



**HUMAN**  
SCIENCES.UZ

ISSN 3093-8961

[www.humansciences.uz](http://www.humansciences.uz)

**INSONSHUNOSLIK FANLARI JURNALI**  
**JOURNAL OF HUMANITIES**  
**ЖУРНАЛ ГУМАНИТАРНЫХ НАУК**

**2026**

**2-JILD | 5-SON**



SAYT: <https://humansciences.uz>

**HUMANSIENCES.UZ**

*№ 5 (2)-2026*

**INSONSHUNOSLIK FANLARI JURNALI**

**JOURNAL OF HUMANITIES**

**ЖУРНАЛ ГУМАНИТАРНЫХ НАУК**

**TOSHKENT-2026**

## **BOSH MUHARRIR:**

Isanova Feruza Tulqinovna

## **TAHRIR HAY'ATI:**

### *07.00.00 – TARIX FANLARI*

Rajapov Mardonbek Qosimboy o'g'li  
Tarix fanlari bo'yicha falsafa doktori (PhD).  
E-mail: [mardonbekoff@gmail.com](mailto:mardonbekoff@gmail.com)  
ORCID: 0000-0002-5245-6021

Xaynazarov Baxromjon Baxtiyorovich  
Tarix fanlari doktori (DSc). Dotsent.  
E-mail: [bahrom\\_bek@mail.ru](mailto:bahrom_bek@mail.ru)  
ORCID: 0000-0002-1266-1557

Saidboboyev Zokirjon Abdukarimovich  
Tarix fanlari nomzodi (Ph.D.). Professor.  
E-mail: [zsaidboboev@yahoo.com](mailto:zsaidboboev@yahoo.com)  
ORCID: 0009-0008-3960-2427

### *08.00.00 – IQTISODIYOT FANLARI*

Urdushev Xamrakul  
Iqtisodiyot fanlari nomzodi. Dotsent.  
E-mail: [xurdushev@gmail.com](mailto:xurdushev@gmail.com)  
ORCID: 0000-0003-4984-0214

Berdiyarov Baxriddin Tavasharovich  
Iqtisodiyot fanlari doktori (DSc). Professor.  
E-mail: [bahriddin.bfa@gmail.com](mailto:bahriddin.bfa@gmail.com)  
ORCID: 0000-0001-8591-6840

Avlokulov Anvar Ziyadullayevich  
Iqtisodiyot fanlari doktori (DSc). Professor.  
E-mail: [anvaravlokulovz@gamail.com](mailto:anvaravlokulovz@gamail.com)  
ORCID: 0000-0002-6683-8995

Norov Asror Egamberdiyevich  
Iqtisodiyot fanlari doktori (DSc).  
E-mail: [a.norov@ilmiy.uz](mailto:a.norov@ilmiy.uz)

Ostonokulov Azamat Abdukarimovich  
Iqtisodiyot fanlari doktori (DSc). Professor.  
E-mail: [a.ostonokulov@tsue.uz](mailto:a.ostonokulov@tsue.uz)  
ORCID: 0000-0003-2792-3174

Rustamova Sayyora Xatamovna  
Iqtisodiyot fanlari bo'yicha falsafa doktori  
(PhD). V.b Dotsent.  
E-mail: [rustamova0302@mail.ru](mailto:rustamova0302@mail.ru)

Shadiyev Xamid Azimovich  
Iqtisodiyot fanlari doktori (DSc). Professor.  
E-mail: [su9795744@gmail.com](mailto:su9795744@gmail.com)

Nasirov Egamkul Ismailovich  
Iqtisodiyot fanlari doktori (DSc). Professor.  
E-mail: [e.nosirov@tsue.uz](mailto:e.nosirov@tsue.uz)  
ORCID: 0000-0002-9355-1973

Kuliboev Azamat Shonazarovich  
Iqtisodiyot fanlari bo'yicha falsafa doktori  
(PhD). Dotsent.  
E-mail: [azamatkuliboyev@gmail.com](mailto:azamatkuliboyev@gmail.com)  
ORCID: 0000-0002-3357-070X

### *09.00.00 – FALSAFA FANLARI*

Turdiyev Bexruz Sobirovich  
Falsafa fanlari doktori (DSc). Professor.  
E-mail: [bekiuz0302@yahoo.com](mailto:bekiuz0302@yahoo.com)  
ORCID: <https://orcid.org/0000-0003-3260-3327>

Bekbaev Rauf Rustamovich  
Falsafa fanlari doktori (DSc). Dotsent.  
E-mail: [rauf.r.bekbaev@gmail.com](mailto:rauf.r.bekbaev@gmail.com)  
ORCID: 0000-0001-5072-3379

Yusubov Jaloliddin Kadamovich  
Falsafa fanlari doktori (DSc). Dotsent.  
E-mail: [yusubovjaloliddin@gmail.com](mailto:yusubovjaloliddin@gmail.com)  
ORCID: 0009-0003-1401-7997

Yuldashev Nurbek Normurodovich  
Falsafa fanlari bo'yicha falsafa doktori (PhD).  
Katta ilmiy xodim.  
O'zbekiston.  
ORCID: 0000-0002-4628-8789

Eshnazarova Farida Jo'raqulovna  
Falsafa fanlari bo'yicha falsafa doktori (PhD).  
Dotsent.  
E-mail: [faridaeshnazarova4@gmail.com](mailto:faridaeshnazarova4@gmail.com)  
ORCID: 0009-0000-2496-4443

Parpiyev Muxammadjon Tolibovich  
Falsafa fanlari bo'yicha falsafa doktori (PhD).  
Dotsent.  
ORCID: 0009-0000-1869-9348

### 10.00.00 – FILOLOGIYA FANLARI

Axmedov Oybek Saporbaevich  
Filologiya fanlari doktori (DSc). Professor.  
E-mail: [oybekakhmedov1978@gmail.com](mailto:oybekakhmedov1978@gmail.com)  
ORCID: 0009-0003-3122-1973

Samigova Xushnuda Batirovna  
Filologiya fanlari doktori (DSc). Professor.  
E-mail: [kabsam@yandex.ru](mailto:kabsam@yandex.ru)  
ORCID: 0009-0005-2327-106X

Eshmo‘minov Asqar Allamurodovich  
Filologiya fanlari doktori (DSc). Professor.  
E-mail: [asqar@list.ru](mailto:asqar@list.ru)

Axmedova Mehrinigor Bahodirovna  
Filologiya fanlari doktori (DSc). Professor v.b.  
E-mail: [mexrisha82@mail.ru](mailto:mexrisha82@mail.ru)  
ORCID: 0000-0003-1198-0326

Absalamova Gulmira Sharifovna  
Filologiya fanlari bo‘yicha falsafa doktori  
(PhD). Dotsent.  
E-mail: [gulmirasharifovna@gmail.com](mailto:gulmirasharifovna@gmail.com)  
ORCID: 0009-0005-6105-4752

Salaxutdinova Musharraf Isamutdinovna  
Filologiya fanlari nomzodi. Dotsent.  
E-mail: [salaxiddinovamusharraf@gmail.com](mailto:salaxiddinovamusharraf@gmail.com)  
ORCID: 0000-0003-0534-5633

Ravshan Turakulovich  
Filologiya fanlari bo‘yicha falsafa doktori  
(PhD). Professor.  
E-mail: [docravshanniyazov@gmail.com](mailto:docravshanniyazov@gmail.com)  
ORCID: 0000-0002-6146-1789

Sanakulov Zayniddin Ibodullayevich  
Filologiya fanlari bo‘yicha falsafa doktori  
(PhD). Dotsent.  
E-mail: [z.sanakulov@cspu.uz](mailto:z.sanakulov@cspu.uz)  
ORCID: 0000-0002-6952-7738

Bawetdinov Muxammeddin Kazimbekovich  
Filologiya fanlari bo‘yicha falsafa doktori  
(PhD).  
E-mail: [b\\_muxammed@karsu.uz](mailto:b_muxammed@karsu.uz)  
ORCID: 0009-0007-9826-175X

### 12.00.00 – YURIDIK FANLAR

Muxitdinova Firyuza Abdurashidovna  
Yuridik fanlar doktori (DSc). Professor.  
E-mail: [feruza.mukhitdinova@gmail.com](mailto:feruza.mukhitdinova@gmail.com)  
ORCID: 0000-0003-1721-0189

Ilhombekov Jasurbek Ilxombek o‘g‘li  
Yuridik fanlari bo‘yicha falsafa doktori (PhD).  
Katta o‘qituvchi.  
E-mail: [jafarbek22@mail.ru](mailto:jafarbek22@mail.ru)  
ORCID: 0000-0002-9867-3363

Imomov Nurillo Fayzullaevich  
Yuridik fanlar doktori (DSc). Professor.  
E-mail: [nurillo\\_1212@mail.ru](mailto:nurillo_1212@mail.ru)  
ORCID: 0000-0001-8090-842X

Pirmatov Otabek Shavkatovich  
Yuridik fanlar doktori (DSc). Professor v.b.  
E-mail: [pirmatov.otabek.89@inbox.ru](mailto:pirmatov.otabek.89@inbox.ru)  
ORCID: 0000-0002-0774-661

Ismoilov Shuhratjon Abdusaminovich  
Yuridik fanlar doktori (DSc). Dotsent.  
E-mail: [ismoilov.shuhrat80@mail.ru](mailto:ismoilov.shuhrat80@mail.ru)  
ORCID: 0000-0003-0947-6163

Matkarimov Kudrat Kalandarovich  
Yuridik fanlar doktori (DSc). Dotsent.  
E-mail: [qudrat1979uzb@gmail.com](mailto:qudrat1979uzb@gmail.com)  
ORCID: 000-0003-0396-4027

Xudaykulov Feruzbek Xurramovich  
Yuridik fanlar doktori (DSc). Dotsent.  
E-mail: [dr.profil14@gmail.com](mailto:dr.profil14@gmail.com)  
ORCID: 0000-0002-4940-3762

Hakimov Komil Baxtiyarovich  
Yuridik fanlar doktori (DSc). Professor.  
E-mail: [professorkomilkhakimov@gmail.com](mailto:professorkomilkhakimov@gmail.com)

Kadirova Moxigul Xamitovna  
Yuridik fanlar doktori (DSc). Professor v.b.  
E-mail: [m.kadirova@tsul.uz](mailto:m.kadirova@tsul.uz)  
ORCID: 0000-0003-1450-7542

### 13.00.00 – PEDAGOGIKA FANLARI

Haqberdiyev Baxtiyor Rustamovich  
Pedagogika fanlari bo‘yicha falsafa doktori  
(PhD). Dotsent.  
E-mail: [bahtiyor.haqberdiyev@mail.ru](mailto:bahtiyor.haqberdiyev@mail.ru)  
ORCID: 0000-0002-2208-7827

Erkulova Feruza Melikuziyevna  
Pedagogika fanlari bo‘yicha falsafa doktori  
(PhD). Dotsent.  
E-mail: [feruzaerkulovauzb@gmail.com](mailto:feruzaerkulovauzb@gmail.com)

Shirnazarova Zamira Allaberdiyevna  
Pedagogika fanlari bo‘yicha falsafa doktori  
(PhD). E-mail: [zamira.sh@terdpi.uz](mailto:zamira.sh@terdpi.uz)  
ORCID: 0000-0001-9870-6295

Oymatova Nilufar Mirjamolovna  
Pedagogika fanlari bo'yicha falsafa doktori  
(PhD). E-mail: [nilufar.oymatova@gmail.com](mailto:nilufar.oymatova@gmail.com)

Eshchanova Xolida Xudayarovna  
Pedagogika fanlari bo'yicha falsafa doktori  
(PhD). E-mail: [eshchanovaxolida@gmail.com](mailto:eshchanovaxolida@gmail.com)

Karshieva Dilbar Eshpulatovna  
Pedagogika fanlari bo'yicha falsafa doktori  
(PhD). Dotsent.  
E-mail: [d.karshiyeva1986@gmail.com](mailto:d.karshiyeva1986@gmail.com)

Raxmatov Otabek Urinbosarovich  
Pedagogika fanlari bo'yicha falsafa doktori  
(PhD). E-mail: [rahmatov.otabek@inbox.ru](mailto:rahmatov.otabek@inbox.ru)  
ORCID: 0000-0003-1288-3042

*23.00.00 – SIYOSIY FANLAR*

Turayev Abrar Saloxiddinovich  
Siyosiy fanlari bo'yicha falsafa doktori (PhD).  
Dotsent. E-mail: [ijtimoiy2017@mail.ru](mailto:ijtimoiy2017@mail.ru)  
ORCID: 0000-0003-1741-6857

---

**INSONSHUNOSLIK FANLARI** elektron  
jurnali 2025-yil 6-iyunda 830912-sonli  
guvohnoma bilan davlat ro'yxatidan  
o'tkazilgan.

**Muassis:** "SCIENCEPROBLEMS TEAM"  
mas'uliyati cheklangan jamiyati.

**TAHRIRIYAT MANZILI:**

Toshkent shahri, Yakkasaroy tumani, Kichik  
Beshyog'och ko'chasi, 70/10-uy. Elektron  
manzil: [scienceproblems.uz@gmail.com](mailto:scienceproblems.uz@gmail.com)

## MUNDARIJA

### **IQTISODIYOT FANLARI**

*G'aniyeva Sabohat*

BOZOR IQTISODIYOTI SHAROITIDA KORXONA RAQOBATBARDOSHLIGINING IQTISODIY MOHIYATI VA UNI SHAKLLANTIRUVCHI OMILLAR TAHLILI .....6-10

### **FILOLOGIYA FANLARI**

*Isanova Feruza*

XALQARO HUQUQ TERMINLARINI INGLIZ TILIDAN O'ZBEK TILIGA TARJIMA QILISH MUAMMOLARI ..... 11-14

### **YURIDIK FANLAR**

*G'iyosov Bilolbek*

RAQAMLI KUZATUV VOSITALARINI QO'LLASHDA SHAXSIY HAYOT DAXLSIZLIGINI TA'MINLASHDA SUN'IY INTELLEKTNING O'RNI ..... 15-19

*Jo'rayev Doston*

SUD TIZIMIDA MEDIATIV KELISHUVNING AMALIY MUAMMOLARI VA ULARNI HAL ETISH YO'LLARI VA BU BORADA XORIJ TAJRIBASI ..... 20-25

*Raximjonova Odinaxon*

WOMEN'S RIGHTS: INTERNATIONAL AND NATIONAL APPROACHES ..... 26-30

**YURIDIK FANLAR – LAW SCIENCES***Article / Original Paper***RAQAMLI KUZATUV VOSITALARINI QO'LLASHDA SHAXSIY HAYOT DAXLSIZLIGINI TA'MINLASHDA SUN'IY INTELLEKTNING O'RNI****G'iyosov Bilolbek Jumazoda**O'zbekiston Respublikasi Huquqni muhofaza qilish akademiyasi  
"Kiberxavfsizlikni huquqiy ta'minlash" mutaxassisligi magistranti

**Annotatsiya.** Ushbu maqolada zamonaviy sun'iy intellekt (AI) texnologiyalarining raqamli kuzatuv tizimlarida qo'llanilishi va ularning shaxsiy hayot daxlsizligiga ta'siri keng qamrovli tahlil qilinadi. Yuz tanish (facial recognition), xulq-atvor tahlili (behavioral analytics), bashoratli kuzatuv (predictive surveillance) va ko'p modalli biometrik identifikatsiya tizimlari xavfsizlikni oshirish bilan birga ma'lumotlar maxfiylikiga jiddiy xavf tug'dirishini ko'rsatadi. Maqolada Federated Learning, Differential Privacy va xavfsiz ko'p tomonlama hisoblash (SMPC) texnologiyalari tahlil qilinib, shu asosda Privacy-Preserving AI (maxfiylikni saqlovchi sun'iy intellekt) arxitekturasini kuzatuv tizimlariga integratsiya qilish yo'llari ilmiy jihatdan asoslanadi.

**Kalit so'zlar:** sun'iy intellekt, raqamli kuzatuv, shaxsiy hayot daxlsizligi, yuz tanish, xulq-atvor tahlili, federated learning, differential privacy, axloqiy AI.

**THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENSURING PRIVACY IN THE USE OF DIGITAL SURVEILLANCE TOOLS****Giyosov Bilolbek Jumazoda**Master's student of the Law Enforcement Academy of the Republic of Uzbekistan  
specialty "Legal Provision of Cybersecurity"

**Annotation.** This article presents a comprehensive analysis of the application of modern artificial intelligence (AI) technologies in digital surveillance systems and their impact on personal privacy. It is demonstrated that facial recognition, behavioral analytics, predictive surveillance, and multimodal biometric identification technologies, while enhancing security, simultaneously pose serious threats to data confidentiality. The paper analyses Federated Learning, Differential Privacy, and Secure Multi-Party Computation (SMPC) technologies, scientifically substantiating pathways for integrating Privacy-Preserving AI architecture into surveillance systems.

**Keywords:** artificial intelligence, digital surveillance, personal privacy, facial recognition, behavioral analytics, federated learning, differential privacy, ethical AI.

DOI: <https://doi.org/10.47390/hum-i5v2y2026/n03>

Raqamli texnologiyalarning jadal sur'atda rivojlanishi zamonaviy davlatlar va xususiy tuzilmalar tomonidan kuzatuv vositalarining ko'lamini misli ko'rilmagan darajada kengaytirishga imkon berdi. 2025-yil ma'lumotlariga ko'ra, jahon bo'ylab bir milliarddan ziyod CCTV kamera faoliyat ko'rsatayotgan bo'lib, ularning sezilarli qismi sun'iy intellekt algoritmlari bilan jihozlangan (Haley, 2025). Ushbu ko'rsatkich kelajakda yanada oshishi kutilmoqda. Bir tomondan, bunday tizimlar jamoat xavfsizligini ta'minlash, jinoyatchilikni oldini olish va favqulodda vaziyatlarga operativ munosabat bildirish imkonini beradi. Ikkinchi tomondan, kuzatuv texnologiyalarining kontrolsiz kengayishi shaxsiy hayot daxlsizligi — konstitutsiyaviy huquqlar sirasida muhim o'rinni egallagan qadriyat — ga jiddiy tahdid soladi.

O'zbekiston Respublikasida ham raqamlashtirish siyosatining jadallashuvi bilan birga aqlli shahar (smart city) kontseptsiyasi doirasida kuzatuv tizimlariga investitsiyalar ortib bormoqda. Raqamli O'zbekiston-2030 strategiyasi va tegishli normativ-huquqiy hujjatlar asosida ko'plab shaharlarda video kuzatuv infratuzilmasi modernizatsiya qilinmoqda. Ayni shu jarayonda ikkita fundamental savol kun tartibiga chiqadi: birinchisi — qanday texnologiyalar qo'llanilmoqda va ular qanchalik samarali; ikkinchisi — ushbu texnologiyalar fuqarolarning shaxsiy hayoti, ma'lumotlari va qadr-qimmatiga qanday ta'sir ko'rsatmoqda. Mazkur maqola ushbu savollarni ilmiy-texnik va axloqiy jihatdan chuqur tahlil qilishga qaratilgan.

Sun'iy intellekt asosidagi kuzatuv (AI surveillance) tizimlarining arxitekturasini bir necha o'zaro bog'liq komponentlardan iborat: ma'lumot yig'ish qatlami (data acquisition layer), qayta ishlash qatlami (preprocessing layer), AI xulosa qilish qatlami (inference layer) va qaror qo'llab-quvvatlash qatlami (decision support layer). Har bir qatlam maxsus deep learning modellari va sensor infratuzilmasi bilan ta'minlanadi. Sanli (2025) IoT asosidagi shahar tizimlarida maxfiylikni saqlovchi AI arxitekturasini tadqiq qilib, markazlashgan ma'lumotlarni qayta ishlash zaruratini bartaraf etuvchi edge computing yondashuvini taklif etgan. Ushbu yondashuv ma'lumotlarni dastlabki manbada qayta ishlab, faqat anonimlashtiri natijalarni markaziy serverga yuborish orqali privacy risklarini sezilarli kamaytiradi.

### **Yuz tanish texnologiyalari va biometrik identifikatsiya**

Yuz tanish (facial recognition) texnologiyasi AI asosidagi kuzatuv tizimlarining muhim komponenti bo'lib, zamonaviy deep learning metodlari tufayli keskin takomillashdi. Yuz tanish pipeline'i bir necha ketma-ket bosqichlardan iborat: yuzni aniqlash (face detection), нормализация (alignment), xususiyatlarni ajratib olish (feature extraction) va moslikni tekshirish (face matching). Deng va boshq. (2019) tomonidan ishlab chiqilgan ArcFace arxitekturasini 512 o'lchamli embedding vektorini hisoblash orqali individual shaxslarni 99,83% aniqlik bilan farqlash qobiliyatini namoyish etgan. Bu natija tijorat tizimlarida de-facto standart maqomiga ega bo'lgan.<sup>1</sup>

Biroq yuz tanish texnologiyasining eng muhim muammolaridan biri — algoritmik xolislik masalasidir. Buolamwini va Gebru (2018) o'tkazgan "Gender Shades" tadqiqoti tijorat yuz tanish tizimlarida demografik disparitetni hujjatli ravishda isbotladi: ushbu tizimlar oq tanli erkaklar uchun 99% aniqlik bilan ishlagan holda, qora tanli ayollar uchun xatolik darajasi 35% gacha yetgan. Bunday disparitet kuzatuv kontekstida yanada jiddiyroq oqibatlariga olib keladi — "noto'g'ri identifikatsiya" (false positive) hollari beg'unoh shaxslarning huquqiy javobgarlikka tortilishi xavfini yuzaga keltiradi. London Metropolitan Police'ning 2019–2020-yillardagi live facial recognition sinovlarida false positive darajasi ayrim hollarda 80% dan oshganligi qayd etilgan.<sup>2</sup>

Biometrik AI faqat yuz tanish bilan cheklanmaydi. Iris scanning, fingerprint analysis, gait analysis (yurish tarzi tahlili) va voice biometrics kabi modalliklar har biri o'ziga xos neural network arxitekturasini talab qiladi. Multimodal biometrik tizimlar — yuz + ovoz + yurish tarzi kombinatsiyasi — alohida modalliklarning aniqligidan oshib ketuvchi performance ko'rsatadi. Haley (2025) biometrik kuzatuv va zo'ravonlikning oldini olish bo'yicha tadqiqotida iris scanning va fingerprint analysis'ning milliy xavfsizlik kontekstida qo'llanilishi batafsil tahlil qilingan. Shuni alohida ta'kidlash lozimki, biometrik ma'lumotlar o'ziga xos xavf tug'diradi: paroldan farqli ravishda, kompromis qilingan biometrik identifikatorni o'zgartirib bo'lmaydi.

### **Xulq-atvor tahlili va bashoratli kuzatuv**

Xulq-atvor tahlili (behavioral analytics) va bashoratli kuzatuv (predictive surveillance) zamonaviy AI kuzatuv tizimlarining passiv video yozuvdan faol razvedka platformasiga aylanishida hal qiluvchi rol o'ynaydi. RNN (Recurrent Neural Network), LSTM (Long Short-Term Memory) va Transformer arxitekturalariga asoslangan modellar vaqt bo'yicha kengaygan harakatlar ketma-ketligini tahlil qilish qobiliyatini namoyon etmoqda. Haley (2025) tadqiqotida zo'ravonlik harakatlarini aniqlash uchun ishlatilgan algoritmlar kicking, punching, shooting va stalking kabi harakatlarni "zo'ravon" deb tasniflash uchun katta hajmli labeled dataset'da oldindan trening qilinishi ko'rsatilgan.<sup>3</sup>

Bashoratli kuzatuv (predictive surveillance) — mavjud ma'lumotlar asosida kelajakdagi voqealarni prognoz qilish texnologiyasi — muhim axloqiy muammolarni yuzaga keltiradi. "Model of Threat Approach" (Haley, 2025) biometrik surveillance, harakatlanish va iste'mol naqshlari, hissiyotlar va muloqotlarni kombinatsiya qilib "erta ogohlantirish" tizimini taklif etadi. Biroq Roberts va boshq. (2021) Afrikadagi oltita mamlakatda o'tkazgan tadqiqoti ko'rsatadiki, bunday tizimlar yetarli nazorat mexanizmlarsiz siyosiy raqiblar va marginallashtirilgan guruhlarini maqsadli qilish uchun suiiste'mol qilinishi mumkin. Xususan, Xitoy Uyg'ur musulmonlariga nisbatan qo'llagan AI surveillance arxitekturasi bu xavfning global ko'lamini yaqqol ko'rsatmoqda.

### **Maxfiylikni saqlovchi AI texnologiyalari: texnik tahlil**

Privacy-Preserving AI (PPAI) — shaxsiy ma'lumotlar maxfiylikni ta'minlagan holda yuqori sifatli AI modellarini yaratish imkonini beruvchi metodologiyalar majmuasi — sun'iy intellekt etikasining eng muhim tadqiqot yo'nalishlaridan biriga aylangan. Ushbu metodologiyalar kuzatuv kontekstida shaxs ma'lumotlarini transmissiya, saqlash yoki agregatsiya jarayonida qanday himoya qilish mumkinligiga texnik javob berishga intiladi.

Federated Learning (FL) — markaziy serverga xom ma'lumotlar yuborilmasdan, taqralgan qurilmalar taqralgan holda model treningi o'tkazish imkonini beruvchi paradigma — maxfiylikni saqlovchi AI arxitekturasi asosiy elementi hisoblanadi. McMahan va boshq. (2017) ishlab chiqqan FedAvg algoritmi lokal qurilmalarda SGD (Stochastic Gradient Descent) ishlatib, faqat model parametrlari (weights va gradients) markaziy serverga uzatilishini nazarda tutadi. Shenoy va boshq. (2025) keng qamrovli tadqiqotida FL'ning arxitekturaviy xilma-xilligi va privacy-enhancing technologies bilan integratsiyasi batafsil yoritilgan. Sanli (2025) IoT asosidagi shahar kuzatuv tizimlari uchun FL + LDP (Local Differential Privacy) kombinatsiyali framework'ni taklif etib, centralized training'ga nisbatan aniqlik yo'qotishini atigi 1,2–1,5% darajasida saqlab qolgan holda memberlik inference hujumlarining muvaffaqiyat darajasini 50% dan ziyod kamaytirdi.<sup>4</sup>

Differential Privacy (DP) — Dwork va boshq. (2006) tomonidan taklif etilgan va Abadi va boshq. (2016) tomonidan Deep Learning'ga tatbiq etilgan matematik framework — algoritm chiqishiga nazorat ostida shovqin (calibrated noise) qo'shish orqali alohida shaxsni ma'lumotlar to'plamidan ajratib olishning imkonini bartaraf etadi. Kuznetsov va boshq. (2026) Federated Learning tizimida Adaptive DP Budget Allocation (AdaDPCS-FL) ni tatbiq etish orqali privacy-accuracy trade-off'da 4% yaxshilashga erishilganini hujjatli ravishda isbotladi. Rawas va Samala (2025) tadqiqotida  $\epsilon = 0,5$  qiymatida aniqlikni 1% dan kam yo'qotish bilan kuchli maxfiylik kafolatlari ta'minlanishi ko'rsatildi.

Homomorphic Encryption (HE) — shifrlangan ma'lumotlar ustida deshifrlashsiz hisob-kitob amallari bajarish imkonini beruvchi kriptografik usul — kuzatuv arxitekturasi

maxfiylikning eng kuchli kafolatini ta'minlaydi. To'liq gomomorf shifrlash (FHE — Craig Gentry, 2009) markaziy serverning individual ma'lumotlarni hech qachon deshifrlangan holda ko'rmasligini ta'minlagan holda analitika natijalarini hisoblashga imkon beradi. Biroq FHE hali yuqori computational overhead tufayli real-time tizimlar uchun muammo bo'lib qolmoqda. Secure Multi-Party Computation (SMPC) bir necha tomon (party) xususiy ma'lumotlarni oshkor qilmagan holda birgalikda funktsiya hisoblashga imkon beradi va federated learning bilan kombinatsiyalangan gradient leakage hujumlariga qarshi samarali himoya beradi.<sup>5</sup>

### **AI kuzatuvining afzalliklari va sistemaviy xatarlari**

AI asosidagi kuzatuv tizimlarining xavfsizlik sohasidagi afzalliklari ob'ektiv ravishda muhimdir. Birinchidan, masshtablik va uzluksiz monitoring: AI inference engine'lari parallel ravishda yuzlab video oqimlarini real-time'da tahlil qila oladi, bu esa inson operatorlariga nisbatan 60% tezroq reaksiya vaqtini ta'minlaydi (Haley, 2025). Ikkinchidan, avtomatlashtirilgan anomaliya aniqlash: One-Class SVM, Autoencoder asosidagi anomaliya aniqlash algoritmlari va Isolation Forest kabi modellar belgilangan naqshlardan og'ishni avtomatik ravishda qayd etadi. Uchinchidan, amaliy jihatdan stadionlar, aeroportlar va transport xablarida crowd dynamics analysis tizimlarining real-time'da qo'llanilishi jamoat xavfsizligini sezilarli oshirganini ko'rsatmoqda.

Biroq AI surveillance'ning tizimaviy xatarlari kuchli counterargument sifatida ko'tariladi. Mass surveillance — butun bir aholini maqsadli ravishda kuzatib borish — AI kuzatuvining eng muhim xatari hisoblanadi. Statista (2025) ma'lumotlariga ko'ra, global data brokerage bozori 2024-yilda 300 milliard dollarni oshib ketgan bo'lib, undagi behavioral data'ning katta qismi kuzatuv tizimlaridan hosil bo'lmoqda. Roberts va boshq. (2021) Afrikadagi bir qator mamlakatlarda davlat kuzatuvining tarixan kamsitilgan guruhlar — faolchilar, jurnalistlar, siyosiy raqiblar — ga nisbatan suiiste'mol qilinganini hujjatli ravishda isbotlagan. Algorithmic bias — xolislik muammosi — Buolamwini va Gebru (2018) tomonidan ilmiy isbotlangan bo'lib, yuz tanish tizimlarida demografik disparitet fuqarolarning tenglik huquqiga tahdid sifatida baholanishi lozim.<sup>6</sup>

Data misuse va secondary use muammosi ham alohida e'tiborni talab etadi. Universal Digital Identity tadqiqotlari (Shen va boshq., 2026) ko'rsatishicha, kuzatuv ma'lumotlarining identity proofing, credential issuance va service access bilan bog'liq holda markaziy agregatsiyasi behavioural profiling uchun xavfli platforma yaratadi. Purpose limitation va proportionality rules'ning nazorat mexanizmlarsiz amalga oshirilishi maqsadli kuzatuvning "creeping surveillance"ga — yashirinib, sekin-asta kengayib boruvchi kuzatuvga — aylanishiga olib keladi.

### **Axloqiy AI va inson markazida yondashuv**

Axloqiy AI surveillance'ning asosini Explainable AI (XAI), Human-in-the-Loop (HITL) va Privacy-by-Design (PbD) printsiplari tashkil etadi. Explainable AI — AI modellarini inson tushunishi uchun interpretabel qilish texnologiyasi — kuzatuv AI'ning accountability'sini ta'minlashda fundamental ahamiyatga ega. LIME (Locally Interpretable Model-agnostic Explanations) va SHAP (SHapley Additive exPlanations) metodlari kuzatuv kontekstida qaror shaffofligini ta'minlashi mumkin. S. 1143202441234 (2022) tadqiqotida case-based explanation metodologiyasi maxfiylikni saqlovchi interpretabel AI uchun amaliy framework sifatida taklif etilgan.

Privacy-by-Design (PbD) — Ann Cavoukian (2009) tomonidan ishlab chiqilgan va keyinchalik GDPR'ning 25-moddasiga singdirilgan prinsip — texnologiyaning loyihalash bosqichidan boshlab maxfiylikni o'zak qilib qo'yishni nazarda tutadi. Kuzatuv AI uchun PbD: data minimization (faqat maqsadli vazifalar uchun zarur ma'lumotlar yig'iladi), purpose limitation (ma'lumotlar yig'ish maqsadi aniq belgilangan bo'lishi va boshqa maqsadlarda qo'llanilmasligi), storage limitation (ma'lumotlar zaruratdan ortiq saqlanmasligi) va integrity and confidentiality (ma'lumotlar butunligi va maxfiyligi) kafolatlanishi lozim. Sanli (2025) privacy-preserving AI framework'ini shahar IoT tizimlari uchun yaratishda PbD prinsiplarini federated learning va edge computing arxitekturasiga muvaffaqiyatli tatbiq etgan.<sup>7</sup>

Inson qadr-qimmatini (human dignity) himoya qilish va raqamli huquqlarni ta'minlash AI kuzatuv tizimlarini tartibga solishning eng fundamental axloqiy asosi hisoblanadi. BMT Inson Huquqlari Kengashi, UDHR va ICCPR shaxsiy hayotni himoya qilish huquqini fundamental huquq sifatida tan olgan. AI kuzatuvining "chilling effect" — shaxslarning o'zlari kuzatilayotganini bilgan holda o'z xatti-harakatlarini o'zgartirishi — demokratik ijtimoiy hayotga tahdid sifatida Crawford (2021) va Zuboff (2019) asarlarida batafsil yoritilgan. Xulosa tariqasida ta'kidlash lozimki, AI kuzatuv va shaxsiy hayot daxlsizligi o'zaro istisno tushunchalar emas: privacy-by-design arxitekturasini AI kuzatuv tizimlariga integratsiya qilish, shaffof va tushuntirib beriladigan algoritmlarni joriy etish, federated va privacy-preserving learning paradigmlarini deployment'ga tatbiq qilish va robust institutional accountability mexanizmlarini yaratish orqali xavfsizlik va shaxsiy hayot daxlsizligi o'rtasidagi muvozanatni ta'minlash texnologik jihatdan mumkin.

#### **Литература/References/Adabiyotlar:**

1. Deng J., Guo J., Xue N., Zafeiriou S. ArcFace: Additive angular margin loss for deep face recognition // Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2019. P. 4690–4699.
2. Buolamwini J., Gebru T. Gender Shades: Intersectional accuracy disparities in commercial gender classification // Proceedings of the 1st Conference on Fairness, Accountability, and Transparency. 2018. P. 77–91.
3. Haley P. The impact of biometric surveillance on reducing violent crime: Strategies for apprehending criminals while protecting the innocent // Sensors. 2025. № 25. P. 3160.
4. Sanli M. Privacy-preserving AI for distributed IoT in urban sustainability networks // Arabian Journal for Science and Engineering. 2025. <https://doi.org/10.1007/s13369-025-10864-w>
5. Shenoy D., Bhat R., Krishna Prakasha K. Exploring privacy mechanisms and metrics in federated learning // Artificial Intelligence Review. 2025. № 58. P. 223.
6. Roberts A. et al. Surveillance and the law in six African countries // Social Sciences. 2021. № 15. P. 155.
7. Rawas S., Samala N. Federated learning and differential privacy for medical IoT applications // Discover Networks. 2025. № 1(8)



SAYT: <https://humansciences.uz>

**HUMANSIENCES.UZ**

*№ 5 (2)-2026*

**INSONSHUNOSLIK FANLARI JURNALI**

**JOURNAL OF HUMANITIES**

**ЖУРНАЛ ГУМАНИТАРНЫХ НАУК**

**INSONSHUNOSLIK FANLARI** elektron jurnali 2025-yil 6-iyunda 830912-sonli guvohnoma bilan davlat ro'yxatidan o'tkazilgan.

**Muassis:** "SCIENCEPROBLEMS TEAM" mas'uliyati cheklangan jamiyati.

**TAHRIRIYAT MANZILI:**

Toshkent shahri, Yakkasaroy tumani, Kichik Beshyog'och ko'chasi, 70/10-uy. Elektron manzil: [scienceproblems.uz@gmail.com](mailto:scienceproblems.uz@gmail.com)