

DRUŽBENI VIDIKI VARNE DIGITALNE PREOBRAZBE V LOKALNI SKUPNOSTI: MED IZVRŠEVANJEM ZAKONODAJE IN ZAGOTAVLJANJEM VARNOSTI

IGOR BERNIK

Univerza v Mariboru, Fakulteta za varnostne vede, Ljubljana, Slovenija
igor.bernik@um.si

Digitalna preobrazba lokalnih skupnosti predstavlja enega ključnih procesov razvoja, pri čemer je vprašanje varnosti pogosto razumljeno predvsem skozi prizmo tehničnih rešitev in formalnega izvajanja zakonodaje. Prispevek zagovarja širši družbeni pogled, po katerem varnost ni zgolj posledica nadzora in sankcioniranja, temveč rezultat zaupanja, legitimnosti in aktivnega vključevanja prebivalcev v okolje. Na podlagi pregleda literature s področja umetne inteligence (UI), digitalne preobrazbe, varnostnih študij in javne uprave razvijamo konceptualni okvir odgovorne uporabe UI v lokalnih skupnostih. Posebej izpostavljamo razliko med formalnim izvajanjem zakonodaje in dejanskim zagotavljanjem varnosti. Prikazani so primeri, ki kažejo, da pretirano rigidno izvrševanje pravil ne vodi nujno k večji varnosti, temveč zmanjšuje zaupanje prebivalcev v institucije. UI omogoča sorazmeren, kontekstualen in preventiven pristop, ki temelji na opozarjanju, izobraževanju in podpori posameznikom. Prispevek poudarja potrebo po razvoju zaupanja vrednih sistemov UI, ki ob spoštovanju zakonodaje prispevajo k večji varnosti, družbeni legitimnosti in kakovosti življenja v lokalnih skupnostih.

DOI

[https://doi.org/
10.18690/um.fvv.4.2026.10](https://doi.org/10.18690/um.fvv.4.2026.10)

ISBN

978-961-299-170-8

Ključne besede:

digitalna preobrazba,
umetna inteligenca,
lokalne skupnosti,
varnost,
zaupanje,
sodobna družba



Univerzitetna založba
Univerze v Mariboru

DOI
[https://doi.org/
10.18690/um.fvv.4.2026.10](https://doi.org/10.18690/um.fvv.4.2026.10)

ISBN
978-961-299-170-8

Keywords:
digital transformation,
artificial intelligence,
local communities,
security,
trust,
modern society

SOCIAL ASPECTS OF SECURE DIGITAL TRANSFORMATION IN THE LOCAL COMMUNITY: BETWEEN LAW ENFORCEMENT AND ENSURING SECURITY

IGOR BERNIK

University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia
igor.bernik@um.si

The digital transformation of local communities is a key development process in which security is often understood mainly through technical solutions and formal law enforcement. This paper argues for a broader social perspective, viewing security not only as the result of control and sanctions but also as a product of trust, legitimacy, and residents' active involvement. Based on a literature review of (trustworthy) artificial intelligence (AI), digital transformation, security studies, and public administration, the paper develops a conceptual framework for the responsible use of AI in local communities. It highlights the distinction between enforcing legislation and actually ensuring security. Selected examples show that excessively rigid rule enforcement may reduce trust in institutions without necessarily improving safety. AI can support a proportionate, contextual, and preventive approach based on warnings, education, and individual support, while respecting the law and strengthening social legitimacy and quality of life.



University of Maribor Press

1 Uvod

Digitalna preobrazba predstavlja enega najpomembnejših razvojnih procesov sodobne družbe. V zadnjem desetletju so lokalne skupnosti postale pomembni akterji uvajanja digitalnih rešitev, saj neposredno vplivajo na kakovost življenja prebivalcev, dostopnost storitev ter občutek varnosti v vsakdanjem življenju. Ob tem se vse pogostejše pojavlja vprašanje, kako zagotoviti, da digitalizacija ne vodi zgolj v večjo avtomatizacijo postopkov, temveč tudi v izboljšanje družbenega okolja in večjo legitimnost javnih institucij. Koncept (sodobne) družbe 5.0, ki izvira iz Japonske, poudarja, da mora biti tehnološki razvoj usmerjen v človeka in njegove potrebe, ne pa zgolj v povečevanje učinkovitosti organizacij (Cabinet Office, 2023). Podobno tudi Evropska komisija pri razvoju regulative umetne inteligence (UI) poudarja načela človekovega dostojanstva, preglednosti, odgovornosti in sorazmernosti (»Uredba (EU) 2024/1689 Evropskega parlamenta in sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci)«, 2024). Varnost je tradicionalno razumljena kot stanje, ki ga zagotavljamo z nadzorom in izvrševanjem pravil. Vendar sodobne varnostne študije opozarjajo, da občutek varnosti ni odvisen zgolj od formalne skladnosti z zakonodajo, temveč predvsem od zaupanja v institucije, zaznane pravičnosti ukrepov in legitimnosti njihovega izvajanja (Tyler, 2021). Posledično se postavlja vprašanje, ali lahko UI prispeva k bolj uravnoteženemu in družbeno sprejemljivemu zagotavljanju varnosti.

Prispevek izhaja iz teze, da namen digitalne preobrazbe ni strožje izvajanje zakonodaje, temveč ustvarjanje varnejšega, pravičnejšega in bolj zaupanja vrednega življenjskega okolja za prebivalce lokalnih skupnosti. Namen prispevka je razviti okvir uporabe UI pri zagotavljanju varnosti v lokalnih skupnostih, ki presega tradicionalno razumevanje izvrševanja zakonodaje in se osredotoča na krepitev zaupanja ter legitimnosti varnostnih institucij. Prispevek temelji na kritičnem pregledu sodobne literature s področja UI, digitalne preobrazbe, legitimnosti institucij in varnostnih študij.

2 Digitalna preobrazba, umetna inteligenca in zagotavljanje varnosti v konceptu sodobne družbe

Družba 5.0 poudarja reševanje družbenih problemov s pomočjo naprednih digitalnih tehnologij (Harayama, 2017). V tem okviru postane varnost večdimenzionalen pojem, ki vključuje: fizično varnost, kibernetsko varnost, organizacijsko odpornost, družbeno kohezijo in zaupanje prebivalcev. Avtorji raziskav ugotavljajo, da digitalna preobrazba pogosto naleti na odpor uporabnikov prav zaradi strahu pred pretiranim nadzorom in izgubo zasebnosti (npr. Mergel idr., 2023). Če prebivalci digitalne sisteme zaznavajo kot instrument represije, se zmanjšuje njihova pripravljenost za sodelovanje in uporaba tehnologije ne doseže pričakovanih učinkov.

Lokalne skupnosti so pri tem posebej občutljivo okolje, saj prebivalci neposredno zaznavajo posledice digitalnih rešitev. V nasprotju z državno upravo so občinske storitve del vsakdanjega življenja, zato ima način izvajanja digitalnih politik neposreden vpliv na odnos prebivalcev do institucij. Prav zato mora biti digitalna preobrazba usmerjena v ustvarjanje dodane vrednosti za skupnost, pri čemer postane UI sredstvo za izboljšanje kakovosti življenja in ne zgolj orodje za učinkovitejše sankcioniranje.

Razvoj UI odpira nove možnosti za upravljanje varnosti v lokalnih skupnostih. Sistemi UI lahko analizirajo velike količine podatkov, prepoznavajo vzorce tveganj ter podpirajo odločanje v realnem času. Vendar pa se v zadnjih letih raziskovalci vse bolj oddaljujejo od vprašanja, kaj UI zmore, in se usmerjajo k vprašanju, kako naj se uporablja (Floridi idr., 2023). Koncept zaupanja vredne UI (angl. *Trustworthy AI*) temelji na treh osnovnih dimenzijah: zakonitosti, etičnosti in tehnični robustnosti (»Uredba (EU) 2024/1689 Evropskega parlamenta in sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci)«, 2024). To pomeni, da uspešnost sistema ni odvisna zgolj od njegove natančnosti, temveč tudi od njegove sposobnosti ustvarjanja zaupanja med uporabniki. Sodobni modeli odgovorne UI (angl. *Responsible AI*) poudarjajo povezavo med zakonitostjo, preglednostjo, odgovornostjo in zaupanjem uporabnikov (Díaz-Rodríguez idr., 2023; Herrera-Poyatos idr., 2025). Sistematični

pregledi uporabe UI v javnem upravljanju kažejo, da uspešnost implementacije ni odvisna zgolj od tehnoloških lastnosti, temveč predvsem od institucionalnega okolja in zaupanja uporabnikov (Arab idr., 2025).

Pri zagotavljanju varnosti se zato odpira pomembna dilema. Ali naj UI deluje predvsem kot avtomatiziran mehanizem za odkrivanje in sankcioniranje prekrškov ali pa kot podporni sistem za preprečevanje tveganj? Večina sodobnih raziskav in avtor prispevka podpirajo preventivni pristop. Namen tehnologije namreč naj ne bi bil povečanje števila izrečenih sankcij, temveč zmanjšanje verjetnosti nastanka škodljivih ali neželenih dogodkov (United Nations Development Programme [UNDP], n. d.).

3 Izvajanje zakonodaje ni enako zagotavljanju varnosti

Kot vemo, sta varnost in zakonitost med seboj povezana, vendar ne identična pojma. Zakonodaja predstavlja formalni okvir za urejanje družbenih odnosov, medtem ko je varnost dejansko stanje zmanjšanega tveganja. Tako npr. Tyler (2021) ugotavlja, da ljudje spoštujejo pravila predvsem takrat, ko postopke zaznavajo kot pravične. Pretirano represivni sistemi lahko sicer povečajo število zaznanih kršitev, vendar dolgoročno zmanjšujejo legitimnost institucij. Teorija postopkovne pravičnosti pojasnjuje, da ljudje pravil ne spoštujejo zgolj zaradi strahu pred sankcijami, temveč predvsem zato, ker institucije zaznavajo kot legitimne in pravične. Kadar postopki temeljijo na spoštovanju, transparentnosti in sorazmernosti, se poveča pripravljenost posameznikov za sodelovanje z institucijami in prostovoljno spoštovanje pravil (Sunshine in Tyler, 2003; Tyler in Jackson, 2014). Bottoms in Tankebe (2012) pa legitimnost razumeta kot dinamičen odnos med institucijami in prebivalci, ki se vzpostavlja skozi dialog, pravičnost in družbeno sprejemljivost delovanja institucij. To pomeni, da legitimnost institucij predstavlja pomemben vir družbenega kapitala, ki lahko dolgoročno prispeva k višji ravni varnosti.

Zgornja izhodišča so posebej pomembna v digitalnem okolju, kjer UI omogoča skoraj popoln nadzor nad vedenjem posameznikov. Vprašanje ni, ali je mogoče zaznati vsako kršitev, temveč ali je takšen pristop družbeno smiseln. Podajmo nekaj primerov:

- Parkirni režimi: v številnih mestih je parkiranje časovno omejeno in vezano na označitev časa prihoda. Če voznik pozabi nastaviti parkirno uro, formalno stori prekršek. Varnostni cilj ukrepa pa ni preverjanje prisotnosti parkirne ure, temveč zagotavljanje kroženja parkirnih mest in njihove dostopnosti. UI lahko ta cilj doseže učinkoviteje. Sistem za samodejno prepoznavo registrskih tablic lahko beleži dejanski čas prihoda vozila in voznika opozori pred iztekom dovoljenega časa. Takšen pristop doseže isti cilj, vendar z bistveno manj konfliktnimi posledicami za prebivalce.
- Varnostne razdalje med vozili: zakonsko določena dvosekundna razdalja temelji na predpostavki človeškega reakcijskega časa. Sodobni sistemi ADAS (angl. *Advanced Driver Assistance Systems*) omogočajo odzivne čase, ki so bistveno krajši od človeških sposobnosti (SAE International, n. d.). Posledično se pojavlja vprašanje, ali enaka pravila za vsa vozila še vedno predstavljajo najboljši približek dejanski varnosti. UI omogoča ocenjevanje dejanske stopnje tveganja in s tem prehod od formalnega preverjanja pravil k ocenjevanju konkretne nevarnosti.
- Merjenja hitrosti v prometu: podobno kot za varnostno razdaljo, velja za nadzor hitrosti. V praksi so pogosto sankcionirane minimalne prekoračitve hitrosti, čeprav objektivna stopnja tveganja ostaja zanemarljiva. Nasprotno pa je lahko vožnja z dovoljeno hitrostjo npr. ob dežju, snegu ali v megli bistveno nevarnejša od nekoliko hitrejša vožnje v idealnih razmerah. UI omogoča vključevanje kontekstualnih podatkov, kot so vremenske razmere, gostota prometa, preglednost ceste in prisotnost ranljivih skupin. Takšen pristop bolje odraža dejansko stopnjo tveganja kot zgolj absolutna hitrost vozila.
- Hrup v urbanem okolju: pametni senzori lahko zaznajo čezmeren hrup. Namesto takojšnjega kaznovanja bi sistem lahko najprej opozoril povzročitelja in omogočil prostovoljno odpravo težave.
- Nepravilno odlaganje odpadkov: klasičen pristop temelji na kaznovanju. Sistem UI pa lahko prepozna vzorce ravnanja in prebivalcem ponuja informacije ter priporočila za pravilno ravnanje.
- Gibanje pešcev in mikromobilnost: npr. električni skiroji predstavljajo novo varnostno tveganje. Namesto množičnega kaznovanja bi lahko sistemi UI uporabnike opozarjali na nevarne lokacije ter prilagajali prometno infrastrukturo dejanskim vzorcem uporabe.

Iz primerov vidimo, da ključno vprašanje prihodnosti ni, koliko podatkov lahko zberemo, temveč kako jih uporabimo za izboljšanje življenja ljudi in posledično ohranjanje oziroma izboljševanje varnosti. Raziskave kažejo, da prebivalci podpirajo uporabo UI predvsem v primerih, ko zaznajo jasno družbeno korist in kadar sistemi delujejo transparentno (Schmager idr., 2024). Če digitalizacija postane sinonim za večji nadzor, se zmanjšuje družbena legitimnost institucij. Če pa prebivalci zaznajo, da tehnologija pomaga reševati probleme, izboljšuje storitve in zmanjšuje tveganja, se krepi zaupanje. Prav zaupanje predstavlja osrednji element varne digitalne preobrazbe!

4 Razprava in zaključki

Tradicionalni modeli regulacije temeljijo na predpostavki, da več nadzora pomeni več varnosti. Digitalne tehnologije omogočajo skoraj popoln nadzor nad vsakodnevnim vedenjem posameznikov. Paradoksalno pa raziskave kažejo, da pretiran nadzor pogosto zmanjšuje zaupanje v institucije, kar dolgoročno zmanjšuje njihovo učinkovitost (Lahusen idr., 2024). Takšne ugotovitve so skladne tudi s teorijo postopkovne pravičnosti, ki poudarja, da legitimnost institucij pomembneje vpliva na spoštovanje pravil kot sama verjetnost sankcioniranja (Sunshine in Tyler, 2003; Tyler in Jackson, 2014). Če prebivalci institucije zaznavajo kot pravične, sorazmerne in usmerjene v skupno dobro, so pripravljeni prostovoljno sodelovati pri zagotavljanju varnosti. Posledično postane zaupanje ne le družbena vrednota, temveč tudi pomemben dejavnik učinkovitosti varnostnih sistemov. Zato mora biti UI razumljena kot orodje za podporo človeku in ne kot mehanizem avtomatizirane represije. V tem smislu se koncept varne digitalne preobrazbe približuje ideji »digitalne humanizacije varnosti«, kjer tehnologija pomaga ljudem sprejemati boljše odločitve, ne pa zgolj kaznovati napačnih.

Prispevek pokaže, da izvajanje zakonodaje in zagotavljanje varnosti nista nujno identična cilja. Čeprav zakonodaja ostaja temelj delovanja javnih institucij, lahko pretirano stroga interpretacija pravil vodi v zmanjšanje zaupanja prebivalcev ter posledično oslabi dolgoročno učinkovitost varnostnih politik. UI omogoča razvoj nove generacije varnostnih pristopov, ki temeljijo na sorazmernosti, kontekstualnem razumevanju tveganj in preventivnem delovanju. Takšni sistemi lahko hkrati izboljšujejo varnost, povečujejo legitimnost institucij ter prispevajo k bolj vključujoči in človeku prijazni digitalni družbi.

4.1 Zaključna refleksija: od države kaznovanja k družbi zaupanja

Digitalna preobrazba lokalnih skupnosti odpira pomembno vprašanje, ki presega tehnologijo, zakonodajo in celo UI: kakšno družbo pravzaprav želimo graditi? Družbo, v kateri je vsak odklon od predpisa samodejno zaznan, evidentiran in sankcioniran, ali družbo, v kateri tehnologija pomaga ljudem razumeti tveganja, sprejemati odgovorne odločitve in prispevati k skupni varnosti? V zadnjih desetletjih so številne varnostne institucije postopoma razvile kulturo, v kateri se uspešnost prepogosto meri s številom zaznanih prekrškov, izdanih glob in izvedenih postopkov. Takšen pristop ustvarja vtis učinkovitosti, vendar ne odgovarja na bistveno vprašanje: ali smo zaradi tega dejansko bolj varni? Kaznovanje voznika zaradi nekaj kilometrov na uro višje hitrosti na prazni in pregledni cesti, sankcioniranje voznika, ki ni nastavil parkirne ure, čeprav parkirnega režima ni zlorabil, ali pregon ravnanj, ki formalno odstopajo od predpisov, vendar objektivno ne povečujejo tveganja, večinoma ne prispevajo k večji varnosti. Prispevajo pa k nečemu drugemu – k občutku, da je namen sistema predvsem iskanje kršiteljev in pobiranje glob. Prav tu UI ponuja zgodovinsko priložnost za spremembo paradigme. Če jo bomo uporabljali zgolj za učinkovitejše odkrivanje in kaznovanje ljudi, bomo ustvarili digitalno družbo nadzora. Če pa jo bomo uporabili za razumevanje okoliščin, prepoznavanje dejanskih tveganj, zgodnje opozarjanje, preventivno delovanje in podporo odgovornemu vedenju, lahko postane eno najmočnejših orodij za krepitev varnosti in zaupanja v zgodovini javnega upravljanja.

To je pomemben izziv tudi za policijo, občinska redarstva in druge institucije, ki skrbijo za varnost. Čas je namreč za premislek institucij o lastni vlogi v digitalni družbi. Prebivalci jih ne bi smeli zaznavati kot organe, katerih primarni namen je iskanje formalnih napak in izrekanje sankcij. Takšna percepcija ustvarja distanco, odpor in nezaupanje. Varnostne institucije morajo ponovno postati tisto, kar bi morale biti od samega začetka – zaupanja vredni partnerji skupnosti, na katere se ljudje obračajo, ko potrebujejo pomoč, zaščito ali podporo. Največji uspeh policista ali redarja ne bi smel biti izrečena globa, temveč preprečena nesreča. Največji uspeh varnostnega sistema ne bi smel biti število odkritih kršitev, temveč zmanjšanje tveganj in povečanje občutka varnosti med prebivalci. In največji uspeh UI ne bo njena sposobnost, da zazna vsako napako posameznika, temveč njena sposobnost, da pomaga ustvarjati okolje, v katerem do teh napak prihaja redkeje, če pa že, so ustrezno varnostno (pre)tehtane.

Družbe prihodnosti ne bodo razdeljene glede na stopnjo digitalizacije, temveč glede na način uporabe tehnologije. Nekatere družbe bodo gradile digitalne sisteme za nadzor, druge digitalne sisteme za podporo ljudem. Ene bodo povečevale število sankcij, druge stopnjo zaupanja. Ene bodo imele državljane, ki se institucij bojijo, druge državljane, ki jim zaupajo. In prav v tem je bistvo varne digitalne preobrazbe! Ne gre za vprašanje, koliko kršitev lahko odkrijemo. Gre za vprašanje, koliko varnosti, zaupanja in družbene povezanosti lahko ustvarimo. Najvarnejše družbe niso tiste, kjer se ljudje bojijo kazni, temveč tiste, kjer ljudje razumejo smisel pravil, zaupajo institucijam in jih spoštujejo tudi takrat, ko jih nihče ne nadzoruje.

Če bo UI pomagala premakniti varnostne institucije od vloge »inkasanta« k vlogi zaupanja vrednega varuha skupnosti, potem ne bo predstavljala le tehnološkega napredka. Predstavljala bo pomemben civilizacijski korak k bolj humani, pravični in resnično varni družbi. To je cilj, ki bi moral biti pomembnejši od vsakega algoritma, vsake globe in vsake statistike uspešnosti!.

Viri in literatura

- Aarab, A., El Marzouki, A., Boubker, O. in El Moutaqi, B. (2025). Integrating AI in public governance: A systematic review. *Digital*, 5(4), 59. doi:10.3390/digital5040059
- Bottoms, A. in Tankebe, J. (2012). Beyond procedural justice: A dialogic approach to legitimacy in criminal justice. *Journal of Criminal Law and Criminology*, 102(1), 119–170.
- Cabinet Office. (2023). *Society 5.0*. https://www8.cao.go.jp/cstp/english/society5_0/
- Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E. in Herrera, F. (2023). Connecting the dots in trustworthy artificial intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *arXiv*. doi:10.48550/arXiv.2305.02231
- Floridi, L., Cowls, J., King, T. C. in Taddeo, M. (2020). How to design AI for social good: Seven essential factors. *Science and Engineering Ethics*, 26, 1771–1796. doi:10.1007/s11948-020-00213-5
- Harayama, Y. (2017). *Society 5.0: Aiming for a new human-centred society: Japan's science and technology policies for addressing global social challenges*. *Hitachi Review*, 66(6), 556–559. https://www.hitachihyoron.com/rev/archive/2017/r2017_06/pdf/p08-13_TRENDS.pdf
- Herrera-Poyatos, A., Del Ser, J., López de Prado, M., Wang, F. Y., Herrera-Viedma, E. in Herrera, F. (2025). Responsible artificial intelligence systems: A roadmap to society's trust through trustworthy AI, auditability, accountability, and governance. *arXiv*. doi:10.48550/arXiv.2503.04739
- Lahusen, C., Maggetti, M. in Slavkovik, M. (2024). Trust, trustworthiness and AI governance. *Scientific Reports*, 14(1), Article 21456. doi:10.1038/s41598-024-71761-0
- Mergel, I., Edelman, N. in Haug, N. (2023). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, 40(1), 101847. doi:10.1016/j.giq.2022.101847
- SAE International. (n. d.). *Advanced driver assistance systems (ADAS) and vehicle automation technologies*. <https://www.sae.org>

- Schmager, S., Gröder, C., Parmiggiani, E., Pappas, I. O. in Vassilakopoulou, P. (2024). Exploring citizens' stances on AI in public services: A social contract perspective. *Data & Policy*, 6, e13. doi:10.1017/dap.2024.13
- Sunshine, J. in Tyler, T. R. (2003). The role of procedural justice and legitimacy in shaping public support for policing. *Law & Society Review*, 37(3), 513–548. doi:10.1111/1540-5893.3703002
- Tyler, T. R. (2021). *Why people obey the law*. Princeton University Press.
- Tyler, T. R. in Jackson, J. (2014). Popular legitimacy and the exercise of legal authority: Motivating compliance, cooperation, and engagement. *Psychology, Public Policy, and Law*, 20(1), 78–95. doi:10.1037/a0034514
- United Nations Development Programme (UNDP). (n. d.). *AI trust and safety re-imagination programme: Building frameworks of the future*. UNDP. <https://www.undp.org/digital/ai-trust-and-safety-re-imagination-programme-building-frameworks-future>
- Uredba (EU) 2024/1689 Evropskega parlamenta in sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci). (2024). *Uradni list Evropske unije*, (2024/1689). https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=OJ:L_202401689