RAQAMLI JAMIYATDA SHAXSIY HAYOT DAXLSIZLIGI HUQUQINING KONSTITUTSIYAVIY KAFOLATLARINI TAKOMILLASHTIRISH

СОВЕРШЕНСТВОВАНИЕ КОНСТИТУЦИОННЫХ ГАРАНТИЙ ПРАВА НА НЕПРИКОСНОВЕННОСТЬ ЧАСТНОЙ ЖИЗНИ В ЦИФРОВОМ ОБЩЕСТВЕ

IMPROVING CONSTITUTIONAL GUARANTEES OF THE RIGHT TO PRIVACY IN THE DIGITAL SOCIETY

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

Annotatsiya: Mazkur maqolada raqamli transformatsiya sharoitida shaxsiy hayot daxlsizligi huquqining konstitutsiyaviy mazmuni, uning axborot texnologiyalari bilan o‘zaro ta’siri hamda huquqiy kafolatlarni kuchaytirish masalalari ilgari so‘rilgan. Shaxsga doir ma’lumotlarni yig‘ish va qayta ishlash, algoritmik profillash, biometrik identifikatsiya, davlat va xususiy sektorning raqamli kuzatuv amaliyotlari bilan bog‘liq xavflar tahlil qilingan.

Kalit so‘zlar: shaxsiy hayot daxlsizligi, konstitutsiyaviy kafolat, shaxsga doir ma’lumotlar, raqamli huquqlar, biometrik ma’lumotlar, algoritmik profillash, mutanosiblik, axborot xavfsizligi, raqamli kuzatuv.

Аннотация: В данной статье рассматриваются конституционно-правовое содержание права на неприкосновенность частной жизни в условиях цифровой трансформации, его взаимосвязь с информационными технологиями, а также вопросы усиления правовых гарантий. Анализируются риски, связанные со сбором и обработкой персональных данных, алгоритмическим профилированием, биометрической идентификацией и практикой цифрового наблюдения, осуществляемой государственными органами и частным сектором.

Ключевые слова: неприкосновенность частной жизни, конституционные гарантии, персональные данные, цифровые права, биометрические данные, алгоритмическое профилирование, соразмерность, информационная безопасность, цифровое наблюдение.

Abstract: This article examines the constitutional and legal dimensions of the right to privacy in the context of digital transformation, its interaction with information technologies, and issues related to strengthening legal safeguards. It analyzes the risks associated with the collection and processing of personal data, algorithmic profiling, biometric identification, and digital surveillance practices carried out by public authorities and the private sector.

Keywords: privacy, constitutional guarantees, personal data, digital rights, biometric data, algorithmic profiling, proportionality, information security, digital surveillance.

Raqamli jamiyat tushunchasi faqat davlat xizmatlarini elektron shaklga o‘tkazish yoki iqtisodiy munosabatlarda ma’lumotlardan foydalanishni anglatmaydi. U shaxsning kundalik xulq-atvori, aloqalari, xarid odatlari, harakatlanish yo‘nalishlari va hatto dunyoqarashiga doir axborot izlari muntazam shakllanadigan ijtimoiy muhitni ham ifodalaydi. Bunday sharoitda shaxsiy hayot daxlsizligi huquqi texnologiyadan voz kechish talabi emas, balki texnologik taraqqiyot jarayonida insonning mustaqil qaror qabul qilishi va o‘ziga oid ma’lumotlar ustidan asosli nazoratni saqlab qolish kafolatidir.

O‘zbekiston Respublikasi Konstitutsiyasining 31-moddasida har kimning shaxsiy hayoti daxlsizligi, shaxsiy va oilaviy sirga ega bo‘lish, o‘z sha’ni va qadr-qimmatini himoya qilish huquqi, shuningdek yozishmalar, telefon orqali so‘zlashuvlar, pochta, elektron va boshqa xabarlar sir

saqlanishi huquqi mustahkamlangan. Ushbu huquq faqat qonunga muvofiq va sud qaroriga asosan cheklanishi mumkinligi belgilangan. Mazkur modda shaxsga doir ma'lumotlarni himoya qilish hamda noto'g'ri ma'lumotlarni tuzatishni va qonunga xilof to'plangan yoxud huquqiy asosini yo'qotgan ma'lumotlarni yo'q qilishni talab etish huquqini ham e'tirof etadi [1].

Konstitutsiyaviy qoida raqamli munosabatlarda ikki xil vazifani bajaradi: birinchidan, davlat organlarining shaxsiy hayotga asossiz aralashuvini cheklaydi; ikkinchidan, qonun chiqaruvchi va huquqni qo'llovchi organlar zimmasiga xususiy raqamli platformalar tomonidan sodir etilishi mumkin bo'lgan aralashuvlardan ham samarali himoya mexanizmlarini yaratish majburiyatini yuklaydi. Demak, daxlsizlikning zamonaviy mazmuni nafaqat "aralashmaslik", balki "himoya qilish va tiklash" majburiyatlari bilan ham belgilanadi.

Shaxsiy hayot daxlsizligi, shaxsga doir ma'lumotlar himoyasi va axborot xavfsizligi o'zaro bog'liq, biroq aynan bir tushuncha emas. Daxlsizlik shaxsning xususiy hayot sohasini tashqi nazoratdan himoya qiladi; ma'lumotlar himoyasi yig'ish, saqlash, uzatish va o'chirish kabi operatsiyalarning huquqiy tartibini belgilaydi; axborot xavfsizligi esa tizimning maxfiyligi, yaxlitligi va mavjudligini ta'minlashga yo'naltirilgan texnik hamda tashkiliy choralarni qamrab oladi. Axborot tizimi texnik jihatdan xavfsiz bo'lishi mumkin, ammo unda ma'lumotlar qonuniy asossiz yoki nomutanosib hajmda qayta ishlansa, konstitutsiyaviy muammo saqlanib qoladi.

"Shaxsga doir ma'lumotlar to'g'risida"gi Qonun shaxsga doir ma'lumotlar bilan ishlashning asosiy tushunchalari, subyekt va operatorning huquq hamda majburiyatlari, qayta ishlash shartlari va himoya mexanizmlarini belgilaydi [2]. "Axborotlashtirish to'g'risida"gi Qonun axborot resurslari va tizimlari bilan bog'liq munosabatlar uchun umumiy huquqiy asos yaratadi [3]. "Kiberxavfsizlik to'g'risida"gi Qonun esa raqamli infratuzilmaga oid xavflarni boshqarish masalalarini tartibga soladi [4]. Shu bilan birga, mazkur hujjatlarning mavjudligi barcha yangi texnologik vaziyatlarga tayyor, batafsil protsessual javob mavjudligini anglatmaydi.

Shu o'rinda ta'kidlash lozimki, ma'lumotni qayta ishlashga rozilik berish huquqiy himoyaning yagona vositasi bo'la olmaydi. Platformadan foydalanish uchun taqdim etiladigan uzun va murakkab shartlar ko'pincha shaxsning ongli, erkin va aniq maqsadga yo'naltirilgan tanlovini ta'minlamaydi. Rozilikni haqiqiy deb baholashda uning tushunarliligi, muayyanligi, qaytarib olish imkoniyati va xizmatdan foydalanish bilan majburiy bog'lanmaganligi hisobga olinishi lozim. Ayniqsa, voyaga yetmaganlar va raqamli savodxonligi past foydalanuvchilar uchun standart shartnomaviy mexanizmlar yetarli bo'lmasligi mumkin.

Raqamli iqtisodiyotda eng ko'p uchraydigan xatarlardan biri — ma'lumotlarning dastlabki maqsaddan chetga chiqib qayta ishlanishidir. Masalan, fuqaroga elektron xizmat ko'rsatish uchun olingan aloqa ma'lumotlarini uning xabarisiz reklama profili yaratish uchun qo'llash yoki xizmat sifati monitoringi uchun yig'ilgan geolokatsiya tarixidan xulq-atvorni baholashda foydalanish dastlabki huquqiy asosni qayta tekshirishni talab etadi. Maqsadni cheklash va ma'lumotlarni minimallashtirish tamoyillari aynan shunday holatlarning oldini olishga xizmat qiladi.

Biometrik identifikatsiya alohida konstitutsiyaviy sezgirlikka ega. Yuz tasviri, barmoq izi yoki ovoz xususiyatlari odatiy paroldan farqli ravishda oson almashtirilmaydi. Shuning uchun biometrik ma'lumotlarning sizib chiqishi uzoq muddatli xavf tug'dirishi mumkin. Ularni qo'llashda qat'iy maqsad, muqobil identifikatsiya usulining mavjudligi, saqlash muddati, foydalanish huquqlari va mustaqil audit mexanizmlari oldindan belgilanishi maqsadga muvofiq. Biometrik texnologiyaning qulayligi o'z-o'zidan uning cheklanmagan qo'llanishini oqlamaydi.

Sun'iy intellekt vositasida amalga oshiriladigan algoritmik profillash shaxs haqidagi alohida faktlarni birlashtirib, uning iqtisodiy ahvoli, qiziqishlari, sog'lig'i yoki boshqa nozik xususiyatlari haqida ehtimoliy xulosalar chiqarishi mumkin. Bunda ma'lumotlarning bir qismi ochiq manbalardan olingan bo'lsa ham, ularning kombinatsiyasi shaxsiy hayotga sezilarli ta'sir ko'rsatishi ehtimoldan xoli emas. Shu sababli "ochiq ma'lumot" tushunchasini "istalgan maqsadda cheksiz foydalanish mumkin bo'lgan ma'lumot" sifatida talqin etish konstitutsiyaviy himoyani zaiflashtiradi.

Davlat tomonidan raqamli kuzatuv qo'llanilganda qonuniylik mezoni alohida ahamiyat kasb etadi. Aralashuvga ruxsat beruvchi norma ochiq, tushunarli va oldindan bashorat qilish mumkin

bo‘lgan darajada aniq bo‘lishi, vakolatli organlar doirasi hamda ma’lumotdan foydalanish maqsadi chegaralanishi lozim. Qonuniy maqsad mavjudligi har qanday vositani avtomatik ravishda oqlamaydi: zarurat va mutanosiblik mustaqil baholanishi, kamroq aralashuvchi muqobil choralar mavjudligi tekshirilishi kerak.

Mutanosiblik sinovi to‘rt bosqichda ifodalanishi mumkin: aralashuvning qonuniy maqsadi aniqlanadi; tanlangan choraning shu maqsadga erishishga yaroqliligi tekshiriladi; kamroq cheklovchi vosita mavjud yoki mavjud emasligi baholanadi; nihoyat, kutilayotgan jamoat foydasi bilan shaxs huquqiga yetkaziladigan zarar o‘zaro solishtiriladi. Bu yondashuv konstitutsiyaviy huquqlarni mavhum e’lon qilishdan amaliy huquqiy nazorat standartiga o‘tishga yordam beradi.

Elektron yozishmalar va xabarlar siriga aralashuv masalasida sud nazorati faqat ruxsat berish bosqichiga qaratilmasligi lozim. Qonunda nazarda tutilgan hollarda aralashuvning davomiyligi, olingan ma’lumotlardan keyingi foydalanish, uchinchi shaxslarga uzatish, saqlash va yo‘q qilish tartibi ham tekshiriladigan bo‘lishi kerak. Maxfiy choralar xususiyati sababli fuqaroni har doim darhol xabardor qilish imkoni bo‘lmasligi mumkin, biroq bu mustaqil nazorat va keyingi samarali shikoyat mexanizmlarining ahamiyatini oshiradi.

Xalqaro huquqda shaxsiy hayotga aralashuvni cheklashning umumiy asoslari Inson huquqlari umumjahon deklaratsiyasining 12-moddasi hamda Fuqarolik va siyosiy huquqlar to‘g‘risidagi xalqaro paktning 17-moddasida ifodalangan [5; 6]. BMT Inson huquqlari qo‘mitasining 16-son umumiy sharhi davlatlarning noqonuniy yoki o‘zboshimchalik bilan aralashuvdan himoya qilish majburiyatlarini izohlaydi [7]. Ushbu standartlar raqamli texnologiyalar davrida ham o‘z ahamiyatini saqlaydi.

Yevropa Ittifoqining Umumiy ma’lumotlarni himoya qilish reglamenti — GDPR — shaxsga doir ma’lumotlarni qayta ishlashning qonuniy asoslari, subyekt huquqlari, hisobdorlik va ma’lumotlarni loyihalash bosqichidan himoyalash kabi institutlari bilan qiyosiy o‘rganishga arziydi [8]. Biroq xorijiy modelni milliy huquqqa mexanik ko‘chirish to‘g‘ri emas: institutsional imkoniyatlar, sud amaliyoti, davlat xizmatlarining raqamlashtirish darajasi va iqtisodiy xarajatlar inobatga olinishi kerak.

Yevropa inson huquqlari sudi amaliyotida shaxsiy hayot tushunchasi keng talqin qilinadi; texnologik kuzatuv va ma’lumotlarni saqlashga oid ishlar nazorat vakolatining aniqligi va suiiste’molga qarshi kafolatlar zarurligini ko‘rsatadi. Xususan, Roman Zakharov v. Russia ishida maxfiy kuzatuvga doir huquqiy kafolatlarning sifati muhokama qilingan [9]. Mazkur yondashuv milliy qonunchilik uchun majburiy ko‘rsatma sifatida emas, balki qiyosiy huquqiy tahlil manbasi sifatida ahamiyatlidir.

Raqamli huquqlarni ta’minlashda konstitutsiyaviy kafolatning samaradorligi faqat normaning mavjudligi bilan emas, balki shaxsning huquqiy holatidagi real natija bilan baholanishi kerak. Fuqaro o‘zi haqida qanday ma’lumot yig‘ilganini bilishi, uning xatoligini tuzattirishi, qonuniy asossiz ishlov berishga e’tiroz bildirishi va zarur hollarda ma’lumotlarni o‘chirishni talab qilishi mumkin bo‘lgan protsedura aniq, qulay va tekshiriladigan bo‘lishi lozim. Murojaat yuborish imkoniyatining o‘zi yetarli emas; murojaatning asosli ko‘rib chiqilishi va qarorning ijrosi ham muhim.

Tadqiqot natijalari shuni ko‘rsatdiki, huquqni himoya qilishning faqat reaktiv modeli — ya’ni huquq buzilgandan keyin shikoyat qilish — raqamli muhitda yetarli emas. Bir marta tarqalgan shaxsiy ma’lumotning nusxalari ko‘payishi, chet el serverlariga uzatilishi yoki avtomatlashtirilgan tizimlarda takror ishlatilishi mumkin. Shu sababli proaktiv yondashuv, ya’ni xavfni oldindan baholash, ma’lumotlar hajmini cheklash, xavfsizlikni tizim arxitekturasiga kiritish va muntazam audit o‘tkazish ustuvor ahamiyatga ega.

Mazkur maqolada shaxsiy hayot daxlsizligining konstitutsiyaviy kafolatlarini baholash uchun “besh mezonli model” taklif etiladi: normativ aniqlik, maqsadga muvofiqlik, mutanosiblik, institutsional hisobdorlik va huquqni amalda tiklash imkoniyati. Har bir yangi raqamli loyiha ushbu mezonlar bo‘yicha tekshirilsa, texnologiyani joriy etishdan oldin inson huquqlariga salbiy ta’sir ko‘rsatishi mumkin bo‘lgan omillarni aniqlash osonlashadi. Model mustaqil huquqiy norma

emas, balki qonunchilik va boshqaruv amaliyotini takomillashtirishga doir ilmiy taklif sifatida ilgari surilmoqda.

Birinchi yo‘nalish sifatida davlat organlari va katta hajmdagi ma’lumotlarni qayta ishlovchi subyektlar uchun yuqori xavfli operatsiyalarga nisbatan shaxsiy hayotga ta’sirni baholash tartibini qonunchilikda batafsil belgilash taklif etiladi. Baholashda ishlov berish maqsadi, ma’lumotlar toifasi, texnologik xavf, ehtimoliy zarar, muqobil yechim va nazorat choralari aks etishi lozim. Bunday tartib joriy etilganda uning doirasi va mezonlari aniq ko‘rsatilishi, kichik biznesga ortiqcha yuk yaratmasligi kerak.

Ikkinchi yo‘nalish — avtomatlashtirilgan qarorlar yuzasidan protsessual kafolatlarni kuchaytirishdir. Agar algoritmik baholash shaxsning huquqlari yoki qonuniy manfaatlariga sezilarli ta’sir etsa, fuqaro qarorning asosiy omillari haqida tushunarli ma’lumot olish, xatolarni ko‘rsatish, inson ishtirokida qayta ko‘rib chiqishni talab qilish va natijadan shikoyat qilish imkoniyatiga ega bo‘lishi maqsadga muvofiq. Bunda tijorat siri va kiberxavfsizlik manfaatlari bilan shaxsning himoyalanish huquqi o‘rtasida oqilona muvozanat saqlanishi zarur.

Uchinchi yo‘nalish biometrik ma’lumotlarni qayta ishlashning yuqori xavfli shakllarini alohida tartibga solishga qaratiladi. Xususan, ommaviy identifikatsiya texnologiyalari bo‘yicha aniq qonuniy asos, maqsad va hududiy-vaqt chegaralari, ma’lumotlarni saqlash muddati, ruxsat va audit mexanizmlari belgilanishi lozim. Texnologiya ishlashidagi xatoliklar ayrim shaxslarning asossiz tekshirilishi yoki xizmatdan chetlashtirilishiga olib kelmasligi uchun inson nazorati kafolatlanishi kerak.

To‘rtinchi yo‘nalish shaxsga doir ma’lumotlarning sizib chiqishi haqida xabardor qilish tizimini rivojlantirish bilan bog‘liq. Xavfning jiddiyligi, hodisa toifasi va oqibatlarini inobatga olgan holda vakolatli organga va zarar ko‘rishi mumkin bo‘lgan shaxslarga xabar berishning aniq muddatlari hamda mazmuni belgilanadigan tartib muhokama qilinishi mumkin. Bunday tizim faqat jazolashga emas, balki zarar ko‘lamini kamaytirish, tezkor himoya choralarini ko‘rish va tizimli xatolarni bartaraf etishga xizmat qilishi lozim.

Beshinchi yo‘nalish raqamli savodxonlik va konstitutsiyaviy huquqiy madaniyatni uzviy rivojlantirishdir. Fuqarolar ma’lumotlarini kim va nima maqsadda qayta ishlayotganini aniqlash, maxfiylik sozlamalaridan foydalanish, fishing va soxta ilovalardan ehtiyot bo‘lish, shuningdek shikoyat qilish tartibini bilishlari kerak. Shu bilan birga, davlat va xususiy tashkilotlarning xodimlari uchun ma’lumotlarni himoya qilishga oid muntazam amaliy o‘quvlar tashkil etilishi qonun talablarini kundalik amaliyotga singdiradi.

Yuqoridagilarni inobatga olgan holda, shaxsiy hayot daxlsizligini ta’minlashning konstitutsiyaviy modeli uch darajada rivojlantirilishi zarur:

birinchisi — aniq moddiy-huquqiy standartlar;

ikkinchisi — mustaqil va hisobdor nazorat institutlari;

uchinchisi — shaxs uchun qulay, tezkor va samarali tiklash vositalari.

Ushbu darajalardan birortasi yetarli ishlamasa, konstitutsiyaviy kafolatning amaliy samarasi pasayadi.

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

- yuqori xavfli ma’lumotlar bilan ishlashni oldindan baholash;
- algoritmik qarorlar ustidan inson nazoratini ta’minlash;
- biometrik ma’lumotlarga nisbatan kuchaytirilgan huquqiy rejimni rivojlantirish;
- raqamli kuzatuvda sud va mustaqil nazorat kafolatlarini mustahkamlash;
- ma’lumotlar buzilishi yuzasidan samarali xabardor qilish va zararni kamaytirish tartiblarini takomillashtirish.

Ushbu takliflar alohida qonunchilik ekspertizasi, manfaatdor tomonlar bilan muhokama va tartibga solish ta’sirini baholashni talab etadi.

Umumiy xulosa qilib aytganda, raqamli jamiyatda shaxsiy hayot daxlsizligi huquqini himoya qilish inson qadr-qimmati, erkinligi va huquqiy davlat tamoyillarining amaliy ifodasidir. O‘zbekiston Konstitutsiyasida mustahkamlangan kafolatlar raqamli muhitdagi yangi xavflarni

baholash uchun mustahkam normativ asos yaratadi. Kelgusidagi ustuvor vazifa ushbu kafolatlarni tushunarli protseduralar, samarali nazorat, texnologik ehtiyotkorlik va real huquqiy tiklash mexanizmlari bilan to‘ldirishdan iborat. Shundagina raqamlashtirish inson huquqlarini cheklovchi emas, balki ularni ro‘yobga chiqaruvchi omilga aylanishi mumkin.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Konstitutsiyasi (2023-yil 30-apreldagi referendumda qabul qilingan yangi tahrir)
2. O‘zbekiston Respublikasining «Shaxsga doir ma’lumotlar to‘g‘risida»gi Qonuni, 2019-yil 2-iyul, O‘RQ-547-son.
3. O‘zbekiston Respublikasining «Axborotlashtirish to‘g‘risida»gi Qonuni, 2003-yil 11-dekabr, 560-II-son.
4. O‘zbekiston Respublikasining «Kiberxavfsizlik to‘g‘risida»gi Qonuni, 2022-yil 15-aprel, O‘RQ-764-son.
5. BMT. Inson huquqlari umumjahon deklaratsiyasi. 1948-yil 10-dekabr, 12-modda.
6. BMT. Fuqarolik va siyosiy huquqlar to‘g‘risidagi xalqaro pakt. 1966-yil 16-dekabr
7. UN Human Rights Committee. General Comment No. 16: Article 17 (Right to Privacy). 1988.
8. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). 27 April 2016.
9. European Court of Human Rights. Roman Zakharov v. Russia [GC], Application No. 47143/06, Judgment of 4 December 2015.