JAMOAT XAVFSIZLIGINI TA’MINLASH TIZIMIDA RAQAMLI TEXNOLOGIYALARDAN FOYDALANISHNI HUQUQIY TARTIBGA SOLISH MASALALARI

ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

ISSUES OF LEGAL REGULATION OF THE USE OF DIGITAL TECHNOLOGIES IN THE PUBLIC SAFETY SYSTEM

Ergashev Jahongir Umarali o‘g‘li
Jamoat xavfsizligi universiteti talabasi

Annotatsiya: Mazkur maqolada jamoat xavfsizligini ta’minlashda raqamli texnologiyalarni qo‘llashning konstitutsiyaviy va ma’muriy-huquqiy asoslari, raqamli kuzatuvning mutanosibligi, shaxsga doir ma’lumotlar muhofazasi, algoritmik qarorlarning shaffofligi hamda idoralararo axborot almashinuvi masalalari tahlil qilingan. Raqamli vositalar samaradorligi ularning texnik imkoniyatlari bilangina emas, balki qonuniylik, zarurat, hisobdorlik va sud nazorati bilan baholanishi asoslanadi. Xavfga asoslangan tartibga solish, inson nazorati, mustaqil audit va samaradorlik indikatorlariga oid takliflar ilgari surilgan.

Kalit so‘zlar: jamoat xavfsizligi, raqamlashtirish, konstitutsiyaviy huquqlar, videokuzatuv, biometrik identifikatsiya, sun’iy intellekt, shaxsga doir ma’lumotlar, mutanosiblik, algoritmik shaffoflik, huquqbuzarliklar profilaktikasi.

Аннотация: В данной статье анализируются конституционные и административно-правовые основы применения цифровых технологий в сфере обеспечения общественной безопасности, вопросы соразмерности цифрового наблюдения, защиты персональных данных, прозрачности алгоритмических решений, а также межведомственного информационного обмена. Обосновывается положение о том, что эффективность цифровых инструментов должна оцениваться не только с точки зрения их технических возможностей, но и с учётом соблюдения принципов законности, необходимости, подотчётности и судебного контроля. Выдвигаются предложения по внедрению риск-ориентированного правового регулирования, обеспечению человеческого контроля, проведению независимого аудита и разработке показателей эффективности.

Ключевые слова: общественная безопасность, цифровизация, конституционные права, видеонаблюдение, биометрическая идентификация, искусственный интеллект, персональные данные, соразмерность, алгоритмическая прозрачность, профилактика правонарушений.

Abstract: This article analyzes the constitutional and administrative legal foundations for the use of digital technologies in ensuring public safety, focusing on the proportionality of digital surveillance, personal data protection, transparency of algorithmic decisions, and interagency information exchange. It argues that the effectiveness of digital tools should be assessed not only in terms of their technical capabilities but also through compliance with the principles of legality, necessity, accountability, and judicial oversight. The article puts

forward proposals for introducing risk-based regulation, ensuring human oversight, conducting independent audits, and developing performance indicators.

Keywords: public safety, digitalization, constitutional rights, video surveillance, biometric identification, artificial intelligence, personal data, proportionality, algorithmic transparency, prevention of offenses.

Zamonaviy jamoat xavfsizligi tizimining taraqqiyoti faqat patrullash kuchlarini ko‘paytirish yoki nazorat texnikasini yangilash bilan o‘lchanmaydi. Raqamli makonda vujudga kelayotgan xavflar, shaharlardagi murakkab transport oqimlari, ommaviy tadbirlarning xavfsizligini ta’minlash zarurati hamda tezkor boshqaruvga bo‘lgan ehtiyoj davlat organlaridan ma’lumotlarga tayangan holda qaror qabul qilishni talab etmoqda. Biroq xavfsizlikni ta’minlash maqsadi insonning shaxsiy hayoti, erkin harakatlanishi, tengligi va samarali huquqiy himoyaga bo‘lgan huquqlarini ikkinchi darajaga tushirish uchun asos bo‘la olmaydi. Shu sababli raqamli texnologiyani joriy etish bilan uni huquqiy chegaralash bir vaqtning o‘zida olib borilishi zarur.

O‘zbekiston Respublikasi Konstitutsiyasi inson huquqlari va erkinliklarining bevosita amal qilishini, davlat organlari faoliyatida qonuniylikni va shaxsiy hayot daxlsizligini kafolatlaydi. Xususan, 31-moddada shaxsiy hayot, shaxsiy va oilaviy sir, yozishmalar hamda boshqa xabarlar sirini himoya qilishga oid kafolatlar belgilangan. Ushbu normalar jamoat joyidagi videotasvirni olish, shaxsni yuz tasviri orqali aniqlash yoki turli reyestrlardagi ma’lumotlarni birlashtirishda ham e’tibordan chetda qolmasligi kerak [1].

Jamoat xavfsizligining normativ konsepsiyasi davlat va jamiyatni tahdidlardan himoya qilishni inson huquqlari va qonuniy manfaatlari ro‘yobga chiqarilishi bilan uzviy bog‘laydi. Prezidentning 2021-yil 29-noyabrdagi PF–27-son Farmoni bilan tasdiqlangan Konsepsiyada mazkur sohaning subyektlari, hamkorlik tamoyillari va xavfsizlikni ta’minlashning kompleks xususiyati ifodalangan. Farmon bilan tasdiqlangan 2022–2025-yillar strategiyasida axborot texnologiyalarini keng joriy etish vazifasi qo‘yilgan bo‘lsa-da, ushbu strategiya davrining tugagani uning maqsadlarini 2026-yildagi amaldagi natijalar deb talqin qilishga asos bermaydi [2].

Raqamli texnologiyalardan foydalanishni huquqiy tartibga solish deganda davlat organining dasturiy ta’minot xarid qilishi yoki axborot tizimini ishga tushirishi emas, balki texnologiyani tanlashdan tortib undan foydalanish natijalarini baholashgacha bo‘lgan munosabatlarning huquqiy rejimini belgilash tushunilishi lozim. Bu rejim vakolat manbaini, ma’lumot yig‘ish maqsadini, kirish huquqini, saqlash muddatini, axborot xavfsizligini, nazorat va shikoyat mexanizmlarini qamrab oladi. Shunday yondashuv texnik infratuzilmani davlat hokimiyatining hisobdor vositasiga aylantiradi.

Raqamli vositalarni huquqiy xavf darajasiga ko‘ra farqlash muhimdir. Masalan, svetoforlarning avtomatik muvofiqlashtirilishi yoki yo‘l qoplamasi holatini sensorlar yordamida o‘lchash, odatda, shaxsiy ma’lumotlarga kamroq ta’sir ko‘rsatadi. Bunga qarama-qarshi ravishda ommaviy yuzni tanish tizimi, fuqarolarning harakatlanish yo‘nalishlarini uzoq muddat kuzatish va ehtimoliy huquqbuzarlik xavfi bo‘yicha shaxsiy reyting tuzish yuqori huquqiy xatar tug‘diradi. Barcha tizimlarga bir xil ruxsat tartibini qo‘llash o‘rniga ularning inson huquqlariga ta’siriga mos nazorat darajasini belgilash maqsadga muvofiq.

“Axborotlashtirish to‘g‘risida”gi Qonun axborot resurslari, axborot tizimlari va ulardan foydalanishga oid umumiy huquqiy asoslarni belgilaydi. Biroq umumiy axborotlashtirish rejimi jamoat xavfsizligidagi har bir maxsus kuzatuv usulini avtomatik ravishda qonuniylashtirmaydi. Davlat organi tomonidan shaxsga oid sezgir ma’lumotlar qayta ishlanayotganida tegishli maxsus vakolat, aniq maqsad va himoya choralarining mavjudligi alohida tekshirilishi kerak [3].

“Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonunda shaxsga doir ma’lumotlarga ishlov berishning huquqiy asoslari va subyekt huquqlari nazarda tutilgan. Ayniqsa, avtomatlashtirilgan ishlov berish asosida yuridik oqibat tug‘diruvchi qarorlar qabul qilinishiga oid 24-modda, biometrik va genetik ma’lumotlarga oid 26-modda raqamli xavfsizlik tizimlari uchun bevosita ahamiyatga ega. Bunda qonunda nazarda tutilgan istisnolarni umumiy va cheklanmagan kuzatuv vakolati sifatida talqin qilish mumkin emas [4].

Videokuzatuv jamoat joylarida xavfli vaziyatni tez aniqlash, bedarak yo‘qolgan shaxslarni izlashga ko‘maklashish, favqulodda holatlarga munosabatni jadallashtirish kabi amaliy imkoniyatlarga ega. Lekin tasvirni real vaqt rejimida ko‘rish, uni uzoq saqlash, boshqa ma’lumotlar bilan bog‘lash va avtomatik identifikatsiya qilish bir xil huquqiy harakat emas. Ularning har biri alohida maqsad, zarurat va mutanosiblik mezonlari bilan baholanishi lozim.

Mutanosiblik tamoyilini amaliyotga tatbiq etishda to‘rt savol hal qiluvchi ahamiyatga ega: aralashuv qonunga asoslanganmi; ko‘zlangan maqsad qonuniymi; aynan shu texnologiya zarurmi; shu maqsadga shaxs huquqlarini kamroq cheklaydigan vosita bilan erishish mumkinmi? Masalan, stadionga kirishda umumiy xavfsizlikni ta’minlash uchun oddiy metall detektor yetarli bo‘lgan sharoitda barcha tomoshabinlarning biometrik profilini doimiy saqlashning zarurati alohida isbot talab etadi.

Shu o‘rinda ta’kidlash lozimki, raqamli tizimdan olingan signal bilan huquqiy faktni tenglashtirish katta xatodir. Algoritm shaxsning harakatini shubhali deb belgilashi mumkin, biroq bunday signalning o‘zi huquqbuzarlik sodir etilganini isbotlamaydi. Signal xodimning tekshiruvini boshlashga yordam berishi mumkin, ammo protsessual qarorlar qonunda belgilangan dalillar va vakolatli shaxsning mustaqil bahosiga asoslanishi zarur.

Algoritmik xatolar faqat dasturlash nuqsoni bilan cheklanmaydi. Ta’lim ma’lumotlaridagi nomutanosiblik, kameraning sifati, yorug‘lik, ma’lumotlarning eskirishi va noto‘g‘ri belgilangan mezonlar ayrim guruhlarga nisbatan asossiz shubha ehtimolini oshirishi mumkin. Shu sababli texnologiya ishlab chiqaruvchisining umumiy aniqlik ko‘rsatkichi yetarli emas: tizim real qo‘llash sharoitida xato ijobiy va xato salbiy natijalar bo‘yicha muntazam sinovdan o‘tishi kerak.

Jamoat xavfsizligi sohasida sun’iy intellektdan foydalanishning eng nozik jihati insonni statistik tavakkalchilik obyektiga aylantirish xavfidir. Ayrim hududda avval sodir etilgan huquqbuzarliklar soni ko‘pligi shu hududdagi har bir fuqaroga nisbatan yuqori shubha prezumpsiyasini yaratmaydi. Hududiy tahlil va individual ayblov o‘rtasidagi chegara qonunchilik va xizmat yo‘riqnomalarida qat’iy ajratilishi lozim.

Idoralararo ma’lumot almashinuvi ham jamoat xavfsizligining muhim resursidir. Ichki ishlar organlari, Milliy gvardiya, favqulodda vaziyatlar tuzilmalari va mahalliy boshqaruv subyektlari o‘rtasida muvofiqlashtirilgan axborot almashinuvi javob choralarini tezlashtiradi. Biroq “yagona platforma” tushunchasi barcha organlar barcha ma’lumotlarni istalgan vaqtda ko‘ra oladi degani emas. Kirish vakolatlari vazifaga bog‘langan, darajalangan va elektron qayd etiladigan bo‘lishi zarur.

Ma’lumotlarni birlashtirishdan oldin ularning kelib chiqishi, yangilanish davriyligi, aniqligi va qonuniy yig‘ilganligi tekshirilishi shart. Bir reyestrdagi texnik xato boshqa platformalarga avtomatik ko‘chirilsa, fuqaro bir vaqtning o‘zida bir necha idorada asossiz cheklovlarga duch kelishi mumkin. Bunday vaziyatda xatoni tuzatish uchun birgina mas’ul organ va muvofiqlashtirilgan tuzatish tartibini belgilash fuqarolarning amaliy himoyasini kuchaytiradi.

Raqamli dalillarning ishonchliligi masalasi ham alohida e’tiborga loyiq. Videoyozuv, geolokatsiya, elektron jurnal yoki avtomatik qayd etilgan hodisa ma’lumotining kelib chiqishi, yaxlitligi, saqlash zanjiri va o‘zgartirilmaganligi tekshirilmasdan unga mutlaq ishonch

bildirish noto‘g‘ri. Xesh qiymatlari, kirish jurnallari, vaqt belgisi va mustaqil ekspertiza kabi texnik vositalar protsessual kafolatlarni to‘ldirishi mumkin, ammo ularning o‘zi qonunda belgilangan dalil maqomini almashtirmaydi.

Kiberxavfsizlik jamoat xavfsizligini raqamlashtirishning ichki shartidir. Tizimga ruxsatsiz kirish, kameralarni boshqarish kanallarini buzish yoki shaxsga doir ma’lumotlarning sizib chiqishi texnik nosozlikdan tashqari fuqarolar xavfsizligiga bevosita tahdid soladi. Shu sababli axborot tizimlarida eng kam vakolat prinsipi, ko‘p omilli autentifikatsiya, zaxira nusxalar, insidentlarni qayd etish va tiklash rejalarini joriy etish zarur. “Kiberxavfsizlik to‘g‘risida”gi Qonun ushbu yo‘nalishdagi umumiy huquqiy asoslardan biridir [5].

Raqamli xizmatlarning xususiy yetkazib beruvchilarga bog‘liqligi alohida shartnomaviy masalalarni keltirib chiqaradi. Davlat organi dasturiy mahsulotni sotib olgach, uning algoritmi, yangilanishlari va ma’lumotlarni saqlash usullari ustidan yetarli nazoratga ega bo‘lmasa, ommaviy vakolatni amalga oshirish amalda tijorat subyektining yopiq texnologiyasiga bog‘lanib qoladi. Xarid shartnomalarida audit huquqi, ma’lumotlarni qaytarish va o‘chirish, insident haqida xabar berish, tizimni mustaqil tekshirish hamda xizmat tugagach migratsiya qilish shartlari aks etishi kerak.

Xorijiy tajribada yuqori xavfli sun’iy intellekt tizimlariga nisbatan maxsus talablarni belgilash tendensiyasi kuzatiladi. Yevropa Ittifoqining 2024/1689-son reglamenti ayrim huquqni muhofaza qilish qo‘llanmalarini yuqori xavf doirasida baholaydi va jamoat joylarida real vaqt rejimidagi masofaviy biometrik identifikatsiyaga nisbatan qat’iy cheklovlar hamda istisno shartlarini nazarda tutadi. Ushbu modelni O‘zbekistonga mexanik ko‘chirish emas, balki uning risklarni tasniflash, mustaqil ruxsat va huquqlar ta’sirini baholash tamoyillarini milliy huquqiy tizimga moslashtirish muhim [6].

Raqamli kuzatuvning qonuniyligi haqida jamoatchilikka umumiy ma’lumot berish xavfsizlikni zaiflashtirmaydi, aksincha uning legitimligini oshirishi mumkin. Maxfiy bo‘lmagan ma’lumotlar doirasida kuzatuvning maqsadi, operatori, saqlash muddati va murojaat tartibi ochiqlanishi fuqaroga o‘z huquqini anglash imkonini beradi. Maxsus operativ tadbirlar bo‘yicha qonuniy sir saqlanishi mumkin, biroq sir rejimi mustaqil nazoratni butunlay istisno etmasligi kerak.

Tadqiqot natijalari shuni ko‘rsatdiki, raqamli texnologiyalarni tartibga solishdagi asosiy muammo alohida qurilma yoki platformaning mavjudligida emas, balki uning hayotiy sikli bo‘yicha javobgarlikning aniq taqsimlanmaganidadir. Loyihalashda texnik topshiriqni kim tasdiqlashi, sinov natijalarini kim tekshirishi, noto‘g‘ri identifikatsiya oqibatida zarar yetganda kim javob berishi va foydalanish to‘xtatilganda ma’lumotlar qanday yo‘q qilinishi oldindan belgilanishi lozim.

Bunda “raqamli huquqiy pasport” mexanizmini joriy etish taklif qilinadi. Har bir yuqori xavfli jamoat xavfsizligi tizimining pasportida normativ asos, maqsad, operator, ma’lumotlar toifasi, xavf bahosi, aniqlik sinovlari, saqlash muddati, mustaqil audit sanasi va shikoyat yo‘li qayd etilishi mumkin. Bu hujjat oddiy texnik inventar ro‘yxati emas, davlat organining raqamli aralashuvi uchun hisobdorlik vositasi bo‘lishi kerak.

Ikkinchi taklif — shaxs huquqlariga ta’sirni oldindan baholash tartibini yaratishdir. Yuqori xavfli tizimni ishga tushirishdan avval uning maqsadi, kutilayotgan foydasi, muqobil usullari, ehtimoliy xatolari va himoya kafolatlari yozma ravishda tahlil qilinadi. Bunda faqat texnik mutaxassislar emas, huquqshunoslar, axborot xavfsizligi ekspertlari va zarur hollarda mustaqil vakillar ishtirok etishi maqsadga muvofiq.

Uchinchi taklif — inson nazoratini mazmunli huquqiy talab sifatida belgilashdir. Operatorning algoritm tavsiyasini shunchaki tasdiqlashi inson nazorati mavjudligini anglatmaydi. Vakolatli xodim tizim xulosasini rad etish, qo‘shimcha dalil so‘rash, xatoni qayd qilish va asoslantirilgan qaror qabul qilish vakolatiga ega bo‘lishi zarur. Ayniqsa shaxs

erkinligi yoki huquqiy maqomiga ta’sir qiladigan qarorlar uchun bu talab ustuvor bo‘lishi lozim.

To‘rtinchi taklif — natijadorlikni faqat aniqlangan huquqbuzarliklar yoki o‘rnatilgan kameralar soni bilan o‘lchamaslikdir. Tizim samaradorligi xavfli hodisalarga javob vaqti, asossiz tekshiruvlar ulushi, noto‘g‘ri identifikatsiya ko‘rsatkichi, fuqarolar shikoyatlarini hal etish muddati, ma’lumotlar xavfsizligi insidentlari va xizmat xarajatlari bilan birgalikda baholanishi kerak. Aks holda texnik qamrovning oshishi huquqiy samaradorlikning o‘sishi sifatida noto‘g‘ri talqin qilinadi.

Beshinchi taklif — raqamli xavfsizlik bo‘yicha xodimlarning huquqiy savodxonligini kasbiy tayyorgarlikning mustaqil mezoniga aylantirishdir. Videoyozuvni olish va saqlash, biometrik ma’lumotlar bilan ishlash, algoritmik xatoni tanish, elektron dalillarni rasmiylashtirish va ma’lumotlar sizib chiqqanda harakat qilish bo‘yicha vaziyatli mashg‘ulotlar muntazam o‘tkazilishi kerak. Raqamli vositaning xavfsiz ishlashi uni boshqarayotgan xodimning huquqiy mas’uliyatidan ajralmasdir.

Yuqoridagilarni inobatga olgan holda, jamoat xavfsizligini raqamlashtirish jarayonida texnologik imkoniyat, normativ vakolat va inson huquqlarini himoya qilish o‘rtasida uch tomonlama muvozanat o‘rnatish zarur. Huquqiy aniqlik bo‘lmagan joyda innovatsiya idoraviy ixtiyoriylikni kuchaytirishi, haddan tashqari umumiy taqiq esa foydali texnologiyalarni joriy etishni sekinlashtirishi mumkin. Maqbul yechim — foydalanish holatiga mos, xavfga asoslangan va muntazam qayta ko‘rib chiqiladigan tartibga solish modelidir.

Maqola doirasida bildirilgan tahlillardan kelib chiqib, quyidagi yo‘nalishlarga alohida e’tibor qaratish maqsadga muvofiq: yuqori xavfli texnologiyalar uchun maxsus ruxsat va audit tartibi; idoralararo ma’lumot almashinuvida maqsadga muvofiqlik va minimalizm; avtomatlashtirilgan xulosalar ustidan inson nazorati; ma’lumotlar subyektining xabardor bo‘lishi va samarali shikoyat qilish imkoniyati; davlat xaridlarida algoritmik hisobdorlik talablarini belgilash. Ushbu yo‘nalishlar alohida-alohida emas, yagona boshqaruv sikli sifatida amalga oshirilganda kutilgan samara beradi.

Umumiy xulosa qilib aytganda, jamoat xavfsizligi tizimida raqamli texnologiyalardan foydalanish davlatning profilaktik va tezkor imkoniyatlarini kengaytiradi, biroq ularning ijtimoiy foydasi faqat huquqiy kafolatlar bilan birgalikda namoyon bo‘ladi. Texnologiya davlatning qonuniy vakolatini almashtirmaydi, algoritm insonning huquqiy mas’uliyatini bekor qilmaydi, axborot ko‘pligi esa shaxsiy hayotga cheklanmagan aralashuvni oqlamaydi. Shu bois O‘zbekistonda raqamli jamoat xavfsizligining istiqbolli modeli qonuniylik, zarurat, mutanosiblik, shaffoflik, inson nazorati va mustaqil hisobdorlik tamoyillariga tayangan holda shakllantirilishi 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 2003-yil 11-dekabrdagi 560-II-son “Axborotlashtirish to‘g‘risida”gi Qonuni. https://lex.uz/acts/-83472
4. O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ–547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni. https://lex.uz/uz/docs/-4396419
5. O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ–764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuni. Qonunchilik ma’lumotlari milliy bazasi, lex.uz.

6. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/1689/oj