JAMOAT XAVFSIZLIGINI TA'MINLASHDA RAQAMLI TEXNOLOGIYALARNING NAZARIY-HUQUQIY ASOSLARI

Jamoat xavfsizligi universiteti magistratura tinglovchisi

Bozorov Xasan Turg'unali o'g'li

Ilmiy rahbar yu.f.b.f.d. (PhD) dotsent **S.R.Tursunova**

xasanbozorov095@gmail.com

Annotatsiya. Maqolada jamoat xavfsizligini ta'minlashda raqamli texnologiyalardan foydalanishning nazariy va huquqiy asoslari tahlil qilinadi. Video kuzatuv, biometrik identifikatsiya, katta ma'lumotlar va sun'iy intellekt vositalarini qo'llash bo'yicha xalqaro standartlar, xorijiy sud amaliyoti va O'zbekiston qonunchiligi qiyosiy o'rganiladi. Muallif qonuniylik, zarurlik va mutanosiblik mezonlarini yagona ketma-ket tekshiruvga birlashtirib, unga xatoni tuzatish imkoniyatini to'rtinchi shart sifatida qo'shishni taklif qiladi, shuningdek, raqamli vositalarni shaxs huquqlariga aralashuv darajasiga ko'ra tabaqalashtiruvchi to'rt pog'onali huquqiy rejim modelini asoslaydi. Maqola oxirida milliy qonunchilikni takomillashtirish bo'yicha aniq takliflar beriladi.

Kalit so'zlar: jamoat xavfsizligi, raqamli texnologiyalar, shaxsga doir ma'lumotlar, biometrik identifikatsiya, mutanosiblik prinsipi, sun'iy intellekt, huquqiy tartibga solish.

Аннотация. В статье анализируются теоретические и правовые основы применения цифровых технологий в обеспечении общественной безопасности. На основе сравнения международных стандартов, зарубежной судебной практики и законодательства Узбекистана автор предлагает модель дифференцированного правового режима цифровых средств в зависимости от степени вмешательства в права личности и обосновывает набор обязательных гарантий для каждого уровня. Сформулированы предложения по совершенствованию национального законодательства.

Ключевые слова: общественная безопасность, цифровые технологии, персональные данные, биометрическая идентификация, принцип соразмерности, искусственный интеллект.

Abstract. The article examines the theoretical and legal foundations of using digital technologies to ensure public safety. Drawing on international standards, foreign case law and the legislation of Uzbekistan, the author proposes a tiered legal regime in which digital tools are classified by the degree of their interference with individual rights, and sets out a mandatory package of safeguards for each tier. Proposals for improving national legislation are offered.

Keywords: public safety, digital technologies, personal data, biometric identification, proportionality, artificial intelligence.

Kirish

So'nggi yillarda jamoat xavfsizligini ta'minlash amaliyoti sezilarli o'zgardi. Davlat xizmatlarining katta qismi elektron shaklga o'tdi, shaharlarda video kuzatuv va «aqlli» tizimlar kengaymoqda, huquqbuzarliklarning bir qismi esa internet makoniga ko'chib ketdi. Bunday sharoitda huquqni muhofaza qilish organlari raqamli vositalarsiz ishlay olmaydi, buni inkor etishning o'zi ma'nosiz.

Biroq masala shu bilan tugamaydi. Kuzatuv kamerasi qayerga va qanday maqsadda o'rnatilishi mumkin, yuz tasviri va boshqa biometrik ma'lumotlarni kim qancha muddat saqlaydi, algoritm xato qilsa, kim javob beradi? Bular texnik emas, huquqiy savollar. Ularga javob topish uchun nazariy jihatdan asoslangan va amalda ishlaydigan huquqiy tartib kerak.

Mavzuning dolzarbligi. O'zbekistonda «Xavfsiz shahar» kabi kompleks tizimlar joriy etilmoqda, raqamli transformatsiya esa davlat boshqaruvining deyarli barcha sohasini qamrab olmoqda. Amaldagi normativ bazani tahlil qilish shuni ko'rsatdiki, «Xavfsiz shahar» tizimi qonun bilan emas, asosan Prezident va Vazirlar Mahkamasi qarorlari asosida shakllantirilgan. Loyiha 2017-yil 29-avgustdagi PQ-3245-son qaror bilan boshlangan, «Xavfsiz shahar» markazining yagona integrator maqomi 2018-yil 21-

noyabrdagi PQ-4024-son qarorda mustahkamlangan, tizimni takomillashtirish esa 2023-yil 28-sentabrdagi PQ-318-son va 2025-yil 3-yanvardagi PQ-1-son qarorlar bilan davom ettirilgan. Bu hujjatlar asosan tizimni yaratish, integratsiya qilish va moliyalashtirish masalalarini hal qiladi; masalan, mahallalarni kuzatuv kameralari hamda sun'iy intellekt bilan ishlovchi dasturiy ta'minot bilan to'liq qamrab olish belgilangan, biroq saqlash muddati, ma'lumotlarga kirish tartibi, huquqlarga ta'sirni baholash va fuqaroning shikoyat qilish tartibi kabi kafolatlar ularning asosiy predmeti emas. Umumiy huquqiy asosni «Shaxsga doir ma'lumotlar to'g'risida»gi Qonun beradi: uning 26-moddasi biometrik ma'lumotlarni ta'riflaydi va shaxsni aniqlash uchun ularga ishlov berishni, qoida bo'yicha, sub'ektning roziligi bilan bog'laydi, 2026-yil 26-martdagi o'zgartirishlarga ko'ra esa biometrik ma'lumotlar O'zbekiston hududida saqlanishi shart.

Tadqiqot maqsadi. Jamoat xavfsizligini ta'minlashda raqamli texnologiyalardan foydalanishning nazariy-huquqiy asoslarini ochib berish va milliy qonunchilik uchun amaliy model taklif qilishdir.

Tadqiqot vazifalari: 1. Jamoat xavfsizligi tushunchasining raqamli muhitdagi mazmunini aniqlash; 2.Xalqaro standartlar va xorijiy sud amaliyotidan kelib chiqadigan umumiy talablarni ajratib olish; 3. O'zbekiston qonunchiligidagi bo'shliqlarni aniqlash; 4.Raqamli vositalarni qo'llashning tabaqalashtirilgan huquqiy rejimini ishlab chiqish.

Tadqiqot ob'ekti. Jamoat xavfsizligini ta'minlash jarayonida yuzaga keladigan ijtimoiy-huquqiy munosabatlardir. Tadqiqot predmeti esa shu jarayonda raqamli texnologiyalardan foydalanishni tartibga soluvchi nazariy qarashlar, xalqaro standartlar va milliy qonunchilik normalaridir.

Metodologiya. Tadqiqotda tahlil va sintez, huquqiy normalarni sharhlash, qiyosiy-huquqiy va tizimli usullardan foydalanildi. Normativ va sud amaliyoti materiallari sifatida xalqaro va milliy hujjatlar, Yevropa Inson huquqlari sudi, Yevropa Ittifoqi Adliya sudi, Buyuk Britaniya va AQSh sudlarining qarorlari hamda ilmiy adabiyotlar olindi.

Ilmiy yangilik. Maqolada quyidagi natijalar muallifning shaxsiy xulosasi sifatida ilgari suriladi. Birinchidan, qonuniylik, zarurlik va mutanosiblik mezonlari odatda alohida

ko'rib chiqiladi; biz ularni yagona ketma-ket tekshiruvga birlashtirib, to'rtinchi shart, ya'ni xatoni tuzatish imkoniyati (fuqaro qarorni bilishi, shikoyat qilishi va natijani o'zgartira olishi) bilan to'ldirishni asoslaymiz. Ikkinchidan, raqamli vositalarni «ruxsat etilgan» va «taqiqlangan» deb ikkiga bo'lish o'rniga, ularni shaxs huquqlariga aralashuv darajasi bo'yicha to'rt pog'onaga ajratuvchi rejim modeli taklif etiladi; har bir pog'ona uchun huquqiy asos, ruxsat beruvchi organ, saqlash muddati, ta'sirni baholash va inson nazorati talablari alohida belgilanadi. Uchinchidan, xorijiy sud amaliyotidan (S. va Marper, Digital Rights Ireland, Bridges, Carpenter) chiqadigan talablar yetti bandli huquqiy tekshiruv ro'yxatiga jamlanadi, uni yangi texnologiyani joriy etishdan oldin qo'llash mumkin. To'rtinchidan, ma'lumotlarning maqsaddan tashqari ishlatilishiga (function creep) qarshi maqsadni qonunda qat'iy qayd etish va uni o'zgartirishni alohida huquqiy asosga bog'lash qoidasi asoslanadi.

Amaliy ahamiyati. Natijalardan «Jinoyatchilikning profilaktikasi to'g'risida»gi va «Shaxsga doir ma'lumotlar to'g'risida»gi qonunlarga o'zgartirishlar tayyorlashda, shuningdek, ichki ishlar organlarining idoraviy hujjatlarini ishlab chiqishda foydalanish mumkin.

1. Jamoat xavfsizligi tushunchasining nazariy asoslari

Keng ma'noda jamoat xavfsizligi fuqarolarning hayoti, sog'lig'i, mol-mulki va huquqlari turli tahdidlardan himoyalangan holatni bildiradi. U milliy xavfsizlikning bir qismi bo'lib, jamoat tartibini, favqulodda vaziyatlardan himoyani va jinoyatchilikka qarshi kurashni qamrab oladi.

Nazariyada bu tushunchaga ikki xil yondashuv uchraydi. Birinchisida davlat va jamiyat manfaati ustun qo'yiladi: xavfsizlik tartib va barqarorlikni saqlash orqali ta'minlanadi deb hisoblanadi. Ikkinchisida markazda inson turadi va xavfsizlik shaxs huquqlari qanchalik himoyalanganiga qarab baholanadi. Huquqiy davlat g'oyasi nuqtai nazaridan bu yondashuvlarni bir-biriga qarshi qo'yish to'g'ri emas, chunki xavfsizlik inson huquqlarini amalga oshirishning shartidir. Ammo huquqlar xavfsizlik nomi bilan

me'yoridan ortiq cheklansa, jamiyat aynan himoya qilmoqchi bo'lgan qadriyatlarning o'zini yo'qotadi.

Raqamli davrda tushuncha kengaydi. Unga endi ko'chadagi tartib bilan birga axborot makonidagi barqarorlik, muhim axborot infratuzilmasini himoya qilish, kiberjinoyatlarga qarshi kurash va yolg'on xabarlar tarqalishining oldini olish ham kiradi. U. Bekning «xavf jamiyati» g'oyasi shu jihatdan muhim: zamonaviy jamiyat tahdidlarni bartaraf etibgina qolmay, ularni oldindan baholashga va boshqarishga majbur. D. Garland esa jinoyatchilikka qarshi siyosat tobora xavflarni boshqarish va nazorat qilish mantig'iga o'tayotganini ko'rsatadi. Bu qarashlar raqamli vositalar jamoat xavfsizligida nega tez tarqalayotganini tushuntiradi, ayni paytda ularni nazoratsiz qoldirish xavfini ham ko'rsatadi.

Raqamli vositalar qo'llanilganda ham jamoat xavfsizligi sohasidagi faoliyat quyidagi tamoyillarga tayanishi kerak:

– inson huquq va erkinliklarining ustuvorligi, ya'ni texnologiya huquqlarni cheklash uchun emas, ularni himoya qilish uchun xizmat qiladi;

– qonuniylik: har bir aralashuvning qonunda nazarda tutilgan asosi bo'lishi shart;

– mutanosiblik: chora maqsadga erishish uchun zarur darajadan oshmasligi lozim;

– maqsadga muvofiqlik va ma'lumotlarni minimallashtirish: faqat aniq maqsad uchun zarur ma'lumot yig'iladi;

– shaffoflik va hisobdorlik: tizim qanday ishlashi, kim nazorat qilishi va kim javob berishi ma'lum bo'ladi;

– inson nazorati: yakuniy qarorni algoritm emas, mas'ul shaxs qabul qiladi.

Bu tamoyillar faqat huquqiy talab emas, amaliy ahamiyatga ham ega. Fuqarolar tizimga ishonmasa, huquqbuzarlik haqida xabar bermaydi, profilaktika tadbirlarida ishtirok etmaydi, natijada eng ilg'or texnologiya ham samarasiz qoladi.

2. Jamoat xavfsizligida qo'llaniladigan raqamli texnologiyalar

Huquqiy tartibga solish predmetini aniqroq ko'rish uchun amaliyotda qo'llanilayotgan asosiy texnologiyalarni qisqacha ko'rib chiqamiz.

Birinchisi video kuzatuv va «Xavfsiz shahar» kabi kompleks tizimlardir. Ular jamoat joylarida tartibni kuzatish, huquqbuzarlikni tez aniqlash va hodisa joyiga kuchlarni yo'naltirish imkonini beradi. Kuzatuv transport oqimini oddiy hisoblashdan tortib shaxsni aniqlashgacha bo'lgan keng doirada ishlashi mumkin va huquqiy oqibatlari ham shunga qarab keskin farq qiladi. Prezident matbuot xizmati ma'lumotiga ko'ra, «Xavfsiz shahar» konsepsiyasi doirasida yagona platforma, 13 ta ma'lumotlarni qayta ishlash markazi, yagona elektron xarita va 42 750 ta intellektual kamera faoliyat yuritmoqda.

Ikkinchisi biometrik identifikatsiya, jumladan, yuzni tanish tizimlari. Ular qidiruvdagi shaxsni topishda foydali bo'lishi mumkin, ammo shaxsning eng nozik va o'zgarmas ma'lumotlari bilan ishlagani uchun xavf ham aynan shu yerda eng yuqori.

Uchinchisi katta ma'lumotlar tahlili va prognoz modellari bo'lib, ular jinoyatchilik xaritalarini tuzish va profilaktikani aniqroq yo'naltirish uchun ishlatiladi. Sun'iy intellekt va avtomatlashtirilgan qaror qabul qilish katta hajmdagi axborotni tez qayta ishlaydi, biroq qaror mantig'ining shaffof emasligi va xato ehtimoli asosiy muammo bo'lib qoladi.

To'rtinchisi elektron hukumat, idoralararo axborot almashinuvi va kiberxavfsizlik vositalaridir. Ular alohida tizimlarni bir-biriga bog'lab, ma'lumotlarning bir joyda to'planishini kuchaytiradi.

Bu texnologiyalarning hammasi ikki tomonlama: xavfsizlikni kuchaytiradi, shu bilan birga shaxsiy hayot daxlsizligiga ham tahdid soladi. Shu sababli ularni bir xil qoida bilan tartibga solib bo'lmaydi; bu fikrga 4-bo'limda qaytamiz.

3. Raqamli texnologiyalardan foydalanishning huquqiy asoslari

3.1. Xalqaro huquqiy standartlar

Shaxsiy hayot daxlsizligi huquqi Inson huquqlari umumjahon deklaratsiyasining 12-moddasida va Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro paktning 17-moddasida mustahkamlangan. Mintaqaviy darajada Yevropa inson huquqlari to'g'risidagi

konvensiyaning 8-moddasi shaxsiy va oilaviy hayotni hurmat qilish huquqini belgilaydi. Yevropa Inson huquqlari sudi amaliyotiga ko'ra bu huquqqa aralashuv qonuniy bo'lishi, legitim maqsadga yo'naltirilishi va demokratik jamiyatda zarur bo'lishi shart.

Shaxsga doir ma'lumotlarni himoya qilishda Yevropa Kengashining 108-sonli Konvensiyasi (2018-yildagi protokol bilan yangilangan holda) va Yevropa Ittifoqining Ma'lumotlarni himoya qilish bo'yicha Umumiy reglamenti (GDPR) asosiy namuna bo'lib xizmat qiladi. Huquqni muhofaza qilish organlarining ma'lumotlar bilan ishlashi uchun Yevropa Ittifoqida alohida hujjat, ya'ni 2016/680-sonli direktiva qabul qilingan. Bu jihat e'tiborga loyiq: jinoyatchilikka qarshi kurash maqsadidagi ma'lumotlar umumiy qoidalardan farq qiladigan, lekin o'ziga xos kafolatlarga ega maxsus rejimda tartibga solinadi. Kiberjinoyatlarga qarshi kurashda esa 2001-yildagi Budapesht konvensiyasi asosiy hujjatlardan biri hisoblanadi.

Yevropa Ittifoqining sun'iy intellekt to'g'risidagi reglamenti (2024/1689) tartibga solishda xavf darajasiga asoslangan yondashuvni joriy etdi. Unga ko'ra huquqni muhofaza qilish maqsadida jamoat joylarida real vaqtda masofaviy biometrik identifikatsiya qilish qoida tariqasida taqiqlanadi. Istisnolar tor doirada, masalan, og'ir jinoyatlar gumonlanuvchisini qidirish, yo'qolgan yoki jabrlangan shaxsni topish yoki hayotga bevosita xavfni oldini olish kabi aniq holatlar uchun nazarda tutilgan va odatda sud yoki mustaqil organning ruxsatini talab qiladi (shoshilinch holatlarda ruxsat keyinroq olinishi mumkin).

3.2. Milliy qonunchilik

O'zbekiston Respublikasi Konstitutsiyasi shaxsiy hayot daxlsizligini va shaxsga doir ma'lumotlarni himoya qilish huquqini kafolatlaydi. Raqamli sohani tartibga soluvchi asosiy hujjatlar quyidagilar:

– «Shaxsga doir ma'lumotlar to'g'risida»gi Qonun (2019-yil 2-iyul, O'RQ-547-son) ma'lumotlarni qayta ishlash tamoyillarini, sub'ekt huquqlarini va operatorlarning majburiyatlarini belgilaydi;

– «Kiberxavfsizlik to'g'risida»gi Qonun (2022-yil 15-aprel, O'RQ-764-son) axborot infratuzilmasi va kiber makonni himoya qilish tizimini tartibga soladi;

– «Axborotlashtirish to'g'risida»gi va «Elektron hukumat to'g'risida»gi qonunlar axborot tizimlari va elektron davlat xizmatlarining huquqiy asosini yaratadi;

– «Jinoyatchilikning profilaktikasi to'g'risida»gi Qonun (2014-yil 14-may) profilaktika sub'ektlarining vakolatlarini belgilaydi;

– sun'iy intellektdan foydalanishdan kelib chiqadigan munosabatlarni tartibga solishga oid 2026-yildagi Qonun (O'RQ-1115) sun'iy intellekt bo'yicha umumiy asoslarni belgilaydi, Adliya vazirligining etika qoidalari esa sun'iy intellekt texnologiyalarini ishlab chiqish va qo'llashning tamoyillarini belgilaydi.

Bulardan tashqari, «Raqamli O'zbekiston – 2030» strategiyasi (Prezidentning 2020-yil 5-oktabrdagi PF-6079-son Farmoni) davlat boshqaruvi va xavfsizlik sohasida raqamli yechimlarni joriy etishning ustuvor yo'nalishlarini belgilab berdi. «Shaxsga doir ma'lumotlar to'g'risida»gi Qonun lex.uz Milliy bazasidagi 2026-yil 12-sentabrdan amal qiluvchi tahrirda keltirildi.

Milliy qonunchilikning kuchli tomoni shundaki, u zamonaviy xalqaro yondashuvlarga yaqinlashib bormoqda. Shunga qaramay, bir qator bo'shliqlar saqlanib qolmoqda:

– Qonunning 3-moddasi huquq-tartibotni saqlash va jinoyatchilikka qarshi kurashish jarayonidagi ishlovni o'z doirasidan chiqaradi, shu bois bu sohada Yevropa Ittifoqidagi 2016/680-sonli direktivaga o'xshash, ma'lumotlarni himoya qilishning maxsus rejimi mavjud emas;

– biometrik identifikatsiya va algoritmik tahlil jamoat xavfsizligi maqsadida qaysi shartlarda qo'llanilishi mumkinligi alohida qonun darajasida belgilanmagan;

– yangi texnologiyani joriy etishdan oldin uning shaxs huquqlariga ta'sirini baholash majburiy emas;

– Qonunning 24-moddasi faqat avtomatlashtirilgan ishlov asosida qaror qabul qilinmaslik huquqini va qarorga e'tiroz bildirish tartibini nazarda tutadi, biroq 3-moddaga ko'ra bu kafolat huquq-tartibotni saqlash jarayoniga tatbiq etilmaydi, shuning uchun jamoat xavfsizligi tizimlarining xulosalari ustidan shikoyat qilishning maxsus mexanizmi yo'q;

– video yozuvlar va ma'lumotlar bazalarini saqlash muddatlari hamda ularga kirish huquqi bo'yicha qoidalar idoraviy darajada qolmoqda.

1) Ma'lumotlarni saqlash muddati va ularga kirish huquqi qonunda belgilanganmi?

2) Joriy etishdan oldin shaxs huquqlariga ta'sir baholanganmi?

3) Mustaqil nazorat va oldindan yoki keyingi ruxsat tartibi mavjudmi?

4) Fuqaro qarorni bilishi va shikoyat qila olishi ta'minlanganmi?

Har bir savolga «yo'q» javobi texnologiyani joriy etishni to'xtatib turish uchun asos bo'lishi mumkin.

Kengashining 108+ Konvensiyasi va GDPR nazorat organlarining to'liq mustaqil ishlashini alohida talab qiladi, institutsional mustaqillik masalasiga o'zbek adabiyotida ham e'tibor qaratilgan. Shu sababli mustaqil nazorat funksiyasini idoraviy tuzilmadan ajratish yoki uni qo'shimcha tashqi nazorat (parlament yoki Ombudsman) bilan to'ldirish maqsadga muvofiq. Bulardan tashqari, jamoatchilik nazorati ham muhim: tizimlar haqida umumiy ma'lumot e'lon qilish, hisobotlarni ochiq taqdim etish va fuqarolik jamiyati institutlarini muhokamaga jalb qilish ishonchni mustahkamlaydi.

Shu sababli Yevropa Ittifoqining xavf darajasiga asoslangan yondashuvidan ilhomlanib, lekin uni jamoat xavfsizligi sohasiga moslab, to'rt pog'onali rejim taklif etamiz (1-jadval).

1-jadval. Raqamli vositalarni qo'llashning tabaqalashtirilgan huquqiy rejimi (muallif modeli)

Mezon	I pog'ona. Past darajadagi aralashuv	II pog'ona. O'rta daraja	III pog'ona. Yuqori daraja	IV pog'ona. Eng yuqori daraja
Vositalar (misol)	Shaxsni aniqlamaydigan va umumlashtirilgan ma'lumotlar: transport oqimini hisoblash, anonim statistik tahlil	Jamoat joylarida shaxsni identifikatsiya qilmaydigan umumiy video kuzatuv, hodisalarni qayd etish	Shaxsni aniqlaydigan yoki profil tuzadigan vositalar: ma'lumotlar bazasi bilan solishtirish, keyinchalik (real vaqtda bo'lmagan) yuzni tanish, prognoz modellari	Jamoat joylarida real vaqtda ommaviy biometrik identifikatsiya; sezgir belgilar (din, millat, siyosiy qarash) bo'yicha profil tuzish
Huquqiy asos	Umumiy qonun va idoraviy nizom	Qonun va uni amalga oshiruvchi hukumat nizomi	Aynan shu vositalarni tartibga soluvchi maxsus qonun	Qoida bo'yicha taqiq; istisno faqat qonunda sanab o'tilgan holatlar uchun

Mezon	I pog'ona. Past darajadagi aralashuv	II pog'ona. O'rta daraja	III pog'ona. Yuqori daraja	IV pog'ona. Eng yuqori daraja
Ruxsat beruvchi organ	Idora rahbarining qarori	Vakolatli hududiy organ qarori; kuzatuv joylari haqida jamoatchilikka xabar berish	Har bir qo'llash uchun prokuror yoki sud ruxsati	Faqat sudning oldindan ruxsati (shoshilinch holatda keyinchalik tasdiqlash)
Saqlash muddati	Maqsad uchun zarur eng qisqa muddat; ma'lumot shaxsga bog'lanmaydi	Qonunda belgilangan aniq muddat, undan keyin o'chiriladi	Qonunda qat'iy cheklangan qisqa muddat; maqsadni o'zgartirish alohida asosni talab qiladi	Maqsad bajarilgach darhol o'chiriladi
Ta'sirni baholash	Qisqa ichki tekshiruv ro'yxati	Joriy etishdan oldin soddalashtirilgan baholash	To'liq mustaqil baholash, natijasi e'lon qilinadi	To'liq mustaqil baholash va ommaviy hisobot

Mezon	I pog'ona. Past darajadagi aralashuv	II pog'ona. O'rta daraja	III pog'ona. Yuqori daraja	IV pog'ona. Eng yuqori daraja
Inson nazorati va shikoyat	Oddiy ichki nazorat	Kirish jurnali (audit izi), prokuror nazorati	Yakuniy qarorni faqat mas'ul inson qabul qiladi; fuqaroga xabar berish va shikoyat tartibi	Doimiy mustaqil nazorat, har bir holat bo'yicha hisobot

5. Asosiy nazariy-huquqiy muammolar

Kuzatuv va erkinlik muvozanati. M. Fuko Bentamning «panoptikon» modelini tahlil qilib, doimiy kuzatilayotganini his qilgan odam xulq-atvorini o'zi cheklay boshlashini ko'rsatgan. Zamonaviy raqamli kuzatuv bu g'oyaning yangi shaklidir. Qoidalar shaffof bo'lmasa, kuzatuv faqat jinoyatchilikka emas, fuqarolarning tabiiy faolligiga ham ta'sir qiladi. Sh. Zubof ma'lumotlarni ommaviy yig'ish va ulardan boshqaruv hamda tijorat maqsadida foydalanish xavfini «kuzatuv kapitalizmi» tushunchasi orqali tahlil qilgan..

Algoritmik xatolar va javobgarlik. Sun'iy intellekt tizimlari o'qitilgan ma'lumotlardagi noaniqliklarni takrorlashi mumkin, natijada ayrim guruhlarga nisbatan asossiz shubha yoki noto'g'ri identifikatsiya yuzaga keladi. Shu sababli algoritm xulosasi hech qachon yagona asos bo'lmasligi, yakuniy qaror esa mas'ul inson tomonidan qabul qilinishi kerak. Texnologiya xato qilganda dasturchi, operator yoki qaror qabul qilgan xodimdan kim javob beradi, degan savolga aniq javob bo'lmasa, jabrlangan shaxs huquqini himoya qila olmaydi. Fuqaro o'ziga nisbatan qo'llangan avtomatlashtirilgan qarorni bilishi va uni shikoyat qila olishi lozim.

Funksiyaning kengayishi (function creep). Dastlab muayyan maqsad uchun, masalan, transport harakatini nazorat qilish uchun yig'ilgan ma'lumotlar vaqt o'tib, boshqa

maqsadlarda ishlatila boshlaydi. Bunga qarshi ikki qoida taklif etiladi: har bir ma'lumotlar bazasi uchun maqsad qonunda yoki unga asoslangan hujjatda aniq yozilishi hamda maqsadni o'zgartirish alohida huquqiy asosni va nazorat organining xabardor qilinishini talab etishi.

6. Takomillashtirish bo'yicha takliflar

Tahlil natijalariga ko'ra quyidagi yo'nalishlarda ish olib borish maqsadga muvofiq:

1) biometrik ma'lumotlar va avtomatlashtirilgan tahlil vositalaridan jamoat xavfsizligi maqsadida foydalanish shartlari, doirasi va cheklovlarini belgilovchi alohida normativ-huquqiy hujjat ishlab chiqish va unda 4-bo'limda taklif etilgan tabaqalashtirilgan rejimni nazarda tutish;

2) video kuzatuv va ma'lumotlar bazalari bo'yicha saqlash muddati, kirish huquqi va maqsadga muvofiqlik tamoyillarini qonun darajasida mustahkamlash;

3) yangi texnologiyalarni keng joriy etishdan oldin shaxs huquqlariga ta'sirini baholash tartibini kiritish;

4) avtomatlashtirilgan tizim xulosalari ustidan inson nazoratini ta'minlash va fuqarolar uchun shikoyat mexanizmini yaratish;

5) mustaqil nazorat organining vakolatlarini kuchaytirish va ma'lumotlardan foydalanish bo'yicha muntazam hisobdorlikni joriy etish;

6) huquqni muhofaza qilish xodimlarining raqamli va huquqiy savodxonligini oshirish;

7) xalqaro hamkorlikni, ayniqsa kiberjinoyatlarga qarshi kurash va ma'lumot almashinuvi sohasida, ilg'or standartlarga tayangan holda kengaytirish.

Takliflarni bosqichma-bosqich amalga oshirish maqsadga muvofiq. Avval mavjud tizimlarning inventarizatsiyasi o'tkaziladi: ular qanday ma'lumot to'plashi va qaysi huquqiy asosda ishlashi aniqlanadi, normativ bazadagi bo'shliqlar baholanadi. Keyin biometrik ma'lumotlar, video kuzatuv va algoritmik tahlil bo'yicha aniq qoidalar ishlab chiqilib, jamoatchilik muhokamasidan o'tkaziladi. Uchinchi bosqichda yangi vositalar cheklangan hududda, aniq baholash mezonlari bilan sinab ko'riladi va natija mustaqil baholanadi.

Nihoyat, muntazam hisobdorlik, xatolar statistikasini yuritish va qoidalarni amaliyotga qarab yangilab borish ta'minlanadi.

Xulosa

Raqamli texnologiyalar jamoat xavfsizligini ta'minlashda samarali vositaga aylandi va uning ahamiyati kelgusida yanada ortadi. Biroq samaradorlik faqat texnik imkoniyatlar bilan emas, huquqiy asosning mustahkamligi, jamoatchilik ishonchi va shaxs huquqlariga hurmat bilan belgilanadi. Tadqiqot natijalari quyidagicha:

1) xavfsizlik va inson huquqlari o'rtasidagi muvozanat qonuniylik, zarurlik va mutanosiblik mezonlariga, shuningdek, xatoni tuzatish imkoniyatiga amal qilish orqali ta'minlanadi;

2) raqamli vositalarni bir xil qoida bilan emas, shaxs huquqlariga aralashuv darajasiga qarab to'rt pog'onali rejim asosida tartibga solish maqsadga muvofiq;

3) O'zbekistonda raqamli sohaning huquqiy bazasi izchil rivojlanmoqda, biroq biometrik identifikatsiya va sun'iy intellektdan foydalanish uchun aniqroq, qonun darajasidagi tartibga solish zarur;

4) ma'lumotlarning maqsaddan tashqari ishlatilishini oldini olish uchun maqsadni qonunda qayd etish va uni o'zgartirishni alohida asosga bog'lash lozim.

Kelgusidagi ilmiy izlanishlar uchun quyidagi yo'nalishlar istiqbolli: sun'iy intellekt qo'llangan qarorlar uchun huquqiy javobgarlik modeli; biometrik ma'lumotlarni saqlash muddatlarining empirik asoslanishi; tabaqalashtirilgan rejim chegaralarini amaliyotda sinash; «aqlli shahar» loyihalarining jinoyatchilik profilaktikasiga ta'sirini sotsiologik va statistik baholash.

Foydalanilgan adabiyotlar

1. O'zbekiston Respublikasining Konstitutsiyasi.

2. O'zbekiston Respublikasining «Shaxsga doir ma'lumotlar to'g'risida»gi Qonuni, 2019-yil 2-iyul, O'RQ-547-son (lex.uz, 2026-yil 12-sentabrdan amal qiluvchi tahrir).

3. O'zbekiston Respublikasining «Kiberxavfsizlik to'g'risida»gi Qonuni, 2022-yil 15-aprel, O'RQ-764-son.

4. O'zbekiston Respublikasining «Axborotlashtirish to'g'risida»gi Qonuni, 2003-yil 11-dekabr.

5. O'zbekiston Respublikasining «Elektron hukumat to'g'risida»gi Qonuni, 2015-yil 9-dekabr.

6. O'zbekiston Respublikasining «Jinoyatchilikning profilaktikasi to'g'risida»gi Qonuni, 2014-yil 14-may.

7. O'zbekiston Respublikasi Prezidentining 2020-yil 5-oktabrdagi PF-6079-son Farmoni («Raqamli O'zbekiston – 2030» strategiyasi).

8. Inson huquqlari umumjahon deklaratsiyasi, 1948.

9. Fuqarolik va siyosiy huquqlar to'g'risidagi xalqaro pakt, 1966.

10. Inson huquqlari va asosiy erkinliklarni himoya qilish to'g'risidagi Yevropa konvensiyasi, 1950.

11. Yevropa Kengashining 108-sonli Konvensiyasi (shaxsga doir ma'lumotlarni avtomatlashtirilgan qayta ishlashda shaxslarni himoya qilish to'g'risida), 1981; 2018-yildagi o'zgartirish protokoli bilan.

12. Kiberjinoyatlar to'g'risidagi Budapesht konvensiyasi, 2001.

13. Regulation (EU) 2016/679 (GDPR).

14. Directive (EU) 2016/680 (Law Enforcement Directive).

15. Regulation (EU) 2024/1689 (Artificial Intelligence Act).

16. Beck U. Risk Society: Towards a New Modernity. London: Sage, 1992.