



Қылмыстық құқық. Қылмыстық процесс. Криминалистика. Криминология / Criminal law. Criminal process. Criminalistics. Criminology / Уголовное право. Уголовный процесс. Криминалистика. Криминология

FTAMP 10.85.01

<https://doi.org/10.32523/2616-6844-2025-153-4-145-159>

Ғылыми мақала

Жеке тұлғаны анықтауда Face ID жүйесін қолдану технологиясының құқықтық негіздері

А.Б. Досжанова¹, Е.Н. Бегалиев*²

¹Қазақстан Республикасы Бас прокуратурасы жанындағы құқық қорғау академиясы, Қосшы, Қазақстан

²Қазақстан Республикасы Жоғары Сот Кеңесі, Астана, Қазақстан

(e-mail: ¹aitok82@mail.ru, ²ernar-begaliyev@mail.ru)

Аңдатпа: Қазіргі жаһандану дәуірінде жеке тұлғаны дәл және сенімді анықтау мәселесі қоғамдық қауіпсіздікті қамтамасыз етуде және құқық қорғау жүйесінің тиімділігін арттыруда маңызды орынға ие болды. Осы орайда, биометриялық технологиялар, оның ішінде Face ID жүйесі – адамның бет-әлпетін автоматтандырылған түрде сәйкестендіруді қамтамасыз ететін инновациялық шешім ретінде кеңінен танылуда. Бұл технология жасанды интеллект пен машиналық оқыту алгоритмдерін қолдана отырып, жеке тұлғаның бет-әлпетін жылдам, дәл және көп жағдайда сенімді түрде анықтауға мүмкіндік береді.

Мақалада Face ID жүйесінің негізгі технологиялық негіздері мен оның құқық қорғау органдарында қолдану практикасы жан-жақты қарастырылады. Қазақстан Республикасында бұл жүйені енгізу және дамыту жағдайы, оның құқықтық негіздері мен нормативтік-құқықтық актілерге сәйкестігі сараланады. Зерттеу барысында Қазақстанның ішкі істер, прокуратура, ұлттық қауіпсіздік органдарында осы технологияның сынақтан өтуі мен практикалық пайдалану мүмкіндіктері талданады.

Сонымен қатар, жеке деректерді қорғау саласындағы халықаралық стандарттар мен талаптар қарастырылып, Қазақстандағы заңнамалық базаға сәйкестік мәселелері жан-жақты зерттеледі. Face ID технологиясын қолдану барысында жеке адамның құқықтары мен бостандықтарын қамтамасыз ету міндеттері, деректердің қауіпсіздігі және этикалық аспектілер ерекше назарға алынады.

Мақалада әлемдік тәжірибе, оның ішінде АҚШ, Еуропалық Одақ елдері, Қытай және Жапонияның құқық қорғау жүйелерінде Face ID технологиясын қолдану үлгілері, олардың нормативтік реттеуін салыстырмалы талдау арқылы қарастырылады. Халықаралық ынтымақтастықтың құқықтық және техникалық аспектілері, ортақ дерекқорлар құрудың маңыздылығы мен технологиялық стандарттарды үйлестіру қажеттілігі де айқындалады.

Зерттеу нәтижелері ретінде Face ID жүйесін құқық қорғау саласында қолдандудың тиімділігі мен оның қауіпсіздік шаралары ұсынылады, сондай-ақ жүйені одан әрі жетілдіру бағытындағы перспективалар мен ұсыныстар беріледі. Бұл технология Қазақстан Республикасының цифрлық трансформация саясатының маңызды құрамдас бөлігі болып табылады және қоғамдық қауіпсіздікті нығайтуға елеулі үлес қосады.

Түйін сөздер: Face ID, биометриялық сәйкестендіру, жеке тұлғаны анықтау, құқық қорғау органдары, деректерді қорғау, жасанды интеллект, цифрлық қауіпсіздік, нормативтік-құқықтық база, халықаралық тәжірибе, этика.

Кіріспе

XXI ғасырдағы ақпараттық технологиялар дәуірінде жеке тұлғаны анықтау және сәйкестендіру әдістері елеулі өзгерістерге ұшырады. Биометриялық технологиялар, оның ішінде Face ID жүйесі, адамның бет-әлпетін цифрлық түрде талдап, автоматтандырылған түрде сәйкестендіруді қамтамасыз етеді. Бұл технология құқық қорғау органдары үшін аса маңызды құралға айналып отыр, себебі ол қылмыскерлерді жылдам анықтау, қоғамдық қауіпсіздікті арттыру және тергеу жұмыстарын оңтайландыруға мүмкіндік береді [1, 2].

Қазақстан Республикасында цифрландыру саласы мемлекеттік бағдарлама аясында қарқынды дамуда. «Цифрлық Қазақстан» бағдарламасы (2017-2021 жж.) құқық қорғау органдарының қызметіне жаңа заманауи технологияларды енгізуді алға тартады. Ішкі істер министрлігінің ресми мәліметтері бойынша, биометриялық сәйкестендіру жүйелерінің көмегімен тұлғаны жедел анықтау көрсеткіші 2019-2024 жылдар аралығында 35%-ға өскен, бұл қоғамдық қауіпсіздікті арттыруға септігін тигізген [3]. Бұл технологияның негізінде жасанды интеллект алгоритмдері мен үлкен деректер қорлары жатыр, олар адам бет-әлпетін өңдеп, ұқсастығын жоғары дәлдікпен анықтайды [4].

Face ID жүйесі бет-бейнедегі ерекше нүктелерді – көз, мұрын, еріннің конфигурациясын және басқа да физикалық белгілерді талдау арқылы жұмыс істейді. Бұл әдіс фото, бейнежазбалардағы адамның бет-әлпетін нақты уақыт режимінде тануға мүмкіндік береді. Құқық қорғау саласында мұндай технология қоғамдық орындардағы бейнебақылау камераларымен бірге күдікті тұлғаларды автоматты түрде анықтауда қолданылады, бұл қылмыстық әрекеттердің алдын алу және тергеу сапасын арттырады [5].

Биометриялық деректерді қорғау мәселесі Қазақстан заңнамасында нақты регламенттелген. «Жеке деректер және оларды қорғау туралы» Заң (2013) биометриялық ақпаратты жинау, сақтау және өңдеу кезінде азаматтардың құқықтарын қорғауды қамтамасыз етеді [6].

Сонымен қатар, деректерді қорғаудың халықаралық стандарттары мен ұсынымдары, соның ішінде OECD және Еуропа Кеңесінің құжаттары, Қазақстан үшін технологиялық және құқықтық саясатты жетілдіруде маңызды негіз болып табылады [7, 8].

Халықаралық тәжірибеде АҚШ, Ұлыбритания, Қытай, Израиль сияқты елдер Face ID және басқа да биометриялық жүйелерді құқық қорғау саласында кеңінен пайдаланады. Бұл елдерде деректердің құпиялылығы мен жеке құқықтарды қорғау бойынша

заңнамалық шаралар қатаң сақталады. Қазақстанның да осы тәжірибені зерделеуі және өз нормативтік-құқықтық базасын жетілдіруі қажет [9, 10].

Осы мақалада Қазақстанда Face ID технологиясын құқық қорғау органдарында қолдану тәжірибесі мен оның тиімділігі, сондай-ақ жеке деректерді қорғау мәселелері жан-жақты қарастырылады. Халықаралық стандарттар мен тәжірибелерге сүйене отырып, құқықтық және техникалық ұсыныстар жасалады.

Әдіснама

Осы зерттеудің әдістемелік негізін биометрикалық технологиялардың құқық қорғау қызметінде қолданылуына қатысты құқықтық, техникалық және әлеуметтік аспектілерін қамтитын кешенді талдау құрайды. Зерттеуде салыстырмалы-талдамалық, эмпирикалық және құқықтық-нормативтік әдістер кешені қолданылды.

Зерттеу объектісі ретінде адамның бет-әлпетін тану арқылы жүзеге асырылатын Face ID жүйесі мен оның Қазақстан Республикасының құқық қорғау органдарындағы қолданылу тәжірибесі алынды. Сонымен қатар, бірқатар шетелдік мемлекеттерде қолданылып жүрген озық тәжірибелер де зерттеу шеңберіне енгізілді.

Дереккөздер және мәліметтер. Негізгі эмпирикалық деректер Қазақстан Республикасы Ішкі істер министрлігі, Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі, сондай-ақ БҰҰ-ның Қылмысқа қарсы күрес жөніндегі басқармасы (UNODC), INTERPOL және Еуропалық Одақтың дербес деректерді қорғау жөніндегі агенттігінің ресми есептері мен статистикалық мәліметтері негізінде алынған:

- Министрліктің ресми деректеріне сәйкес, 2023-2025 жылдар аралығында қоғамдық қауіпсіздік жүйелеріне 1,5 миллионнан астам бейнебақылау камерасы қосылып, оның ішінде жасанды интеллект және Face ID технологиясымен жабдықталған камералар саны 320 мыңға жетті [11]. Бұл жүйелер «Сергек», «Safe City», және жаңадан енгізіліп жатқан «Astana Smart Vision» жобалары арқылы орталықтандырылған түрде жұмыс істейді.

- ҚР Цифрлық даму министрлігінің 2024 жылғы статистикасы бойынша, мемлекеттік мәліметтер базасында 15,5 миллионнан астам адамның биометриялық деректері тіркелген, оның ішінде 11,3 миллион бет-әлпет бейнесі сақталған [12].

- INTERPOL деректеріне сүйенсек, 2021-2024 жылдары халықаралық іздеуде жүрген 5 500-ден астам адам Face Recognition System арқылы анықталып, 106 мемлекетте ұсталған [13].

Қолданылған әдістер:

Салыстырмалы құқықтық талдау әдісі. Салыстырмалы құқықтық талдау әдісі арқылы Қазақстан Республикасының құқықтық базасы мен халықаралық тәжірибе арасындағы айырмашылықтар мен ұқсастықтар сараланды. Бұл әдіс биометрикалық деректерді қолдану мен қорғау саласындағы заңнамалық сәйкестікті бағалауда маңызды.

Мысалы, Қазақстанда «Дербес деректер және оларды қорғау туралы» Заңы (2013 ж.) биометриялық деректерді дербес деректердің ерекше санаты ретінде танып, оларды жинау мен өңдеуге нақты шектеулер қояды. Алайда, заңда "бет-әлпет биометриясы" немесе "автоматтандырылған тану жүйелері" секілді заманауи түсініктер толықтай көрініс таппаған.

Ал Еуропалық Одақтың Жалпы деректерді қорғау регламенті (GDPR, 2016/679) бет-әлпет деректерін «биометрикалық деректер» ретінде нақтылайды және оларды өңдеуге

тек айқын, ерікті және нақты келісім болғанда ғана рұқсат етеді. Сонымен қатар, GDPR құқық қорғау органдарының бұл деректерді өңдеуіне арнайы баптар мен шектеулер енгізеді (мысалы, 9-бап, 10-бап) [14].

Салыстыру нәтижесінде, Қазақстанның құқықтық реттеуінде әлі де құқықтық олқылықтар мен техникалық терминдердің толық еместігі байқалды, бұл Face ID жүйесін кең көлемде құқық қорғау саласында қолдану үшін нақты құқықтық негіздің қажеттілігін көрсетеді.

Контент-анализ әдісі. Контент-анализ – ресми құжаттар мен ақпараттық жүйелердің мазмұнын жүйелі түрде талдауға мүмкіндік беретін әдіс. Бұл зерттеу аясында Қазақстан Республикасы ІІМ, Бас прокуратурасы, сондай-ақ халықаралық ұйымдардың (INTERPOL, UNODC, EUROPOL) ресми есебі мен жарияланымдары талданды.

Мысалы, ҚР ІІМ-нің 2024 жылғы есебінде елдегі 19 000 камерада Face ID модулі бар екені көрсетілген [15]. Сонымен қатар, UNODC 2022 жылғы баяндамасында биометриялық технологиялардың қылмысқа қарсы күрестегі рөлін ерекше атап өтеді. Онда бет-әлпетті тану жүйесі арқылы заңсыз мигранттар мен іздеудегі қылмыскерлердің анықталған жағдайлары сипатталған [16].

Контент-анализ нәтижесінде Face ID технологиясының нақты қолданылу салалары: құқық қорғау қызметі (қылмыскерлерді тану);

шекаралық бақылау (шекарадан заңсыз өтуді алдын алу);

– қоғамдық қауіпсіздік (ірі іс-шараларда тұлғаларды бақылау) – анықталды.

Интервью және сараптамалық сұхбат әдісі. Бұл әдіс аясында Қазақстан Республикасының құқық қорғау органдары қызметкерлерімен және IT мамандармен құрылымданған сұхбаттар жүргізілді. Сұхбаттар 2024 жылдың шілде-қараша айлары аралығында Нұр-Сұлтан, Алматы және Шымкент қалаларында өткізілді. Барлығы 12 респондент қатысты.

Сұхбатта көтерілген негізгі мәселелер:

– Face ID жүйесін енгізу кезіндегі техникалық қиындықтар (мысалы, камера сапасы мен жарықтық деңгей сәйкестігі);

– Құқықтық негіздің жеткіліксіздігі (сотта дәлел ретінде қолдану қиындығы);

– Қоғамның биометриялық жүйелерге сенім деңгейі (азаматтардың дербес деректерінің қауіпсіздігіне алаңдаушылығы).

Мысалы, Алматы қалалық ПД өкілі берген ақпаратқа сәйкес, 2024 жылы бет-әлпетті тану арқылы 342 күдікті танылып, олардың 89-ы қылмыстық жауапкершілікке тартылған. Бұл сұхбаттар биометрикалық жүйелердің тәжірибелік тиімділігі мен олардың құқықтық реттелуі арасындағы алшақтықты көрсетеді.

Кейс-стади (оқиға талдауы) әдісі. Кейс-стади – нақты жағдайды талдау арқылы теориялық тұжырымдарды нақты дәлелдермен бекітуге мүмкіндік беретін әдіс. Бұл зерттеуде Қазақстандағы екі нақты оқиға қарастырылды:

Оқиға. Астана қаласында 2024 жылы «Астана Опера» театрында өткен халықаралық форум кезінде күдікті ретінде іздеуде жүрген азамат Face ID жүйесі арқылы камера көмегімен анықталып, 5 минут ішінде ұсталған. Бұл іс ІІМ-нің ресми баспасөз релизінде жарияланған [17].

Оқиға. Алматы қаласында 2024 жылдың желтоқсан айында такси жүргізушісіне шабуыл жасаған күдікті 3 күн ішінде Face ID модулі бар камера арқылы анықталған. Камера бейнесінен күдіктінің бет-әлпеті танылып, криминалистік база арқылы сәйкестік орнатылған.

Бұл әдіс Face ID технологиясының нақты қылмыстық істерде қалай жұмыс істейтінін және оның құқық қорғау тәжірибесіне енгізілуі қандай нәтиже беретіні туралы шынайы деректер береді.

Жоғарыда сипатталған әдістердің әрқайсысы зерттеудің мақсаттарына жетуге бағытталған және өзара үйлесімді түрде қолданылды. Бұл ғылыми негізделген әдіснама арқылы Face ID технологиясын құқық қорғау саласында қолданудың тиімділігі мен проблемалық тұстарын нақты, дәлелді әрі жүйелі түрде ашып көрсетуге мүмкіндік берді.

Нәтижелер мен талқылау

Бүгінгі таңда тұлғаны биометриялық идентификациялауда бет-әлпетті тану жүйелерінің тиімділігі бірнеше маңызды параметрлермен анықталады: алгоритмдердің дәлдігі, қателік деңгейі, жауап беру жылдамдығы және деректерді өңдеу қауіпсіздігі. Жүргізілген талдау нәтижесінде келесі негізгі қорытындылар алынды:

Технологиялық дәлдік және эволюциясы. Бет-әлпетті тану технологиясының тиімділігі соңғы онжылдықта жасанды интеллект пен нейрожелілік алгоритмдердің дамуымен айтарлықтай артты. АҚШ Ұлттық стандарттар және технологиялар институтының (NIST) Face Recognition Vendor Test (FRVT) жобасы аясында жүргізілген зерттеулерге сәйкес, бет-әлпетті тану жүйелерінің сәйкестендіру дәлдігі 2015 жылы 76,2% болса, 2024 жылы бұл көрсеткіш 99,5%-ға дейін жетті [18]. Бұл серпін биометрикалық идентификацияның сапалық жаңа деңгейге көтерілгенін білдіреді.

Алгоритмдердің эволюциясы:

- 2015 – CNN (Convolutional Neural Networks): дәстүрлі әрі базалық нейрожелілік архитектура. Бұл кезеңде жүйелердің тану қабілеті жарық түсуі мен бұрышқа өте сезімтал болатын.

- 2018 – DeepFace (Meta/Facebook): деректер көлемін үлкейтіп, терең нейрондық желілерді қолданып, 3D теңшеу арқылы танудың дәлдігін арттырды. Бұл жүйе 4 миллионнан астам бет бейнесімен оқытылды.

- 2021 – ArcFace (InsightFace командасы): ArcFace моделі шекаралық softmax функциясын пайдалану арқылы тұлғалар арасындағы ажыратымдылықты едәуір күшейтті. Жоғары дәлдікке қоса, бұл модельдер деректердің демографиялық ерекшеліктерін ескеруге мүмкіндік берді.

- 2024 – InsightFace (MS1MV3 датасетімен): әлемдегі ең дәл және сенімді алгоритмдердің бірі ретінде танылды. Қазіргі таңда бұл модель құқық қорғау және шекара қызметтерінде кеңінен қолданылады.

NIST FRVT 2023 есебі негізінде төмендегі кестеде әр жылдардағы жетекші алгоритмдердің сәйкестендіру дәлдігі келтірілген [19]:

Жыл	Алгоритм атауы	Дәлдік (%)	Еркін тану уақыты (ms)
2015	CNN	76.2	850
2018	DeepFace	92.4	500
2021	ArcFace	98.6	290
2024	InsightFace	99.5	180

Қазақстанда енгізу нәтижелері. Қазақстанда бет-әлпетті тану технологияларын енгізу 2020 жылдан бастап әсіресе, қоғамдық қауіпсіздік саласында қарқын алды. Үкіметтің «Цифрлық Қазақстан» бағдарламасы аясында бірнеше ірі жоба жүзеге асырылды, олардың ішінде ең елеулісі – "Сергек" интеллектуалды бейнебақылау жүйесі.

Нақты нәтижелер:

Қазақстан Республикасы Ішкі істер министрлігінің ресми мәліметтері бойынша, 2022–2024 жылдар аралығында Астана (Нұр-Сұлтан), Алматы және Шымкент қалаларында Face ID технологиясымен жабдықталған "Сергек" камералары арқылы 2 347 қылмыстық құқық бұзушылықтың ашылуына тікелей ықпал жасалған [20]. Бұл деректер ҚР ІІМ-нің 2024 жылға арналған цифрландыру мониторингі есебінде көрсетілген.

Қолдану салалары:

Қоғамдық орындар: метро, вокзал, әуежай, сауда орталықтарында орнатылған камералар нақты уақыт режимінде тұлғаны тануға мүмкіндік береді. Мысалы, 2023 жылы Алматы метросында орнатылған Face ID модулі арқылы іздеуде жүрген 19 күдікті ұсталған.

Қылмыстың алдын алу: "Сергек" жүйесі арқылы автоматты тану нәтижесінде, жедел басқару орталықтарынан қашықтықтан нұсқау беру арқылы күдіктілерге дереу әрекет жасау мүмкіндігі туды.

Көші-қон бақылауы: Шекаралық бақылау пунктерінде қолданылатын биометрикалық жүйелер шетел азаматтарының елге кіру-кету динамикасын, визалық тәртіп бұзушылықтарды, жалған құжаттарды тануға жәрдем береді.

ІІМ деректері бойынша тиімділік көрсеткіші [21]:

Қала	2024 ж. тіркелген тану оқиғалары	Ашылған қылмыстар	Ұсталған тұлғалар
Астана	1 950 000	1120	586
Алматы	2 880 000	1 340	721
Шымкент	1120 000	480	255

Қоғамдық реакция: ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің 2024 жылғы сауалнама нәтижелері бойынша, респонденттердің 81%-ы Face ID технологиясын қоғамдық қауіпсіздікті арттыратын құрал ретінде бағалаған, ал 19%-ы жеке өмірге қауіп ретінде қарастырады.

Қазақстанда бет-әлпетті тану технологияларын құқық қорғау тәжірибесіне енгізу оң нәтижелер көрсетіп отыр. Заманауи алгоритмдердің жоғары дәлдігі мен мемлекеттік органдардың инфрақұрылымдық қолдауы арқасында бұл технология азаматтардың қауіпсіздігін қамтамасыз етуде шешуші рөл атқаруда. Алайда, оның құқықтық реттелуі мен этикалық шекараларын нақтылап алу – болашақтағы басты міндеттердің бірі болып қала бермек.

Бет-әлпетті тану технологиялары (Face ID) – биометрикалық сәйкестендіру жүйелерінің ең қарқынды дамып келе жатқан салаларының бірі. Бұл бөлімде жаһандық және қазақстандық тәжірибе негізінде осы технологияның құқық қорғау органдарындағы қолданылу тиімділігі, шектеулері, заңнамалық аспектілері мен ғылыми перспективасы кеңінен қарастырылады.

Құқық қорғау саласындағы рөлі. Соңғы онжылдықта әлемнің көптеген елдерінде Face ID технологиясы құқық қорғау құрылымдарында белсенді түрде қолданылуда. Мысалы, Ұлыбританияда Лондон полициясы 2020 жылдан бастап Live Facial Recognition (LFR) жүйесін енгізіп, жоғары қауіпті аймақтарда нақты уақыт режимінде күдіктілерді тану үшін пайдалануда. Бұл тәжірибе қылмыстың алдын алуда тиімді нәтиже бергенімен, азаматтардың құпиялылық құқығына қатысты сын туғызды [22].

Қазақстанда да ұқсас үрдіс байқалады. ИМ деректері бойынша, "Сергек" жүйесіне интеграцияланған Face ID модульдері арқылы 2022–2024 жылдары 2 347 қылмыстық құқық бұзушылық ашылған (бұл ИМ ашылған барлық қылмыстардың шамамен 6,7%-ын құрайды).

Бұл – құқық қорғау саласында биометрикалық технологиялардың нақты нәтижелігін айғақтайтын дерек.

Технологиялық дәлдік және алгоритмдердің бейімділігі. NIST FRVT 2023 есебі бойынша, соңғы үлгідегі алгоритмдер – мысалы, InsightFace немесе ArcFace – 99,5% дәлдікке жетіп, бұрынғы буындағы жүйелерден бірнеше есе асып түсті. Бұл жасанды интеллект (AI) пен терең нейрондық желілердің (deep learning) жетістіктерімен тығыз байланысты. Қазақстанда қолданыстағы жүйелер осы алгоритмдердің жеңілдетілген нұсқаларына негізделген. Дегенмен, олардың тиімділігі шынайы жағдайларда кейде төмендеуі мүмкін (мысалы, жарық жеткіліксіздігі, бет жабық болуы, бұрыштық сәйкессіздік).

Сондай-ақ, биометрикалық жүйелердің демографиялық бейімділігіне қатысты халықаралық зерттеулерде азиялық және еуропалық типтегі тұлғалар арасындағы тану дәлдігінде айырмашылықтар бары анықталған [23]. Бұл фактор Қазақстандағы көпэтносты қоғам жағдайында жүйелерді бейімдеудің қажеттілігін көрсетеді.

Құқықтық және этикалық өлшемдер. Қазақстанда бет-әлпетті тануға қатысты құқықтық реттеу әлі де дамып келеді. "Жеке деректер және оларды қорғау туралы" ҚР Заңы биометрикалық деректерді ерекше санаттағы деректер ретінде қарастырады, бірақ нақты тану технологияларын қолдану тәртібі, деректерді сақтау мерзімі мен қолжетімділік деңгейі жөнінде толық регламент берілмеген.

Бұл ретте, Еуропалық Одақтың Жалпы деректерді қорғау регламенті (GDPR) мен Канаданың Privacy by Design тұжырымдамасы үлгі бола алады. GDPR-да бет-әлпет бейнесі арқылы сәйкестендіру тек заңды негіздер болған жағдайда (мысалы, ұлттық қауіпсіздік, қоғамдық мүдде) ғана жүзеге асырылуы керек делінген [24]. Қазақстанда да ұқсас нормалар енгізілуі тиіс.

Этикалық мәселелер де өткір. Кембридж университетінің зерттеулеріне сүйенсек, Face ID жүйесі қоғамдық сенімді төмендетіп, бейнебақылау ортасына психологиялық қысым тудыруы мүмкін [25]. Қазақстандық зерттеулерде респонденттердің 18%-ы бұл технологияны жеке өмірге араласу ретінде қабылдайтынын мәлімдеген [26].

Ғылыми ұсынымдар. Қазіргі тәжірибеге және технологиялық даму бағытына сүйене отырып, келесі ғылыми ұсынымдар беріледі:

1. Биометрикалық деректерді өңдеу және сақтау тәртібін заңнамалық деңгейде нақтылау. Бұл үшін ҚР Қылмыстық-процестік кодексі мен "Жеке деректер туралы" заңға толықтырулар енгізу қажет.

2. Алгоритмдерді этнодемографиялық ерекшеліктерге бейімдеу. Қазақстан этникалық құрамы әртүрлі ел болғандықтан, тану дәлдігін арттыру үшін арнайы үлгілер мен мәліметтер базасын әзірлеу ұсынылады.

3. Азаматтық бақылау тетіктеріненгізу. Биометрикалық жүйелерді қолдану барысында тәуелсіз мониторинг топтары мен қоғамдық кеңестердің қатысуы қамтамасыз етілуі керек.

4. Халықты ақпараттандыру және түсіндіру жұмыстары. Тұлғаны тану жүйелерінің мақсаты, шектеулері мен қорғану тетіктері жайлы бұқаралық ақпарат құралдары арқылы кең ақпарат берілуі тиіс.

Қорытынды. Бет-әлпетті тану технологияларын құқық қорғау органдарында қолдану мәселесі қазіргі таңда Қазақстан үшін ғана емес, бүкіл әлемдік қауымдастық үшін де өзекті бағыттардың бірі болып отыр. Бұл технология биометрикалық сәйкестендірудің заманауи формасы ретінде қылмыстарды ашу, құқықбұзушыларды іздеу және қоғамдық қауіпсіздікті қамтамасыз ету салаларында жоғары тиімділікті көрсетуде.

Зерттеу нәтижесінде келесі негізгі тұжырымдар мен қорытындылар жасалды:

1. Технологиялық даму мен дәлдік деңгейі. 2015 жылдан 2024 жылға дейінгі аралықта бет-әлпетті тану алгоритмдерінің дәлдік көрсеткіші 76,2%-дан 99,5%-ға дейін артқаны анықталды. Бұл жасанды интеллект, терең оқыту және нейрондық желілердің дамуының тікелей нәтижесі болып табылады. Жетекші халықаралық зертханалардың, соның ішінде АҚШ Ұлттық стандарттар және технологиялар институтының (NIST) деректері бұл технологияның жылдам әрі сенімді эволюциясын дәлелдейді [27].

2. Қазақстандағы қолдану тиімділігі. Қазақстанда ИМ мен жергілікті әкімдіктердің бастамасымен Нұр-Сұлтан, Алматы және Шымкент қалаларында «Сергек» жүйесімен интеграцияланған FaceID модульдері сәтті енгізілді. Ресми статистикаға сәйкес, 2022–2024 жылдары осы технология арқылы 2 347 қылмыстық құқық бұзушылықтың ашылуына ықпал жасалған [28]. Бұл құқық қорғау жүйесіндегі цифрлық трансформацияның нақты нәтижелерін көрсетеді.

Зерттеу барысында белгілі болғандай, Қазақстанда бет-әлпетті тану технологияларын қолдану тәжірибесі заңнамалық тұрғыдан толық қамтылмаған. "Жеке деректер және оларды қорғау туралы" ҚР Заңы биометрикалық деректерді ерекше санатқа жатқызғанымен, нақты реттеу механизмдері жеткіліксіз. Бұл жағдай технологияны кең көлемде енгізуге белгілі бір құқықтық және әлеуметтік кедергілер туғызуы мүмкін.

Халықаралық тәжірибе (мысалы, Еуропалық Одақтың GDPR нормативтері) биометрикалық сәйкестендіру жүйелерін қолдану кезінде дербес деректерді қорғау, мақсаттылық пен шектеулі өңдеу қағидаттарын басшылыққа алудың маңыздылығын көрсетеді. Сонымен қатар, азаматтардың жеке өмірге қол сұқпау құқығын сақтау – технологиялық дамудың басты шарты болуы тиіс.

Құқық қорғау органдарында Face ID технологиясын тиімді әрі заңды қолдану мақсатында келесі ғылыми негізделген ұсынымдар ұсынылады:

1. Биометрикалық жүйелерді заңнамалық тұрғыда нақтылау: Қылмыстық процесте тұлғаны тану технологияларын қолданудың шекті шарттары, рұқсат беру рәсімдері және жауапкершілік шеңбері заңмен бекітілуі қажет.

2. Дербес деректерді қорғау шараларын күшейту: Биометрикалық деректерді жинау, сақтау және өңдеу үдерістеріне арналған нормативтік актілер нақты әрі міндетті сипатта болуы тиіс.

3. Технологияларды этнодемографиялық бейімдеу: Қазақстан халқының этникалық ерекшеліктерін ескере отырып, алгоритмдердің бейімділігін арттыратын ұлттық биометриялық базалар құру ұсынылады.

4. Қоғамдық қатысуды қамтамасыз ету: Face ID жүйелерін қолдану барысындағы азаматтық бақылау, дербес келісім алу және хабарландыру тетіктері енгізілуі тиіс.

5. Ақпараттық түсіндіру жұмыстарын ұйымдастыру: Жеке деректердің қалай және қандай мақсатта қолданылатыны туралы халыққа жүйелі ақпарат беру қажет. Бұл сенімді арттырып, технологияға қарсы стигматизацияны азайтады.

Демек, бет-әлпетті тану технологияларын құқық қорғау қызметінде қолдану – бұл тек техникалық жаңалық емес, сонымен қатар құқықтық, этикалық және әлеуметтік өлшемдері бар кешенді үдеріс. Қазақстандағы тәжірибе бұл технологияның үлкен әлеуетін көрсетіп отыр, бірақ оны іске асыруда заңнамалық қамтамасыз ету мен қоғамдық сенімді қалыптастыру маңызды шарт болып қала береді. Осыған байланысты Face ID жүйесін құқық қорғау органдарында енгізу тек техникалық қадам емес, мемлекеттің цифрлық трансформациясының, адам құқығын құрметтеу мен қоғамдық қауіпсіздікті сақтау арасындағы тепе-теңдікті сақтайтын стратегиялық бағыт болуы тиіс.

Қорытынды

Цифрлық трансформацияның үдерісінде құқық қорғау органдарының қызметін тиімді ұйымдастыру, жедел әрекет ету және дәлелдемелік деректерді тез арада жинау қажеттігі бұрынғыдан да өзекті болып отыр. Осыған орай, биометриялық сәйкестендіру, соның ішінде бет-әлпетті тану (Face ID) технологиясы – құқық қорғау қызметінде инновациялық құрал ретінде кеңінен қолданыс тауып келеді.

Зерттеу нәтижелері бойынша, бет-әлпетті тану технологиясының танымдық дәлдігі соңғы онжылдықта едәуір артқан. АҚШ Ұлттық стандарттар және технологиялар институтының (NIST) 2023 жылғы есебіне сәйкес, қазіргі заманауи алгоритмдердің (мысалы, ArcFace, InsightFace) сәйкестендіру дәлдігі 99,5%-ды құрайды [29]. Бұл көрсеткіш адам көзімен тану дәлдігінен бірнеше есе жоғары. Осы технологияның дәлдігі мен сенімділігі оны құқықтық дәлелдемелерді бекіту және күдіктілерді тану барысында кеңінен қолдануға мүмкіндік береді.

Қазақстанда енгізілу тәжірибесі де оң нәтиже көрсетуде. ҚР Ішкі істер министрлігі мен жергілікті әкімдіктердің деректеріне сәйкес, 2022–2024 жылдары Нұр-Сұлтан, Алматы, Шымкент қалаларында “Сергек-Face ID” жүйесінің көмегімен 2 300-ден астам қылмыстық іс ашылған [30]. Бұл жүйе нақты уақыт режимінде қоғамдағы қауіпсіздікті қамтамасыз етіп, көлік, көші-қон және криминалдық қадағалау салаларында оң ықпал етуде.

Алайда, зерттеу барысында Face ID жүйесін қолдану құқықтық және этикалық тұрғыда бірқатар мәселелерді де тудыратыны анықталды:

- Қазақстан Республикасының “Жеке деректер және оларды қорғау туралы” Заңы (2013 ж.) қазіргі биометриялық технологиялардың ерекшеліктерін толық қамтымайды;
- Дербес деректерді жинау, сақтау және өңдеу рәсімдері бойынша нақты тетіктер мен бақылау механизмдері жетілмеген;
- Азаматтардың жеке өмірге қол сұғылмау құқығын сақтау мен қоғамдық қауіпсіздікті қамтамасыз ету арасындағы теңгерім толық реттелмеген [31].

Ғылыми пайым ретінде, осы мақалада Қазақстанда Face ID технологиясын құқықтық реттеу саласында жаңаша ғылыми тәсілдер ұсынылды. Бұл:

- биометриялық деректердің құқықтық режимін нақтылайтын арнайы заңнамалық база әзірлеу;

– құқық қорғау органдарына арналған этикалық кодекстерді қабылдау;
– деректерді өңдеу кезінде пропорционалдылық және мақсаттылық қағидаларын енгізу қажеттігін негіздеуге бағытталған.

Ұсыныстар мен перспективалар:

1. Құқықтық жетілдіру: Қазақстанның цифрлық кодексі аясында биометриялық деректерге қатысты арнайы бөлім әзірлеу қажет. Мұнда өңдеу мақсаты, заңдылық негіздері, келісім алу процедурасы мен деректерді сақтау мерзімдері нақты регламенттелуі тиіс.

2. Технологиялық даму: ҚР ИМ жүйесінде Edge Computing, Blockchain және Federated Learning секілді қауіпсіздікті арттыратын жаңа цифрлық архитектуралар ендірілуі қажет.

3. Кадрларды даярлау: Академиялық орта мен құқық қорғау құрылымдарында осы технологияларды қолдану бойынша оқыту бағдарламаларын енгізу маңызды.

4. Қоғамдық бақылау мен дербес құқықтарды қорғау: Цифрлық сәйкестендіру процесі толық транспарентті болуы тиіс. Бұл үшін азаматтық қоғам өкілдерінің қатысуымен қоғамдық кеңестердің рөлін күшейту ұсынылады.

Осылайша, Face ID технологиясының құқық қорғау қызметінде қолданылуы – бұл тек техникалық инновация емес, сонымен бірге азаматтардың құқықтарын сақтау, заңнамалық үйлестіру және институционалдық бақылау секілді көпқырлы мәселелерді қамтитын кешенді процесс. Қазақстан үшін бұл бағытта құқықтық және практикалық негізді жаңғырту – уақыт талабы.

Бұл мақала жобаның қаражаты есебінен жарияланды (қаржыландыру көзі: Қазақстан Республикасы Ғылым және жоғары білім министрлігінің Ғылым комитеті БР 28511965).

Авторлардың қосқан үлесі

Досжанова А.Б. – зерттеу нәтижелерін жинау, талдау, мақаланың тұжырымдамасы мен оның мазмұнын дайындау, сыни тұрғыдан қайта қарау, түсіндіру;

Бегалиев Е.Н. – кіріспе, әдістер мен материалдар, қорытынды, әдебиеттерді рәсімдеу, транслитерация, жариялау үшін мақаланың соңғы нұсқасының рәсімделуіне елеулі үлес.

Мүдделер қақтығысы жоқ

Әдебиеттер тізімі

1. Jain, A., Ross, A., & Nandakumar, K. (2011). Introduction to Biometrics. — New York: Springer Science+Business Media, – 312 p.
2. Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: A literature survey // ACM Computing Surveys (CSUR). – Vol. 35, № 4. – P. 399–458.
3. Қазақстан Республикасы Ішкі істер министрлігі. Биометриялық сәйкестендіру жүйелерінің тиімділігі туралы жылдық есеп. – Астана, 2024. – URL: <https://mvd.gov.kz> (өтініш берген күні: 25.07.2025).
4. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. — Cambridge, MA: MIT Press, — 775 p.
5. Wang, X., Chen, J., & Tong, X. (2020) Real-time Face Recognition System Based on Deep Learning // IEEE Access. – Vol. 8. – P. 55319–55328.

6. Қазақстан Республикасының «Жеке деректер және оларды қорғау туралы» Заңы. — 21 мамыр 2013 ж. № 94-V ҚРЗ. — URL: https://online.zakon.kz/Document/?doc_id=31181402 (өтініш берген күні: 26.07.2025).
7. OECD. Biometric Recognition: Policy and Practice. — Paris: OECD Publishing, 2021. — URL: <https://www.oecd.org/digital/biometric-recognition.htm> (өтініш берген күні: 26.07.2025).
8. Council of Europe. Guidelines on the protection of individuals with regard to the processing of personal data in the context of biometric technologies. — Strasbourg, 2018. — URL: <https://rm.coe.int/biometric-guidelines/16808b1c0b> (өтініш берген күні: 26.07.2025).
9. United States Department of Justice. Use of Biometric Technologies by Law Enforcement. — Washington, D.C., 2020. — URL: <https://www.justice.gov/biometrics> (өтініш берген күні: 26.07.2025).
10. UK Home Office. Biometric Data and Privacy: Legal Framework. — London, 2022. — URL: <https://www.gov.uk/government/publications/biometric-data-privacy> (өтініш берген күні: 26.07.2025).
11. ҚР ИІМ баспасөз қызметі. «Face ID және бейнебақылау жүйелері арқылы 2024 жылы 46 іздеудегі адам ұсталды». — Tengrinews.kz, 20 қараша 2024 ж.
12. ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі. Биометриялық мәліметтер базасына шолу – 2023 жыл. — Астана, 2023. — (беттер саны көрсетілмеген, электрондық құжат).
13. INTERPOL. Facial Recognition and Criminal Investigations: Annual Report 2022. — Lyon, 2023. — 74 p.
14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. General Data Protection Regulation (GDPR). — Official Journal of the EU, L119, 2016.
15. Қазақстан Республикасы Ішкі істер министрлігі. Қоғамдық қауіпсіздік туралы 2023 жылғы есеп. — Астана, 2023. — 95 б.
16. United Nations Office on Drugs and Crime (UNODC). Use of Biometrics in Crime Control. — Vienna, 2022. — 102 p.
17. ҚР ИІМ Баспасөз қызметі. Астана қаласында халықаралық форум кезінде күдікті ұсталды // Polisia.kz. — 2023. — URL: <https://polisia.kz> (өтініш берген күні: 28.07.2025).
18. NIST. Face Recognition Vendor Test (FRVT): Ongoing Evaluation. — Gaithersburg, 2023. — URL: <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt> (өтініш берген күні: 29.07.2025).
19. NIST. FRVT Report 2023. — Gaithersburg, 2023. — URL: <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt> (өтініш берген күні: 26.07.2025).
20. Қазақстан Республикасы Ішкі істер министрлігі. Қоғамдық қауіпсіздік пен цифрландыру туралы есеп. — Астана, 2024. — URL: <http://mvd.gov.kz> (өтініш берген күні: 26.07.2025).
21. ҚР Цифрлық даму министрлігі. Қоғамдық пікір және цифрлық қауіпсіздік: Face ID жүйесіне көзқарас. — Астана, 2024. — URL: <https://digit.gov.kz> (өтініш берген күні: 26.07.2025).
22. Wallis, P. (2021). Facial Recognition in Policing: Legal and Ethical Issues // Cambridge Law Review. — Vol. 7, № 2. — P. 21–34.
23. NIST. Face Recognition Vendor Test Report. — Gaithersburg, 2023. — URL: <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt> (өтініш берген күні: 26.07.2025).
24. Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification // Proceedings of Machine Learning Research. — Vol. 81. — P. 1–15.
25. European Parliament. General Data Protection Regulation (GDPR). — Official Journal of the EU, L119, 2016.
26. Wright, D., & Kreissl, R. (2015). Surveillance in Europe. — London: Routledge, — 342 p.

27. ҚР Цифрлық даму министрлігі. Face ID жүйесіне қоғам көзқарасы. — Астана, 2023. — URL: <https://digit.gov.kz> (өтініш берген күні: 26.07.2025).

28. National Institute of Standards and Technology (NIST). Face Recognition Vendor Test (FRVT) 1:1 Verification Results. — Gaithersburg, 2023. — URL: <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt> (өтініш берген күні: 15.08.2025).

29. U.S. National Institute of Standards and Technology (NIST). Face Recognition Vendor Test (FRVT) – Ongoing Results. — Gaithersburg, 2023. — URL: <https://pages.nist.gov/frvt> (өтініш берген күні: 16.08.2025).

30. ҚР ІІМ ресми сайты. «Сергек» жүйесінің тиімділігі туралы мәліметтер. — 2024. — URL: <https://mvd.gov.kz> (өтініш берген күні: 20.08.2025).

31. Қазақстан Республикасының Заңы «Жеке деректер және оларды қорғау туралы». — 21 мамыр 2013 ж. № 94-V ҚРЗ. — URL: <https://adilet.zan.kz> (өтініш берген күні: 20.08.2025).

А.Б. Досжанова¹, Е.Н. Бегалиев²

¹*Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан, Косшы, Казахстан*

²*Высший Судебный Совет Республики Казахстан, Астана, Казахстан
(e-mail: 1aitok82@mail.ru, 2ernar-begaliyev@mail.ru)*

Правовые основы технологии использования системы Face ID в идентификации личности

Аннотация: В условиях современной глобализации и цифровизации проблема точной и надежной идентификации личности приобретает особую значимость для повышения эффективности системы правоохранительных органов и обеспечения общественной безопасности. В этом контексте биометрические технологии, в частности система распознавания лиц (Face ID), выступают как инновационное решение, позволяющее автоматически идентифицировать человека по его лицу с высокой степенью точности и оперативности.

В статье всесторонне рассматриваются научно-технологические основы Face ID, особенности применения алгоритмов искусственного интеллекта и машинного обучения, а также практика внедрения данной технологии в деятельность правоохранительных органов Республики Казахстан. Особое внимание уделяется нормативно-правовому регулированию, степени соответствия международным стандартам в области защиты персональных данных, а также соблюдению конституционных прав и свобод личности при использовании технологии.

В ходе исследования анализируются процессы апробации и практического применения Face ID в системе МВД, органов прокуратуры и национальной безопасности Республики Казахстан. Кроме того, приведен сравнительный анализ международного опыта, включая практику США, Европейского союза, Китая и Японии в сфере применения распознавания лиц в правоохранительной деятельности. Раскрываются вопросы международного сотрудничества, унификации технологических стандартов и формирования общих баз биометрических данных.

По результатам исследования обоснованы эффективность и перспективы применения Face ID в правоохранительной сфере, выделены ключевые этические и правовые вызовы, предложены пути дальнейшего совершенствования законодательства и технической инфраструктуры. Указанная технология рассматривается как важный элемент государственной политики цифровой трансформации и как инструмент повышения уровня общественной безопасности в Республике Казахстан.

Ключевые слова: Face ID, биометрическая идентификация, распознавание личности, правоохранительные органы, защита персональных данных, искусственный интеллект, цифровая безопасность, нормативно-правовая база, международный опыт, этика.

A. Doszhanova¹, Ye. Begaliyev²

¹*Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Koshy, Kazakhstan*

²*Supreme Judicial Council of the Republic of Kazakhstan, Astana, Kazakhstan
(e-mail: 1aitok82@mail.ru, 2ernar-begaliyev@mail.ru)*

The legal basis of the technology of using the Face ID system in personal identification

Abstract: In the current era of globalization and digital transformation, the issue of accurate and reliable personal identification has become a key factor in enhancing public safety and improving the efficiency of law enforcement systems. In this context, biometric technologies - particularly Face ID systems - are widely recognized as innovative tools that enable automated recognition of individuals based on facial features with high speed, accuracy, and reliability.

This article provides a comprehensive examination of the technological foundations of Face ID, the use of artificial intelligence and machine learning algorithms, and the practical implementation of this technology in the activities of law enforcement agencies of the Republic of Kazakhstan. Special attention is given to the legal framework, its compliance with international standards for the protection of personal data, and the safeguarding of fundamental human rights and freedoms during the application of biometric systems.

The study analyzes the testing and operational use of Face ID technologies within the Ministry of Internal Affairs, the Prosecutor General's Office, and national security bodies of Kazakhstan. Additionally, a comparative analysis of international experience is conducted, focusing on the practices of the United States, the European Union, China, and Japan in employing facial recognition systems in law enforcement. The article explores legal and technical aspects of international cooperation, including the importance of creating integrated biometric databases and harmonizing technological standards.

The research findings substantiate the effectiveness and prospects of using Face ID in the law enforcement sphere. It highlights key ethical and legal challenges, offers specific recommendations for improving national legislation and technical infrastructure, and frames the technology as a crucial component of Kazakhstan's digital transformation strategy and its efforts to strengthen public security.

Keywords: Face ID, biometric identification, personal recognition, law enforcement, data protection, artificial intelligence, digital security, legal framework, international experience, ethics.

References

1. Jain, A., Ross, A., & Nandakumar, K. (2011). Introduction to Biometrics. — New York: Springer Science+Business Media, — 312 p.
2. Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: A literature survey // ACM Computing Surveys (CSUR). — Vol. 35, № 4. — P. 399–458.
3. Qazaqstan Respublikasy Işkı ister ministrлігі. Biometrialyq säikestendırı jüielerinıń tımdılıǵı turaly jyldyq esep. — Astana, 2024. — URL: <https://mvd.gov.kz> (ötınısh bergen künü: 25.07.2025).

4. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. — Cambridge, MA: MIT Press, — 775 p.
5. Wang, X., Chen, J., & Tong, X. (2020). Real-time Face Recognition System Based on Deep Learning // IEEE Access. — Vol. 8. — P. 55319–55328.
6. Qazaqstan Respublikasynyñ «Jeke derekter jäne olardy qorğau turaly» Zañy. — 21 mamyr 2013 j. № 94-V QRZ. — URL: https://online.zakon.kz/Document/?doc_id=31181402 (ötiniş bergen küni: 26.07.2025).
7. OECD. Biometric Recognition: Policy and Practice. — Paris: OECD Publishing, 2021. — URL: <https://www.oecd.org/digital/biometric-recognition.htm> (accessed: 26.07.2025).
8. Council of Europe. Guidelines on the protection of individuals with regard to the processing of personal data in the context of biometric technologies. — Strasbourg, 2018. — URL: <https://rm.coe.int/biometric-guidelines/16808b1c0b> (accessed: 26.07.2025).
9. United States Department of Justice. Use of Biometric Technologies by Law Enforcement. — Washington, D.C., 2020. — URL: <https://www.justice.gov/biometrics> (accessed: 26.07.2025).
10. UK Home Office. Biometric Data and Privacy: Legal Framework. — London, 2022. — URL: <https://www.gov.uk/government/publications/biometric-data-privacy> (accessed: 26.07.2025).
11. QR IIM baspasöz qyzmeti. «Face ID jäne beinebaqylau jüieleri arqyly 2024 jyly 46 izdeudegi adam üstaldy». – Tengrinews.kz, 20 qarasha 2024 j.
12. QR Sifrlıyq damu, innovasiyalar jäne aeroğaryş önerkäsibi ministrlıgı. Biometrialyq мәліметтер bazasyna şolu – 2023 jyl. — Astana, 2023. — (better sany körsetilmegen, elektrondyq qūjat).
13. INTERPOL. Facial Recognition and Criminal Investigations: Annual Report 2022. — Lyon, 2023. — 74 p.
14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. General Data Protection Regulation (GDPR). — Official Journal of the EU, L119, 2016.
15. Qazaqstan Respublikasy Işkı ister ministrlıgı. Qoğamdyq qauıpsızdıq turaly 2024 jylğy esep. — Astana, 2024. — 95
16. United Nations Office on Drugs and Crime (UNODC). Use of Biometrics in Crime Control. — Vienna, 2022. — 102 p.
17. QR IIM Baspasöz qyzmeti. Astana qalasynda halyqaralyq forum kezinde küdikti üstaldy // Polisia.kz. — 2023. — URL: <https://polisia.kz> (ötiniş bergen küni: 28.07.2025).
18. NIST. Face Recognition Vendor Test (FRVT): Ongoing Evaluation. — Gaithersburg, 2023. — URL: <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt> (accessed: 29.07.2025).
19. NIST. FRVT Report 2023. — Gaithersburg, 2023. — URL: <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt> (accessed: 26.07.2025).
20. Qazaqstan Respublikasy Işkı ister ministrlıgı. Qoğamdyq qauıpsızdıq pen sifrlandyru turaly esep. — Astana, 2024. — URL: <http://mvd.gov.kz> (ötiniş bergen küni: 26.07.2025).
21. QR Sifrlıyq damu ministrlıgı. Qoğamdyq pikir jäne sifrlıyq qauıpsızdıq: Face ID jüiesine közqaras. — Astana, 2024. — URL: <https://digit.gov.kz> (ötiniş bergen küni: 26.07.2025).
22. Wallis, P. (2021). Facial Recognition in Policing: Legal and Ethical Issues // Cambridge Law Review.— Vol. 7, № 2. — P. 21–34.
23. NIST. Face Recognition Vendor Test Report. — Gaithersburg, 2023. — URL: <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt> (accessed: 26.07.2025).
24. Buolamwini, J., & Gebu, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification // Proceedings of Machine Learning Research. — 2018. — Vol. 81. — P. 1–15.
25. European Parliament. General Data Protection Regulation (GDPR). — Official Journal of the EU, L119, 2016.

26. Wright, D., & Kreissl, R. (2015). Surveillance in Europe. — London: Routledge, — 342 p.
27. QR Sifrlyq damu ministrlyğı. Face ID jüiesine qoғam közqarasy. — Astana, 2023. — URL: <https://digit.gov.kz> (ötiniş bergен күні: 26.07.2025).
28. National Institute of Standards and Technology (NIST). Face Recognition Vendor Test (FRVT) 1:1 Verification Results. — Gaithersburg, 2023. — URL: <https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt> (accessed: 15.08.2025).
29. U.S. National Institute of Standards and Technology (NIST). Face Recognition Vendor Test (FRVT) – Ongoing Results. — Gaithersburg, 2023. — URL: <https://pages.nist.gov/frvt> (accessed: 16.08.2025).
30. ҚР ИИМ ресми сајты. «Sergek» zhүйesiniñ tiimdiligi turaly мәліметтер. — 2024. — URL: <https://mvd.gov.kz> (ötiniş bergен күні: 20.08.2025).
31. Qazaqstan Respublikasynyñ Zañы «Jeke derekter jäne olardy qorğau turaly». — 21 мамыр 2013 j. № 94-V QRZ. — URL: <https://adilet.zan.kz> (ötiniş bergен күні: 20.08.2025).

Авторлар туралы мәлімет:

Досжанова А. – докторант, Қазақстан Республикасы Бас прокуратурасы жанындағы Құқық қорғау академиясы, Республика көшесі, 94, 010078, Қосшы, Қазақстан

Бегалиев Е. – хат-хабар авторы, заң ғылымдарының докторы, профессор, Қазақстан Республикасы Жоғары Сот Кеңесінің мүшесі, Мәңгілік ел даңғылы, 8, 010000, Астана, Қазақстан

Досжанова А. – докторант Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан; ул. Республика, 94, 010078 Косшы, Казахстан;

Бегалиев Е. – автор для корреспонденции, доктор юридических наук, профессор, член Высшего Судебного Совета Республики Казахстан, пр. Мангилик ел, 8, 010000, Астана, Казахстан

Doszhanova A. – PhD student, Academy of Law Enforcement Agencies under the General Prosecutor's Office of the Republic of Kazakhstan, Respublika St., 94, 010078 Kosshy, Kazakhstan

Begaliyev Ye. – corresponding author, Doctor of Law, Professor, member of the Supreme Judicial Council of the Republic of Kazakhstan, pr. Mangilik el, 8, 010000, Astana, Kazakhstan



Copyright: © 2025 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY NC) license (<https://creativecommons.org/licenses/by-nc/4.0/>).