НОВАЯ ЭРА НАУКИ И ЗНАНИЙ
МЕЖДУНАРОДНЫЙ НАУЧНЫЙ ЖУРНАЛ
global-science-review.com
editor@global-science-review.com

# JAMOAT XAVFSIZLIGINI TA’MINLASHDA SUN’IY INTELLEKT VA RAQAMLI MONITORING TEXNOLOGIYALARIDAN FOYDALANISHNING HUQUQIY ASOSLARI

# ПРАВОВЫЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ТЕХНОЛОГИЙ ЦИФРОВОГО МОНИТОРИНГА В ОБЕСПЕЧЕНИИ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

# LEGAL FRAMEWORK FOR THE USE OF ARTIFICIAL INTELLIGENCE AND DIGITAL MONITORING TECHNOLOGIES IN ENSURING PUBLIC SAFETY

**ERGASHEV JAHONGIR UMARALI O‘G‘LI**

*Jamoat xavfsizligi universiteti talabasi*

**Annotatsiya:** Mazkur maqolada jamoat xavfsizligini ta’minlash jarayoniga sun’iy intellekt, intellektual videokuzatuv, prediktiv tahlil va raqamli monitoring tizimlarini joriy etishning konstitutsiyaviy-huquqiy, tashkiliy hamda protsessual asoslari tadqiq etiladi. O‘zbekiston qonunchiligi, raqamli transformatsiya strategiyalari va xorijiy tartibga solish tajribasi qiyosiy tahlil qilinadi. Algoritmik xatolik, shaxsga doir ma’lumotlarning daxlsizligi, inson nazorati, kamsitmaslik, shaffoflik va huquqiy javobgarlik masalalari o‘rtasidagi uzviy bog‘liqlik asoslanadi. Jamoat xavfsizligi uchun xavfga mutanosib tartibga solish modeli va mustaqil audit mexanizmlariga oid takliflar ilgari surilgan.

**Kalit so‘zlar:** jamoat xavfsizligi, sun’iy intellekt, raqamli monitoring, intellektual videokuzatuv, shaxsga doir ma’lumotlar, biometrik identifikatsiya, algoritmik javobgarlik, inson huquqlari, huquqbuzarliklar profilaktikasi.

**Аннотация:** В данной статье исследуются конституционно-правовые, организационные и процессуальные основы внедрения искусственного интеллекта, интеллектуального видеонаблюдения, предиктивного анализа и систем цифрового мониторинга в процесс обеспечения общественной

безопасности. Проводится сравнительный анализ законодательства Республики Узбекистан, стратегий цифровой трансформации и зарубежного опыта правового регулирования. Обосновывается взаимосвязь вопросов алгоритмических ошибок, неприкосновенности персональных данных, человеческого контроля, недискриминации, прозрачности и юридической ответственности. Выдвигаются предложения по разработке модели правового регулирования, соразмерной рискам в сфере обеспечения общественной безопасности, а также по внедрению механизмов независимого аудита.

**Ключевые слова:** общественная безопасность, искусственный интеллект, цифровой мониторинг, интеллектуальное видеонаблюдение, персональные данные, биометрическая идентификация, алгоритмическая ответственность, права человека, профилактика правонарушений.

**Abstract:** This article examines the constitutional, legal, organizational, and procedural foundations for integrating artificial intelligence, intelligent video surveillance, predictive analytics, and digital monitoring systems into public safety operations. It provides a comparative analysis of the legislation of the Republic of Uzbekistan, digital transformation strategies, and international approaches to legal regulation. The article substantiates the interrelationship between algorithmic errors, personal data privacy, human oversight, non-discrimination, transparency, and legal accountability. It puts forward proposals for developing a risk-proportionate regulatory framework for public safety and introducing independent audit mechanisms.

**Keywords:** public safety, artificial intelligence, digital monitoring, intelligent video surveillance, personal data, biometric identification, algorithmic accountability, human rights, crime prevention.

Zamonaviy jamiyatda jamoat xavfsizligini ta’minlash faqat sodir etilgan huquqbuzarlikka munosabat bildirish bilan chegaralanmaydi. Axborot oqimining tezlashuvi, shahar infratuzilmasining murakkablashuvi va raqamli muhitdagi

tahdidlarning ko‘payishi xavfni erta aniqlash, holatni baholash va vakolatli organlar faoliyatini muvofiqlashtirishning yangi vositalarini talab etmoqda. Bunday sharoitda sun’iy intellekt texnologiyalari davlatning profilaktik imkoniyatlarini kengaytirishi mumkin, biroq ularning qo‘llanishi qonuniylik va inson huquqlari kafolatlaridan ajralgan holda baholanishi mumkin emas [1; 2].

Jamoat xavfsizligi sohasida raqamli monitoring deganda kuzatuv vositalari, sensorlar, videokameralar, axborot tizimlari va tahliliy dasturlar orqali jamoat makonidagi vaziyat to‘g‘risida ma’lumotlarni yig‘ish, uzatish, tizimlashtirish va tahlil qilish jarayoni tushuniladi. Sun’iy intellekt esa ushbu jarayonda ma’lumotlar orasidagi qonuniyatlarni aniqlash, xavf signallarini ajratish yoki inson tomonidan qabul qilinadigan qarorlarni axborot bilan qo‘llab-quvvatlashga xizmat qiladi. Muhimi, oddiy videoyozuv, avtomatlashtirilgan qoidaviy signal va mashinaviy o‘qitish asosidagi baholash bir xil huquqiy xavf tug‘dirmaydi; ularni bitta tartibga solish rejimiga kiritish metodologik jihatdan to‘g‘ri emas [5].

O‘zbekiston Respublikasi Konstitutsiyasi insonning sha’ni va qadr-qimmati, shaxsiy hayoti daxlsizligi, shaxsga doir ma’lumotlarning himoyasi va davlat organlari faoliyatining qonuniyligi uchun asosiy mezonlarni belgilaydi. Shu sababli xavfsizlikni kuchaytirish maqsadi har qanday ma’lumot yig‘ish yoki har qanday avtomatlashtirilgan xulosani oqlovchi cheksiz vakolat sifatida talqin qilinmasligi lozim. Har bir aralashuv qonuniy asosga, aniq maqsadga, zaruratga va mutanosiblikka ega bo‘lishi kerak [1].

O‘zbekiston Respublikasi Prezidentining 2021-yil 29-noyabrdagi PF-27-son Farmoni bilan tasdiqlangan Jamoat xavfsizligi konsepsiyasi va 2022–2025-yillarga mo‘ljallangan strategiya zamonaviy axborot texnologiyalarini joriy etish, faoliyatni raqamlashtirish va idoralararo muvofiqlashtirishga e’tibor qaratgan. Mazkur strategiyada tizimni raqamlashtirishni 90 foizga yetkazish maqsadi qayd etilgan. Biroq ushbu ko‘rsatkich dasturiy maqsad bo‘lib, uning amalda erishilgan natija

ekanini anglatmaydi; 2022–2025-yillarga mo‘ljallangan hujjatni 2026-yildagi yangi reja sifatida ko‘rsatish ham to‘g‘ri emas [2].

Prezidentning 2024-yil 14-oktabrdagi PQ-358-son qarori bilan tasdiqlangan Sun’iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasi sun’iy intellektning huquqiy, texnologik va iqtisodiy asoslarini shakllantirishga qaratilgan. Strategiyada intellektual videotahlil, nutqni tanib olish va qarorlarni intellektual qo‘llab-quvvatlash singari texnologiyalar tilga olinadi. Shu o‘rinda ta’kidlash lozimki, umumiy texnologik rivojlanish strategiyasi muayyan shaxsni biometrik aniqlash yoki unga nisbatan majburlov chorasi qo‘llash uchun o‘z-o‘zidan yetarli protsessual vakolat yaratmaydi [5].

Jamoat xavfsizligida sun’iy intellektning amaliy qo‘llanishini shartli ravishda uch darajaga ajratish mumkin. Birinchi daraja — transport oqimi, gavjumlik va favqulodda holat belgilarini shaxsni aniqlamasdan kuzatish. Ikkinchi daraja — ehtimoliy xavfli vaziyatlarni, masalan, tashlab ketilgan buyum yoki keskin zichlashuvni operatorga signal sifatida ko‘rsatish. Uchinchi daraja — muayyan shaxsni aniqlash, harakat trayektoriyasini tiklash yoki shaxsga nisbatan xavf ballini shakllantirish. Aynan uchinchi darajada shaxsiy hayot, tenglik va erkin harakatlanish huquqlariga aralashuv ehtimoli eng yuqori bo‘ladi.

Mazkur tasnifning ilmiy ahamiyati shundaki, u texnologiya nomiga emas, uning huquqiy oqibatiga qarab nazorat intensivligini belgilashga imkon beradi. Masalan, chorrahada transport tirbandligini aniqlovchi tizim bilan biror fuqaroning yuz tasvirini doimiy ravishda identifikatsiya qiluvchi tizimga bir xil talab qo‘yish oqilona emas. Birinchisida ma’lumotlarni minimallashtirish va texnik xavfsizlik yetakchi bo‘lsa, ikkinchisida aniq qonuniy vakolat, qat’iy foydalanish chegarasi, kuchaytirilgan audit va shikoyat mexanizmlari zarur.

2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun ma’lumotlarga ishlov berishning asosiy huquqiy doirasini belgilaydi. Videokuzatuv ma’lumotlari shaxsni bevosita yoki bilvosita aniqlash imkonini

bergan taqdirda shaxsga doir ma’lumotlar bilan bog‘liq talablar dolzarb bo‘ladi. Biometrik xususiyatlar bilan ishlash esa yanada ehtiyotkor yondashuvni talab qiladi. Ma’lumotni olishning qonuniyligi uni istalgan muddat saqlash, boshqa maqsadda ishlatish yoki cheklanmagan doirada almashish huquqini anglatmaydi [3].

Raqamli monitoring tizimida ma’lumotlarning butun hayotiy sikli huquqiy tartibga solinishi zarur: dastlabki yig‘ish, saralash, belgilash, saqlash, uchinchi tomonga berish, algoritmni o‘qitishda ishlatish, arxivlash va yo‘q qilish. Har bir bosqichda mas’ul subyekt, huquqiy asos, kirish darajasi va qayd jurnali aniqlashtirilmasa, tashqi tomondan xavfsiz ko‘ringan tizim ham huquqiy noaniqlik manbaiga aylanadi. Ayniqsa, bir maqsadda olingan videotasvirni boshqa idoraning mos kelmaydigan maqsadi uchun ishlatish alohida huquqiy tekshiruvdan o‘tishi lozim.

Algoritmik xatolik muammosi nazariy ehtimol bilan cheklanmaydi. Yuzni tanish tizimi tasvir sifati, yorug‘lik, kamera burchagi va ma’lumotlar bazasining tarkibiga bog‘liq holda noto‘g‘ri moslik berishi mumkin. Bunday natija “shaxs aniqlangan” degan huquqiy xulosa emas, balki vakolatli xodim tekshirishi lozim bo‘lgan texnik signal sifatida ko‘rilishi kerak. Aks holda xato ijobiy natija asossiz to‘xtatish, tekshirish yoki shaxs sha’niga zarar yetkazish xavfini kuchaytiradi [8].

Tadqiqot natijalari shuni ko‘rsatdiki, sun’iy intellektga asoslangan monitoringning eng muhim muammosi faqat algoritm aniqligi emas, balki qaror zanjiridagi mas’uliyatni to‘g‘ri taqsimlashdir. Dasturchi modelni yaratadi, texnik operator tizimni yuritadi, davlat organi undan foydalanish maqsadini belgilaydi, mansabdor shaxs esa yakuniy huquqiy qarorni qabul qiladi. Ushbu rollar aralashib ketganda fuqaro noto‘g‘ri qaror uchun kimga murojaat qilishini aniqlashda qiynaladi. Shu bois algoritmik yordam va davlatning yuridik ahamiyatga ega qarori o‘rtasida aniq chegara saqlanishi lozim.

Xalqaro tajribada xavfga asoslangan tartibga solish alohida o‘rin tutadi. Yevropa Ittifoqining 2024/1689-sonli Sun’iy intellekt to‘g‘risidagi reglamenti

muayyan sun’iy intellekt tizimlari uchun risk darajasiga qarab majburiyatlar belgilaydi, ayrim biometrik amaliyotlarga nisbatan esa alohida cheklovlar nazarda tutadi. Bu hujjat O‘zbekistonda bevosita amal qiladigan qonun emas, biroq xavfli texnologiyalarni differensial nazorat qilish uchun qiyosiy-huquqiy model bo‘la oladi [7].

Yevropa Kengashining inson huquqlari, demokratiya va qonun ustuvorligi doirasida sun’iy intellektga oid 2024-yilgi Ramka konvensiyasi ham texnologik boshqaruvni fundamental huquqlar bilan bog‘lash zarurligini aks ettiradi. Mazkur hujjatni barcha davlatlar uchun bir xil darajada majburiy deb talqin etish mumkin emas: uning tatbiqi ishtirokchilik va tegishli xalqaro-huquqiy shartlarga bog‘liq. Shunga qaramay, inson huquqlariga ta’sirni baholash va javobgarlikni institutsionallashtirish tamoyillari milliy muhokama uchun foydalidir [9].

Birlashgan Millatlar Tashkilotining UNESCO tomonidan 2021-yilda qabul qilingan Sun’iy intellekt etikasi bo‘yicha tavsiyasida inson huquqlarini hurmat qilish, mutanosiblik, xavfsizlik, adolatlilik va hisobdorlik masalalari muhim o‘rin egallaydi. Tavsiya qonun bilan bir xil yuridik kuchga ega bo‘lmasa-da, davlat organlari uchun ichki etik standartlar, xarid talablari va mutaxassislar tayyorlash dasturlarini ishlab chiqishda konseptual tayanch vazifasini o‘tashi mumkin [10].

Shu o‘rinda ta’kidlash lozimki, “prediktiv politsiya” atamasi ostida bir-biridan farqli yondashuvlar birlashtiriladi. Hududiy hodisalar statistikasi asosida patrul resurslarini taqsimlash bilan shaxsning kelgusida jinoyat sodir etish ehtimolini hisoblash huquqiy jihatdan teng emas. Birinchi holatda ham tarixiy ma’lumotlar noto‘g‘ri yoki notekis bo‘lishi mumkin; ikkinchi holatda esa aybsizlik prezumpsiyasi, kamsitmaslik va individual javobgarlik bilan bog‘liq xavflar keskin kuchayadi. Statistik korrelyatsiya shaxsning aybi yoki huquqbuzarlik sodir etganini isbotlamaydi.

Raqamli tizimlar uchun “inson nazorati” shunchaki ekranda operator mavjudligini anglatmasligi kerak. Samarali nazorat uchun xodim algoritm chiqargan

natijaning cheklovlarini tushunishi, unga e’tiroz bildira olishi, qarorni to‘xtatish vakolatiga ega bo‘lishi va o‘z harakatining sababini hujjatlashtirishi zarur. Tizim tomonidan berilgan tavsiya amalda avtomatik buyruqqa aylanib qolsa, inson ishtiroki faqat rasmiy ko‘rinishga ega bo‘ladi.

Jamoat xavfsizligida qo‘llanadigan algoritmlarning huquqiy ekspertizasi loyiha foydalanishga topshirilgandan keyin emas, xarid va loyihalash bosqichidan boshlanishi lozim. Texnik topshiriqda maqsadning aniqligi, foydalaniladigan ma’lumotlar toifasi, sinov mezonlari, xato ko‘rsatkichlari, kiberxavfsizlik, audit izi, ma’lumotni o‘chirish imkoniyati va yetkazib beruvchining javobgarligi oldindan ko‘rsatilishi zarur. Shartnomadagi tijorat siri davlat organini fuqaro huquqlarini himoya qilish majburiyatidan ozod qilmaydi.

Raqamli monitoringning legitimligi jamiyat ishonchi bilan ham belgilanadi. Fuqaro qaysi jamoat makonida videokuzatuv borligini, ma’lumotdan qanday maqsadda foydalanilishini va qaysi vakolatli organ javobgar ekanini umumiy tartibda bilishi kerak. Operativ-qidiruv yoki boshqa qonun bilan himoyalangan ma’lumotlar bo‘yicha asosli istisnolar mavjud bo‘lishi mumkin, biroq maxfiylik umumiy qoida emas, qonunda belgilangan istisno sifatida qo‘llanishi lozim.

Huquqni muhofaza qiluvchi organlar o‘rtasida ma’lumot almashinuvi tezkorlikni oshiradi, lekin vakolatlar chegarasini xiralashtirish xavfini ham keltirib chiqaradi. Ma’lumotlar integratsiyasi “hamma ma’lumot hammaga ochiq” tamoyiliga emas, xizmat vazifasiga mos cheklangan kirish, so‘rovni asoslash va har bir harakatni qayd etish tamoyillariga tayanishi kerak. Tizimlararo moslik texnik talab bo‘lsa, vakolatlarning aniqligi huquqiy talabdir.

Kiberxavfsizlik jamoat xavfsizligi tizimining yordamchi elementi emas, uning uzviy tarkibiy qismidir. Kamera tarmog‘i yoki tahliliy platformaga ruxsatsiz kirish faqat ma’lumot sizib chiqishiga emas, yolg‘on signal, noto‘g‘ri yo‘naltirilgan patrul yoki muhim voqea haqidagi ma’lumotning yo‘qolishiga olib kelishi mumkin. Shu

bois uzluksizlik rejasi, zaxira nusxalari, kirish nazorati, texnik sinov va hodisalarni qayd etish standartlari majburiy tashkiliy talab sifatida qaralishi lozim [4].

Raqamli texnologiyalarning samaradorligini baholashda o‘rnatilgan kameralar soni yoki qayta ishlangan yozuvlar hajmi yetarli indikator emas. Huquqbuzarliklarning oldi olinishi, hodisaga javob berish vaqti, xato signallar ulushi, fuqarolar shikoyatlarining ko‘rib chiqilishi, noqonuniy kirish holatlari va tizim xarajatlarining natijaga nisbati birgalikda o‘rganilishi kerak. Sabab-oqibat munosabatini aniqlash uchun tajriba va nazorat hududlari, boshlang‘ich ko‘rsatkichlar hamda mustaqil baholash metodikasi talab etiladi.

Yuqoridagilarni inobatga olgan holda, jamoat xavfsizligi uchun sun’iy intellekt tizimlarining to‘rt bosqichli huquqiy hayot siklini taklif etish mumkin: dastlabki huquqiy ta’sir bahosi; chegaralangan sinov; vakolatli organ tomonidan ruxsat etilgan ekspluatatsiya; davriy audit va zarurat tug‘ilganda to‘xtatish. Ushbu model texnologiyani bir marta sotib olib, cheksiz ishlatish yondashuvini cheklaydi. Algoritmning ma’lumotlari yoki vazifasi jiddiy o‘zgarsa, dastlabki baholashni yangilash talab etilishi maqsadga muvofiq.

Maqola doirasida bildirilgan tahlillardan kelib chiqib quyidagi yo‘nalishlarga alohida e’tibor qaratish maqsadga muvofiq:

birinchidan, jamoat xavfsizligida yuqori xavfli sun’iy intellekt tizimlari uchun alohida huquqiy talablarni belgilash;

ikkinchidan, biometrik identifikatsiya qo‘llanishining aniq asoslari, maqsadlari va muddatlarini normativ jihatdan chegaralash;

uchinchidan, algoritmik natijani mustaqil tekshirmasdan shaxsga nisbatan yuridik oqibat tug‘diruvchi qaror qabul qilishni taqiqlash;

to‘rtinchidan, mustaqil audit, shikoyat va zarar o‘rnini qoplash mexanizmlarini mustahkamlash.

beshinchidan, davlat xaridlarida algoritmning sinov natijalari, ma’lumotlar sifati va axborot xavfsizligi bo‘yicha tekshiriladigan talablarni joriy etish;

oltinchidan, jamoat xavfsizligi xodimlari uchun raqamli dalillar, algoritmik xatolar va inson huquqlariga ta’sirni baholash bo‘yicha maxsus o‘quv modullarini ishlab chiqish;

yettinchidan, pilot loyihalarning samaradorligi va huquqiy xavflari haqida shaxsga doir ma’lumotlarni oshkor qilmagan holda davriy umumlashtirilgan hisobotlar e’lon qilish taklif etiladi.

Taklif etilayotgan normalarni amaliyotga tatbiq etishda ikki qarama-qarshi xavfdan qochish kerak. Bir tomondan, texnologik innovatsiyani haddan tashqari cheklash davlat organlarining real tahdidlarga tez javob berish imkoniyatini kamaytirishi mumkin. Ikkinchi tomondan, nazoratsiz kengayish jamoat xavfsizligi nomi ostida ommaviy kuzatuvni odatiy holga aylantiradi. Shu sababli huquqiy siyosatning vazifasi innovatsiya va huquq kafolatlari o‘rtasida mavhum muvozanatni e’lon qilish emas, balki har bir texnologiya uchun o‘lchanadigan, tekshiriladigan va sudda bahslashilishi mumkin bo‘lgan chegaralarni belgilashdan iborat.

Umumiy xulosa qilib aytganda, sun’iy intellekt va raqamli monitoring texnologiyalari jamoat xavfsizligini ta’minlashning samarali yordamchi vositasiga aylanishi mumkin, biroq ularning ijtimoiy qiymati faqat tezkorlik yoki texnik aniqlik bilan o‘lchanmaydi. Asosiy mezon — ushbu vositalar qonuniy vakolat doirasida, zarur va mutanosib tarzda, inson nazorati ostida ishlashi hamda fuqarolarga samarali huquqiy himoya imkonini qoldirishidir. Davlat xavfsizlikni ta’minlar ekan, insonni algoritm uchun ma’lumot obyektiga aylantirmasligi, aksincha, texnologiyani inson huquqlarini ishonchli himoya qiladigan boshqaruv vositasiga aylantirishi lozim.

**Foydalanilgan adabiyotlar:**

1. O‘zbekiston Respublikasi Konstitutsiyasi. https://lex.uz/docs/-6445145
2. O‘zbekiston Respublikasi Prezidentining 2021-yil 29-noyabrdagi PF-27-son Farmoni “O‘zbekiston Respublikasi jamoat xavfsizligi konsepsiyasini

tasdiqlash va uni amalga oshirish chora-tadbirlari to‘g‘risida”. https://lex.uz/uz/acts/-5749291

3. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son Qonuni “Shaxsga doir ma’lumotlar to‘g‘risida”. https://lex.uz/acts/-4396419
4. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son Qonuni “Kiberxavfsizlik to‘g‘risida”. https://lex.uz/docs/-5960604
5. O‘zbekiston Respublikasi Prezidentining 2024-yil 14-oktabrdagi PQ-358-son qarori “Sun’iy intellekt texnologiyalarini 2030-yilga qadar rivojlantirish strategiyasini tasdiqlash to‘g‘risida”. https://lex.uz/acts/-7158604
6. Russell S., Norvig P. Artificial Intelligence: A Modern Approach. 4th ed. Pearson, 2021.
7. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
8. Grother P., Ngan M., Hanaoka K. Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects. NISTIR 8280. National Institute of Standards and Technology, 2019. https://doi.org/10.6028/NIST.IR.8280
9. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. CETS No. 225, 2024. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence
10. UNESCO. Recommendation on the Ethics of Artificial Intelligence. Paris, 2021. https://unesdoc.unesco.org/ark:/48223/pf0000381137