SUN'IY INTELLEKT YORDAMIDA YARATILADIGAN DEEPFAKE MATERIALLARI ORQALI SHAXS HUQUQLARINING BUZILISHI: NOQONUNIY KREDIT RASMIYLASHTIRISH VA TOVLAMACHILIKNING HUQUQIY JIHATLARI

Feruzaxon Usmonova
TDYU huzuridagi H.K. Muhitdinova nomidagi
akademik litseyi Tillar kafedrasi o'qiuvchisi
e-mail: feruzausmonova1113@gmail.com
Tel: +998936737078
Zuhiraliyeva Mahmuda
TDYU huzuridagi H.K. Muhitdinova nomidagi
akademik litsey 1-bosqich 101-guruh talabasi
e-mail: zuhiraliyevamahmuda@gmail.com
Tel: +998883739313
https://doi.org/10.5281/zenodo.24102939

Annotatsiya. Ushbu maqolada sun'iy intellekt texnologiyalari ta'siri ostida insonning yuzi, ovozi va boshqa biometrik belgilarini sun'iy ravishda yaratish yoki o'zgartirish imkonini beruvchi deepfake texnologiyalarining huquqiy jihatlari tahlil qilinadi. Xususan, ushbu-texnologiyalardan shaxsga doir ma'lumotlardan noqonuniy foydalanish, boshqa shaxs nomidan kredit rasmiylashtirish, firibgarlik va tovlamachilik sodir etishda foydalanish bilan bog'liq xavflar o'rganiladi. O'zbekiston Respublikasining shaxsga doir ma'lumotlar, jinoyat va ma'muriy javobgarlikka oid qonunchiligi doirasida mavjud huquqiy himoya vositalari tahlil etilib, sun'iy intellekt asosida yaratilgan soxta materiallarni aniqlash, raqamli dalillarni saqlash, masofaviy identifikatsiya xavfsizligini kuchaytirish hamda jabrlanuvchilarning huquqlarini tiklashga qaratilgan takliflar ilgari suriladi. Shuningdek, Yevropa Ittifoqining sun'iy intellektni tartibga solish tajribasi qiyosiy-huquqiy nuqtayi nazardan ko'rib chiqiladi.
Kalit so'zlar: sun'iy intellekt, deepfake, biometrik ma'lumotlar, shaxsga doir ma'lumotlar, shaxsni identifikatsiya qilish, kredit firibgarligi, tovlamachilik, kiberjinoyatchilik, raqamli dalillar, huquqiy javobgarlik.

Abstract. This article examines the legal implications of deepfake technologies that use artificial intelligence to generate or manipulate human faces, voices, and other biometric features. Particular attention is given to the misuse of personal data, fraudulent loan applications, identity-related fraud, and extortion involving synthetic media. The article analyses relevant legal safeguards under the legislation of the Republic of Uzbekistan and considers comparative approaches to AI transparency in the European Union. It proposes measures to strengthen remote identity verification, preserve digital evidence, improve institutional responses, and protect the rights of victims.
Keywords: artificial intelligence, deepfake, biometric data, personal data protection, identity fraud, loan fraud, extortion, cybercrime, digital evidence, legal liability.

Kirish. Raqamli texnologiyalarning jadal rivojlanishi davlat boshqaruvi, bank-moliya xizmatlari, elektron tijorat va kundalik ijtimoiy munosabatlarda yangi imkoniyatlarni yuzaga keltirmoqda. Bunga qo'shimcha ravishda, sun'iy intellektdan foydalanish insonning shaxsiy hayoti, shaxsga doir ma'lumotlari, mol-mulki va sha'ni bilan bog'liq huquqiy munosabatlarga yangi va dolzarb xavflarni ham olib kirmoqda. Bunday xavflarning muhim ko'rinishlaridan biri deepfake texnologiyalaridir.

Deepfake — sun'iy intellekt vositalari orqali mavjud insonning yuzi, ovozi yoki harakatlarini taqlid qiluvchi yoxud ularni o'zgartiruvchi sintetik audio, video yoki tasvir materialidir. Ushbu texnologiyalar ijodiy faoliyat, ta'lim va audiovizual ishlab chiqarishda qonuniy maqsadlarda ishlatilishi mumkin. Biroq ular insonning roziligisiz soxta tasvir yoki ovoz yaratish, shaxsni noto'g'ri tanitish, uning nomidan moliyaviy operatsiyalarni amalga oshirish va soxta materiallar bilan qo'rqitish kabi noqonuniy harakatlarda ham qo'llanishi mumkin.

Muammoning dolzarbligi shundaki, raqamli muhitda shaxsni aniqlash uchun foydalaniladigan tasvir va ovozning tashqi jihatdan ishonarli ko'rinishi har doim ham uning haqiqiy ekanini kafolatlamaydi.Shu sababli jamiyat a'zolari orasida muammolar kelib chiqadi. Natijada an'anaviy identifikatsiya usullariga ortiqcha ishonish shaxsiy ma'lumotlar va moliyaviy xavfsizlikka tahdid tug'dirishi mumkin.

Tadqiqotning maqsadi deepfake texnologiyalari yordamida sodir etilishi mumkin bo'lgan huquqbuzarliklarning huquqiy xususiyatlarini aniqlash, O'zbekiston qonunchiligidagi tegishli himoya mexanizmlarini tahlil qilish hamda huquqni qo'llash amaliyotini takomillashtirish bo'yicha takliflar ishlab chiqishdan iborat.

Agar shaxsning tasviri yoki ovozi uning roziligisiz noqonuniy maqsadda ishlatiladigan bo'lsa, vaziyatga qarab shaxsga doir ma'lumotlar to'g'risidagi qonunchilik, shaxsiy hayot daxlsizligi va boshqa tegishli huquqiy normalar qo'llanishi mumkin. O'zbekiston Respublikasi Ma'muriy javobgarlik to'g'risidagi kodeksining 46^2-moddasi shaxsga doir ma'lumotlar to'g'risidagi qonunchilikni buzish uchun javobgarlikni nazarda tutadi. Jinoyat kodeksining 141^2-moddasida esa mazkur qonunchilikni buzish bilan bog'liq jinoiy javobgarlik masalalari tartibga solinadi . Ushbu normalarni qo'llashda qonunda nazarda tutilgan huquqbuzarlik belgilari va javobgarlik shartlari aniqlanishi zarur. Har qanday deepfake materialini yaratish yoki tarqatish avtomatik ravishda aynan shu moddalardagi huquqbuzarlik tarkibini yuzaga keltiradi, degan xulosaga kelib bo'lmaydi. **Deepfake yordamida kredit rasmiylashtirish va firibgarlik.**

Raqamli bank xizmatlarining kengayishi mijozlarni masofadan identifikatsiya qilish imkoniyatlarini oshirmoqda. Biroq yuz tasviri yoki ovoz orqali tekshirish tizimlari sun'iy ravishda yaratilgan materiallardan foydalanish xavfini ham yuzaga keltirishi mumkin. Shartli misol sifatida, noma'lum shaxs fuqaroning ochiq manbalardagi videolaridan foydalanib uning yuz ifodasi va ovoziga taqlid qiluvchi material tayyorlaydi hamda shu material orqali masofaviy kredit olishga urinadi. Agar aldash yoki ishonchni suiiste'mol qilish orqali o'zganing mulki yoki mulkka bo'lgan huquqi qo'lga kiritilgan bo'lsa, qilmishning holatlariga qarab O'zbekiston Respublikasi Jinoyat kodeksining 168-moddasida nazarda tutilgan firibgarlik alomatlari mavjud bo'lishi mumkin. Ammo faqat kredit olishga urinish yoki identifikatsiya jarayonida soxta materialdan foydalanishning o'zi barcha holatlarda tugallangan firibgarlikni anglatmaydi. Qilmishning bosqichi, ayb shakli, maqsadi, amalda yuz bergan natija va boshqa yuridik

ahamiyatga ega holatlar tergov hamda sud tomonidan baholanishi kerak. Shuningdek, jabrlanuvchi nomiga uning roziligisiz kredit rasmiylashtirilganida ikki alohida masala yuzaga keladi: birinchisi, kredit tashkilotini aldagan shaxsning ehtimoliy javobgarligi; ikkinchisi, nomidan kredit rasmiylashtirilgan fuqaroning huquqiy holati. Ikkinchi masala kredit hujjatlari, elektron tasdiqlash izlari, identifikatsiya usuli va boshqa dalillarni o‘rganish orqali hal qilinishi kerak. Shuning uchun jabrlanuvchiga kredit majburiyati avtomatik ravishda yuklanadi yoki avtomatik ravishda bekor qilinadi, deb umumiy xulosa chiqarish mumkin emas. **Deepfake orqali tovlamachilik qilish.**

Deepfake materiallari tovlamachilik uchun ham ishlatilishi mumkin. Masalan, shaxsning yuzidan foydalanib soxta video tayyorlanadi va uni internetda tarqatish bilan qo‘rqitib pul talab qilinadi. Yoki sun’iy yaratilgan ovozli xabar orqali jabrlanuvchiga bosim o‘tkaziladi. O‘zbekiston Respublikasi Jinoyat kodeksining 165-moddasi tovlamachilikka oid javobgarlikni belgilaydi. Mazkur moddaning mazmunida zo‘rlik ishlatish, mulkka zarar yetkazish, axborot resurslariga ta’sir ko‘rsatish, sir saqlanishi lozim bo‘lgan ma’lumotlarni oshkor qilish yoki sharmanda qiluvchi uydirmalarni tarqatish bilan qo‘rqitib mulk yoki mulkiy huquqni talab qilish kabi holatlar nazarda tutilgan. Shu sababli sun’iy ravishda yaratilgan soxta tasvir yoki video bilan qo‘rqitib pul talab qilish holati, mavjud dalillar va qonundagi belgilar mos kelgan taqdirda, tovlamachilik sifatida baholanishi mumkin. Biroq yakuniy huquqiy baho materialning soxta ekanligigagina emas, balki tahdidning mazmuni, mulkiy talabning mavjudligi, shaxsning qasdi va boshqa holatlarga bog‘liq. Mazkur muammoning alohida jihati — jabrlanuvchining ikki karra zarar ko‘rish xavfidir: u bir tomondan soxta materialning tarqalishi bilan bog‘liq obro‘ yoki ruhiy zarar xavfiga, ikkinchi tomondan esa pul berishga majburlashga duch kelishi mumkin. Shu bois bunday holatlarda dalillarni tezkor saqlash, noqonuniy material tarqalishini cheklashning qonuniy mexanizmlaridan foydalanish va vakolatli organlarga murojaat qilish muhimdir.

Sun’iy intellektga oid 2026-yilgi qonunchilikdagi yangiliklar.

Tadqiqot mavzusi uchun muhim normativ yangiliklardan biri — 2026-yil 21-yanvardagi O‘RQ-1115-sonli “Sun’iy intellektni qo‘llash orqali yuzaga keladigan munosabatlarni tartibga solish munosabati bilan O‘zbekiston Respublikasining ayrim qonun hujjatlariga qo‘shimcha va o‘zgartirishlar kiritish to‘g‘risida”gi Qonundir. Mazkur qonun bilan sun’iy intellekt texnologiyalaridan foydalanishning huquqiy asoslari takomillashtirildi. Rasmiy tushuntirishga ko‘ra, insonning huquq va erkinliklariga aloqador yuridik ahamiyatga ega qarorlarni qabul qilishda faqat sun’iy intellekt asosidagi axborot tizimlari xulosalariga tayanishga yo‘l qo‘yilmaydi. Shuningdek, sun’iy intellekt yordamida shaxsga doir ma’lumotlarga qonunga xilof ravishda ishlov berish uchun ma’muriy javobgarlik belgilangan . Ushbu qoidalar deepfake bilan bog‘liq huquqiy munosabatlarni o‘rganishda alohida ahamiyatga ega. Masalan, bank yoki boshqa tashkilotning avtomatlashtirilgan tizimi shaxsning yuz tasvirini haqiqiy deb topgani uning kredit olishga rozilik bildirganini yoki tegishli bitimni aynan o‘sha shaxs tuzganini har doim ham to‘liq isbotlamaydi. Bunday holatlarda qarorning huquqiy asoslari, identifikatsiya jarayoni, texnik ma’lumotlar va inson tomonidan tekshirish imkoniyati muhim ahamiyat kasb etadi. Biroq ushbu qonunchilikdagi talablarni barcha avtomatlashtirilgan tekshiruvlarni taqiqlash sifatida talqin qilish mumkin emas. Muhim jihat — insonning huquq va erkinliklariga

daxldor yuridik ahamiyatga ega qarorlarni faqat sun’iy intellekt xulosasiga asoslamaslikdir. Shunday qilib, O‘zbekiston qonunchiligida sun’iy intellekt bilan bog‘liq ayrim xavflarga nisbatan huquqiy mexanizmlar mavjud. Endilikda ularni bank amaliyoti, elektron identifikatsiya va raqamli dalillar bilan ishlash jarayonlarida samarali qo‘llash masalasi dolzarb bo‘lib qolmoqda. Qiyosiy-huquqiy tahlil: Yevropa Ittifoqi tajribasi.

Deepfake materiallarining huquqiy oqibatlarini tahlil qilishda xorijiy tajriba ham muhim ahamiyatga ega. Xususan, Yevropa Ittifoqining 2024/1689-sonli Sun’iy intellekt to‘g‘risidagi reglamenti — AI Act — sun’iy intellekt tizimlaridan foydalanishda shaffoflikni ta’minlashga qaratilgan qoidalarni o‘z ichiga oladi .

Reglamentning 50-moddasida ayrim sun’iy intellekt tizimlari bilan bevosita muloqot qilayotgan shaxslarni bu haqda xabardor qilish, sun’iy yaratilgan yoki o‘zgartirilgan materiallarning kelib chiqishini belgilash va deepfake materiallari sun’iy ravishda yaratilgan yoki o‘zgartirilganini oshkor etish bilan bog‘liq talablar nazarda tutilgan. Mazkur qoidalar tegishli shartlar va istisnolarni ham o‘z ichiga oladi.

Yevropa Ittifoqining rasmiy izohida 50-moddaning shaffoflikka oid qoidalari 2026-yil 2-avgustdan qo‘llanilishi ko‘rsatilgan . Biroq ushbu talablarning amal qilish doirasi reglamentdagi tegishli shartlar va istisnolar bilan belgilanadi; ularni barcha deepfake materiallariga nisbatan bir xil, mutlaq taqiq deb talqin qilish noto‘g‘ri.

Qiyosiy tahlil O‘zbekiston uchun uchta amaliy yo‘nalishni ko‘rsatadi.

Birinchidan, sun’iy intellekt yordamida yaratilgan audio va video materiallarining kelib chiqishini aniqlash imkoniyatlarini rivojlantirish lozim. Ikkinchidan, muhim huquqiy oqibatlarga olib keladigan raqamli operatsiyalarda avtomatlashtirilgan tizim natijalarini boshqa tekshiruv usullari bilan birgalikda baholash zarur. Uchinchidan, fuqarolarning shikoyat qilish va o‘z huquqlarini himoya qilish mexanizmlarini amaliy jihatdan qulaylashtirish maqsadga muvofiq.

Bunda xorijiy tajribani milliy huquq tizimiga to‘g‘ridan-to‘g‘ri ko‘chirish emas, balki mavjud qonunchilik va institutsional imkoniyatlarga moslashtirish muhimdir.

Huquqni qo‘llash amaliyotidagi muammolar.

Deepfake yordamida sodir etilishi mumkin bo‘lgan huquqbuzarliklarni aniqlash va ularga huquqiy baho berishda bir qator amaliy muammolar mavjud.

Birinchi muammo — materialning haqiqiyligini aniqlash. Tashqi ko‘rinishidan ishonarli video yoki ovozli yozuv insonning haqiqatan ham muayyan harakatni amalga oshirganini yoki muayyan gapni aytganini o‘z-o‘zidan isbotlamaydi. Shu sababli raqamli materialni uning manbasi, yaratilish tarixi va boshqa dalillar bilan birgalikda tekshirish zarur.

Ikkinchi muammo — shaxsni identifikatsiya qilishdagi xatolar. Yuzni tanish yoki ovoz orqali tekshirish tizimlari qo‘shimcha xavfsizlik choralari bilan ta’minlanmasa, soxta materiallar yoki boshqa texnik usullar orqali chalg‘itilishi mumkin. Shu sababli bitta biometrik belgi asosida moliyaviy majburiyatni rasmiylashtirish xavflarni to‘liq bartaraf etmaydi.

Uchinchi muammo — dalillarni saqlash va tekshirish. Soxta materialning internetda tarqalishi, keyinchalik o‘chirib yuborilishi yoki bir necha marta qayta ishlanishi uning kelib chiqishini aniqlashni qiyinlashtirishi mumkin. Shu sababli asl fayllar, xabarlar, vaqt belgilari, tegishli tizim qaydlari va boshqa texnik ma’lumotlarni qonuniy tartibda saqlash muhim.

To‘rtinchi muammo — jabrlanuvchining huquqiy holati. Boshqa shaxs tomonidan uning nomidan kredit rasmiylashtirilgan fuqaro kredit hujjatlari va elektron tasdiqlash jarayoniga oid ma’lumotlarni tekshirishga muhtoj bo‘ladi. Kredit tashkiloti, vakolatli organlar va sud tomonidan ushbu dalillarni o‘rganish jabrlanuvchining huquqlarini himoya qilishda muhim ahamiyat kasb etadi.

Beshinchi muammo — texnologik va huquqiy baholashning o‘zaro bog‘liqligi. Sun’iy intellekt yordamida yaratilgan materialni aniqlash texnik mutaxassislikni talab qilishi mumkin, lekin texnik xulosa qilmishning huquqiy kvalifikatsiyasini avtomatik belgilamaydi. Yakuniy huquqiy baho amaldagi qonun va barcha tegishli holatlar asosida berilishi kerak.

Qonunchilik va amaliyotni takomillashtirish bo‘yicha takliflar.

Yuqoridagi tahlildan kelib chiqib, quyidagi takliflarni ilgari surish mumkin.

1. Masofaviy kredit rasmiylashtirishda ko‘p bosqichli identifikatsiyani rivojlantirish. Bank va kredit tashkilotlarida yuz yoki ovoz orqali tekshirishni yagona xavfsizlik mezoni sifatida qo‘llash o‘rniga, xavf darajasiga mos qo‘shimcha tekshiruvlar joriy etish tavsiya etiladi. Bunda shaxsning roziligini tasdiqlash, mustaqil aloqa kanali orqali xabardor qilish va shubhali operatsiyalarni qayta tekshirish kabi usullar ko‘rib chiqilishi mumkin.

2. Shubhali kredit operatsiyalari bo‘yicha tezkor xabardor qilish tartibini kuchaytirish. Fuqaroga uning nomidan kredit arizasi berilgani yoki shartnoma rasmiylashtirilgani haqida imkon qadar tez xabar yetkazish firibgarlikni erta aniqlashga yordam berishi mumkin. Xabarnoma olish va e’tiroz bildirish jarayoni sodda hamda tushunarli bo‘lishi lozim.

3. Raqamli dalillarni saqlash va tekshirish tartiblarini takomillashtirish. Deepfake bilan bog‘liq ishlar yuzasidan asl faylni saqlash, faylning texnik xususiyatlarini qayd etish, o‘zgartirishlar tarixini tekshirish va ekspertiza o‘tkazish bo‘yicha amaliy tavsiyalar ishlab chiqish maqsadga muvofiq. Materialning sun’iy yaratilganini ko‘rsatuvchi texnik belgilarning mavjudligi yoki yo‘qligi boshqa dalillarni tekshirish zaruratini bekor qilmasligi kerak.

4. Jabrlanuvchilarning huquqlarini tiklash mexanizmlarini aniqlashtirish. Boshqa shaxs nomidan noqonuniy kredit rasmiylashtirilgan holatlarda arizani ko‘rib chiqish, kredit tashkilotidan tegishli hujjatlarni so‘rash, nizoli operatsiyalarni tekshirish va huquqiy himoya vositalaridan foydalanish tartibi bo‘yicha fuqarolarga tushunarli yo‘riqnomalar taqdim etish zarur.

5. Deepfake materiallari bilan bog‘liq huquqbuzarliklar bo‘yicha idoralararo hamkorlikni kuchaytirish. Huquqni muhofaza qiluvchi organlar, banklar, raqamli xizmat ko‘rsatuvchilar va shaxsga doir ma’lumotlarni himoya qilish sohasidagi vakolatli tuzilmalar o‘rtasida qonuniy axborot almashinuvi va dalillarni saqlash tartiblarini takomillashtirish lozim.

6. Sun’iy intellekt yordamida yaratilgan materiallarni belgilash mexanizmlarini o‘rganish. Xalqaro tajriba asosida sun’iy yaratilgan materiallarning kelib chiqishini aniqlashga yordam beradigan texnik belgilar va ixtiyoriy yoki majburiy oshkor qilish mexanizmlarini milliy sharoitga moslashtirish masalasini o‘rganish taklif etiladi. Bunday belgilar mutlaq ishonchli vosita deb qaralmasligi va boshqa tekshiruv usullarini almashtirmasligi kerak.

7. Huquqiy savodxonlik va profilaktikani kuchaytirish. Fuqarolarga shaxsiy fotosurat, video va ovoz yozuvlarini internetda tarqatish xavflari, shubhali xabarlarni tekshirish, hisob

ma’lumotlarini himoya qilish hamda tovlamachilik holatlarida dalillarni saqlash bo‘yicha tushuntirish ishlari olib borilishi lozim.

8. Maxsus huquqiy normalarga ehtiyojni tizimli baholash. Deepfake bilan bog‘liq barcha holatlar uchun alohida jinoyat tarkibini joriy etish masalasi mavjud qonun normalari qamrovi, amaliyotda uchrayotgan bo‘shliqlar va huquqni qo‘llash muammolari o‘rganilgandan keyin hal qilinishi kerak. Bunda texnologiyadan qonuniy foydalanish erkinligi va shaxs huquqlarini himoya qilish o‘rtasidagi muvozanat saqlanishi zarur.

Xulosa.

Sun’iy intellekt yordamida yuzaga keltiriladigan deepfake materiallari shaxsga doir ma’lumotlar daxlsizligi, shaxsiy hayot, mulkiy manfaatlar va jamoat ishonchi bilan bog‘liq yangi huquqiy muammolarni yuzaga keltirmoqda. Ayniqsa, shaxsning yuz yoki ovoziga taqlid qiluvchi materiallardan foydalanib kredit rasmiylashtirish, firibgarlik qilish yoki pul talab etish holatlari huquqiy himoya mexanizmlarini yanada takomillashtirish zaruratini ko‘rsatadi.

Tahlil natijasida O‘zbekiston qonunchiligida bunday holatlarning ayrim jihatlarini tartibga soluvchi huquqiy asoslar mavjudligi aniqlandi. Xususan, shaxsga doir ma’lumotlarni muhofaza qilish to‘g‘risidagi qonunchilik, Jinoyat kodeksining firibgarlik va tovlamachilikka oid normalari hamda 2026-yilda sun’iy intellektdan foydalanish bilan bog‘liq qabul qilingan qonunchilik o‘zgarishlari ushbu masalani o‘rganishda muhim ahamiyatga ega.

Shu bilan birga, huquqiy normalarning mavjudligi ularning amaliyotda samarali ishlashini o‘z-o‘zidan kafolatlamaydi. Buning uchun masofaviy identifikatsiyani mustahkamlash, raqamli dalillar bilan ishlash usullarini rivojlantirish, shubhali moliyaviy operatsiyalarni tezkor aniqlash va jabrlanuvchilarning huquqlarini tiklash mexanizmlarini takomillashtirish zarur.

Muallifning fikricha, deepfake bilan bog‘liq huquqbuzarliklarga qarshi kurashishning samarali modeli uchta yo‘nalishni birlashtirishi lozim: texnik profilaktika, mavjud qonunchilikni izchil qo‘llash va zarur hollarda normativ-huquqiy bazani takomillashtirish. Bunday yondashuv bir tomondan inson huquqlarini himoya qilishga, ikkinchi tomondan esa sun’iy intellekt texnologiyalaridan qonuniy va mas’uliyatli foydalanishni qo‘llab-quvvatlashga xizmat qiladi.

Foydalanilgan adabiyotlar

1. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. LexUZ. https://lex.uz/uz/docs/-4396419
2. O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeksi, 46²-modda. LexUZ. https://lex.uz/uz/acts/-97664
3. O‘zbekiston Respublikasining Jinoyat kodeksi, 141²-, 165- va 168-moddalar. LexUZ. https://lex.uz/uz/acts/-111453
4. O‘zbekiston Respublikasining 2026-yil 21-yanvardagi O‘RQ-1115-son “Sun’iy intellektni qo‘llash orqali yuzaga keladigan munosabatlarni tartibga solish munosabati bilan O‘zbekiston Respublikasining ayrim qonun hujjatlariga qo‘shimcha va o‘zgartirishlar kiritish to‘g‘risida”gi Qonuni. LexUZ. https://lex.uz/uz/docs/-8008401

5. O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi. “Sun’iy intellekt yordamida shaxsga doir ma’lumotlarga noqonuniy ishlov berganlik uchun javobgarlik belgilandi”. 21.01.2026. https://gov.uz/oz/digital/news/view/122739
6. European Parliament and Council of the European Union. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
7. European Commission. AI Act Service Desk. “Article 50: Transparency obligations for providers and deployers of certain AI systems”. https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-50
8. Council of Europe. Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. 2024. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence