

BIOMETRIK MA'LUMOTLARNI HIMOYA QILISHNING KONSTITUTSIYAVIY VA XALQARO-HUQUQIY ASOSLARI

Komilova Roza Hamrobek qizi

Davlat boshqaruvi huquqi yo'nalishi magistranti

Toshkent davlat yuridik universiteti

e-mail: hamrayevvnaa@gmail.com

O'zbek tilida annotatsiya. Ushbu maqola biometrik ma'lumotlarni himoya qilishning konstitutsiyaviy hamda xalqaro-huquqiy asoslarini tizimli tahlil qiladi. Tadqiqotning maqsadi shaxsning daxlsizligi, xususiy hayot sir-asrirlari va axborot xavfsizligi kesishmasida biometrik identifikatsiya amaliyotlarining huquqiy chegaralarini aniqlash hamda ularni milliy tartibga solishning takomillashuv yo'nalishlarini asoslashdan iborat. Metodologiya sifatida normativ-huquqiy tahlil, qiyosiy-huquqiy yondashuv, huquqni qo'llash amaliyotini doktrinal sharhlash va riskga asoslangan baholash modeli qo'llanildi. Ilmiy yangilik biometrik ma'lumotlarni "maxsus toifadagi shaxsiy ma'lumotlar" sifatida konstitutsiyaviy mutanosiblik testi orqali himoya qilish konsepsiyasini hamda xalqaro standartlar bilan uyg'unlashtirilgan minimal kafolatlar matritsasini taklif etishdadir. Amaliy ahamiyat nazorat mexanizmlari, rozilik institutining sifat mezonlari va transchegaraviy uzatishda kafolatlarining huquqiy dizaynini aniqlashtirish bilan ifodalanadi.

Аннотация на русском языке. Данная статья представляет системный анализ конституционных и международно-правовых основ защиты биометрических данных. Цель исследования состоит в определении правовых границ практик биометрической идентификации на пересечении неприкосновенности личности, тайны частной жизни и информационной безопасности, а также в обосновании направлений совершенствования национального регулирования в данной сфере. В качестве методологии применялись нормативно-правовой анализ, сравнительно-правовой подход, доктринальное толкование правоприменительной практики и модель оценки на основе рисков. Научная новизна выражается в предложении концепции защиты биометрических данных как «персональных данных особой категории» посредством теста конституциональной соразмерности, а также матрицы минимальных гарантий, согласованной с международными стандартами. Практическая значимость определяется уточнением правового дизайна механизмов надзора, качественных критериев института согласия и гарантий при трансграничной передаче данных.

Abstract in English. This article presents a systematic analysis of the constitutional and international legal foundations of biometric data protection. The

purpose of the research is to determine the legal boundaries of biometric identification practices at the intersection of personal inviolability, privacy, and information security, as well as to substantiate the directions for improving national regulation in this sphere. The methodology employed includes normative-legal analysis, a comparative-legal approach, doctrinal interpretation of law enforcement practice, and a risk-based assessment model. The scientific novelty lies in proposing a concept for protecting biometric data as "special category personal data" through a constitutional proportionality test, along with a matrix of minimum guarantees aligned with international standards. The practical significance is expressed in clarifying the legal design of oversight mechanisms, the qualitative criteria of the consent institution, and guarantees in cross-border data transfers.

Kalit soʻzlar. biometrik maʼlumotlar; shaxsiy hayot daxlsizligi; konstitutsiyaviy kafolatlar; xalqaro standartlar; mutanosiblik testi; transchegaraviy uzatish; rozilik

Ключевые слова. биометрические данные; неприкосновенность частной жизни; конституционные гарантии; международные стандарты; тест соразмерности; трансграничная передача; согласие

Keywords. biometric data; privacy; constitutional guarantees; international standards; proportionality test; cross-border transfer; consent

Introduction.

Biometrik maʼlumotlar shaxsni tanib olishga xizmat qiladigan fiziologik yoki xulq-atvor belgilarining raqamli ifodasidir, ularning huquqiy tabiatida alohida sezgirlik mavjud boʻlib, “shaxs” kategoriyasini bevosita identifikatsiya bilan bogʻlaydi. Ushbu sezgirlik mexanizmi shundaki, biometrik identifikatorlar parol yoki kartadan farqli ravishda almashtirilishi qiyin boʻlgan “tanaga bogʻliq kalit” boʻlib, bir marta sizib chiqqanida uzoq muddatli xavfni shakllantiradi. Masalan, yuz geometriyasi, barmoq izi, iris shabloni yoki ovoz spektri boʻyicha yaratilgan shablonlar masofadan turib tekshirishga imkon bergani uchun nazoratning koʻlamini kengaytiradi va xususiy hayotga aralashuv ehtimolini oshiradi. Xalqaro amaliyotda biometrika joriy etilishi bilan bogʻliq xavflar tez oʻsmoqda: identifikatsiya tizimlari kengaygani sayin millionlab subyektlar qamrab olinadi, ayrim yurisdiksiyalarda yirik biometrik bazalar oʻnlab million yozuvlardan iborat boʻlib, ularda xatoliklar va kamsitish xavfi ham ortadi. Ilmiy izoh shundan iboratki, biometrik maʼlumotlar nafaqat identifikatsiya, balki profil yaratish, kuzatuv va xulqni bashorat qilish uchun ham asos boʻla oladi, shu sababli ularni konstitutsiyaviy darajada himoya qilish “inson qadr-qimmatini” va “xususiy hayot” prinsiplarining amaliy koʻrinishi sifatida qaraladi [1; 2].

Biometrik maʼlumotlarni himoya qilish muammosi konstitutsiyaviy huquqlar kolliziyasi kontekstida dolzarb boʻlib, xavfsizlik, jinoyatchilikka qarshi kurash, davlat xizmatlari raqamlashtirilishi va shaxsiy erkinliklar oʻrtasidagi muvozanatni talab

qiladi. Bu kolliziya mexanizmi huquqiy cheklovlar qo'yishda qonuniylik, zaruriyat va mutanosiblik mezonlari ishlashiga bog'liq bo'lib, har bir biometrik ishlov berish maqsadi uchun alohida asos, chegaralar va nazorat kafolatlari zarur bo'ladi. Masalan, pasportlashtirish yoki chegara nazorati kabi sohalarda biometrik tekshiruv "ommaviy xizmat" ko'rinishini olsa-da, ayni ma'lumotlarning ikkilamchi maqsadlarda, masalan, ommaviy videokuzatuvda identifikatsiya qilish uchun qo'llanishi aralashuv intensivligini keskin oshiradi. Normativ tizimlar bu farqni aks ettirmasa, "maqsadning kengayib borishi" hodisasi yuzaga keladi va bu huquqiy aniqlikni susaytiradi; natijada shaxs roziligi formal tus olishi yoki umuman aylanib o'tilishi ehtimoli kuchayadi. Ilmiy izoh sifatida, zamonaviy doktrinada biometrika bilan ishlashni "riskga asoslangan tartibga solish" orqali baholash taklif qilinadi, chunki bir xil texnologiya turli kontekstda turlicha konstitutsiyaviy og'irlikka ega bo'ladi [3].

Mavjud adabiyotlar holati shuni ko'rsatadiki, biometrik ma'lumotlar ko'pincha shaxsiy ma'lumotlar rejimi doirasida tahlil qilinadi, biroq konstitutsiyaviy yondashuvda ularni "daxlsizlik" kafolatlari bilan bevosita bog'lash zarurati yetarli darajada ochilmay qolmoqda. Bu bo'shliqning mexanizmi shundaki, oddiy ma'lumotlar himoyasi qoidalari ko'proq ma'lumot aylanishi sikliga qaratilgan bo'lsa, konstitutsiyaviy tahlil aralashuvning legitim maqsadi, vositaning zarurligi va zarar-foйда nisbatini baholashni talab etadi. Masalan, ayrim tadqiqotlar rozilik institutini markaziy kafolat sifatida ko'rsa-da, davlat-hokimiyat munosabatlarida rozilik erkinligi cheklangan bo'lishi, xizmatdan foydalanish alternativasi mavjud emasligi tufayli "majburiy rozilik" paydo bo'lishi mumkin. Statistik kuzatuvlarda ma'lumotlar sizib chiqishi hodisalari yildan-yilga ko'payib borishi, ayniqsa markazlashgan bazalarning kiberxavfsizlikka yuqori talab qo'yishini tasdiqlaydi; bu esa "ma'lumot minimallashtirish" va "dezentralizatsiya"ning konstitutsiyaviy mazmunini kuchaytiradi. Ilmiy izohda esa biometrik shablonlarni qayta tiklash (inversion) yoki o'xshashlik bo'yicha moslashtirish xatolari (false match, false non-match) inson huquqlari nuqtai nazaridan "xato identifikatsiya" xavfini oshirishi qayd etiladi [4].

Ushbu maqolaning maqsadi biometrik ma'lumotlarni himoya qilishning konstitutsiyaviy va xalqaro-huquqiy asoslarini integratsiyalashgan model sifatida asoslash, shuningdek, milliy huquqiy tartibga solish uchun minimal kafolatlar to'plamini konseptual taklif qilishdan iborat. Mazkur maqsadning mexanizmi bir tomondan konstitutsiyaviy normalar va ularning huquqiy talqini, ikkinchi tomondan esa xalqaro shartnomalar va yumshoq huquq standartlari o'rtasida muvofiqlikni izlash orqali ta'minlanadi. Masalan, xususiy hayot daxlsizligi, shaxsiy ma'lumotlarni himoya qilish, samarali huquqiy himoya vositasi va kamsitmaslik prinsiplarini yagona "kafolatlar zanjiri" sifatida ko'rib, biometrik ishlov berishning barcha bosqichlari uchun talablar ishlab chiqiladi. Raqamli davlat xizmatlarida biometrik autentifikatsiya ulushi oshgani sari, huquqiy dizaynning aniqligi amaliy samaradorlikka ham ta'sir

ko'rsatadi, chunki noaniq qoidalar nizolar va ishonch tanqisligini kuchaytiradi. Ilmiy yangilik sifatida maqola mutanosiblik testini biometrik ishlov berishning "asos, maqsad, hajm, muddat, nazorat" parametrlari bilan operatsionlashtiradi va transchegaraviy uzatish uchun ekvivalent himoya mezonlarini taklif etadi [2; 5].

Materials and Methods.

Tadqiqot biometrik ma'lumotlar himoyasini normativ va doktrinal manbalar asosida o'rganishga tayangan bo'lib, konstitutsiyaviy-huquqiy tahlil markaziy usul sifatida tanlandi. Bu yondashuvning mexanizmi shundaki, biometrik ishlov berish shaxs huquqlariga aralashuv bo'lgani uchun uning asoslanishi faqat sohaviy qonunlar bilan emas, balki konstitutsiyaviy prinsiplar, jumladan qonuniylik va mutanosiblik bilan ham tekshiriladi. Masalan, har bir qayta ishlash holati uchun "aniq maqsad", "zarur minimal hajm" va "mustaqil nazorat" mezonlari bo'yicha normativ konstruktsiya qurilib, u xalqaro standartlar bilan qiyoslandi. Tadqiqotda ochiq manbalardagi normativ hujjatlar, xalqaro shartnomaviy standartlar va ma'lumotlarni himoya qilish bo'yicha asosiy doktrinal ishlar tahlil qilindi, bu esa dalillarning tekshiriluvchanligini oshirdi. Ilmiy izoh sifatida, konstitutsiyaviy metod shaxs huquqlarini "cheklash mumkin bo'lgan" va "mutlaq" elementlarga ajratib, biometrik identifikatsiya amaliyotida qaysi komponentlar alohida kafolat talab qilishini ko'rsatishga yordam beradi.

Metodologik majmua doirasida qiyosiy-huquqiy tahlil va funksional yondashuv qo'llanib, turli tizimlarda biometrik ma'lumotlar "maxsus toifa" sifatida qanday belgilanishi hamda qanday protsessual kafolatlar bilan ta'minlanishi solishtirildi. Bu mexanizm normativ matnlar o'xshash bo'lsa ham, ularning ishlash usuli institutlar, nazorat organlari va sanksiya tizimiga bog'liqligini ochib beradi. Masalan, ayrim yurisdiksiyalarda mustaqil ma'lumotlarni himoya qilish organlari kuchli vakolatga ega bo'lsa, boshqalarda sud nazorati ustun bo'lishi mumkin, bu esa biometrik qayta ishlashning amaliy "hisobdorlik" darajasini belgilaydi. Qiyosiy tahlilda transchegaraviy uzatish, avtomatlashtirilgan qaror qabul qilish va profil yaratish bilan bog'liq normalar alohida blok sifatida ko'rib chiqildi, chunki ular biometrik ishlov berishda eng yuqori xavfli zonani tashkil etadi. Ilmiy izoh shundan iboratki, funksional qiyoslash texnik terminlarni emas, huquqiy natijalarni solishtiradi va shu yo'l bilan milliy modellarning integratsiya salohiyatini oshiradi [5].

Tadqiqotda riskga asoslangan baholash modeli yordamida biometrik ma'lumotlar aylanishining bosqichlari bo'yicha huquqiy xavflar xaritasi tuzildi. Mazkur modelning mexanizmi identifikatsiya, autentifikatsiya va verifikatsiya kabi turli ishlatish ssenariylarida aralashuv intensivligi, xatolik ehtimoli va kamsitish tavakkalini alohida hisobga olishdan iborat. Masalan, bir martalik autentifikatsiya uchun lokal saqlash bilan markaziy bazaga yig'ishning xavf profili keskin farq qiladi, chunki markaziy bazada sizib chiqish oqibatlari ko'p subyektlarga bir vaqtning o'zida

ta'sir etadi. Tadqiqot mezonlari sifatida maqsad cheklovi, ma'lumot minimallashtirish, saqlash muddatining aniqligi, shifrlash va pseudonimlashtirish kabi texnik choralar, shuningdek, shikoyat va sudga murojaat qilish imkoniyatlari kiritildi; bu mezonlar bo'yicha normativ moslik baholandi. Ilmiy izohda, risk modeli huquqiy siyosatni "hamma uchun bir xil" qoidalar to'plamidan "kontekstga mos" kafolatlar tizimiga o'tkazishga xizmat qiladi, bu esa biometrika kabi dinamik texnologiyalar uchun metodologik jihatdan asosli hisoblanadi.

Results.

Biometrik ma'lumotlarni konstitutsiyaviy himoya qilishning birinchi natijasi shundan iboratki, ularni shaxsiy hayot daxlsizligi doirasida alohida sezgir ma'lumot sifatida tasniflash huquqiy aniqlikni oshiradi. Bu tasniflash mexanizmi biometrik shablonning identifikatsiya quvvatini e'tirof etib, uni qayta ishlashga qo'yiladigan talablarni oddiy kontakt ma'lumotlariga nisbatan qat'iyroq qilishni nazarda tutadi. Masalan, biometrik identifikatsiya qo'llanadigan davlat xizmatlarida alternativ identifikatsiya kanali mavjud bo'lishi rozilikning erkinligini kuchaytiradi va xizmatdan foydalanishdan chetlashtirish xavfini kamaytiradi. Natija sifatida minimal kafolatlar matritsasi taklif etildi: qonuniy asosning aniqligi, maqsad cheklovi, minimallashtirish, saqlash muddatlari, mustaqil nazorat va samarali huquqiy himoya vositalari alohida bandlar sifatida belgilandi. Ilmiy izoh sifatida, bunday matritsa konstitutsiyaviy prinsiplarni operatsion mezonlarga aylantirib, normativ ijodkorlik va huquqni qo'llashda bir xil standartni shakllantiradi.

Ikkinchi natija biometrik ishlov berishning qonuniyligi mutanosiblik testining to'rt bosqichli konstruksiyasi bilan baholanishi mumkinligidir: legitim maqsad, yaroqlilik, zaruriyat va tor ma'nodagi mutanosiblik. Bu mexanizm har bir bosqichda dalillash yukini kuchaytiradi, ya'ni organ yoki operator nima uchun aynan biometrika zarur bo'lganini, nima uchun kamroq aralashuvchi usul yetarli emasligini asoslab berishi kerak bo'ladi. Masalan, binoga kirishda biometrik kirish nazorati o'rniga kartali tizim yoki ikki faktorli autentifikatsiya yetarli bo'lsa, biometrik majburiy joriy etish zaruriyat mezonidan o'ta olmaydi. Tahliliy natijada biometrik bazalar uchun saqlash muddatini "maqsadga bog'liq minimal muddat" tarzida belgilash va muddat tugagach qayta tiklab bo'lmaydigan o'chirishni talab qilish taklifi shakllantirildi. Ilmiy izoh sifatida, tor ma'nodagi mutanosiblik bosqichi aynan xatolik ehtimoli va kamsitish oqibatlarini inobatga olgani uchun biometrik tizimlarning adolatli ishlashini konstitutsiyaviy darajada himoya qiladi.

Uchinchi natija xalqaro-huquqiy asoslar biometrik himoyani "ekvivalent kafolatlar" tamoyili orqali mustahkamlashini ko'rsatadi, ayniqsa transchegaraviy uzatish va bulut infratuzilmasidan foydalanishda. Bu mexanizm shundan iboratki, biometrik ma'lumotlar boshqa davlat yoki yurisdiksiyaga uzatilganda, u yerda ham mazmunan teng himoya darajasi ta'minlanishi, aks holda uzatish cheklanishi yoki

qo'shimcha shartlar bilan ruxsat etilishi kerak bo'ladi. Masalan, shartnomaviy bandlar, texnik shifrlash va audit talablarini birlashtirgan "kombinatsiyalashgan kafolatlar" modeli transchegaraviy riskni pasaytiradi, chunki faqat bitta instrument odatda yetarli bo'lmaydi. Natijada biometrik uzatish bo'yicha huquqiy dizayn uchun uch pog'onali filtr taklif etildi: maqsadning aniqligi, qabul qiluvchi tarafdagi himoya darajasi, va doimiy monitoring hamda shikoyat mexanizmlarining mavjudligi. Ilmiy izoh sifatida, ekvivalentlik tamoyili xalqaro me'yorlarning milliy qonunchilikka "ko'chirilishi" emas, balki ularning huquqiy natijalarini ta'minlashni anglatadi va bu yondashuv turli huquqiy tizimlar o'rtasida muvozanatli integratsiyani qo'llab-quvvatlaydi [2; 6].

To'rtinchi natija texnik va huquqiy choralar o'rtasidagi o'zaro bog'liqlik biometrik himoyaning ajralmas komponenti ekanini ko'rsatadi. Bu bog'liqlik mexanizmi shundaki, huquqiy prinsiplar, masalan minimallashtirish yoki maxfiylik, amalda shifrlash, hashing, shablon himoyasi va kirish nazorati kabi texnik yechimlarsiz "deklarativ" bo'lib qoladi. Masalan, biometrik shablonlarni saqlashda qayta tiklashni qiyinlashtiruvchi transformatsiya usullari qo'llansa, sizib chiqish oqibatlari kamayadi, biroq bu usullar noto'g'ri joriy etilsa autentifikatsiya xatolari ortishi mumkin. Natijaviy jadval sifatida biometrik ishlov berish bosqichlari bo'yicha minimal kafolatlar keltiriladi, bunda har bir bosqich uchun huquqiy talab va texnik chora juftlab beriladi. Raqamli ko'rsatkich sifatida baholash shkalasi 0 dan 3 gacha darajalar bilan taklif qilinib, 0 daraja kafolat yo'qligini, 3 daraja esa to'liq moslikni anglatadi; bu yondashuv audit jarayonini standartlashtirishga yordam beradi. Ilmiy izohda, huquqiy-texnik muvofiqlik "hisobdorlik" prinsipining amaliy o'lchovini beradi, chunki operator faqat qoidaga murojaat qilish bilan emas, balki real himoya konfiguratsiyasi bilan javobgar bo'ladi.

Raqamli amaliyot nuqtai nazaridan, shifrlash va hashing aralashmasi bo'lgan yondashuvlar auditda tekshiriladigan ko'rsatkichlarga ega bo'lib, masalan, kalit aylanish davriyligi yoki ruxsatlar modeli kabi parametrlar orqali baholanadi. Ilmiy izoh sifatida, texnik choralarning huquqiy tizimda "minimal talab" sifatida tan olinishi operatorning ehtiyot choralarni standartlashtiradi va kiberxavfsizlikdagi inson omili xatarlarini qisman kompensatsiya qiladi.

Discussion.

Olingan natijalar shuni anglatadiki, biometrik ma'lumotlar himoyasi faqat shaxsiy ma'lumotlar to'g'risidagi umumiy qoidalar bilan cheklanmasdan, konstitutsiyaviy prinsiplar bilan mustahkamlangan alohida kafolatlar tizimini talab qiladi. Bu xulosa mexanizmi mavjud doktrinadagi "ma'lumotga egalik" yondashuvidan ko'ra "aralashuv intensivligi" yondashuvi kuchliroq ekanini ko'rsatadi, chunki biometrika inson tanasi bilan uzviy bog'liq bo'lgan identifikator sifatida huquqiy oqibatlarni og'irlashtiradi. Masalan, xalqaro standartlarda biometrik ma'lumotlar ko'pincha maxsus toifa sifatida ko'rilishi, rozilikdan tashqari alohida

asoslar, kuchaytirilgan xavfsizlik choralari talab qilishi natijalarimiz bilan uyg'unlashadi. Raqamli jihatdan, markazlashgan bazalarning ko'lamlashuvi bilan "bir nuqtali ishdan chiqish" xavfi ortadi, bu esa minimallashtirish va dezentralizatsiya bo'yicha tavsiyalarimizni mantiqan qo'llab-quvvatlaydi. Ilmiy izoh sifatida, konstitutsiyaviy mutanosiblik testi xalqaro standartlar bilan birga qo'llanganda milliy siyosatda texnologik neytrallikni saqlab, yangi biometrik modalitlar paydo bo'lganda ham asosiy kafolatlarni barqaror ushlab turadi [2; 5].

Natijalarni mavjud yondashuvlar bilan qiyosiy tahlil qilish biometrik ishlov berishda rozilik instituti "yagona tayanch" bo'la olmasligini ko'rsatadi. Bu mexanizm shaxs va davlat yoki yirik platformalar o'rtasidagi kuchlar nomutanosibligi bilan izohlanadi, ya'ni rozilik ko'pincha xizmat shartiga bog'lab qo'yiladi va erkin tanlov elementi kamayadi. Masalan, identifikatsiya tizimi majburiy bo'lgan vaziyatda rozilik formal bo'lib qoladi, shu sababli mustaqil nazorat, shaffoflik va shikoyat mexanizmlari kabi kafolatlar rozilikni to'ldiruvchi asosiy komponentga aylanadi. Raqamlar bilan ifodalaganda, riskga asoslangan baholash shkalasida rozilik mavjudligi 1 ballni berishi mumkin, biroq mustaqil audit va minimallashtirish bo'lmasa, umumiy moslik darajasi 3 ballga chiqmaydi; bu "kafolatlar paket" sifatida ishlash zarurligini ko'rsatadi. Ilmiy izohda, biometrik ma'lumotlar bo'yicha "hisobdorlik" konsepsiyasi operatorning protsessual majburiyatlarini, jumladan hujjatlashtirish, ta'sirni baholash va insidentlarni xabar qilishni kuchaytirishni talab qiladi, bu esa xalqaro amaliyotdagi zamonaviy tendensiyalar bilan mos keladi [6].

Muvozanatli yondashuv nuqtai nazaridan, xavfsizlik manfaatlari bilan shaxsiy hayot daxlsizligi o'rtasidagi ziddiyat "nol yig'indi" sifatida talqin qilinmasligi lozim, chunki yaxshi dizayn qilingan kafolatlar tizimi ikkala maqsadni ham bir vaqtda qo'llab-quvvatlashi mumkin. Bu mexanizm shundaki, aniq maqsad va minimallashtirish xavfsizlik tizimlarining sifatini pasaytirmaydi, aksincha ortiqcha ma'lumot yig'ishdan keladigan kiberxatarlarni kamaytiradi va tizimga bo'lgan ishonchni oshiradi. Masalan, lokal saqlashga asoslangan autentifikatsiya yechimlari markazlashgan bazaga nisbatan kamroq "jamoaviy zarar" keltiradi, chunki bir qurilmaning buzilishi barcha foydalanuvchilarga ta'sir qilmaydi. Statistik yondashuv sifatida, markazlashgan bazalarda insidentning o'rtacha zarar ko'lami ko'proq subyektlarni qamrab olishi mantiqan kutiladi; shu bois huquqiy siyosat riskni tarqatish tamoyilini qo'llashi maqsadga muvofiq. Ilmiy izoh sifatida, texnologik arxitektura va huquqiy normalar o'rtasidagi uyg'unlikni ta'minlash "privacy by design" konsepsiyasiga yaqin bo'lib, u konstitutsiyaviy qadriyatlarni tizim ichiga joylashtirishning institutsional usuli sifatida qaraladi [3].

Tadqiqotning cheklovlari shundan iboratki, maqola asosan normativ va doktrinal tahlilga tayanadi hamda amaliy sud qarorlari va empirik audit ma'lumotlari bilan keng ko'lamda boyitilmagan. Bu cheklov mexanizmi biometrik tizimlar bo'yicha

ko'plab ma'lumotlar yopiq yoki cheklangan kirishli bo'lishi, shuningdek, texnik konfiguratsiyalar tez yangilanib turishi bilan bog'liq. Masalan, bir xil biometrik modalit turli algoritmlar va ma'lumotlar to'plamlari bilan turlicha xatolik profiliga ega bo'ladi, biroq normativ tahlil buni faqat umumiy risk sifatida ifodalay oladi. Shunga qaramay, raqamli siyosat ishlab chiqishda normativ "minimal kafolatlar" konsepsiyasi barqaror yo'nalish berishi mumkin, chunki u texnik tafsilotlar o'zgarsa ham huquqiy mezonlarni saqlab qoladi. Ilmiy izoh sifatida, kelajak tadqiqotlari biometrik tizimlarning aniqlik ko'rsatkichlari, kamsitish risklari va insident statistikasi bo'yicha empirik ma'lumotlarni normativ mutanosiblik testiga integratsiya qilish orqali huquqiy baholashning dalillilik darajasini oshirishi lozim [4; 6].

Conclusion.

Biometrik ma'lumotlar shaxsni bevosita identifikatsiya qiluvchi va almashtirilishi qiyin bo'lgan sezgir axborot sifatida konstitutsiyaviy himoyaning kuchaytirilgan rejimini talab qiladi. Tadqiqot biometrik ishlov berishning qonuniy chegaralari qonuniylik, zaruriyat va mutanosiblik mezonlari bilan baholanishi, shuningdek, maqsad cheklovi va minimallashtirish prinsiplarini operatsion talablar sifatida joriy etish zarurligini asoslab berdi. Natijalar biometrik ma'lumotlar uchun minimal kafolatlar matritsasini taklif qilib, yig'ishdan o'chirishgacha bo'lgan siklda huquqiy va texnik choralar uyg'unligini ko'rsatdi. Transchegaraviy uzatish holatlarida ekvivalent himoya tamoyili va kombinatsiyalashgan kafolatlar modeli risklarni pasaytirishning markaziy instrumenti sifatida belgilandi. Rozilik instituti muhim bo'lsa-da, u mustaqil nazorat, shaffoflik, audit va samarali shikoyat mexanizmlari bilan to'ldirilmaganda yetarli kafolat bera olmasligi umumlashtirildi. Umuman olganda, konstitutsiyaviy va xalqaro-huquqiy asoslarni integratsiyalash biometrik texnologiyalar joriy etilayotgan sharoitda huquqiy aniqlik, ishonch va xavfsizlikni bir vaqtda ta'minlashga xizmat qiladi.

Adabiyotlar ro'yxati.

1. Warren S. D., Brandeis L. D. The Right to Privacy. Boston, Harvard Law Review, 1890. 29 p.
2. Kuner C. Transborder Data Flows and Data Privacy Law. Oxford, Oxford University Press, 2013. 352 p.
3. Solove D. J. Understanding Privacy. Cambridge, Harvard University Press, 2008. 256 p.
4. Jain A. K., Ross A., Prabhakar S. An Introduction to Biometric Recognition. New York, IEEE Transactions on Circuits and Systems for Video Technology, 2004. P. 4-20.
5. De Hert P., Papakonstantinou V. The GDPR as a Legal Instrument for Biometric Data Protection. Brussels, European Data Protection Law Review, 2018. P. 1-15.
6. Bygrave L. A. Data Privacy Law. Oxford, Oxford University Press, 2014. 272 p.