oko utvrđivanja uzročnosti i krivnje (pravnih i fizičkih) osoba iza takvih samostalnih vozila te da postojeće kazneno pravo neće uvijek imati prikladan odgovor, što dovodi do pravnih praznina.[23]

2.3. Vojna industrija i odgovornost zapovjednika

Ovo područje predstavlja možda i najveći izazov kada je riječ o uređenju kaznenih djela UI-ja. Ta tvrdnja dobiva na težini ako se uzme u obzir da tipična međunarodna kaznena djela (međunarodni zločini) poput genocida, ratnog zločina, zločina protiv čovječnosti i zločina agresije redovito podrazumijevaju velik broj ljudskih, najčešće civilnih žrtava. Tradicionalni koncept odgovornosti zapovjednika počiva na učenju o krivnji i predvidljivosti posljedica.[24] Dosadašnji pokušaji uvođenja odgovornosti za eksces u figurama poput zajedničkog (udruženog) zločinačkog pothvata u pravilu nisu nailazili na odobravanje kontinentalnih kaznenih pravnika.[25]

Istraživanja posljednjih pokazuju da vodeće svjetske vojne sile intenzivno rade na dizajniranju autonomnog oružja, koje im omogućuje veliku taktičku i logističku prednost u ratovanju. Pritom se pod pojmom autonomnog oružja uglavnom podrazumijeva takva vrsta naoružanja koja, kada se jednom aktivira, dalje djeluje bez ikakva ljudskog nadzora i samostalno odabire metu koju potom napada i uništava.[26] Jedan od prvih primjera uporabe ovakve vrste oružja uočen je tijekom sukoba između Azerbajdžana i Armenije u Nagorno-Karabakhu 2016. godine. Tada je autonomno oružje omogućilo azerbajdžanskoj vojsci stjecanja velike taktičke prednosti. Konkretno, radilo se o korištenju naprednog izraelskog autonomnog oružja IAI Harop *loitering munition*, poznatog još pod nazivom kamikaza-dronovi (engl. *kamikaza drones*).[27] Riječ je o posebnoj, visoko sofisticiranoj vrsti raketa koje, jednom kada su lansirane, mogu satima lebdjeti

---

[23] Za više vidi npr. Douma, F.; Palodichuk, S. A., *Criminal Liability Issues Created by Autonomous Vehicles*, Santa Clara Law Review, *vol.* 52, br. 4, 2012., str. 1157 – 1169.

[24] Martinez, J. S., *Understanding Mens Rea in Command Responsibility*, Journal of International Criminal Justice, *vol.* 5, br. 3, 2007., str. 647 – 660.

[25] Vidi npr. European Parliament resolution of 16 February 2011 on the 2010 progress report on Croatia, para. 15, dostupno na: https://www.europarl.europa.eu/doceo/document/TA-7-2011-0059_EN.pdf (23. listopada 2023.)

[26] Tako npr. UK Ministry of Defence, Joint Doctrine Publication 0-30.2. Unmaned Aircraft Systems, 2017., p. 13, dostupno na: https://assets.publishing.service.gov.uk/media/5a823670ed915d74e6236640/doctrine_uk_uas_jdp_0_30_2.pdf (23. listopada 2023.).

[27] Postma, J., *Drones over Nagorno-Karabakh: A glimpse at the future of war?*, Atlantisch Perspectief , *vol.* 45, br. 2, 2021., str. 15 – 20.

u zraku i "vrebati" neprijateljske ciljeve, u koje se potom zalijeću i uništavaju ih, na isti način kako su to činile japanski kamikaze u II. svjetskom ratu.[28]

U poredbenoj praksi bilo je slučajeva uporabe oružja za masovno uništenje koje je djelovalo u poluautonomnom načinu i dovelo do višestrukih ljudskih žrtava, pri čemu nitko za to nije bio kazneno odgovoran. Može se navesti primjer iz 1988. godine, kada je američki radarski sustav *Aegis*, kojemu je svrha bila zaštita bojnih brodova od zračnih napada, zamijenio iranski civilni zrakoplov Iran Air 665 s vojnim zrakoplovom i ispalio protuzračnu raketu, što je rezultiralo smrću svih 290 putnika i članova posade.[29]

U literaturi se s pravom upozorava da institut zapovjedne odgovornosti, čak i uz najšire moguće tumačenje namjere i nehaja, može pokriti samo one situacije u kojima je moguće dokazati povredu određene objektivno odredive dužnosti zapovjednika. Ovdje se mogu ubrojiti situacije povrede dužnosti redovnog održavanja i testiranja određenog autonomnog sustava, zatim odluke da se koristi sustavom koji nije dovoljno testiran ili je još u eksperimentalnoj fazi, povjeravanje rukovanja sustavom neadekvatno obučenom osoblju, propuštanje da se organizira odgovarajuća obuka, različite mjere uštede koje ugrožavaju sigurnost upravljanja sustavom i sl. No, postojeći koncept zapovjedne odgovornosti neće pružati dostatna jamstva u slučajevima u kojima je zapovjednik uložio sve potrebne napore, a osobito neće biti adekvatan ako je riječ o oružanim sustavima koji su posve samostalni. U takvim okolnostima će združeni problemi načela krivnje, uzročnosti i zabranjene analogije predstavljati zapreku kaznenoj odgovornosti.[30] Moglo bi se dodati da je to ujedno i jedan od najvažnijih razloga zašto bi razvoj ovakvog oružja trebalo zaustaviti.

2.4. Medicina i odgovornost za pogreške u liječenju

Medicina je jedno od područja u kojima je razvoj UI-ja najizraženiji. Višestruke su prednosti korištenja opreme zasnovane na UI tehnologiji: od veće točnosti i preciznosti, preko povećanja učinkovitosti i broja sati rada (što uključuje i znatno smanjenje liste čekanja) pa do pojeftinjenja cjelokupnog procesa liječenja. Prema određenim procjenama, realno je očekivati da će u području medicinske dijagnostike te osobito u području radiologije UI u dogledno vrijeme

---

[28] Postma, J., *op. cit.* u bilj. 9, str. 15 – 20.

[29] Više o tome dostupno je na: https://simpleflying.com/iran-air-flight-655-1988-shootdown-anniversary/ (23. listopada 2023.).

[30] Tako npr. Bo, M., *Autonomous Weapons and the Responsibility Gap in light of the Mens Rea of the War Crime of Attacking Civilians in the ICC Statute*, Journal of International Criminal Justice, *vol.* 19, br. 2, 2021., str. 275 – 299.

pretežno zamijeniti čovjeka.[31] Neka predviđanja kažu da će se u području kirurgije prisutnost UI mehanizama razviti do razine da će UI roboti-kirurzi moći samostalno obavljati složene operativne zahvate te da pritom neće biti potreban ljudski nadzor. Mnogi autori pokazuju velik entuzijazam spram takvog razvoja, upućujući uglavnom na njegove neupitne prednosti.[32] Istodobno je takav smjer napretka često predmetom kritika u stručnoj literaturi, uz obrazloženje da kirurgiju nikada ne treba prepustiti posve u ruke UI-ja jer kirurške procese naprosto nije moguće unaprijed definirati putem odgovarajućih obrazaca, nego je uvijek potreban individualni pristup, praćen odgovarajućim iskustvom, kirurškom intuicijom i procjenom etičnog načina postupanja.[33]

Ovakav razvoj događaja s pravom otvara pitanja o održivosti koncepta pravne zaštite u slučaju eventualnih pogrešaka u liječenju, koji se temelji na sustavu odgovornosti za pogrešku. Neki autori drže da će razvoj UI sustava u medicinskoj dijagnostici zahtijevati i razvoj posebnih, novih postupaka UI vještačenja te da bi to u konačnosti moglo narušiti i dovesti u pitanje postojeće standarde medicinskih pogrešaka te na taj način poljuljati čitav sustav pravne zaštite od nesavjesnog liječenja kakav trenutačno poznajemo.[34]

Dvojbe se mogu pojaviti u različitim područjima medicine, a ne samo u dijagnostici. Može se tako postaviti pitanje odgovornosti za kirurške pogreške, zatim u intenzivnoj njezi, u sklopu koje se može javiti vrlo osjetljiv problem propuštanja daljnjeg liječenja smrtno bolesnih pacijenata priključenih na uređaje za održavanje vitalnih funkcija[35] i sl. Zato se u kaznenopravnoj literaturi s pravom upozorava na moguće nedostatke u utvrđivanju kaznene odgovornosti, posebice u onim sustavima koji za postojanje takve odgovornosti traže kumulativno ispunjene uvjete uzročnosti, krivnje i povrede pravila struke.[36]

---

31 Basu, K.; Sinha, R.; Ong, A; Basu, T., *Artificial Intelligence: How is It Changing Medical Sciences and Its Future?*, Indian Journal of Dermatology, *vol.* 65, br. 5, 2020., str. 365 – 370.

32 Noorbakhsh-Sabet, N.; Zand, R.; Zhang, Y.; Abedi, V., *Artificial Intelligence Transforms the Future of Health Care*, The American Journal of Medicine, *vol.* 132, br. 7, 2019., str. 795 – 801.

33 Kinoshita T.; Komatsu, M., *Artificial Intelligence in Surgery and Its Potential for Gastric Cancer*, Journal of Gastric Cancer, *vol.* 23, br. 3, 2023., str. 400 – 409.

34 Froomkin, M. A.; Kerr, I. R.; Pineau, J., *When AIs Outperform Doctors: Confronting the Challenges of a Tort-Induced Over-Reliance on Machine Learning*, Arizona Law Review, *vol.* 61, br. 1, 2019., str. 39 – 98.

35 Korošec, D., *Criminal Law Dilemmas in Withholding and Withdrawal of Intensive Care*, Medicine, Law & Society, *vol.* 9, br. 1, 2016., str. 21 – 39.

36 O tome vidi npr. Ludvigsen, K. R.; Nagaraja, S., *Dissecting liabilities in adversarial surgical robot failures: A national (Danish) and EU law perspective*, Computer Law & Security Review, *vol.* 44, 2022., str. 1 – 20. Vidi također i Chan, B., *Applying a Com-*

2.5. Financije i gospodarski kriminalitet

U financijskom sektoru je prodor tehnologija zasnovanih na UI-ju također sve intenzivniji, posebice u posljednjih deset godina. Glavni je razlog tomu činjenica da automatizirani softveri omogućuju mnogo veću dobit u poslovanju. No, istodobno autonomni algoritmi preuzimaju i više rizika te u procjeni prihvatljive granice riskiranja ne postupaju uvijek prema načelima uobičajenima za ljude.[37] Neki od takvih rizika mogu predstavljati i kaznena djela. U literaturi se najčešće spominju primjeri manipulacija tržištem, umjetnog namještanja cijena i kolizije kao slučajevi u kojima može doći do pitanja kaznene odgovornosti.[38]

To se može dogoditi ako UI sustavi, koji raspolažu sposobnošću učenja i donošenja samostalnih odluka na temelju podataka iz svoje okoline i programiranih podataka, počnu davati određene informacije korisnicima s namjerom obmanjivanja ugovorne strane. Neka su istraživanja pokazala da takva umjetna inteligencija može usavršiti tehnike slanja lažnih narudžbi (koje nikada neće biti izvršene) i zaključivanja lažnih transakcija, s ciljem prijevare dobronamjerne treće osobe i ostvarivanja veće dobiti. Takav razvoj događaja nije nerealan jer je UI programiran da, među ostalim, pronađe najprofitabilnije poslovne modele. Stoga je moguće da određeni UI financijski softver prepozna zaključivanje fiktivnih poslova kao najprofitabilniju mogućnost i da onda dalje postupa prema tom zaključku. Nadalje, postoji mogućnost različitih vrsta nezakonitih manipulacija na burzi širenjem lažnih informacija o vrijednosti dionica putem algoritamskih trgovinskih agenata.[39]

U nedavnoj prošlosti bilo je drastičnih primjera u kojima su *autonomous trading algorithms* doveli do velikih financijskih posljedica. Godine 2010. dogodio se financijski incident, poznat pod nazivom "Flash Crash". Zahvaljujući interakciji nekoliko takvih algoritama, prouzročeni su znatni financijski gubitci za više subjekata. Najdrastičniji primjer predstavlja događaj iz 2012. godine, kada je trgovački softver (koji je imao grešku) poslao dionice vrijedne sedam milijuna dolara tvrtke Knight Capital Group u nekontroliranu kupovinu (engl. *shopping spree*). Prema pravilima burze, Knight je trebao platiti te dionice tri dana kasnije, no to nije bio moguće jer ta trgovina nije bila namjerna i nije imala nikakvu

mon Enterprise Theory of Liability to Clinical AI Systems, American Journal of Law & Medicine, *vol.* 47, br. 4, 2021., str. 351 – 385.

37 Borch, C., *Machine learning, knowledge risk, and principal-agent problems in automated trading*, Technology in Society, *vol.* 68, 2022., str. 713 – 725.

38 King *et al., op. cit.* u bilj. 9, str. 97 – 100.

39 *Ibid.*

financijsku pozadinu.[40] Knight se zatim borio kako bi poništio te transakcije, no taj je napor odbijen jer se smatralo da bi to bilo nepravedno prema trgovinskim partnerima (većini dionica) od strane Komisije za vrijednosne papire i burze (SEC). To je izazvalo financijsku katastrofu za Knight, uzrokujući gubitak od 460 milijuna dolara te je rezultiralo kasnijim pripojenjem tvrtki Getco LLC.[41]

Iz tog i sličnih primjera s manjim posljedicama određeni autori izvlače zaključak da postojeći okviri gospodarskih kaznenih djela, temeljenih uglavnom na dokazivanju (prijevarne) namjere počinitelja, u bližoj budućnosti neće biti dovoljni da adekvatno obuhvate sve moguće slučajeve ovakvih oblika kriminala.[42]

2.6. Odgovornost za povredu osobnih podataka i pitanje kibernetičke sigurnosti

Još jedno od područja visokog rizika odnosi se na zaštitu osobnih podataka i privatnosti osoba. Unatoč tomu što uporaba UI-ja otvara znatne prednosti, pojavljuje se i mnogo praktičnih problema, uključujući profiliranje, diskriminatorne odluke i nedostatak transparentnosti. Nepredvidljivost koja proizlazi iz načina djelovanja UI tehnologije može prouzročiti određene poteškoće, koje u pravilu nisu na zadovoljavajući način riješene pravnim okvirima većine zemalja u svijetu.[43]

Za učinkovito djelovanje UI tehnologije potreban je unos velikih količina podataka, među kojima mogu biti i osobni podatci građana pa se može javiti opasnost od ugrožavanja privatnosti takvih podataka. Ovdje se kao primjer može navesti nedavni slučaj iz Mađarske, gdje je jedna financijska institucija automatski putem UI-ja analizirala snimke razgovora svoje korisničke službe s klijentima. Rezultati takve analize su potom korišteni kako bi se odredilo koje klijente treba opet nazvati, pri čemu je ključna bila analiza emocionalnog stanja glasa i drugih psiholoških osobina klijenta koje su proizlazile iz razgovora.[44]

---

40 Borch, C., *High-frequency trading, algorithmic finance and the Flash Crash: reflections on eventalization*, Economy and Society, *vol.* 45, br. 3-4, 2016., str. 350 – 378.

41 Kirilenko, A.; Kyle, A. S.; Samadi, M.; Tuzun, T., *The Flash Crash: High Frequency Trading in an Electronic Market*, The Journal of Finance, *vol.* 72, br. 3, 2017., str. 967 – 998.

42 Yeoh, P., *Artificial intelligence: accelerator or panacea for financial crime?,* Journal of Financial Crime, *vol.* 26, br. 2, 2019., str. 634 – 646.

43 Detaljno o tome Ishii, K., *Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects*, AI & Society, *vol.* 34, br. 3, 2019., str. 509 – 533.

44 Miró-Llinares, *op. cit.* u bilj. 10, str. 31.

Neželjeno prikupljanje različitih vrsta osobnih podataka može biti povezano i s drugim vrstama kaznenih djela, poput krađe identiteta. Primjer iz kineskog prava, u kojem se UI tehnologijom koristilo kako bi se provalilo u sustav automatskog prepoznavanja lica (engl. *facial recognition*) te kako bi se ukrali određeni osobni podatci koji su se poslije zlorabili u protuzakonite svrhe.[45]

Baze podataka u policiji i kaznenom pravosuđu u kombinaciji s upotrebom UI-ja također donose niz specifičnih problema. Naime, policija i tijela kaznenog pravosuđa posjeduju goleme baze podataka o ljudima, događajima i navodnim kaznenim djelima, pri čemu se tu mogu nalaziti i podatci o rasnom ili etničkom podrijetlu, te druge informacije kojih je obradba zabranjena.[46] Navedena tijela na temelju tih podataka donose niz odluka koje mogu znatno utjecati na najviša osobna dobra pojedinca. Ove se odluke mogu donositi i uz primjenu UI alata za procjenu vjerojatnosti nastupanja neke buduće okolnosti poput opasnosti od bijega, uništavanja tragova kaznenog djela, utjecaja na svjedoke ili počinjenja novog kaznenog djela.[47]

Ovakvi UI alati za profiliranje i predikciju mogu pritom presudno utjecati na donošenje odluke o uhićenju i pritvaranju neke osobe odnosno određivanju istražnog zatvora, provođenju dokaznih radnji poput pretrage ili (tajnih) posebnih dokaznih radnji, te u bitnome utjecati na odluku o provođenju kaznenog postupka i ograničavanju prava i sloboda konkretnog okrivljenika. U ovakvim sustavima za predikciju i profiliranje teško je izbjeći problem pristranosti i diskriminatornih učinaka.[48] Naime, premda se na prvi pogled može činiti da bi baš UI alat trebao biti nepristraniji od čovjeka, činjenica je da dizajn i način upravljanja takvim alatima producira i pogoršava diskriminaciju na temelju rase, etničke pripadnosti, socioekonomskog statusa i sl.[49] Uz sve mjere opreza,

---

45 *Ibid.*

46 Odredbama Kaznenog zakona izričito je kažnjiva obradba i korištenje podataka fizičkih osoba koji se odnose na rasno ili etničko podrijetlo, politička stajališta, vjerska ili druga uvjerenja, sindikalno članstvo, zdravlje ili spolni život te osobne podatke o kaznenom ili prekršajnom postupku. Vidi čl. 146. st. 3. KZ-a.

47 Vidi: Novokmet, A.; Tomičić, Z.; Vinković, Z., *Pretrial risk assessment instruments in the US criminal justice system – what lessons can be learned for the European Union*, International Journal of Law and Information Technology, *vol.* 30, br. 1, 2022, str. 1 – 22.

48 *Ibid.*, str. 9 – 11.

49 Na primjer, u Nizozemskoj, lista "Top 600" pokušava "predvidjeti" koji će mladi ljudi počiniti određena kaznena djela. Svaki treći od "Top 600", od kojih su mnogi prijavili da ih policija prati i maltretira, marokanskog je podrijetla. U Italiji, sustav predviđanja kojim se koristi policija pod nazivom Delia uključuje podatke o etničkoj pripadnosti za profiliranje i "predviđanje" budućeg kriminala ljudi. Drugi sustavi nastoje "predvidjeti" gdje će se kazneno djelo dogoditi, opetovano ciljajući na rasno etiketirana područja ili siromašnije zajednice. Usp. https://www.fairtrials.

nije teško zamisliti situacije u kojima bi UI alat za pružanje rezultata obradbe podataka "povukao" i neku zabranjenu informaciju. Naime, naoko nepovezane baze mogu imati i neke rupe u protokolima koje bi UI mogao prepoznati i "povući" podatke iz npr. neformalnih policijskih bilješki, ali i tajne obavještajne podatke prikupljene za potrebe sigurnosnih provjera (tajnih službi) mimo postupanja vezanog uz kaznena djela.[50] U takvim situacijama čak ni savjesna kontrola i nadzor ovlaštenog službenika nisu nužno dovoljno jamstvo protiv zlouporabe. Uporaba UI sustava u promatranom kontekstu lako bi mogla rezultirati npr. nezakonitim odlukama o oduzimanju slobode ili poduzimanju nezakonitih pretraga kao konkretnim kaznenim djelima (čl. 136. i 298. KZ-a), premda nisu posve jasni uvjeti tko bi i pod kojim pretpostavkama trebao biti odgovoran.

Na slične probleme nailazimo i u primjeni tehnologija i sustava za automatsko prepoznavanje lica (engl. *facial recognition technology*; dalje: FRT). Preciznost ovih tehnologija je pod "povećalom", posebice jer stope pogrešne identifikacije mogu dosegnuti alarmantne razine, postavljajući pitanja o njihovoj pouzdanosti i prikladnosti za široku uporabu.[51] Potencijalne zlouporabe i kršenja privatnosti proizlaze i iz nejasnog pravnog okvira, odnosno pitanja vezanih uz razloge zašto se netko nalazi na "listi za praćenje" te diskrecijskog prava pri odabiru lokacije za raspoređivanje FRT sustava. U tom smislu postoji opravdana bojazan da ovi sustavi mogu neproporcionalno utjecati na određene demografske skupine, što dovodi do diskriminirajućih ishoda. Nadalje, građani mogu biti podvrgnuti prepoznavanju lica bez njihova znanja, što izaziva etičku zabrinutost u vezi s transparentnošću takve prakse i kršenjem prava pojedinca na privatnost.[52] Uz

org/campaigns/ai-algorithms-data/?gad_source=1&gclid=CjwKCAiAvJarBhA1EiwAGgZl0BgH4GI0jjZuussTyS7itkCN56WbtY6gJu_o7M8S3Rdtf8_kvn3kBRoCx7EQAvD_BwE (26. listopada 2023.).

50 Usp. Roksandić, S.; Protrka, N.; Engelhart, M., *Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?*, 2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2022, str. 1225 – 1232, doi: 10.23919/MIPRO55190.2022.9803606.

51 Vidi: Novokmet, A.; Tomičić, Z.; Vidaković, I., *Facial Recognition Technology in EU Criminal Justice - Human Rights Implications and Challenges*, u: Duić, D.; Petrašević, T. (ur.), *EU and Comparative Law Issues and Challenges Series (ECLIC), Digitalization and Green Transformation of the EU, vol. 7*, Faculty of Law, Josip Juraj Strossmayer University of Osijek, Osijek, 2023., str. 550 – 561, doi: https://doi.org/10.25234/eclic/27461.

52 Roksandić Vidlička, S.; Elīna Liepiņa, L.; Ostapchuk, S., *Bioethical and Legal Challenges of Artificial Intelligence and Human Dignity* u: Jovanović, M.; Virady, T., (ur.), *Human rights in 21st century*, Eleven International Publishing, Nizozemska, 2020., str.

sve navedeno, uporaba FRT sustava može dovesti do konkretnih postupanja policije i pravosudnih tijela poput uhićenja, poduzimanja dokaznih radnji te pokretanja kaznenog postupka.[53] Nezakonita postupanja u tom smislu mogu rezultirati i već navedenim kaznenim djelima iz čl. 136. i 298. KZ-a. Odluka o snimanju javnog okupljanja ili mirnog prosvjeda FRT sustavom potencijalno može predstavljati i povredu prava na okupljanje i prosvjed iz čl. 128 KZ-a.[54]

Naposljetku, UI se rabi kako bi se povećala učinkovitost različitih oblika kibernetičkih napada. Oblici postupanja poput provala u računalne sustave, krađe podataka iz takvih sustava, računalnih prijevara, *phishinga* i slično pokazuju se znatno opasnijima ako se provode putem UI-ja. Primjerice, kada je riječ o računalnim prijevarama i *phishingu*, UI može unaprijediti metode obmane žrtve jer može prikupiti podatke koji su relevantni baš za konkretnu žrtvu. Ovdje se može navesti primjer jednog takvog napada iz 2019. godine, kada je UI softver zlorabljen u jednoj korporaciji u SAD-u na način da je putem telefona imitirao glas izvršnog direktora i podređenim osobama naredio provođenje isplate koja je zapravo bila prijevarna.[55]

3. OSVRT IZ PERSPEKTIVE POSEBNOG DIJELA KZ-A I SMJERNICE HRVATSKOM ZAKONODAVCU

Hrvatsko kazneno materijalno pravo je prije nešto više od deset godina prošlo kroz značajne reforme. Donošenjem KZ/11[56] u hrvatski sustav je u potpunosti implementirana većina suvremenih kaznenopravnih standarda. Na taj je način domaći kaznenopravni okvir usklađen s poredbenim, europskim i svjetskim trendovima. No, reforma tu nije stala jer je, nakon donošenja, KZ/11 dopunjavan i mijenjan ukupno devet puta, što govori o postojanju svojevrsne kulture razmjerno čestog mijenjana propisa i, unatoč tomu što se u pravni sustav na taj način stalno unose novi međunarodni standardi, može dovesti u pitanje jasnoću tumačenja i pravnu sigurnost. Zato se na ovom mjestu svrstavamo među protivnike tako čestih zakonskih izmjena.

269 – 288.

53 Kotsoglou, K. N.; Oswald, M., *The long arm of the algorithm? Automated Facial Recognition as evidence and trigger for police intervention*, Forensic Science International: Synergy, *vol.* 2, 2020., str. 86 – 89.

54 Sama činjenica da se događaj nadzire FRT sustavom odvraća građane od dolaska na okupljanje odnosno prosvjed.

55 Miró-Llinares, *op. cit.* u bilj. 10, str. 36.

56 Kazneni zakon, Narodne novine, br. 125/2011, 144/2012, 56/2015, 61/2015, 101/2017, 118/2018, 126/2019, 84/2021, 114/2022, 114/2023.

Kada se govori o odgovornosti osoba koje stoje iza UI-ja, jedna od važnih tema odnosi se na uređenje kaznene odgovornosti pravnih osoba. U tom je pogledu potrebno naglasiti da hrvatsko kazneno pravo ima više od 20 godina iskustva u tom području.[57, 58] U tom smislu, pravni okvir hrvatskog prava je načelno bolji od pravnih okvira u nekim drugim značajnim europskim sustavima (npr. u njemačkom pravu), koji ne poznaju kaznenu odgovornost pravnih osoba.[59]

Hrvatsko pravo prihvaća model odgovornosti pravne osobe zasnovan na kaznenoj odgovornosti odgovorne fizičke osobe, ali je i u teoriji i u praksi prihvaćeno stajalište prema kojem je pravnu osobu moguće osuditi i u određenim slučajevima u kojima nije moguće osuditi odgovornu fizičku osobu[60], što je vrlo značajno za kontekst teme koja se ovdje obrađuje. Uvid u praksu pokazuje kako je u nekim predmetima bilo jasno da postoji odgovornost fizičke osobe, ali se nije moglo identificirati tko je konkretna fizička osoba koja je odgovorna. Takve situacije su se onda presuđivale tako da je protiv odgovorne osobe postupak obustavljen, ali je unatoč tomu pravna osoba osuđena. To je obrazloženo na način da je za kaznenu odgovornost pravne osobe dovoljno utvrditi da je njena odgovorna osoba učinila propust. Ako se identitet te osobe ne može utvrditi, to ne utječe na postojanje odgovornosti pravne osobe. Ovo je primjerice slučaj u situaciji u kojoj je poslovođa gradilišta, koji je bio odgovoran za neprovođenje zaštitnih mjera, u trenutku pada radnika s neosigurane skele bio na dugotrajnom bolovanju, a nije moglo biti utvrđeno tko ga je mijenjao jer o tome nije bila donesena pisana odluka.[61] Može se, stoga, zaključiti da je kaznena odgovornost pravnih osoba u praksi ponajprije povezana s odgovornošću fizičke osobe zadužene za poslovanje pravne osobe. Potrebno je dokazati da je u pogledu određene radnje ili propusta postojala određena dužnost pravne osobe[62], zatim da je fizička osoba zadužena za izvršenje te dužnosti svoju obvezu povrijedila te da je takva povreda prouzročila posljedicu iz opisa kaznenog djela.[63] Oprav-

[57] Temeljitu analizu prvih deset godina primjene kaznene odgovornosti pravnih osoba daju Derenčinović, D.; Novosel, D., *Zakon o odgovornosti pravnih osoba za kaznena djela – prolazne dječje bolesti ili (ne)rješiva kvadratura kruga*, Hrvatski ljetopis za kazneno pravo i praksu, *vol.* 19, br. 2, 2012., str. 585 – 613.

[58] U hrvatskom kaznenom pravu ova je materija iscrpno uređena Zakonom o odgovornosti pravnih osoba za kaznena djela, Narodne novine, br. 151/2003, 110/2007, 45/2011, 143/2012, 114/2022, 114/2023 (dalje: ZOPOKD).

[59] Gless, Silverman, Weigend, *op. cit*. u bilj. 20, str. 418.

[60] Usp. Novoselec, P., *Opći dio kaznenog prava*, Pravni fakultet Osijek, Osijek, 2016., str. 461.

[61] Županijski sud u Varaždinu, Kž-401/2019.

[62] U ovom smislu došlo je do svojevrsnog proširenja odgovornosti prigodom posljednjih izmjena ZOPOKD-a. Usp. čl. 3. st. 2. ZOPOKD.

[63] Novoselec, *op. cit.* u bilj. 60, str. 463.

dano je, dakle, reći da je odgovornost fizičke osobe i u zakonodavstvu i u praksi konstitutivna pretpostavka za osudu pravne osobe, pri čemu je djelomična iznimka ipak moguća u slučaju kada je utvrđeno da određena dužnost pripada u djelokrug poslova odgovorne fizičke osobe, ali identitet te osobe nije moguće utvrditi. To znači da će, u slučajevima zlonamjerne uporabe UI-ja, ipak biti moguće osuditi pravnu osobu, čak i ako se odgovornu fizičku osobu ne može identificirati ili osuditi.

U nastavku teksta osvrnut ćemo se na odabrana poglavlja posebnog dijela, koja se odnose na prethodno promatrana područja najvećeg rizika zlonamjerne uporabe UI-ja. Cilj je utvrditi jesu li postojeće odredbe adekvatne za pokrivanje potencijalnih slučajeva kaznene odgovornosti.

3.1. Osvrt na odabrana poglavlja posebnog dijela KZ/11

Iz prethodnog uspostavljanja fenomenologije ugrožavajućih i rizičnih uporaba UI tehnologije proizlazi da se u određenim situacijama takva tehnologija rabi isključivo u (zlonamjernoj) interakciji čovjeka i UI-ja, dok se u nekim drugim slučajevima može raditi i o samostalnom protuzakonitom i štetnom djelovanju UI-ja, neovisno o čovjeku. U prvu skupinu situacija spadaju ugrožavanja i povređivanja najviših osobnih dobara. U hrvatskom su kaznenom pravu takve situacije pokrivene kaznenim djelima protiv života i tijela, protiv osobne slobode, protiv spolne slobode i protiv spolnog zlostavljanja i iskorištavanja djece te djelomično kaznenim djelima protiv zdravlja (u dijelu koji se odnosi na trgovanje drogama). Mišljenja smo da ovo područje neće uzrokovati suviše problema jer je u pravilu riječ o kaznenim djelima koja se čine s namjerom i kod kojih će UI predstavljati samo sredstvo počinjenja. Također, kod ovih kaznenih djela će se rijetko raditi o počiniteljima pravnim osobama pa će tu uglavnom u potpunosti biti primjenjiva sva ona tradicionalna pravila koja se odnose na uzročnost i krivnju fizičkih osoba. Ipak, treba primijetiti da KZ/11 ne propisuje korištenje UI-ja u svrhe napada na najviša osobna dobra kao kvalifikatornu okolnost pa bi o tome svakako trebalo razmisliti u budućnosti. Alternativu bi predstavljalo uzimanje u obzir te okolnosti kao otegotne pri odmjeravanju kazne, za slučaj da se zakonodavac ne odluči na uvođenje dodatnih kvalifikatornih okolnosti. Opravdanje za posebno vrednovanje ovih okolnosti, po našem mišljenju, leži u činjenici da je riječ o zlouporabi suvremenih tehnologija kojima je primarna svrha poboljšanje kvalitete života te da takva zlouporaba neizravno može imati dalekosežne posljedice za društvo.

U pogledu kaznenopravne zaštite prometa, slažemo se sa stajalištem prema kojemu KZ/11 predviđa zadovoljavajući kazneni okvir. Tako će se odgovornost

vozača prosuđivati prema uvjetima kaznenog djela izazivanja prometne nesreće u cestovnom prometu (čl. 272. KZ/11), dok će se odgovornost svih ostalih uključenih osoba (vlasnika vozila koji nije vozač ili je samo putnik u vozilu, programera, proizvođača i prodavača) prosuđivati prema pravilima garantne odgovornosti, u okviru kaznenog djela dovođenja u opasnost života i imovine općeopasnom radnjom ili sredstvom (čl. 215. KZ/11) ili teških kaznenih djela protiv opće sigurnosti (čl. 222. KZ/11).[64] Ovdje će do izražaja doći i ono što je prije rečeno o kaznenoj odgovornosti pravnih osoba. Poseban problem nastaje ako u vozilu nema vozača. U tom slučaju u obzir dolazi odgovornost vlasnika vozila, i to ponajprije za djelo iz čl. 215. KZ/11.

Kada je riječ o autonomnom naoružanju, problem postaje složeniji. Naime, mišljenja smo da institut zapovjedne odgovornosti, čak i uz najšire moguće tumačenje pitanja krivnje i odgovornosti za nehajni oblik, može obuhvatiti slučajeve korištenja UI-ja samo u situacijama u kojima je moguće dokazati povredu određene objektivno odredive dužnosti zapovjednika (npr. povrede dužnosti redovnog održavanja i testiranja određenog autonomnog sustava, odluke da se koristi sustavom koji nije dovoljno testiran ili je još u eksperimentalnoj fazi, povjeravanje rukovanja sustavom neadekvatno obučenom osoblju, propuštanje da se organizira odgovarajuća obuka, različite mjere uštede koje ugrožavaju sigurnost upravljanja sustavom i sl.). U slučaju takvih povreda, bit će moguće konstruirati pravni standard povrede dužne pažnje, što će biti osnova za nehajni oblik odgovornosti zapovjednika (uz pretpostavku da se sudska praksa otvori prema takvom tumačenju). No, ovaj institut naprosto neće biti dostatan u situacijama u kojima je zapovjednik uložio sve potrebne napore, a osobito neće dostajati ako je riječ o oružanim sustavima koji su posve autonomni (kako u fazi *targetinga*, tako i u fazi gađanja). U takvim slučajevima će združeni problemi načela krivnje, uzročnosti i zabranjene analogije predstavljati zapreku kaznenoj odgovornosti.[65] Problem će, dakle, ponajprije predstavljati odgovornost za nehaj, ali isto tako i za ona kaznena djela kod kojih je moguća samo izravna namjera prvoga stupnja, kao što su djela počinjena s točno određenim ciljem ili motivom (npr. genocid, kod kojeg je potrebno dokazati tzv. genocidnu namjeru). Ovdje, međutim, treba napomenuti kako barem zasad nije realno očekivati da će se ove dvojbe doista i pojaviti u sudskoj praksi, s obzirom na činjenicu da hrvatska vojska ne razvija i ne rabi sustave autonomnog naoružavanja kako to čine neki drugi vojni sustavi u svijetu.

---

64 Usp. Mrčela, Vuletić, *op. cit.* u bilj. 20, str. 486.

65 Tako Vuletić, I., *Rethinking superior liability in terms of emerging AI weapons*, u: Duić, D.; Petrašević, T. (ur.), *EU and Comparative Law Issues and Challenges Series (ECLIC), Special Issue – Law in the Age of Modern Technologies*, *vol.* 7, Faculty of Law, Josip Juraj Strossmayer University of Osijek, Osijek, 2023., str. 163 – 180.

Područje medicine i odgovornost za nesavjesno liječenje predstavljaju vrlo složenu problematiku u kontekstu hrvatskog kaznenog prava. Naime, za dokazivanje kaznene odgovornosti kod kaznenog djela nesavjesnog liječenja (čl. 181. KZ/11) traži se kumulativno ispunjenje pretpostavki očite (teške) povrede pravila struke, uzročne veze između takve povrede (ili propusta) i nastupile posljedice te krivnje (namjere ili nehaja).[66] Pritom, značajnu poteškoću u sudskoj praksi najčešće predstavlja upravo utvrđivanje je li posljedica rezultat povrede pravila struke ili nekih drugih neovisnih čimbenika, što je potrebno dokazati izvan svake razumne sumnje.[67] Ovdje će se problemi javiti ako u budućnosti UI preuzme određen dio medicinske djelatnosti posve samostalno (što je realno očekivati osobito u polju dijagnostike i radiologije) jer će tada kriterij povrede pravila struke biti neadekvatan. Naime, može se pretpostaviti da će UI sustavi biti programirani da djeluju na temelju pravila struke (u smislu podataka iz udžbenika, znanstvenih i stručnih radova te odgovarajućih smjernica i naputaka strukovnih udruženja) pa tu neće dolaziti do postupanja na "očito nesavjestan način", kako to traži zakonski opis. Nadalje, utvrđivanje uzročne veze bit će puno složenije, a upitno je i tko će biti podoban za vještaka u tim situacijama (čovjek ili UI).[68] Osim navedenoga, problem će predstavljati i trenutačno uređenje ovog djela kao tzv. posebnog kaznenog djela (*delictum proprium*), pri kojem počinitelj mora imati svojstvo zdravstvenog radnika, a sve osobe koje to svojstvo nemaju mogu biti samo poticatelji i pomagatelji.[69] Zato će zasigurno biti potrebno pristupiti odgovarajućoj reformi ovog kaznenog djela.

Područje gospodarskih kaznenih djela, po našem mišljenju, također otvara vrlo složene probleme dokazivanja krivnje. Ranije je opisano kako UI sustavi, koji se već rabe u financijskom poslovanju, mogu utjecati na štetne pojave na tržištu i ostvarivati obilježja prijevare u gospodarskom poslovanju i sličnih kaznenih djela. Pritom je važno da takvi sustavi ponekad mogu do takvih posljedica dovesti neovisno o ljudskom djelovanju, postupajući u cilju stjecanja najveće moguće dobiti. Poznato je da je djelovanje ovakvih autonomnih sustava redovito povezano s određenim financijskim korporacijama koje se takvim sustavima koriste u funkcioniranju. U većini sustava u svijetu, uključujući ovdje i hrvatsko kazneno pravo, gospodarska su kaznena djela koncipirana kao namjerna djela, što znači da ih nije moguće počiniti iz nehaja. Štoviše, u hrvat-

66 Turković K. i dr., *Komentar kaznenog zakona*, Narodne novine, Zagreb, 2013., str. 240.

67 Roksandić Vidlička, S., *Aktualna pitanja pojedinih kaznenih djela protiv zdravlja ljudi,* u: Turković K. i dr. (ur.), *Hrestomatija hrvatskog medicinskog prava*, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2016., str. 825.

68 Tako i Froomkin, Kerr, Pineau, *op. cit.* u bilj. 30, str. 50.

69 Novoselec, *op. cit.* u bilj. 54, str. 312.

skom pravu je uglavnom riječ o djelima kod kojih je u sudskoj praksi prihvaćena isključivo izravna namjera, u smislu znanja i htijenja kaznenog djela, što je ponekad povezano s poteškoćama oko dokazivanja takve namjere i specifičnog cilja djelovanja.[70] Hrvatska sudska praksa primjerice nije prihvatila tumačenje prema kojem se krađa ili prijevara, kao tipična imovinska djela, mogu počiniti i s neizravnom namjerom, pa uglavnom zahtijeva dokaz o postojanju izravne namjere.[71] Već je rečeno da se taj oblik krivnje mora dokazati odgovornoj fizičkoj osobi, na što se onda nadovezuje utvrđenje o postojanju krivnje pravne osobe. Ako se, međutim, u bližoj budućnosti financijsko poslovanje krene dominantno odvijati putem autonomnih algoritama, postat će praktično nemoguće utvrditi odgovornost fizičkih osoba jer one više neće sudjelovati u tom procesu. Zato smo mišljenja da postojeći koncept vezivanja odgovornosti pravnih osoba uz krivnju odgovornih fizičkih osoba više neće biti adekvatan da obuhvati gospodarska kaznena djela, nego će biti potrebno rješenje tražiti u osmišljavanju novih modela autonomne krivnje pravnih osoba. Istodobno će biti potrebno razmotriti uvođenje novih oblika kaznenih djela apstraktnog ugrožavanja, čije će se nepravo sastojati u stavljanju u pravni promet financijskih algoritama koji mogu dovesti do odgovarajućih kaznenih djela protiv gospodarstva i platnog prometa. To su, po našem mišljenju, središnja pitanja kojima će se baviti buduća istraživanja iz polja gospodarskog kriminaliteta.

U području zaštite osobnih podataka KZ/11 propisuje kazneno djelo nedozvoljene uporabe osobnih podataka (čl. 146. KZ/11).[72] Iz dostupne prakse proizlazi da se do sada za to djelo osuđivalo isključivo fizičke osobe[73] (nema dostupnih presuda protiv pravnih osoba) te da su se javljali problemi u vještačenju koji su u pravilu dovodili do oslobađajućih presuda. Naime, vještačenjem nije uvijek bilo moguće pouzdano dokazati vezu između određene manipulacije osobnim podatcima i konkretnog počinitelja, posebice u situacijama u kojima nije nađen uređaj kojim je zlouporaba osobnih podataka učinjena (npr. mobitel ili računalo).[74] Može se pretpostaviti da će takvu povezanost biti još složenije

---

70 Usp. npr. Sokanović, L., *Oblici prijevara u Kaznenom zakonu*, Hrvatski ljetopis za kaznene znanosti i praksu, *vol*. 24, br. 2, 2017., str. 589.

71 Više o tome npr. u Bojanić, I.; Kuharić, Z., *Prijevara u gospodarskom poslovanju*, Hrvatski ljetopis za kazneno pravo i praksu, *vol.* 14, br. 2, 2007., str. 588.

72 Za iscrpnu analizu obilježja ovog kaznenog djela vidi Miletić, L., *Kaznenopravna zaštita osobnih podataka u hrvatskom i mađarskom kaznenom zakonodavstvu* (diplomski rad), Sveučilište u Rijeci, Pravni fakultet, Rijeka, 2019.

73 Vidi npr. Općinski sud u Osijeku, K 428/2021-43; Općinski sud u Osijeku, K 650/2022-13; Općinski sud u Osijeku, Kmp 89/2020-14; Općinski sud u Osijeku, K 19/2023-2.

74 Vidi npr. Općinski sud u Osijeku, K 346/2022-10; Županijski sud u Bjelovaru, Kž

dokazati kada je riječ o sofisticiranim softverima i kada je moguće da počinitelj djeluje iz neke druge zemlje ili čak preko neke pravne osobe registrirane u nekoj od poreznih oaza (tada će se otvoriti i pitanje uspostavljanja jurisdikcije). Rečeno *mutatis mutandis* vrijedi i za kaznena djela protiv računalnih sustava, programa i podataka (Glava XXV. KZ/11), koja su također prilagođena ponajprije ljudima počiniteljima. Osim toga, kod ovih kaznenih djela nabavljanje alata (tu ulaze i UI softveri) za počinjenje u pravilu predstavlja nekažnjivu pripremnu radnju.[75]

Iz provedene analize proizlazi zaključak da je pozitivno hrvatsko kazneno materijalno pravo samo djelomično prilagođeno izazovima koje može otvoriti rastuća uporaba UI-ja u bliskoj budućnosti. Ono će pružiti odgovarajući zakonski okvir u svim slučajevima kada se radi o namjernim kaznenim djelima kod kojih se UI rabi samo kao sredstvo u rukama počinitelja i kada je moguće dokazati povezanost između UI-ja i počinitelja. Tu ipak treba istaknuti da će ponekad u takvim situacijama zasigurno biti potrebna složena vještačenja te je upitno postoje li trenutačno u domaćem sustavu odgovarajući vještački kapaciteti. S druge strane, mišljenja smo da hrvatski okvir pokazuje ozbiljne manjkavosti kod svih nehajnih kaznenih djela (jer će biti izazovno uspostaviti kriterij povrede dužne pažnje uvijek kada je određeni UI mehanizam atestiran i odobren u skladu sa zakonom), zatim kod djela kod kojih se već sada dokazivanje uzročne veze pokazuje kao poteškoća u sudskoj praksi i kod *delicta propria*. Imajući to u vidu, smatramo da će u budućnosti biti potrebno pristupiti opsežnijoj reformi posebnog dijela i prilagoditi ga zahtjevima UI-ja. U nastavku ćemo iznijeti nekoliko ideja kako to učiniti.

3.2. Smjernice za razvoj *de lege ferenda*

S obzirom na ono što je prethodno rečeno, smatramo da bi najbolji pristup budućoj reformi posebnog djela bio razvijati posebna kaznena djela ugrožavanja (*lex specialis*), kod kojih bi naglasak bio na apstraktnom ugrožavanju. U tom smislu, zakonski opisi trebaju biti jasni pa se preporučuje koristiti se izrazima poput "može stvoriti opasnost" ili "radnja koja je podobna da dovede do šte-

163/2023-4.

[75] Treba napomenuti da takav pristup kod djela računalnog kriminaliteta nije neuobičajen ni u poredbenom pravu. Primjerice, ni u njemačkom pravu nabavljanje sredstava za počinjenje ovih kaznenih djela nije kažnjivo. Usp. npr. Seidl, A., *Debit Card Fraud: Strafrechtliche Aspekte des sog. «Skimmings»*, Zeitschrift für Internationale Strafrechtsdogmatik, *vol.* 7, br. 8-9, 2012., str. 417.

te"[76] jer će se tako jasno odrediti da je riječ o apstraktnom ugrožavanju i da nije potrebno dokazivati nastup konkretne opasnosti ni nastup štetne posljedice. Ovo napominjemo stoga što se u dosadašnjoj sudskoj praksi pokazalo da je razlikovanje apstraktnog od konkretnog ugrožavanja i povređivanja nejasno te da su donošene oslobađajuće presude na temelju pogrešnog tumačenja da posljedica nije ostvarena. To se često može primijetiti kod određenih kaznenih djela protiv okoliša, koja su uglavnom koncipirana kao djela apstraktnog ugrožavanja. Kao primjer možemo navesti oslobađajuću presudu u predmetu u kojem se optuženiku stavljalo na teret da je u plinskoj boci u Republiku Hrvatsku unio radi uporabe 13,6 kg tvari freon R 22, iako je bio svjestan da je riječ o tvari koja može štetno djelovati na okoliš. Optužen je za kazneno djelo ugrožavanja ozonskog sloja (čl. 195. st. 1. KZ/11), ali su ga sudovi oslobodili odgovornosti jer je izostala posljedica (prema tumačenju sudova, posljedica se trebala sastojati u oštećenju ozonskog sloja, iako je prema zakonskom opisu za postojanje ovog djela dovoljno samo da je tvar podobna da ošteti ozonski sloj, a ne da ga mora zaista i oštetiti).[77] Smatramo da će se usporedive situacije susretati i kod kaznenih djela vezanih uz UI pa je iz tog razloga potrebno djela apstraktnog ugrožavanja jasno zakonski propisati, a također i provoditi odgovarajuća usavršavanja praktičara radi davanja nedvosmislenih smjernica u tumačenju.

Nadalje, preporučuje se za određene situacije propisati i čisto formalna kaznena djela, kojih se nepravo sastoji u nepoduzimanju određene radnje, a kažnjivost ne ovisi o posljedici (posljedica nije sastavni dio bića). Na taj se način izbjegava složeno dokazivanje uzročne veze. Dakako, kod takvih djela kazneni okvir ne smije biti suviše strog, nego mora odgovarati standardima i zakonskim parametrima kaznenih okvira koji već postoje za formalna kaznena djela.

Naposljetku, potrebno je uvesti korištenje UI-ja u nezakonite svrhe kao posebnu vrstu kvalifikatorne okolnosti kod teških kaznenih djela s posljedicom u biću (tzv. materijalnih kaznenih djela). Alternativno, ako zakonodavac ne propiše takve kvalifikatorne okolnosti, preporučljivo je da ih sudovi vrednuju kao otegotne prigodom odmjeravanja kazne. Takav se pristup može opravdati time što se zlouporabom UI tehnologije ugrožavaju ne samo individualni nego i kolektivni interesi te se negativno utječe na razvoj društva i tehnološki napredak u cjelini, s obzirom na to da se stvara osjećaj nepovjerenja građana prema novim tehnologijama.[78]

---

[76] Usp. Vukušić, I., *"Odustanak" kod posebnih kaznenih djela ugrožavanja okoliša*, Zbornik radova Pravnog fakulteta u Splitu, *vol.* 53, br. 2, 2016., str. 583.

[77] Županijski sud u Varaždinu, Kž-204/2018.

[78] Tako i Miró-Llinares, *op. cit.* u bilj. 10, str. 39.

4. ZAKLJUČAK

Prilagođenost kaznenopravnog sustava uvjetima umjetne inteligencije predstavlja ključni izazov u suvremenom pravosuđu. U ovom radu prikazana su područja u kojima postoji najveći kaznenopravni rizik zlouporabe UI-ja te je tako uspostavljena svojevrsna fenomenologija kriminaliteta UI-ja, što predstavlja prvi ovakav pokušaj u domaćoj literaturi. Na podlozi takve fenomenologije učinjena je analiza odgovarajućih područja posebnog dijela KZ/11 te je zaključeno da postojeće odredbe samo djelomično pružaju pravnu zaštitu te da će u bližoj budućnosti biti potrebno pristupiti temeljitoj reformi posebnog dijela. U tom su smislu dane određene načelne smjernice za budući razvoj. Propisivanje novih kaznenih djela usmjerenih na štetnu uporabu umjetne inteligencije očito se nameće kao imperativ kako bi se suvremeni pravni sustav prilagodio izazovima digitalnog doba.

Uvođenjem novih inkriminacija (ili preoblikovanjem postojećih), pravni sustav može bolje zaštititi građane od različitih oblika prijevare, zlouporabe podataka i kibernetičkih napada koji se koriste UI-jem te tako osigurati pravnu sigurnost i jasnoću u odnosu na postupke koji se smatraju neetičnima ili štetnima za društvo. Time će se ujedno promovirati odgovorno ponašanje u razvoju i upotrebi UI-ja, što potiče inovacije i etičku uporabu tehnologije, ali i olakšati rad pravosudnim tijelima u istraživanju i procesuiranju ove vrste kaznenih predmeta.

I u pogledu različitih suvremenih alata zasnovanih na tehnologiji za prepoznavanje lica, prediktivnim policijskim alatima i alatima za procjenu vjerojatnosti da će okrivljenik na slobodi ostvariti neki kaznenopravno relevantan rizik potrebno je naglasiti da u njihovom postanku i primjeni odlučujuću ulogu ima čovjek. Zbog toga čovjek mora biti taj koji donosi konačnu odluku, odnosno koji kontrolira izlazni podatak koji je generirao alat zasnovan na umjetnoj inteligenciji, pa bi već i samo propuštanje takve radnje moglo predstavljati kazneno djelo.

LITERATURA

Antonialli, F.; Martinesco, A.; Mira-Bonnardel, S., *Artificial intelligence as a determinant for reshaping the automotive industry and urban mobility services*, International Journal of Automotive Technology and Managment, *vol.* 22, br. 3, 2022., str. 324 – 351.

Basu, K.; Sinha, R.; Ong, A.; Basu, T., *Artificial Intelligence: How is It Changing Medical Sciences and Its Future?*, Indian Journal of Dermatology, *vol*. 65, br. 5, 2020., str. 365 – 370.

Bikeev, I.; Kabanov, P.; Begishev, I.; Khisamova, Z., *Criminological Risks and Legal Aspects of Artificial Intelligence Implementation*, AIIPCC '19: Proceedings of the International Conference on Artificial Intelligence, Information Processing and Cloud Computing, December 2019, Article No. 20, str. 1 – 7, dostupno na: https://dl.acm.org/doi/pdf/10.1145/3371425.3371476 (17. 10. 2023.).

Bo, M., *Autonomous Weapons and the Responsibility Gap in light of the Mens Rea of the War Crime of Attacking Civilians in the ICC Statute*, Journal of International Criminal Justice, *vol.* 19, br. 2, 2021., str. 275 – 299.

Bojanić, I.; Kuharić, Z., *Prijevara u gospodarskom poslovanju*, Hrvatski ljetopis za kazneno pravo i praksu, *vol.* 14, br. 2, 2007., str. 575 – 589.

Borch, C., *High-frequency trading, algorithmic finance and the Flash Crash: reflections on eventalization*, Economy and Society, *vol*. 45, br. 3-4, 2016., str. 350 – 378.

Borch, C., *Machine learning, knowledge risk, and principal-agent problems in automated trading*, Technology in Society, *vol.* 68, 2022., str. 713 – 725.

Chan, B., *Applying a Common Enterprise Theory of Liability to Clinical AI Systems*, American Journal of Law & Medicine, *vol.* 47, br. 4, 2021., str. 351 – 385.

Derenčinović, D.; Novosel, D., *Zakon o odgovornosti pravnih osoba za kaznena djela – prolazne dječje bolesti ili (ne)rješiva kvadratura kruga*, Hrvatski ljetopis za kazneno pravo i praksu, *vol.* 19, br. 2, 2012., str. 585 – 613.

Douma, F.; Palodichuk, S. A., *Criminal Liability Issues Created by Autonomous Vehicles*, Santa Clara Law Review, *vol.* 52, br. 4, 2012., str. 1157 – 1169.

Froomkin, M. A.; Kerr, I. R.; Pineau, J., *When AIs Outperform Doctors: Confronting the Challenges of a Tort-Induced Over-Reliance on Machine Learning*, Arizona Law Review, *vol.* 61, br. 1, 2019., str. 33 – 99.

Gless, S.; Silverman, E.; Weigend, T., *If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability*, New Criminal Law Review, *vol.* 19, br. 3, 2016., str. 412 – 436.

Gleβ, S.; Weigend, T., *Intelligente Agenten und das Strafrecht,* Zeitschrift für die gesamte Strafrechtswissenschaft, *vol.* 126, br. 3, 2014., str. 561 – 591.

Ishii, K., *Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects*, AI & Society, *vol.* 34, br. 3, 2019., str. 509 – 533.

King, T. C.; Aggarwal, N.; Taddeo, M.; Floridi, L., *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, Science and Engineering Ethics, *vol.* 26, br. 1, 2020., str. 89 – 120.

Kinoshita, T.; Komatsu, M., *Artificial Intelligence in Surgery and Its Potential for Gastric Cancer*, Journal of Gastric Cancer, *vol.* 23, br. 3, 2023., str. 400 – 409.

Kirilenko, A.; Kyle, A. S.; Samadi, M.; Tuzun, T., *The Flash Crash: High Frequency Trading in an Electronic Market*, The Journal of Finance, *vol.* 72, br. 3, 2017., str. 967 – 998.

Korošec, D., *Criminal Law Dilemmas in Withholding and Withdrawal of Intensive Care*, Medicine, Law & Society, *vol.* 9, br. 1, 2016., str. 21 – 39.

Kotsoglou, K. N.; Oswald M., *The long arm of the algorithm? Automated Facial Recognition as evidence and trigger for police intervention*, Forensic Science International: Synergy, *vol.* 2, 2020., str. 86 – 89.

Lagioia, F.; Sartor, G., *AI Systems Under Criminal Law: a Legal Analysis and a Regulatory Perspective*, Philosophy & Technology, *vol.* 33, br. 3, 2020., str. 433 – 465.

Ludvigsen, K. R.; Nagaraja, S., *Dissecting liabilities in adversarial surgical robot failures: A national (Danish) and EU law perspective*, Computer Law & Security Review, *vol.* 44, 2022., str. 1 – 20.

Mantelero, A., *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, Computer Law & Security Review, *vol.* 34, br. 4, 2018., str. 754 – 772.

Martinez, J. S., *Understanding Mens Rea in Command Responsibility*, Journal of International Criminal Justice, *vol.* 5, br. 3, 2007., str. 638 – 664.

Miletić, L., *Kaznenopravna zaštita osobnih podataka u hrvatskom i mađarskom kaznenom zakonodavstvu* (diplomski rad), Sveučilište u Rijeci, Pravni fakultet, 2019.

Miró-Llinares, F., *Association International de Droit* Pénal – International *Association of Penal Law XXI International Congres of Penal Law: "Artificial Intelligence and Criminal Justice", International Colloquium of Section II (Criminal Law-specific offences in the Criminal code)*, 2023.

Mrčela, M.; Vuletić, I., *Kazneno pravo pred izazovima robotike: tko je odgovoran za prometnu nesreću koju je prouzročilo neovisno vozilo?*, Zbornik Pravnog fakulteta u Zagrebu, *vol*. 68, br. 3-4, 2018., str. 465 – -491.

Noorbakhsh-Sabet, N.; Zand, R.; Zhang, Y.; Abedi, V., *Artificial Intelligence Transforms the Future of Health Care*, The American Journal of Medicine, *vol.* 132, br. 7, 2019., str. 795 – 801.

Novokmet, A.; Tomičić, Z.; Vidaković, I., *Facial Recognition Technology in EU Criminal Justice - Human Rights Implications and Challenges*, u: Duić, D.; Petrašević, T. (ur.), *EU and Comparative Law Issues and Challenges Series (ECLIC), Digitalization and Green Transformation of the EU*, *vol. 7*, Faculty of Law, Josip Juraj Strossmayer University of Osijek, Osijek, 2023., str. 550 – 561, https://doi.org/10.25234/eclic/27461.

Novokmet, A.; Tomičić, Z.; Vinković, Z., *Pretrial risk assessment instruments in the US criminal justice system—what lessons can be learned for the European Union*, International Journal of Law and Information Technology, *vol.* 30, br. 1, 2022., str. 1 – 22.

Novoselec, P., *Opći dio kaznenog prava*, Pravni fakultet Osijek, Osijek, 2016.

Postma, J., *Drones over Nagorno-Karabakh: A glimpse at the future of war?*, Atlantisch Perspectief , *vol.* 45, br. 2, 2021., str. 15 – 20.

Rodrigues, R., *Legal and human rights issues of AI: Gaps, challenges and vulnerabilities,* Journal of Responsible Technology, *vol.* 4, 2020., str. 1 – 12.

Roksandić Vidlička, S., *Aktualna pitanja pojedinih kaznenih djela protiv zdravlja ljudi*, u: Turković K. i dr. (ur.), *Hrestomatija medicinskog prava*, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2016.

Roksandić Vidlička, S.; Elīna Liepiņa, L.; Ostapchuk, S., *Bioethical and Legal Challenges of Artificial Intelligence and Human Dignity*, u: Jovanović, M., Virady, T., (ur.), *Human rights in 21st century*, Eleven International Publishing, Nizozemska, 2020., str. 269 – 288.

Roksandić, S.; Protrka, N.; Engelhart, M., *Trustworthy Artificial Intelligence and its use by Law Enforcement Authorities: where do we stand?*, 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2022., str. 1225 – 1232, doi: 10.23919/MIPRO55190.2022.9803606.

Seidl, A., *Debit Card Fraud: Strafrechtliche Aspekte des sog. «Skimmings»*, Zeitschrift für Internationale Strafrechtsdogmatik, *vol*. 7, br. 8-9, 2012., str. 415 – 424.

Sokanović, L., *Oblici prijevara u Kaznenom zakonu*, Hrvatski ljetopis za kaznene znanosti i praksu, *vol.* 24, br. 2, 2017., str. 583 – 615.

Turković, K. i dr., *Komentar kaznenog zakona*, Narodne novine, Zagreb, 2013.

Vukušić, I., *"Odustanak" kod posebnih kaznenih djela ugrožavanja okoliša*, Zbornik radova Pravnog fakulteta u Splitu, *vol.* 53, br. 2, 2016., str. 581 – 600.

Vuletić, I., *Rethinking superior liability in terms of emerging AI weapons*, u: Duić, D.; Petrašević T. (ur.), *EU and Comparative Law Issues and Challenges Series (ECLIC), Special Issue – Law in the Age of Modern Technologies*, *vol.* 7, Faculty of Law, Josip Juraj Strossmayer University of Osijek, Osijek, 2023., str. 163 – 180.

West, D. M.; Allen, J. R., *How artificial intelligence is transforming the world*, dostupno na: https://www.brookings.edu/articles/how-artificial-intelligence-is-transforming-the-world/ (11. srpnja 2023.).

Yeoh, P., *Artificial intelligence: accelerator or panacea for financial crime?,* Journal of Financial Crime, *vol.* 26, br. 2, 2019., str. 634 – 646.

Summary

Igor Vuletić*
Ante Novokmet**
Zvonimir Tomičić***

THE CHALLENGES OF THE SPECIAL PART OF CRIMINAL LAW FACING THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE WITH A PARTICULAR FOCUS ON CROATIAN CRIMINAL LAW

Artificial intelligence is making an increasingly profound impact on various aspects of everyday life. The advantages of artificial intelligence in terms of enhancing efficiency and cost-effectiveness in many tasks make it an indispensable factor in societal development. Although this development is still more pronounced in the United States and certain more developed Asian countries, it is undeniable that this trend will soon enough dominate Europe as well. Given that the application of artificial intelligence also poses various types of risks, some of which directly threaten fundamental legal interests such as life, body, or property, the question arises of how to achieve an appropriate level of criminal legal protection in this area. Traditional criminal law is based on principles adapted to humans as perpetrators of criminal acts, so new trends necessitate a re-evaluation of the fundamental tenets of criminal law. This paper examines the aforementioned issues from the perspective of the special part of criminal law. It first identifies the areas of primary interest for criminal legal protection when it comes to AI-related criminal activities. It then analyzes and assesses Croatian legislation to determine whether the existing provisions of the special part of the Criminal Code in the observed areas are sufficient to ensure an adequate criminal legal response. It is concluded that this is only partially the case, and there are legal gaps in this regard. The authors also propose certain de lege ferenda

* Igor Vuletić, Ph. D., Professor, Faculty of Law, Josip Juraj Strossmayer University of Osijek, S. Radića 13, 31000 Osijek; ivuletic@pravos.hr;
ORCID ID: orcid.org/0000-0001-5472-5478

** Ante Novokmet, Ph. D., Associate Professor, Faculty of Law, Josip Juraj Strossmayer University of Osijek, S. Radića 13, 31000 Osijek; ante.novokmet@pravos.hr;
ORCID ID: orcid.org/0000-0001-8833-9751

*** Zvonimir Tomičić, Ph. D., Associate Professor, Faculty of Law, Josip Juraj Strossmayer University of Osijek, S. Radića 13, 31000 Osijek; tomicic.zvonimir@pravos.hr;
ORCID ID: orcid.org/0000-0001-6159-6475

changes where they appear purposeful and necessary.

Key words: artificial intelligence; special part; criminality; traffic; weapons; criminal liability