

JOURNAL OF DIGITAL LAW AND INNOVATION (JDLI)

LAW • TECHNOLOGY • INNOVATION • JUSTICE

 OPEN
ACCESS

ISSN
3093-9364



OUR FIELDS

- Digital law
- Cybersecurity law
- Artificial intelligence and robotics law
- Intellectual property law
- LegalTech and legal innovations
- E-government and digital public services
- Legal aspects of AgroTech and GreenTech
- Smart city and digital governance



OUR INDEXING

 Google Scholar

 Zenodo

 DOI

 OpenAIRE

 Open Access



AI



UNAUTHORIZED
ACCESS

SYSTEM
BREACH



CYBER ATTACK



DIGITAL LAW



<https://unireview.uz/index.php/jdli>



Published by
UniLex Global



VOLUME 2 | ISSUE 1



AUGUST 2026



“UNILEX GLOBAL” LLC

**Raqamli huquq va innovatsiya
jurnali
Journal of Digital Law and
Innovation**

**August, 2026
VOLUME 2, ISSUE 1**



EDITORIAL TEAM

Editor-in-Chief, Tukhtashev Hikmatilla Ismatillaevich - Head of the Department of Legal Sciences, Doctor of Philosophy in Legal Sciences (PhD), TIAME National Research University, Tashkent, Republic of Uzbekistan.

1. **Editorial Board Member Borotov Mirodiljon Xomudjonovich** — Doctor of Legal Sciences, Professor, Head of the Department of Civil Law, International Law and International Organizations, Institute of State and Law of the Academy of Sciences of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
2. **Editorial Board Member Maripova Sevarxon Aribjanovna** — Doctor of Philosophy in Legal Sciences (PhD), Associate Professor, Department of Social Sciences, Cyber University State University, Tashkent, Republic of Uzbekistan.
3. **Editorial Board Member Kaharova Munira Maxamajanovna** — Doctor of Political Sciences (DSc), Researcher, Institute of Criminology of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
4. **Editorial Board Member Yuldashev Mutalib Ibrohimovich** — Doctor of Economic Sciences, Professor, Department of Economics, Tashkent University of Science and Technology, Tashkent, Republic of Uzbekistan.
5. **Editorial Board Member Bafaev Shukhrat Gafurovich** — Doctor of Legal Sciences, Head of the Tashkent City Branch, Center for the Analysis of Democratic Processes, Tashkent, Republic of Uzbekistan.
6. **Editorial Board Member Khodjaeva Aziza Bakhtiyarovna** — Doctor of Philosophy in Legal Sciences (PhD), "Academy of Labor and Social Relations" under the Federation of Trade Unions of the Republic of Uzbekistan, Tashkent, Republic of Uzbekistan.
7. **Editorial Board Member Khudoyberdieva Viloyat Jabbrovanovna** — Candidate of Legal Sciences (PhD), Olmazor District Department of Public Education, Tashkent City, Republic of Uzbekistan.
8. **Editorial Board Member Boboumarova Munira Kurbonovna** — Doctor of Philosophy in Legal Sciences (PhD), Department for Organization of Investigative Activities, Investigation Division, Tashkent City Internal Affairs Department, Tashkent, Republic of Uzbekistan.
9. **Editorial Board Member Usmonov Vosid Muhammadievich** — Doctor of Philosophy in Legal Sciences (PhD), Diplomatic University, Tashkent, Republic of Uzbekistan.
10. **Editorial Board Member Mirzayeva Malika Baxadirovna** — Doctoral Researcher, PhD, Associate Professor, Department of Digital Technologies and Artificial Intelligence, Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
11. **Editorial Board Member Allayorov Tulqin Ruziqulovich** — Doctor of Philosophy in Philology (PhD), Associate Professor, Nizami Named Tashkent State Pedagogical University, Tashkent, Republic of Uzbekistan.
12. **Editorial Board Member Tosheva Maftuna Anvar kizi** — Doctor of Philosophy in Legal Sciences (PhD), Tashkent Institute of Irrigation and Agricultural Mechanization Engineers – National Research University, Tashkent, Republic of Uzbekistan.
13. **Editorial Board Member Askarov Jaloliddin Toychievich** — Doctor of Philosophy in Legal Sciences (PhD), Deputy Head, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
14. **Editorial Board Member Abdixakimov Islombek Bahodir o'g'li** — Master of Law (LL.M), Head of the Artificial Intelligence and Legal Tech Laboratory, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
15. **Editorial Board Member Kalandarov Aminjon Amondullayevich** — Doctor of Philosophy in Legal Sciences (PhD), Acting Associate Professor, Department of Business Law, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.
16. **Editorial Board Member Hakimov Komil Bakhtiyarovich** — Doctor of Legal Sciences (DSc), Professor, Head of the Department of Criminal Law, Criminology and Anti-Corruption, Tashkent State University of Law, Tashkent, Republic of Uzbekistan.

DEEPPAKE TEXNOLOGIYASIDAN FOYDALANISHDA SHAXS HUQUQLARINI HIMOYA QILISHNING HUQUQIY MEXANIZMLARI

To'xtasinova Sarvinoz Donyorbek qizi

“Cyber University” davlat universiteti 1-kurs talabasi
tohtasinovasarvinoz2007@gmail.com

Samarov Sherzod Hamrayevich

“Cyber University” davlat universiteti
“Huquq va biznes” fakulteti uslubchisi
samarovsherzod78@gmail.com

MAQOLA MA'LUMOTI

Kalit so'zlar:

deepfake,
sun'iy intellekt,
shaxs huquqlari,
shaxsiy hayot daxlsizligi,
shaxsga doir ma'lumotlar,
biometrik ma'lumotlar,
raqamli identitet,
platforma javobgarligi,
raqamli dalillar,
AI Act.

ANNOTATSIYA

Mazkur maqolada sun'iy intellekt texnologiyalarining jadal rivojlanishi natijasida yuzaga kelayotgan “deepfake” fenomenining shaxs huquqlari va shaxsiy hayot daxlsizligiga ta'siri qiyosiy-huquqiy jihatdan o'rganilgan. Tadqiqot O'zbekiston Respublikasi Konstitutsiyasi, shaxsga doir ma'lumotlar va sun'iy intellektidan foydalanishni tartibga soluvchi milliy qonunchilik, raqamli dalillarga oid protsessual normalar, shuningdek Yevropa Ittifoqining AI Act, GDPR va Digital Services Act hujjatlari hamda tegishli ilmiy adabiyotlar asosida olib borilgan. Tahlil natijalari milliy qonunchilikda shaxsning sha'ni va qadr-qimmatini, biometrik ma'lumotlarini hamda sud orqali himoyalash huquqini ta'minlovchi umumiy huquqiy asoslar mavjudligini ko'rsatadi. Biroq deepfake tushunchasining huquqiy mazmuni, sintetik kontentni belgilash talablari, shaxsning raqamli qiyofasidan uning roziligisiz foydalanish, platformalarning bunday kontentga nisbatan tezkor choralar ko'rish majburiyatlari hamda deepfake materiallarining haqiqiylikni tekshirish mezonlari yetarli darajada tartibga solinmagan. Mazkur bo'shliqlarni bartaraf etish maqsadida oldini olish, aniqlash, tezkor huquqiy choralar ko'rish, shuningdek javobgarlikni belgilash va buzilgan huquqlarni tiklash bosqichlarini qamrab oluvchi to'rt bosqichli huquqiy himoya mexanizmini joriy etish taklif qilinadi.

LEGAL MECHANISMS FOR PROTECTING INDIVIDUAL RIGHTS IN THE USE OF DEEPPAKE TECHNOLOGY

ARTICLE INFO

Keywords:

deepfake,
artificial intelligence,
individual rights,
right to privacy,
personal data,
biometric data,
digital identity,
platform liability,
digital evidence,
AI Act.

ABSTRACT

This article examines, from a comparative legal perspective, the impact of the “deepfake” phenomenon arising from the rapid development of artificial intelligence technologies on individual rights and the right to privacy. The study is based on the Constitution of the Republic of Uzbekistan, national legislation governing personal data and the use of artificial intelligence, procedural rules concerning digital evidence, as well as the European Union’s Artificial Intelligence Act (AI Act), General Data Protection Regulation (GDPR), Digital Services Act, and relevant academic literature. The findings demonstrate that national legislation contains general legal safeguards for the protection of human honour and dignity, biometric data, and the right to judicial protection. However, the legal definition of deepfake, requirements for labelling synthetic content, the use of a person’s digital likeness without consent, platforms’ obligations to respond promptly to such content, and criteria for verifying the authenticity of deepfake materials remain insufficiently regulated. To address these gaps, the article proposes the introduction of a four-stage legal protection mechanism encompassing prevention, detection, prompt legal response, as well as the determination of liability and restoration of violated rights.

ПРАВОВЫЕ МЕХАНИЗМЫ ЗАЩИТЫ ПРАВ ЛИЧНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ТЕХНОЛОГИИ DEEPPAKE

ИНФОРМАЦИЯ СТАТЬИ

Ключевые слова:

deepfake,
искусственный интеллект,
права личности,
неприкосновенность
частной жизни,
персональные данные,
биометрические данные,
цифровая идентичность,

АННОТАЦИЯ

В статье с сравнительно-правовой точки зрения исследуется влияние феномена «deepfake», возникающего вследствие стремительного развития технологий искусственного интеллекта, на права личности и неприкосновенность частной жизни. Исследование проведено на основе Конституции Республики Узбекистан, национального законодательства, регулирующего персональные данные и использование искусственного интеллекта, процессуальных норм, касающихся цифровых доказательств, а также Акта Европейского союза об

ответственность
платформ, цифровые
доказательства, AI Act.

искусственном интеллекте (AI Act), Общего регламента по защите данных (GDPR), Акта о цифровых услугах (Digital Services Act) и соответствующей научной литературы. Результаты анализа показывают, что национальное законодательство содержит общие правовые основы, обеспечивающие защиту чести и достоинства личности, её биометрических данных и права на судебную защиту. Вместе с тем правовое содержание понятия deepfake, требования к маркировке синтетического контента, использование цифрового образа личности без её согласия, обязанности платформ по оперативному реагированию на такой контент, а также критерии проверки подлинности deepfake-материалов урегулированы недостаточно. В целях устранения выявленных пробелов предлагается внедрить четырёхэтапный механизм правовой защиты, охватывающий предупреждение, выявление, принятие оперативных правовых мер, а также установление ответственности и восстановление нарушенных прав.

KIRISH

Sun'iy intellekt texnologiyalarining rivojlanishi raqamli axborotni yaratish, qayta ishlash va tarqatish usullarini tubdan o'zgartirdi. Generativ modellar insonning yuzi, ovozi va xatti-harakatlarini yuqori darajada realistik tarzda qayta yaratishi mumkin. Ushbu imkoniyatning eng murakkab ko'rinishlaridan biri deepfake bo'lib, u mavjud shaxs yoki voqeaga o'xshash, biroq sun'iy yaratilgan yoki manipulyatsiya qilingan tasvir, audio yoxud videoni anglatadi. Yevropa Ittifoqining AI Act hujjati ham deepfake'ni mavjud shaxslar, obyektlar, joylar yoki voqealarga sezilarli darajada o'xshaydigan hamda yolg'ondan haqiqiy deb qabul qilinishi mumkin bo'lgan AI yaratgan yoki manipulyatsiya qilgan kontent sifatida belgilaydi [6].

Deepfake an'anaviy soxta axborotdan vizual va audiovizual ishonchlilik darajasi bilan farq qiladi. Shaxs real hayotda aytmagan gapni aytgan yoki sodir etmagan harakatni bajargan sifatida ko'rsatilishi mumkin. Natijada uning tasviri va ovozi axborot obyektidan mustaqil ravishda boshqariladigan "raqamli qiyofa"ga aylanadi. Ilmiy adabiyotlarda bunday texnologiya shaxsga nisbatan ekspluatatsiya, reputatsion sabotaj, tovlamachilik, firibgarlik va roziliksiz intim kontent yaratish xavfini kuchaytirishi qayd etilgan [10, 14]. Texnik tadqiqotlar esa deepfake yaratish va aniqlash vositalari parallel ravishda rivojlanayotgani sababli aniqlashning o'zi barqaror huquqiy yechim bo'la olmasligini ko'rsatadi [11–13].

O'zbekiston Respublikasi Konstitutsiyasining 26-moddasi insonning sha'ni va qadrigimmati daxlsizligini, 31-moddasi esa shaxsiy hayot, shaxsiy va oilaviy sir, o'z sha'ni va qadr-

qimmatini himoya qilish hamda shaxsga doir ma'lumotlarning himoya qilinishini kafolatlaydi [1]. Shu bois deepfake muammosi faqat axborot xavfsizligi yoki texnik soxtalashtirish masalasi emas; u konstitutsiyaviy huquqlar, shaxsga doir va biometrik ma'lumotlar, fuqarolik-huquqiy javobgarlik, platformalar majburiyatlari hamda sudda raqamli dalillardan foydalanish bilan bog'liq kompleks huquqiy hodisadir.

“Shaxsga doir ma'lumotlar to'g'risida”gi Qonun shaxsga doir ma'lumotlarga ishlov berishning qonuniyligi, maqsadga muvofiqligi, rozilik, biometrik ma'lumotlar, ma'lumotlar subyektining axborot olish va sudga murojaat qilish huquqlarini belgilaydi [2]. 2026-yilda qabul qilingan O'RQ-1115-son Qonun bilan sun'iy intellekt tushunchasi qonun darajasida mustahkamlandi, AI asosida yaratilgan axborot resurslari insonning sha'ni, qadr-qimmati va boshqa ajralmas huquqlariga putur yetkazmasligi belgilandi, shuningdek AI yordamida shaxsga doir ma'lumotlarga qonunga xilof ravishda ishlov berish va ularni tarqatish uchun javobgarlik kuchaytirildi [3]. Mazkur o'zgarishlar muhim huquqiy asos yaratadi, biroq deepfake'ning o'ziga xos hayotiy siklini to'liq qamrab olmaydi.

Qiyosiy tajribada AI Act sintetik kontent bo'yicha shaffoflik majburiyatlarini, GDPR shaxsga doir ma'lumotlarni qayta ishlashning qonuniy asoslari va subyekt huquqlarini, Digital Services Act esa hosting xizmatlari uchun noqonuniy kontent to'g'risidagi xabarnomalarni qabul qilish va ko'rib chiqish mexanizmini nazarda tutadi [6–8]. UNESCOning Sun'iy intellekt etikasi bo'yicha tavsiyasi shaxsiy hayot, inson qadr-qimmati, shaffoflik, izohlanuvchanlik, javobgarlik va inson nazoratini AI tizimlari hayotiy siklining barcha bosqichlari bilan bog'laydi [9].

METODOLOGIYA

Tadqiqotda formal-yuridik, tizimli-huquqiy, qiyosiy-huquqiy va doktrinal tahlil metodlaridan foydalanildi. Formal-yuridik metod yordamida O'zbekiston Respublikasi Konstitutsiyasi, “Shaxsga doir ma'lumotlar to'g'risida”gi Qonun, sun'iy intellektdan foydalanishga oid O'RQ-1115-son Qonun, raqamli dalillar bilan ishlash tizimini takomillashtirgan O'RQ-1003-son Qonun va fuqarolik-huquqiy himoya vositalari tahlil qilindi [1–5].

Tizimli-huquqiy metod deepfake'ni faqat yolg'on axborot sifatida emas, balki bir vaqtning o'zida shaxsiy hayot, sha'n va qadr-qimmat, biometrik ma'lumotlar, raqamli identitet, platforma boshqaruvi, protsessual dalillar va transchegaraviy ijro masalalarini qamrab oluvchi kompleks munosabat sifatida baholash imkonini berdi. Normativ qoidalar deepfake hayotiy siklining yaratilish, aniqlash, tarqatish, cheklash va huquqni tiklash bosqichlari bilan taqqoslandi.

Qiyosiy-huquqiy tahlilda Yevropa Ittifoqining AI Act, GDPR va Digital Services Act hujjatlaridagi shaffoflik, ma'lumotlarni himoya qilish hamda xabarnoma va chora ko'rish mexanizmlari o'rganildi [6–8]. Ushbu hujjatlar tayyor model sifatida emas, balki O'zbekiston huquq tizimiga moslashtirilishi mumkin bo'lgan funksional yechimlar manbasi sifatida ko'rib chiqildi.

NATIJALAR

Tahlil natijalari O'zbekistonda deepfake bilan bog'liq huquqlarni himoya qilish uchun mutlaqo huquqiy asos mavjud emas, degan xulosani rad etadi. Aksincha, konstitutsiyaviy kafolatlar, shaxsga doir ma'lumotlar rejimi, sun'iy intellektdan foydalanishga doir umumiy talablar, fuqarolik-huquqiy himoya va raqamli dalillarni baholash qoidalari birgalikda muayyan himoya tizimini shakllantiradi [1–5]. Asosiy muammo ushbu vositalarning deepfake'ning texnologik xususiyatlari va juda tez tarqalish dinamikasiga moslashtirilmaganidadir.

Birinchi natija deepfake'ning himoya qilinadigan huquqiy manfaatlari bir nechta ekanini ko'rsatdi. Kontent shaxsning yuz yoki ovozidan foydalangan taqdirda biometrik ma'lumotlar rejimi, yolg'on xatti-harakat yoki bayonot yaratganda sha'n, qadr-qimmat va ishchanlik obro'si, shaxsiy yoki intim mazmun ishlab chiqilganda shaxsiy hayot daxlsizligi, firibgarlikda foydalanilganda esa mulkiy manfaatlar va axborot xavfsizligi bir vaqtning o'zida buzilishi mumkin. Shu sababli deepfake'ni faqat “yolg'on axborot” deb tasniflash uning huquqiy mohiyatini toraytiradi.

Ikkinchi natija shaxsga doir ma'lumotlar qonunchiligining muhim, ammo chegaralangan rolini ko'rsatdi. Qonunning 18, 19, 21, 26 va 30-moddalari rozilik, ishlov berish maqsadining qonuniyligi, biometrik ma'lumotlar va subyekt huquqlarini tartibga soladi [2]. Biroq ochiq internet manbasiga qonuniy joylashtirilgan fotosuratdan shaxsning rozilgisiz yangi sintetik video yaratish oddiy qayta tarqatish bilan bir xil emas. Bunda dastlabki ma'lumotdan yangi, shaxsga nisbat beriladigan voqelik yaratiladi. Amaldagi normalarda bunday “raqamli qiyofani sintetik qayta yaratish” alohida kategoriya sifatida ifodalanmagan.

Uchinchi natija 2026-yildagi qonunchilik yangiliklari umumiy AI mas'uliyatini kuchaytirganini, ammo deepfake uchun maxsus shaffoflik va tezkor javob mexanizmini yaratmaganini ko'rsatdi. O'RQ–1115-son Qonun AI resurslari insonning sha'ni, qadr-qimmatini va boshqa ajralmas huquqlariga putur yetkazmasligini talab qiladi hamda AI yordamida shaxsga doir ma'lumotlarga qonunga xilof ishlov berish va ularni internetda tarqatishni ma'muriy javobgarlik bilan bog'laydi [3]. Shunga qaramay, deepfake ta'rifi, sintetik kontentni

ko‘rinadigan shaklda belgilash, parodiya va badiiy foydalanish istisnolari hamda platformalarning tekshiruv tartibi ochiq qolmoqda.

To‘rtinchi natija raqamli dalillar bo‘yicha umumiy protsessual bazaning mavjudligini tasdiqladi. O‘RQ–1003-son Qonun raqamli dalillarni to‘plash, taqdim etish, saqlash, tekshirish va baholash qoidalarini protsessual kodekslarga kiritdi [4]. Biroq deepfake’ni sudda baholashda faylning kelib chiqishi, metama’lumotlar yaxlitligi, tahrirlash izlari, qo‘llangan modelning ehtimoliy xatoligi, ekspertiza usulining takrorlanuvchanligi va asl manba bilan bog‘liqlik kabi maxsus mezonlar talab etiladi. Umumiy raqamli dalil qoidalari ushbu texnik mezonlarning o‘rnini avtomatik ravishda bosa olmaydi.

Aniqlangan holatlar quyidagi jadvalda huquqiy yo‘nalish, mavjud tartibga solish darajasi va maxsus bo‘shliq bo‘yicha umumlashtirildi.

1-jadval. O‘zbekistonda deepfake bilan bog‘liq mavjud huquqiy mexanizmlarning yetarliligi

Huquqiy yo‘nalish	Mavjud tartibga solish	Baho	Aniqlangan maxsus bo‘shliq
Konstitutsiyaviy himoya	Sha’n va qadr-qimmat, shaxsiy hayot va shaxsga doir ma’lumotlar himoyasi	Qisman yetarli	Deepfake oqibatida raqamli qiyofani manipulyatsiya qilish alohida huquqiy kategoriya sifatida belgilanmagan
Shaxsga doir va biometrik ma’lumotlar	Rozilik, maqsadga muvofiqlik, biometrik ma’lumotlarga ishlov berish va sudga murojaat qilish qoidalari	Qisman yetarli	Ochiq manbadagi tasvir yoki ovozdan yangi sintetik shaxsiy kontent yaratish oqibatlari maxsus tartibga solinmagan
Sun’iy intellektdan foydalanish	AI resurslari inson huquqlariga putur yetkazmasligi va noqonuniy ishlov uchun javobgarlik qoidalari	Qisman yetarli	Deepfake ta’rifi, uning majburiy markirovkasi va tarqatuvchilar majburiyatlari nazarda tutilmagan
Sha’n, qadr-qimmat va obro‘	Fuqarolik-huquqiy himoya, rad etish hamda zarar va ma’naviy zararni qoplash vositalari	Qisman yetarli	Sintetik kontentning tez tarqalishi va uzoq muddatli raqamli zararini baholash mezonlari aniqlashtirilmagan

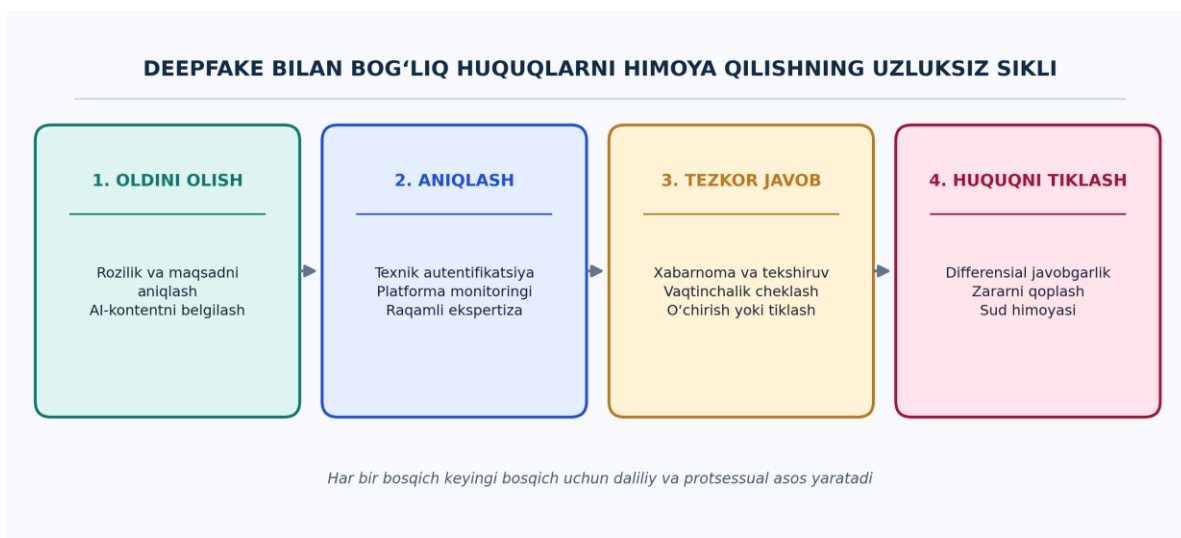
Huquqiy yo'nalish	Mavjud tartibga solish	Baho	Aniqlangan maxsus bo'shliq
Platformalar faoliyati	Axborot va internet munosabatlariga oid umumiy talablar	Yetarli emas	Deepfake bo'yicha xabarnoma, vaqtinchalik cheklash, tekshirish va olib tashlashning maxsus tartibi yo'q
AI-kontentni belgilash	Universal majburiy markirovkalash tizimi mavjud emas	Yetarli emas	Foydalanuvchining sintetik kontentni haqiqiy deb qabul qilish xavfi saqlanib qoladi
Raqamli dalillar	Raqamli dalillarni to'plash, taqdim etish, tekshirish va baholashning umumiy protsessual qoidalari	Qisman yetarli	Deepfake autentifikatsiyasi, kelib chiqish zanjiri va ekspert xulosasiga qo'yiladigan maxsus mezonlar belgilanmagan
Tezkor huquqiy himoya	Vakolatli organ yoki sudga murojaat qilish imkoniyati	Yetarli emas	Sudgacha bo'lgan tezkor himoya chorasi kontentning virusli tarqalish tezligiga moslashtirilmagan
Transchegaraviy ijro	Xalqaro hamkorlikning umumiy mexanizmlari	Yetarli emas	Yaratuvchi, server, platforma va jabrlanuvchi turli davlatlarda bo'lganda yurisdiksiya hamda qaror ijrosi murakkablashadi

Manba: Muallif tomonidan milliy qonunchilik va qiyosiy-huquqiy tahlil asosida tuzilgan [1–8].

Jadval shuni ko'rsatadiki, konstitutsiyaviy, ma'lumotlarni himoya qilish va fuqarolik-huquqiy vositalar “qisman yetarli” darajada ishlashi mumkin, chunki ular jabrlanuvchiga umumiy talab va da'vo vositalarini beradi. Eng katta bo'shliqlar esa deepfake'ni oldindan belgilash, platformada tezkor ko'rib chiqish, kontentning tarqalishini vaqtincha cheklash, raqamli qiyofadan roziliksiz foydalanish va transchegaraviy ijro bilan bog'liq. Shu bois samarali himoya faqat yakuniy sud qaroriga emas, huquqbuzarlik sodir bo'lishidan oldingi va darhol keyingi bosqichlarga ham tayanishi kerak.

Tadqiqot natijalarini tizimlashtirish asosida deepfake bilan bog'liq huquqlarni himoya qilishning to'rt bosqichli modeli ishlab chiqildi.

1-rasm. Deepfake bilan bog'liq huquqlarni himoya qilishning to'rt bosqichli modeli



Manba: Muallif tomonidan milliy qonunchilik, Yevropa Ittifoqi hujjatlari va ilmiy adabiyotlar asosida ishlab chiqilgan [1–14].

Modelning birinchi bosqichi rozilikni, ma'lumotlardan foydalanish maqsadini va AI-kontentni belgilashni nazarda tutadi. Ikkinchi bosqich texnik autentifikatsiya, platforma monitoringi va raqamli ekspertizani birlashtiradi. Uchinchi bosqich jabrlanuvchining xabarnomasini qabul qilish, xavf darajasini baholash, zarur bo'lsa kontent tarqalishini vaqtincha cheklash va asoslantirilgan qaror qabul qilishni qamrab oladi. To'rtinchi bosqichda huquqbuzarlik ishtirokchilarining rolga qarab differensial javobgarlik, zararni qoplash, kontentni olib tashlash yoki rad etish hamda sud himoyasi ta'minlanadi. Ushbu bosqichlar alohida choralar emas, uzluksiz protsessual zanjir sifatida ishlashi lozim.

MUHOKAMA

Olingan natijalar Robert Chesney va Danielle Citronning deepfake'ga qarshi javob faqat jinoiy yoki fuqarolik javobgarligi bilan cheklanmasligi, texnik autentifikatsiya, platforma siyosati, huquqiy choralar va jabrlanuvchini himoya qilish vositalari birgalikda qo'llanishi kerakligi haqidagi xulosalari bilan mos keladi [10]. Biroq ushbu tadqiqot mazkur yondashuvni O'zbekiston huquq tizimiga moslashtirib, himoyani oldini olishdan huquqni tiklashgacha bo'lgan protsessual zanjir sifatida ifodalaydi. Bu yondashuv javobgarlikni kechikib qo'llashdan ko'ra, zarar tarqalishini dastlabki bosqichda cheklashga ustuvor ahamiyat beradi.

Yisroel Mirsky va Wenke Lee deepfake yaratish hamda aniqlash usullarining doimiy texnologik raqobatda ekanini ko'rsatadi [11]. Masood va hammualliflar, shuningdek Juefei-Xu

va hammualliflar aniqlash algoritmlarining ma'lumotlar to'plami, manipulyatsiya turi va yangi hujum usullariga bog'liqligini qayd etadilar [12, 13]. Mazkur tadqiqot natijalari ushbu texnik xulosalarni huquqiy nuqtayi nazardan davom ettiradi: qonun muayyan detektor yoki algoritmni mutlaq ishonchli deb qabul qilmasligi, ekspert xulosasining usuli, xatolik ehtimoli va takroriy tekshiruv imkoniyatini protsessual talab sifatida belgilashi kerak.

Roziliksiz intim deepfake alohida huquqiy yondashuvni talab qiladi. Danielle Citronning seksual daxlsizlik konsepsiyasi bunday kontentni oddiy reputatsion zarar emas, balki shaxsiy avtonomiya, tenglik va hayotiy imkoniyatlarga ta'sir qiluvchi huquqbuzarlik sifatida baholash zarurligini asoslaydi [14]. Shu jihatdan tezkor himoya mexanizmi zarar yetkazilganidan keyin faqat pul kompensatsiyasi bilan cheklanmasligi; kontentni indekslashni cheklash, nusxalarni aniqlash, jabrlanuvchiga xabar berish va qayta tarqalishni kamaytirish choralari ham qamrab olishi lozim.

AI Actning shaffoflik modeli deepfake kontentini foydalanuvchi anglay oladigan tarzda belgilash uchun muhim qiyosiy manba hisoblanadi [6]. O'zbekiston qonunchiligida ham AI yordamida yaratilgan yoki sezilarli darajada manipulyatsiya qilingan audio, video va tasviriy kontent uchun ko'rinadigan markirovka hamda mashina o'qiy oladigan kelib chiqish ma'lumotlarini saqlash talabi joriy etilishi mumkin. Biroq bunday talab satira, parodiya, badiiy ijod, ta'lim va jurnalistika bilan bog'liq qonuniy foydalanishni mutanosib ravishda hisobga olishi kerak. Markirovka kontentni avtomatik taqiqlash emas, uning sintetik xususiyati to'g'risida xabardor qilish vositasi bo'lishi lozim.

Digital Services Actdagi xabarnoma va chora ko'rish mexanizmi platforma majburiyatlarini shakllantirishda funksional namuna beradi [8]. Milliy tartibda shaxs o'zining yuzi yoki ovozidan roziliksiz foydalanilgan deepfake haqida standart shaklda xabar berishi, platforma kontentning ehtimoliy zararini va xabarning asoslanganligini tezkor baholashi, qaror sabablarini tomonlarga bildirishi hamda noto'g'ri cheklov ustidan ichki shikoyat imkonini ta'minlashi maqsadga muvofiq. Bunda platforma har qanday bahsli kontentni avtomatik o'chiradigan subyektga aylantirilmasligi, so'z erkinligi va jabrlanuvchi huquqlari o'rtasida mutanosiblik saqlanishi zarur.

Tahlildan kelib chiqib, amaldagi qonunchilikka "deepfake", "sintetik audiovizual kontent" va "raqamli qiyofa" tushunchalarini kiritish taklif etiladi. Raqamli qiyofa shaxsning yuzi, ovozi, biometrik belgisi yoki o'ziga xos xatti-harakatlari asosida uning identifikatsiyasini yuzaga keltiruvchi sintetik tasvir sifatida talqin qilinishi mumkin. Bunday norma fotosuratni oddiy qayta

tarqatish bilan shaxs nomidan yangi yolgʻon voqelik yaratishni huquqiy jihatdan farqlashga yordam beradi.

Javobgarlik kontentni yaratish, buyurtma qilish, bila turib tarqatish, tijorat maqsadida foydalanish va asosli xabardan keyin chora koʻrmaslik kabi harakatlarga qarab differensiallashtirilishi lozim. Hazil yoki parodiya maqsadidagi ochiq belgilangan kontent bilan firibgarlik, saylovga noqonuniy taʼsir, tovlamachilik yoki roziliksiz intim kontent bir xil huquqiy oqibat tugʻdirmasligi kerak. Qasddan yetkazilgan zarar, auditoriya koʻlami, tarqalish tezligi, kontentning takroriy joylashtirilishi va jabrlanuvchining zaif holati javobgarlikni belgilash mezonlari boʻlishi mumkin.

Nihoyat, deepfakeʼning transchegaraviy tabiati milliy vakolatning oʻzi bilan cheklanmaydigan hamkorlikni talab qiladi. Platforma, server, yaratuvchi va jabrlanuvchi turli yurisdiksiyalarda boʻlishi mumkin. Shu sababli elektron dalillarni saqlab qolish, vakolatli organlar oʻrtasida tezkor axborot almashish, xorijiy platformalarga huquqiy talab yuborish va sud qarorlarini tan olish mexanizmlarini xalqaro hamkorlik vositalari bilan uygʻunlashtirish zarur.

XULOSA

Deepfake texnologiyasini huquqiy tartibga solishni takomillashtirish mavjud konstitutsiyaviy, axborot-huquqiy, fuqarolik-huquqiy va protsessual mexanizmlarning vazifalari hamda oʻzaro ketma-ketligini aniq belgilashni talab etadi. Shaxsga doir va biometrik maʼlumotlarni himoya qilish, AI-kontentni markirovkalash, platformalarning xabarnomalarni tezkor koʻrib chiqishi, raqamli ekspertiza va differensial javobgarlik yagona huquqiy zanjirda ishlashi lozim. Deepfakeʼni maxsus taʼriflash va “raqamli qiyofa” tushunchasini mustahkamlash esa roziliksiz sintetik kontentni oddiy axborot tarqatishdan huquqiy jihatdan farqlash imkonini beradi.

Xulosa qilib aytganda, samarali himoya yangi alohida qonun qabul qilish bilangina emas, balki oldini olish, aniqlash, tezkor javob berish hamda javobgarlik va huquqni tiklash bosqichlarining uzluksizligi bilan belgilanadi. Taklif etilgan toʻrt bosqichli model shaxsning shaʼni, shaxsiy hayoti va raqamli identitetini himoya qilish bilan birga, qonuniy ijod, axborot erkinligi va sunʼiy intellekt innovatsiyalari oʻrtasida mutanosib muvozanatni taʼminlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. O'zbekiston Respublikasi Konstitutsiyasi. 30.04.2023. <https://lex.uz/uz/docs/-6445145>
2. O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi O'RQ-547-son Qonuni. 02.07.2019 (amaldagi tahrir). <https://lex.uz/uz/docs/-4396419>
3. O'zbekiston Respublikasining "Sun'iy intellektni qo'llash orqali yuzaga keladigan munosabatlar tartibga solinishi munosabati bilan O'zbekiston Respublikasining ayrim qonun hujjatlariga qo'shimcha va o'zgartirishlar kiritish to'g'risida"gi O'RQ-1115-son Qonuni. 21.01.2026. <https://lex.uz/uz/docs/-8008401>
4. O'zbekiston Respublikasining "O'zbekiston Respublikasining ayrim qonun hujjatlariga raqamli dalillar bilan ishlash tizimini takomillashtirishga qaratilgan o'zgartirish va qo'shimchalar kiritish to'g'risida"gi O'RQ-1003-son Qonuni. 21.11.2024. <https://lex.uz/docs/-7228758>
5. O'zbekiston Respublikasining Fuqarolik kodeksi (birinchi qism). 21.12.1995 (amaldagi tahrir). <https://lex.uz/docs/-111189>
6. European Parliament and Council of the European Union. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 13 June 2024. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
7. European Parliament and Council of the European Union. Regulation (EU) 2016/679 (General Data Protection Regulation). 27 April 2016. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
8. European Parliament and Council of the European Union. Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act). 19 October 2022. <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>
9. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris, 2021. <https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>
10. Chesney, R., & Citron, D. K. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107, 1753–1820, 2019. https://scholarship.law.bu.edu/faculty_scholarship/640/
11. Mirsky, Y., & Lee, W. The Creation and Detection of Deepfakes: A Survey. ACM Computing Surveys, 54(1), Article 7, 1–41, 2021. DOI: 10.1145/3425780. <https://doi.org/10.1145/3425780>
12. Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. Deepfakes generation and detection: state-of-the-art, open challenges, countermeasures, and way forward. Applied Intelligence, 53, 3974–4026, 2023. <https://doi.org/10.1007/s10489-022-03766-z>
13. Juefei-Xu, F., Wang, R., Huang, Y., Guo, Q., Ma, L., & Liu, Y. Countering Malicious DeepFakes: Survey, Battleground, and Horizon. International Journal of Computer Vision, 130, 1678–1734, 2022. <https://doi.org/10.1007/s11263-022-01606-8>