Ilmiy tadqiqotlar va ularning yechimlari jurnali
Aoka guvohnoma № 323759 ISSN: 3060-4818

SUN'IY INTELLEKT TEXNOLOGIYALARINING HUQUQIY TARTIBGA SOLINISHI

Raxmonova Dinara Muxtorali qizi
Toshkent xalqaro universiteti (Tashkent International University)
Yurisprudensiya yo'nalishi, 3-bosqich talabasi
Email: dinararaxmonova55@gmail.com
Doi: https://doi.org/10.5281/zenodo.20099141

Annotatsiya: Ushbu maqola kiberxavfsizlik huquqi doirasida sun'iy intellekt (SI) texnologiyalarini tartibga solishning konseptual asoslarini o'rganishga bag'ishlangan. Tadqiqotning dolzarbligi SI tizimlarining kiberfazoda keng ko'lamli qo'llanilishi va buning natijasida yuzaga kelayotgan yangi turdagi huquqiy bo'shliqlar bilan belgilanadi. Maqolaning maqsadi — SI tizimlaridan xavfsiz foydalanishni ta'minlovchi huquqiy mexanizmlarni tahlil qilish va milliy qonunchilikni takomillashtirish bo'yicha ilmiy asoslangan takliflar ishlab chiqishdir.Tadqiqot jarayonida qiyosiy-huquqiy, mantiqiy va tizimli tahlil metodlaridan foydalanildi. Xususan, Yevropa Ittifoqining SI to'g'risidagi akti (AI Act) va xalqaro kiberxavfsizlik standartlari milliy huquqiy muhit bilan qiyoslandi. Natijada, SI algoritmlarining avtonomligi sababli yuzaga keladigan kiber-zararlar uchun huquqiy javobgarlikni taqsimlashning o'ziga xos xususiyatlari aniqlandi. Shuningdek, ma'lumotlar maxfiyligini ta'minlashda SIning roli va unga nisbatan qo'yiladigan texnik-huquqiy talablar tasniflandi.Muhokama qismida SIning "qora quti" (black box) muammosi va algoritmlarning shaffofligini ta'minlashning huquqiy kafolatlari ko'rib chiqiladi. Muallif tomonidan kiberxavfsizlik huquqiga "algoritmik javobgarlik" tushunchasini kiritish va SI tizimlarini kiber-bardoshli (cyber-resilient) holatga keltirish bo'yicha normativ talablarni qat'iylashtirish zaruriyati asoslangan.

Kalit so'zlar: Sun'iy intellect, Kiberxavfsizlik huquqi , Huquqiy tartibga solish , Algoritmik shaffoflik , Ma'lumotlar himoyasi , Kiberjavobgarlik , Raqamli qonunchilik , Kiberhujum

Kirish(introduction)

Insoniyat taraqqiyotining hozirgi bosqichida sun'iy intellekt (SI) texnologiyalari raqamli transformatsiyaning asosiy harakatlantiruvchi kuchiga aylandi. Iqtisodiyot, tibbiyot va ta'lim kabi sohalar qatori kiberxavfsizlik sohasi ham SI yordamida tubdan yangilanmoqda. Biroq, ushbu texnologik yutuqlar o'zi bilan birga an'anaviy huquqiy tizimlar uchun jiddiy chaqiriqlarni ham olib keldi. Kiberxavfsizlik huquqi doirasida sun'iy intellektni tartibga solish masalasi bugungi kunda nafaqat texnik, balki fundamental huquqiy muammo hisoblanadi. Chunki sun'iy intellekt tizimlari o'z-o'zini o'rgatish va avtonom qaror qabul qilish xususiyatiga ega bo'lib, bu jarayonlar ustidan inson nazoratining susayishi huquqiy javobgarlik masalasini murakkablashtirmoqda.

Kiberxavfsizlik huquqi sohasidagi asosiy muammo — sun'iy intellektning "ikki yoqlama foydalanish" (dual-use) tabiatidir. Bir tomondan, SI tizimlari kiberhujumlarni real vaqt rejimida aniqlash va ularga qarshi turishda samarali vosita bo'lsa, ikkinchi tomondan, kiberjinoyatchilar ushbu texnologiyalardan yanada murakkab va avtomatlashtirilgan hujumlarni amalga oshirishda foydalanmoqdalar. Bunday vaziyatda amaldagi normativ-huquqiy hujjatlar ko'pincha texnologik o'zgarishlar tezligiga moslasha olmayapti. "Huquqiy kechikish" (legal lag) hodisasi kiberfazoda tartibga solinmagan sohalarning ko'payishiga va natijada shaxsiy ma'lumotlar daxlsizligi hamda milliy xavfsizlikka tahdidlarning ortishiga olib kelmoqda.Ushbu maqolaning dolzarbligi sun'iy intellekt tizimlarining algoritmlari shaffof emasligi ("qora quti" effekti) va ularning kiberxavfsizlik talablariga muvofiqligini aniqlashning aniq huquqiy mezonlari mavjud emasligi bilan izohlanadi. Xalqaro miqyosda, xususan, Yevropa Ittifoqining Sun'iy intellekt to'g'risidagi akti (AI Act) kabi hujjatlar orqali ushbu sohani tartibga solishga urinishlar boshlangan bo'lsa-da, kiberjavobgarlik va raqamli etika

masalalari hali ham ochiq qolmoqda. O‘zbekiston sharoitida ham "Raqamli O‘zbekiston – 2030" strategiyasi doirasida SI texnologiyalarini joriy etish jadallashmoqda, biroq ularning kiberxavfsizlik huquqi prizmasidagi o‘rni tizimli ravishda tadqiq etilmagan.Mazkur maqolaning maqsadi sun’iy intellekt texnologiyalarini kiberxavfsizlik huquqi doirasida tartibga solishning nazariy va amaliy jihatlarini tahlil qilishdan iborat. Tadqiqot davomida SI tizimlaridan foydalanishda yuzaga keladigan huquqiy risklarni tasniflash, xalqaro tajribani o‘rganish va milliy qonunchilikni modernizatsiya qilish bo‘yicha tavsiyalar ishlab chiqish ko‘zda tutilgan. Shuningdek, maqolada SI sub’yektlarining (ishlab chiquvchi, operator va foydalanuvchi) huquqiy maqomi va kiber-hujumlar oqibatida yetkazilgan zarar uchun javobgarlik masalalari ilmiy tahlil qilinadi.

Metodlar (methods)

Ushbu maqolada sun’iy intellekt (SI) texnologiyalarini kiberxavfsizlik huquqi doirasida tartibga solishning huquqiy mexanizmlarini o‘rganish uchun kompleks metodologik yondashuvdan foydalanildi. Tadqiqotning metodologik asosi sifatida huquqiy voqelikni ob’ektiv tahlil qilish imkonini beruvchi umumilmiy va maxsus usullar tanlab olindi. Mazkur yondashuv kiberfazodagi murakkab texnologik jarayonlarni huquq normalari bilan o‘zaro bog‘liqlikda ko‘rib chiqishga xizmat qiladi.

Tadqiqotning eng muhim metodlaridan biri qiyosiy-huquqiy tahlil (comparative legal analysis) metodidir. Ushbu metod yordamida sun’iy intellektni tartibga solish bo‘yicha xalqaro tajriba, xususan, Yevropa Ittifoqining "Sun’iy intellekt to‘g‘risidagi akti" (EU AI Act), AQShning SI xavfsizligi bo‘yicha ijroiya farmonlari va Xitoyning algoritmik boshqaruvga oid qonunchiligi o‘rganildi. Ushbu xalqaro model va standartlar O‘zbekiston Respublikasining "Kiberxavfsizlik to‘g‘risida"gi qonuni va boshqa sohaviy normativ-huquqiy hujjatlar bilan qiyoslandi. Bu esa milliy qonunchilikdagi huquqiy bo‘shliqlarni aniqlash va xalqaro ilg‘or tajribani milliy manfaatlarni hisobga olgan holda adaptatsiya qilish imkonini berdi.

Ikkinchi asosiy metod sifatida tizimli-strukturaviy tahlil (system-structural analysis) qo‘llanildi. Sun’iy intellekt texnologiyalari kiberxavfsizlik huquqining sub’ekti va ob’ekti sifatida yaxlit bir tizim sifatida ko‘rib chiqildi. Bunda SI tizimlarining hayotiy sikli — ma’lumotlarni yig‘ish, algoritmlarni o‘rgatish, amaliyotga joriy etish va natijalarni nazorat qilish bosqichlarining har biri huquqiy nuqtayi nazardan tahlil qilindi. Ushbu metod SI tizimlaridagi "qora quti" muammosini huquqiy shaffoflik tamoyillari bilan bog‘lashga va har bir bosqichda kiberxavfsizlik talablarining bajarilishini tekshirish mexanizmlarini ishlab chiqishga yordam berdi.Shuningdek, tadqiqotda riskka asoslangan yondashuv (risk-based approach) metodologiyasi qo‘llanildi. Kiberxavfsizlik huquqida barcha SI tizimlariga bir xil talab qo‘yish innovatsiyalar rivojiga to‘sqinlik qilishi mumkinligini hisobga olib, SI texnologiyalari ulardan kelib chiqadigan potensial xavf darajasiga ko‘ra (past, o‘rta, yuqori va nomaqbul) toifalarga ajratildi. Ushbu tasniflash metodikasi orqali har bir toifa uchun alohida kiberxavfsizlik protokollari va huquqiy javobgarlik choralari belgilanishi zarurligi asoslab berildi.

Tadqiqot davomida mantiqiy-huquqiy interpretatsiya (legal interpretation) va deduksiya usullaridan ham foydalanildi. Amaldagi huquq normalarining sun’iy intellekt tomonidan sodir etilishi mumkin bo‘lgan kiber-jinoyatlarga nisbatan qo‘llanilishi nazariy jihatdan modellashtirildi. Xususan, "sub’yektiv javobgarlik" tushunchasining avtonom algoritmlarga nisbatan transformatsiyasi mantiqiy xulosalar orqali yoritildi. Ma’lumotlar bazasi sifatida kiberxavfsizlik bo‘yicha xalqaro hisobotlar, sud amaliyoti namunalari va texnik standartlar (masalan, ISO/IEC 42001) tahlilga tortildi.

Yakuniy bosqichda, olingan natijalarni umumlashtirish uchun prognostika (prognostic) metodi qo‘llanildi. Bu metod kelajakda SI texnologiyalari rivojlanishi natijasida kiberxavfsizlik huquqida yuzaga kelishi kutilayotgan yangi tahdidlarni (masalan, kvant hisoblash tizimlari bilan integratsiyalashgan SI) oldindan ko‘rish va ularga qarshi preventiv huquqiy choralar ishlab chiqish imkonini berdi. Jami metodlar majmui tadqiqotning har tomonlama asoslanishini va xulosalarning ilmiy qimmatini ta’minladi.

Natijalar (results)

Ushbu maqola doirasida amalga oshirilgan tahlillar sun’iy intellekt (SI) tizimlarini kiberxavfsizlik huquqi nuqtayi nazaridan tartibga solishning bir qancha ustuvor yo‘nalishlarini ko‘rsatib berdi. Birinchi navbatda, xalqaro huquqiy hujjatlar va milliy qonunchilik bazasini qiyosiy o‘rganish natijasida SI tizimlarining xavflilik darajasi bo‘yicha huquqiy tasnifi ishlab chiqildi. Maqola natijalari shuni ko‘rsatadiki, SI texnologiyalarini tartibga solishda "unifikatsiyalashgan yondashuv" samarasiz bo‘lib, har bir tizimning kiberfazoga ta’sir darajasidan kelib chiqib alohida huquqiy rejimlar o‘rnatish zarur.

Maqolada aniqlangan eng muhim natijalardan biri — kiberxavfsizlikni ta’minlashda SI sub’yektlari o‘rtasidagi huquqiy mas’uliyatning taqsimlanishidir. Tahlillar shuni tasdiqladiki, kiberhujum yoki ma’lumotlar sizib chiqishi holatlarida an’anaviy "ayb" tushunchasi SI algoritmlarining avtonomligi sababli o‘zgarishga uchraydi. Shunga ko‘ra, maqola doirasida SI tizimlarining hayotiy siklidagi ishtirokchilar uchun majburiy kiberxavfsizlik mezonlari belgilandi.

Quyidagi jadvalda maqola davomida ishlab chiqilgan, SI tizimlarining kiberxavfsizlik xavfi darajalari va ularga nisbatan taklif etilayotgan huquqiy choralar aks ettirilgan:

1-jadval. SI tizimlarining kiberxavfsizlik xavfi darajalari va huquqiy tartibga solish mexanizmlari

Xavf darajasi	**Tizim misoli**	**Huquqiy talab va nazorat choralari**	**Kiberjavobgarlik sub’yekti**
Nomaqbul xavf	Ijtimoiy reyting tizimlari, manipulyativ SI	To‘liq taqiqlash, foydalanishga yo‘l qo‘ymaslik	Ishlab chiquvchi va buyurtmachi
Yuqori xavf	Kritik infratuzilmani boshqarish, biometrik identifikatsiya	Majburiy kiber-audit, algoritmik shaffoflik sertifikati	Operator va nazorat qiluvchi
Cheklangan xavf	Chat-botlar, tavsiya beruvchi algoritmlar	Shaffoflik majburiyati (SI ekanligini bildirish)	Foydalanuvchi va provayder
Minimal xavf	Spam-filtrlar, videoo‘yinlardagi SI	Ixtiyoriy axloq kodekslari va umumiy standartlar	Umumiy fuqarolik javobgarligi

Natijalari shuni tasdiqlaydiki, yuqori xavfli tizimlar uchun kiberxavfsizlik talablarini buzish oqibatida yetkazilgan zarar uchun "ob’ektiv javobgarlik" (strict liability) modelini qo‘llash maqsadga muvofiqdir. Bu model zarar yetkazilganda aybning mavjudligidan qat’i nazar, SI tizimining egasi yoki operatori javobgarligini nazarda tutadi, bu esa jabrlanuvchilarning huquqlarini himoya qilishda samarali vositadir.Bundan tashqari, maqolada O‘zbekiston kiberxavfsizlik qonunchiligiga "algoritmik javobgarlik" tushunchasini kiritish bo‘yicha huquqiy konstruksiya yaratildi. Bu konstruksiya SI tomonidan sodir etilgan kiberhujumlarni tergov qilishda raqamli dalillarni to‘plash va algoritmlarning ishlash mantig‘ini huquqiy ekspertizadan o‘tkazish tartibini belgilaydi. Shuningdek, ma’lumotlar bazasining daxlsizligini ta’minlash maqsadida SIning "privacy-by-design" (loyihalashda maxfiylik) prinsipi huquqiy majburiyat sifatida taklif etildi.

Muhokama (discussion)

Ushbu maqola doirasida aniqlangan natijalar kiberxavfsizlik huquqi sohasidagi bir qator fundamental va zamonaviy bahslarni yuzaga chiqaradi. Eng avvalo, sun’iy intellekt (SI) tizimlarini huquqiy tartibga solishda innovatsiyalarni qo‘llab-quvvatlash va xavfsizlikni ta’minlash o‘rtasidagi muvozanat masalasi markaziy o‘rinda turadi. Maqolada ilgari surilgan riskka asoslangan yondashuv

(risk-based approach) Yevropa Ittifoqining tajribasiga tayansa-da, milliy qonunchilikning o‘ziga xos xususiyatlarini hisobga olgan holda o‘zgartirilishi lozimligi muhokama qilinadi.

Muhokamaning asosiy nuqtalaridan biri — SI algoritmlarining "shaffofligi" va "tushuntirilishi" (explainability) muammosidir. Maqola natijalari shuni ko‘rsatadiki, agar SI tizimi kiberhujumni amalga oshirsa yoki muhim infratuzilmaga zarar yetkazsa, uning qaror qabul qilish jarayonini huquqiy tilda "tarjima qilish" deyarli imkonsizdir. Bu borada huquqshunos olimlar o‘rtasida ikki xil yondashuv mavjud: bir guruh olimlar SIni "elektron shaxs" sifatida tan olishni taklif qilsa, boshqalari (jumladan, ushbu maqola muallifi ham) javobgarlikni faqat inson sub’yektlariga — ishlab chiquvchi yoki operatorga yuklash tarafdoridir. SIni huquq sub’yekti sifatida tan olish kiberjinoyatchilikka qarshi kurashda javobgarlikdan qochish uchun "huquqiy qalqon" bo‘lib xizmat qilishi mumkin, bu esa kiberxavfsizlik prinsiplariga zid keladi.Shuningdek, maqolada taklif etilgan "ob’ektiv javobgarlik" (strict liability) modeli kiberxavfsizlik huquqining klassik tamoyillarini qayta ko‘rib chiqishni talab qiladi. An’anaviy huquqda zarar uchun ayb isbotlanishi shart bo‘lsa, SI kontekstida zarar algoritmlarning kutilmagan kombinatsiyasi natijasida yuzaga kelishi mumkin. Muhokama jarayonida shunday xulosaga kelindiki, yuqori xavfli SI tizimlaridan foydalanuvchi tashkilotlar uchun majburiy kiber-sug‘urtalash tizimini joriy etish zarur. Bu nafaqat yetkazilgan zararni qoplash, balki SI bozorida xavfsizlik standartlarini oshirishga xizmat qiladi.

Maqolaning yana bir muhim jihati — ma’lumotlar daxlsizligi bilan bog‘liq. SI tizimlari kiberxavfsizlikni ta’minlash uchun ulkan hajmdagi shaxsiy ma’lumotlarni qayta ishlaydi. Bu jarayonda "xavfsizlik uchun maxfiylikni qurbon qilish" dilemmasi yuzaga keladi. Muhokamada ta’kidlanishicha, O‘zbekiston qonunchiligida "privacy-by-design" (loyihalash bosqichida maxfiylik) tamoyilini majburiy etib belgilash kiber-tahdidlarning oldini olishda eng samarali profilaktik chora bo‘ladi.Bundan tashqari, kiberxavfsizlik huquqida "huquqiy qumloqlar" (regulatory sandboxes) rejimini joriy etish masalasi ham alohida e’tiborga loyiq. Maqola doirasida o‘tkazilgan tahlillar shuni ko‘rsatadiki, bunday rejimlar davlat nazorati ostida SI tizimlarini xavfsiz sinovdan o‘tkazish imkonini beradi. Bu esa kiber-xatarlarni oldindan prognoz qilish va huquqiy normalarni texnologiyaga mos ravishda "jonli" tarzda ishlab chiqishga sharoit yaratadi.

Xulosa (conclusion)

Sun’iy intellekt (SI) texnologiyalarining kiberxavfsizlik sohasiga integratsiyalashuvi raqamli huquqning yangi evolyutsion bosqichini boshlab berdi. Ushbu maqola doirasida o‘tkazilgan tahlillar shuni ko‘rsatadiki, SI tizimlarini huquqiy tartibga solish endilikda shunchaki tavsiyaviy xarakterga ega bo‘la olmaydi; u milliy kiberxavfsizlik strategiyasining fundamental asosiga aylanishi shart. Maqola davomida ko‘rib chiqilgan masalalar SI texnologiyalarining avtonomligi va "qora quti" effekti an’anaviy kiberjavobgarlik institutlarini isloh qilish zaruriyatini tug‘dirayotganini tasdiqladi.

Maqolaning asosiy xulosasi sifatida ta’kidlash lozimki, kiberxavfsizlik huquqida "riskka asoslangan yondashuv"ni joriy etish eng samarali yo‘ldir. Bu yondashuv innovatsiyalarni bo‘g‘ib qo‘ymagan holda, inson huquqlari va kritik infratuzilma xavfsizligiga tahdid soluvchi yuqori xavfli tizimlarni qat’iy nazorat ostiga olish imkonini beradi. Shuningdek, maqola natijalari shuni ko‘rsatdiki, SI tomonidan sodir etilgan kiber-zararlar uchun "ob’ektiv javobgarlik" modelini qo‘llash va kiber-sug‘urtalash tizimini joriy etish huquqiy himoyaning eng maqbul mexanizmlari hisoblanadi.

O‘zbekiston Respublikasi qonunchiligini takomillashtirish nuqtayi nazaridan, "Kiberxavfsizlik to‘g‘risida"gi qonun hujjatlariga SI tizimlarining algoritmik shaffofligi va kiber-bardoshliligi (cyber-resilience) bo‘yicha maxsus moddalarni kiritish taklif etiladi. Maqolada asoslanganidek, SI sub’ektlari (ishlab chiquvchi, operator, foydalanuvchi) o‘rtasida javobgarlikning aniq chegaralarini belgilash kiber-jinoyatlarni tergov qilish samaradorligini oshiradi. Bundan tashqari, "huquqiy qumloqlar" (regulatory sandboxes) rejimini joriy etish yangi texnologiyalarni huquqiy vakuumda qolib ketishidan asraydi.

Maqolaning natijalari va muhokama qismidan kelib chiqib, kiberxavfsizlik huquqi doirasida sun’iy intellektni tartibga solish bo‘yicha quyidagi 7 ta tavsiyani taklif etamiz:

1. Riskka asoslangan huquqiy klassifikatsiyani joriy etish: SI tizimlarini kiberxavfsizlikka soladigan xavf darajasiga ko‘ra (nomaqbul, yuqori, cheklangan va minimal) toifalarga ajratish va har bir toifa uchun alohida huquqiy rejim hamda texnik talablar belgilash lozim.
2. Algoritmik shaffoflik va "tushuntirilishi" majburiyatini yuklash: Yuqori xavfli SI tizimlaridan foydalanuvchi tashkilotlar uchun algoritmlarning qaror qabul qilish mantig‘ini shaffof qilish va kiber-auditdan o‘tkazish majburiyatini qonunchilikda mustahkamlash zarur.
3. "Privacy-by-Design" (Loyihalashda maxfiylik) tamoyilini qat’iylashtirish: SI tizimlarini ishlab chiqishning ilk bosqichidan boshlab shaxsiy ma’lumotlar himoyasi va kiber-bardoshlilik (cyber-resilience) mexanizmlarini texnik arxitekturaga integratsiya qilishni huquqiy norma sifatida belgilash lozim.
4. Kiberjavobgarlikning aniq sub’yektlarini belgilash: SI tomonidan sodir etilgan kiberhujumlar yoki zararli harakatlar uchun javobgarlikni "ishlab chiquvchi – operator – foydalanuvchi" zanjiri bo‘yicha aniq taqsimlash va "ob’ektiv javobgarlik" (strict liability) modelini joriy etish.
5. Majburiy kiber-sug‘urtalash tizimini yo‘lga qo‘yish: Yuqori xavfli SI tizimlarini amaliyotga joriy etuvchi sub’yektlar uchun kiber-tahdidlar natijasida yetkazilishi mumkin bo‘lgan zararni qoplash maqsadida majburiy sug‘urta polislari tizimini ishlab chiqish.
6. "Regulatory Sandboxes" (Huquqiy qumloqlar) rejimini tashkil etish: Yangi SI texnologiyalarini real vaqt rejimida, lekin cheklangan va nazorat ostidagi huquqiy muhitda sinovdan o‘tkazish mexanizmini yaratish orqali innovatsiyalar va xavfsizlik o‘rtasidagi muvozanatni ta’minlash.
7. Kiber-etika va xatti-harakatlar kodeksini ishlab chiqish: SI tizimlarini yaratuvchi muhandislar va ulardan foydalanuvchi tashkilotlar uchun kiberxavfsizlikning axloqiy standartlarini o‘z ichiga olgan milliy "SI etikasi va xavfsizligi kodeksi"ni qabul qilish.

Ushbu tavsiyalar maqolaning ilmiy va amaliy qiymatini oshirishga xizmat qiladi.

Yakuniy xulosa qilib aytganda, sun’iy intellekt texnologiyalarining huquqiy tartibga solinishi kiberfazoda texnologik suverenitetni ta’minlashning muhim kafolatidir. Ushbu maqolada ilgari surilgan taklif va tavsiyalar raqamli makonda xavfsiz, ishonchli va inson manfaatlariga xizmat qiluvchi SI ekotizimini yaratish uchun huquqiy poydevor bo‘lib xizmat qilishi kutilmoqda.

Adabiyotlar ro‘yxati (references)

O‘zbekiston Respublikasi normativ-huquqiy hujjatlari:

1. O‘zbekiston Respublikasining Qonuni. *Sun’iy intellektdan foydalanishdan kelib chiqadigan munosabatlarni tartibga solish munosabati bilan O‘zbekiston Respublikasining ayrim qonun hujjatlariga o‘zgartish va qo‘shimchalar kiritish to‘g‘risida.* (O‘RQ-1115-son, 2026-yil 21-yanvarda kuchga kirgan).
2. O‘zbekiston Respublikasi Prezidentining Qarori. *Sun’iy intellekt texnologiyalarini rivojlantirish hamda tartibga solish bo‘yicha normativ-huquqiy hujjatlar bazasini shakllantirish chora-tadbirlari to‘g‘risida.* (PQ-358-son, 14.10.2024).
3. O‘zbekiston Respublikasi Adliya vazirligi. *Sun’iy intellekt texnologiyalarini ishlab chiqish va qo‘llashdagi etika qoidalari va tamoyillari.* (2026-yil 17-iyundan kuchga kiradi).
4. Xalqaro va xorijiy adabiyotlar (2023–2026):
5. European Union. *The Artificial Intelligence Act (Regulation (EU) 2024/1689).* (2024-yil 1-avgustda kuchga kirgan).
6. Marwala, T., & Mpedi, L. G. *Artificial Intelligence and the Law.* Springer Nature, 2024. ISBN: 9819728266.
7. Wolters Kluwer. *International Handbook of AI Law: A Guide to Understanding and Resolving Legal Questions.* November 2024.

8. Calvi, A. *Data Protection Impact Assessment under the EU General Data Protection Regulation: A feminist reflection.* Computer Law & Security Review, Volume 53, 2024.

Veb-saytlar va elektron manbalar:

9. EU Artificial Intelligence Act Platform. *Up-to-date developments and implementation timeline.* https://artificialintelligenceact.eu/ (2026-yilgi yangilanishlar bilan).
10. Lex.uz – O‘zbekiston Respublikasi Qonunchilik ma’lumotlari milliy bazasi. *Sun’iy intellektga oid so‘nggi normativ hujjatlar to‘plami.* https://lex.uz/docs/-7158604. [1, 2]