ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТІРЛІГІ

«SDU UNIVERSITY» МЕКЕМЕСІ

ҚҰҚЫҚ ЖӘНЕ ӘЛЕУМЕТТІК ҒЫЛЫМДАР ФАКУЛЬТЕТІ
«ҚҰҚЫҚТАНУ» КАФЕДРАСЫ

«Қорғауға жіберілді»
«Құқықтану»
кафедрасының меңгерушісі
PhD, ассистент-профессор
Копбаева А.Б.

«30» мамыр 2025 жыл

МАГИСТРЛІК ДИССЕРТАЦИЯ

Тақырыбы: «Қазақстандағы биометриялық технологиялардың интеграциясы: инновацияларды, тәуекелдерді және құқықтық аспектілерді талдау»

7М04202 – «Ақпараттық технологиялар құқығы»

Орындаған: Тортай Е.К.

Ғылыми жетекші:
заң ғылымдарының
канидаты, доцент Омарова А.Б.

Қаскелең 2025

КҮНТІЗБЕЛІК КЕСТЕ

«Қазақстандағы биометриялық технологияларды интеграциялау: инновацияларды, тәуекелдерді және құқықтық аспектілерді талдау» тақырыбы бойынша магистрлік диссертацияны орындау және ұсыну күнтізбелік кестесі

2-курс магистранты, «7М04202» - «Ақпараттық технологиялар құқығы» мамандығы

№	Бөлім атаулары	Жетекшіге ұсыну мерзімдері	Орындалуы	Ғылыми жетекшінің қолы
1	Магистрлік диссертация тақырыбын таңдау және бекіту. Жетекшіні тағайындау.	02.10.2023	орындалды	
2	Магистрлік диссертацияны орындау үшін тапсырмаларды алу және әзірлеу	09.10.2023	орындалды	
3	Теориялық материалды таңдау және ғылыми жетекшіге ұсыну	15.11.2023	орындалды	
4	Практикалық материалдарды іріктеу, теориялық және практикалық материалдарды жүйелеу және ғылыми жетекшіге ұсыну	13.12.2023	орындалды	
5	Магистрлік диссертацияның/жобаның бірінші бөлімін жазу	18.01.2024-03.05.2024	орындалды	
6	Магистрлік диссертацияның/жобаның екінші бөлімін жазу	01.09.2024-03.11.2024	орындалды	
7	Магистрлік диссертацияның/жобаның үшінші бөлімін жазу	06.12.2024-29.12.2024	орындалды	
8	Магистрлік диссертацияны/жобаны рәсімдеу	01.04.2025	орындалды	

9	Плагиаттың бар немесе жоқтығын тексеру үшін магистрлік диссертацияны / жобаны жіберу	12.05.2025	орындалды	
10	Магистрлік диссертацияны / жобаны норма бақылауға бағыттау	13.05.2025	орындалды	
11	Магистрлік диссертацияны / жобаны алдын-ала қорғау	19.05.2025	орындалды	
12	Магистрлік диссертацияның / жобаның пікір алуға жолдау	20.05.2025	орындалды	
13	Магистрлік диссертацияны / жобаны кері қайтарып алу және МАК-ға қарастыруға жолдау	01.06.2025	орындалды	
14	Магистрлік диссертацияны/ жобаны қорғау	19.06.2025	орындалды	

Тапсырманы беру күні «09» қазан 2023 ж.

«Құқықтану» кафедрасының меңгерушісі: PhD, ассистент – профессор Копбаева А.Б.

Ғылыми жетекші: заң ғыл. кандидаты, доцент Омарова А.Б.

Тапсырманы орындауға қабылдаған магистрант: Тортай Е.К.

МАЗМҰНЫ

КІРІСПЕ

Қазақстандағы биометриялық технологиялардың интеграциясы елдің цифрлық трансформациясының негізгі бағыттарының біріне айналуда. Ақпараттық технологиялардың қарқынды дамуы және мемлекеттік қызметтердің қауіпсіздігі мен тиімділігін арттыру қажеттілігінің артуының негізінде беттерді, саусақ іздерін және басқа да бірегей биометриялық параметрлерді тануға негізделген жүйелерді пайдалану қоғамдық өмірдің әртүрлі салаларын оңтайландырудың маңызды әлеуетін білдіреді. Алайда, бұл инновацияларды енгізу бірқатар маңызды сын-қатерлермен байланысты. Олардың ішінде дербес деректерді қорғау, құпиялылықты қамтамасыз ету және технологияларды теріс пайдаланудың алдын алу мәселелері шешуші болып табылады. Биометриялық ақпарат көлемінің өсуімен инновациялық мүмкіндіктер мен азаматтардың жеке өміріне қол сұғылмаушылық құқықтары арасындағы тепе-теңдікті қамтамасыз етуге қабілетті нормативтік-құқықтық базаны құру және жетілдіру қажеттілігі туындайды.

Диссертациялық зерттеу тақырыбының өзектілігі. Бастапқыда ақпараттық технологиялардың қарқынды дамуы және өңделетін деректер көлемінің өсуі пайдаланушыларды сәйкестендіру мен аутентификациялаудың жаңа әдістерін енгізуді талап етеді. Бірегей физиологиялық және мінез-құлық сипаттамаларына негізделген биометриялық технологиялар цифрлық қызметтердің қауіпсіздігі мен тиімділігін арттырудың ең перспективалы құралдарының бірі болып табылады. Еліміздегі барлық мемлекеттік қызметтердің 90%-дан астамы онлайн режимде, ал электрондық үкіметтің даму деңгейі бойынша Қазақстан алдыңғы орындарда тұр. Бұл елімізде биометриялық технологияның даму қарқыны жоғары екенін көрсетеді. Жаһандық цифрландыру жағдайында елдер азаматтардың мемлекеттік органдармен өзара іс-қимылын оңтайландыруға, заңнаманың сақталуын бақылауды жақсартуға және көрсетілетін қызметтердің сапасын арттыруға мүмкіндік беретін бірыңғай цифрлық инфрақұрылым құруға ұмтылады. Оң инновациялық мүмкіндіктермен қоса, биометриялық жүйелердің интеграциясы бірқатар маңызды тәуекелдерді алып келеді. Олардың ішінде жеке деректер құпиялылығын бұзылу қаупі, биометриялық ақпаратқа рұқсатсыз қол жеткізу мүмкіндігі, сәйкестендірудегі қателіктер, бір реттеуші органның болмауы, биометриялық деректерді реттейтін заң нормаларының болмауы. Мұндай аспектілер озық технологияларды пайдалану мен азаматтардың жеке өміріне қол сұғылмаушылық құқықтарын қамтамасыз ету арасындағы тепе-теңдікті қалыптастыруға мүмкіндік беретін кешенді ғылыми талдауды қажет етеді.

Қазақстан Республикасы Бас прокуратурасының «Qamqor» Құқықтық статистика және арнайы есепке алу жөніндегі комитеті әкімшілік құқық бұзушылықтар туралы жариялаған статистикасына сәйкес, Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі (бұдан әрі-ҚР ЦДИАӨМ) жинағының 2024 жылдың 12 айы бойынша «Уәкілетті органдармен әкімшілік құқық бұзушылықтар жөніндегі істерді қарау нәтижелері туралы» №1-ӘІ нысанды статистикалық есебінің дерегіне сәйкес, ҚР

ӘҚБтК 79-бабы «Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасын бұзу» бойынша 387 әкімшілік құқық бұзушылық тіркелген, 78 731 900 тенге айыппұл салынған. 2025 жылдың 1 квартлдағы статистикалық есебі бойынша 24 әкімшілік құқық бұзушылық ісі тіркелген, 1 769 400 тенге айыппұл салынған. Жоғары да келтірілген статистикалық деректер дербес деректерді қорғау саласындағы құқықбұзушылықтардың жыл сайын артып келе жатқанын көрсетеді.

Биометриялық технологияларды енгізудің құқықтық аспектісі де маңызды. Қазақстанның қолданыстағы нормативтік-құқықтық базасы көбінесе технологиялардың қарқынды дамуына ілесе алмайды, бұл құқықтық олқылықтар туғызады және сот тәжірбиесінің қалыптаспауына ықпал етеді. Бұл тұрғыда биометриялық технологияларды интеграциялаудың құқықтық аспектілерін зерттеу ерекше өзектілікке ие, өйткені ол инновациялық шешімдерді қауіпсіз және тиімді қолдануды қамтамасыз етуге қабілетті құқықтық негіз қалыптастыруға мүмкіндік береді.

Сонымен қатар, биометриялық технологиялардың интеграциясы елдің ұлттық қауіпсіздігі мен экономикалық дамуы үшін стратегиялық маңызға ие. Мұндай жүйелерді енгізу алаяқтық деңгейін төмендетуге, қаржы және денсаулық сақтау саласында, экономиканың түрлі секторларындағы процестерді сәйкестендіру және автоматтандыру рәсімдерін жеңілдетуге ықпал етеді. Бұл өз кезегінде цифрлық экономиканың дамуын ынталандырады және Қазақстанның халықаралық технологиялық қоғамдастықтағы ұстанымын нығайтуға ықпал етеді.

Осылайша, Қазақстандағы биометриялық технологиялардың интеграциясын зерттеу, олардың инновациялық әлеуетін, ілеспе тәуекелдер мен құқықтық сын-қатерлерді талдау қажетті болып табылады.

Диссертациялық зерттеу объектісі - биометриялық технологияларды сәйкестендіру үшін техникалық шешімдерді қолдануды, қызмет салаларына енгізудің ұйымдастырушылық тетіктерін, сондай-ақ биометриялық деректерді пайдаланудың құқықтық аспектілерін қоса алғанда, Қазақстанның цифрлық инфрақұрылымына интеграциялау болып табылады.

Диссертациялық зерттеудің пәні - биометриялық технологияларды қолдануды құқықтық реттеу, оның ішінде заңнаманы және дербес деректерді қорғаудың құқықтық институты болып табылады.

Диссертациялық зерттеудің мақсаты - Қазақстанда биометриялық технологияларды қолданудың нормативтік-құқықтық базасын жетілдіру, дербес деректерді және азаматтардың биометриялық деректерін қорғауға бағытталған теориялық, практикалық аспектілері тұрғысынан талдау және заңнаманы жетілдіру бойынша жаңа ұсыныстар дайындау болып табылады.

Диссертациялық зерттеудің міндеттері:

- Биометриялық технологиялардың түсінігі, түрлері мен ерекшеліктерін анықтау;
- Биометриялық технологиялардың даму тенденцияларын, өмірдің әртүрлі салаларында, қызметтерде пайдаланудың тәуекелдерін анықтау;
- Биометриялық деректерді жинау, сақтау, өңдеу және қорғауды қамтамасыз

ететін нормативтік-актілерді талдау;

- Дербес деректерді қорғау туралы заңнаманы іске асыру мәселелерін анықтау;
- Қазақстандағы және шет елдердегі биометриялық технологияларды пайдалануды салыстырмалы құқықтық талдау;
- Дербес деректерді қорғау бойынша сот практикасын талдау мен құқық қолдану мәселелерін жетілдіру жолдарын ұсыну болып табылады.

Диссертациялық зерттеудің методологиялық негізін - талдау, синтез, индукция, дедукция сияқты жалпы ғылыми әдістер, салыстырмалы-құқықтық, және сот практикасын, шетел мемлекеттерінің заңдарын, халықаралық стандарттар мен зерттеулерін талдауға негізделген эмпирикалық әдістер құрады. Аталған әдістер Қазақстан Республикасындағы биометриялық технологияларды қолдану кезінде орын алатын тәуекелдердің салдарын зерттеу мен заңнаманы жетілдіру бойынша ұсыныстар дайындауға мүмкіндік берді.

Диссертациялық зерттеу тақырыбының ғылыми зерттеу деңгейін биометриялық деректердің пайда болуы және ғылыми анықтамасын беріп зерттеген шетелдік Anil K. Jain, Patrick Flynn, Arun A. Ross және Karthik Nandakumar, Альфонс Бертильон, Маркус Шаттен, Мирослав Бака және Мирко Цубрило, James Wayman сынды ғалымдардың еңбектері қолданылды. Ресейлік осы саладағы А.В.Ворона, А.Суомалайнен, Георгий Кухарев авторлардың кітаптары қолданылды. Осы саладағы ғылыми мақалалардан: Г.С.Кодашева, А.М.Мадиев, Ж.Б.Шурен, Л.С.Асаинова, Л.К. Терещенко, П.А.Чипигина, А.Б.Сейданов, Р.Т.Дайырбеков сынды зерттеушілердің еңбектері қарастырылды. Биометриялық технологияларды енгізу арқылы оларды пайдалануда, құқықтық тәртіпті қалыптастыруда теориялық және практикалық тұрғыдан осы саладағы құқықты толықтай зерттеу өзекті болып табылады.

Диссертациялық зерттеудің нормативтік базасын - Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Дербес деректер және оларды қорғау туралы Заңы, Мемлекеттік қызметтер көрсету кезінде жеке тұлғалардың биометриялық деректерін олардың биометриялық аутентификациясы үшін жинау, өңдеу және сақтау үшін Қазақстан Республикасы цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2020 жылғы 27 қазандағы № 406/НҚ бұйрығы, Еуропалық Одақтың Деректерді қорғаудың жалпы регламенті (GDPR; 2016/679) атты Қаулысы сонымен қатар биометриялық технологиялар бойынша халықаралық стандарттар мен шетел мемлекеттерінің заңдары құрады.

Диссертациялық зерттеудің эмпирикалық негізін - биометриялық технологияларды пайдалану бойынша Mordor Intelligence статистикалық мәліметтері, Spherical Insights есебі, TADVISER статистикалық мәліметтері, Қазақстан Республикасы Бас прокуратурасының «Qamqor» Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің әкімшілік құқық бұзушылықтар бойынша статистикасы, ҚР ЦДИАӨМ жинағының 2024 жылдың 12 айы бойынша «Уәкілетті органдармен әкімшілік құқық бұзушылықтар жөніндегі істерді қарау нәтижелері туралы» №1-ӘІ нысанды статистикалық деректері, ҚР Әкімшілік құқық бұзушылық туралы Кодексінің 79-бабы 1-бөлігі

«Қазақстан Республикасы азаматтарының дербес деректерін заңсыз жинау және өңдеу үшін» бойынша қаралған әкімшілік істері, Қазақстан Республикасы цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің сауалнамаға жауап хаттары, Мемлекеттік техникалық қызметтің (МТҚ) кибершабуылдар бойынша жүргізген тексеру нәтижелері, Экономикалық ынтымақтастық және даму ұйымы (ЭЫДҰ) нұсқаулықтары, банктер мен мемлекеттік мекемелердің биометриялық технологияларды қолдану бойынша статистикалық деректері, GDPR регламенті мен биометриялық технологияға қатысты халықаралық стандарттар, шетел мемлекеттерінің заңдары, бұқаралық ақпарат құралдарының ақпараттарынан тұрады.

Диссертациялық зерттеудің ғылыми жаңалығы - дербес деректерді қорғау туралы заңнамада биометриялық деректерді тереңінен қарастыру және биометриялық деректердің дербес деректерден ара жігін ажырату, осы деректерді пайдалану кезінде құқықтық жаңа нормаларды ұсынудан тұрады. Балаларға қатысты биометриялық деректерді өңдеуге байланысты арнайы құқықтық режимді қалыптастыру ұсынылады. Бір ғана дербес деректерді қорғау заңнамасы жеткіліксіз сондықтан заңға біршама өзгертулер мен толықтырулар қажет екендігі туралы жаңа нормалар ұсынылды. Азаматтардың жеке өмірі мен құқықтарын қорғау мақсатында дербес деректерді жинайтын және сақтайтын бірыңғай ұлттық базаны құру, сонымен бірге әкімшілік және қылмыстық санкцияларды қатаңдату бойынша ұсынымдар енгізілді.

Диссертациялық зерттеудің теориялық және тәжірибелік маңыздылығы –биометриялық технологияларды құқықтық реттеудің жаңа тұжырымдамалық тәсілдерін әзірлеу болып табылады, бұл қоғамның қазіргі цифрлық инновациялар мен құқықтық нормалардың өзара іс-қимылын түсінуді тереңдетуге мүмкіндік береді.

Ал зерттеудің тәжірибелік маңыздылығы дербес деректерді қорғауға және инновациялық технологиялар мен азаматтардың құқықтары арасындағы тепе-теңдікті қамтамасыз етуге бағытталған Қазақстанның нормативтік-құқықтық базасын жетілдіру жөніндегі нақты ұсынымдарды тұжырымдаудан тұрады. Дербес деректер және оларды қорғау туралы заңына толықтырулар енгізу және құқықбұзушылықтардың жауапкершілігін қатаңдату бойынша ұсыныстар берілді. Зерттеу нәтижесін мемлекеттік органдар, сот тәжірибесінде, құқық қолдану практикасында пайдалана алады.

Диссертациялық зерттеу нәтижелерін сынақтан өткізу және тәжірибеге енгізу. Зерттеудің нәтижелері ғылыми журналдардың жарияланымдарында, ғылыми-практикалық конференцияларда жарияланды. «Биометриялық деректерді жинау, сақтау, өңдеу және қауіпсіздікті қамтамсыз етудің заңнамалық негіздері мен тәуекелдері» атты мақаласы Д. А. Қонаев атындағы Еуразия заң академиясының хабаршысы №1 2024 жарық көрді. «Биометриялық технологияларды құқықтық реттеу: АҚШ, Еуропа Одағы және Қазақстан заңдарының мысалында» ғылыми мақаласы Eurasian Science Review (January 27, 2025, Baku, Azerbaijan) (ISSN 3006-1164) Халықаралық ғылыми конференциясында жарияланды.

Диссертациялық зерттеудің құрылымы - кіріспеден, жеті бөлімді

біріктіретін үш тараудан, қорытындыдан және пайдаланылған әдебиеттердің тізімінен тұрады.

Диссертациялық зерттеудің бірінші тарауында биологиялық сипаттамалары бойынша тану жүйелерінің түсінігі, түрлері, биометриялық технологиялардың даму тенденциялары, интеграциясы, өмірдің әртүрлі салаларында, процестерде, қызметтерде пайдаланудың тәуекелдері қарастырылды. Тарауда биометрика ұғымына және биологиялық сипаттама жүйелерінің түрлеріне жеке талдау жасалып, биометриялық технологияның дамуына тоқталдық. Биометриялық технологиялардың қазіргі таңда экономикаға тигізіп жатқан әсері туралы, қаржы, денсаулық, білім, мемлекеттік секторларда кеңінен қолданылып жатқаны туралы, сонымен қатар пайдалану кезінде туындайтын техникалық және құқықтық салдарға талдау жасалды, тәуекелдердің алдын алу шаралары бойынша ұсыныстар берілді.

Диссертациялық зерттеудің екінші тарауында биометриялық деректерді өңдеу, жинау, сақтау және қорғауды қамтамасыз ету үшін қойылатын талаптарға жеке тоқталамыз. Биометриялық деректерді жинау бойынша мемлекеттік қағидалармен танысамыз. Дербес деректер заңнамасының биометриялық ақпаратқа қалай қолданылатынын саралаймыз. Дербес деректердің субъектілерінің құқықтары мен міндеттерін заң нормаларымен қарастырамыз. Дербес деректерді қорғау туралы заңды талдап, осы саладағы құқықтық мәселелерге тоқталып, сот практикасына талдау жүргіземіз. Дербес деректерді қорғау кезінде орын алатын тәуекелдерді жіктеп, құқықтық баға бере отырып, деректерді қорғаудың жаңа механизмдері бойынша ұсыныстар беріледі.

Диссертациялық зерттеудің үшінші тарауында дербес деректерді қорғау және биометриялық технологияларды пайдалану саласындағы халықаралық заңнамалар мен халықаралық стандарттарды жеке қарастырамыз. Биометриялық деректерді қорғау бойынша қандай санкциялар қарастырылғанын, жинау және өңдеуге қойылатын талаптарына талдау жасалынады. Еуропа, АҚШ, Қытай сияқты шет елдердегі осы технологияларды қолдану бойынша ұлттық заңнамаларын еліміздегі ұлттық заңнамамен салыстырмалы құқықтық талдау жасалынып, жетілдіру бойынша ұсыныстар беріледі.

1 Құқық доктринасында биометриялық технологияларды қолданудың заманауи тұжырымдамалары

1.1 Биологиялық сипаттамалары бойынша тану жүйелерінің түсінігі, түрлері (биометриялық технологиялар)

Әлемде болып жатқан жаһандық процестер биометриялық сәйкестендіру және верификация технологияларының дамуына үлкен әсер етеді. Биометриялық технологиялар қазіргі уақытта ақпараттық технологиялардың қарқынды дамып келе жатқан бағыттарының біріне айналды. Пайдаланушылардың жылдам, сенімді және ыңғайлы аутентификациясын қажет ететін салалардың кең ауқымын тізімдеу оңай: дербес компьютерге немесе смартфонға қол жеткізу, электрондық поштаға қол жеткізу, банктік операциялар, есіктерді ашу және автомобиль қозғалтқышын іске қосу, үй-жайларға кіруді бақылау, мемлекеттік шекаралардан өту және сәйкестендіруді қажет ететін кез келген мемлекеттік органдармен өзара әрекеттесу. Биометриялық сәйкестендіру көбінесе таза немесе нақты деп аталады, өйткені ол виртуалды кілтке немесе құпия сөзге емес, жеке функцияға сүйенеді.

Биометрия немесе (биометриялық тану) (грек тілінен. βίος "өмір" және μετρέω-өлшеу) - жеке тұлғалардың мінез-құлық және биологиялық сипаттамаларына негізделген автоматты тану дегеннен шыққан. Автоматты тану шеңберіндегі индивид термині тек адамға қатысты қолданылады. Биометрия термині физика және ақпараттық қауіпсіздік саласында 1980 жылдан бастап, ал 1970 жылы автоматты сәйкестендіру термині қолданыла бастады [2]. Биометрия деп бұл адамға тікелей қатысты оның биологиялық және физикалық сипаттамаларынан алынған биометриялық деректерді айтамыз.

Биометриялық технологияның шығу тегі Ежелгі Египеттен бастау алады деседі. Тарихи жазбаларға көз жүгіртсек ұлы пирамидаларды жасаушылар алдын-ала жазылған дене сипаттамалары бойынша жұмысшыларды артықшылықтары арқылы анықтаған. Он тоғызыншы ғасырдың аяғында ғана адамдарды анықтау үшін саусақ іздері мен басқа да физикалық сипаттамаларды қолданатын жүйелер пайда бола бастады деген деректер бар. Биометрия саласын зерттеген ғалымдардың еңбектері де әуел бастан оның тек жеке адамға қатысты сипаттамалары екеніне тоқталған.

Jain, Ross және Nandakumardың «Биометрикаға кіріспе» (2016) атты кітабында авторлар биометрияны "адамның бірегей физиологиялық және мінез-құлық сипаттамаларын талдау негізінде тұлғаны автоматты түрде тану" деп анықтама береді [4]. Бұл анықтама биометриялық жүйелер тұлғаны анықтау немесе тексеру үшін өлшенетін сипаттамаларда (мысалы: саусақ іздері, бет ерекшеліктері, дауыс жазбаларында) пайдаланатынын көрсетеді.

«Biometric Systems: Technology, design and Performance Evaluation» (2017) жұмысында авторлар биометрияны «жеке тұлғаны анықтау немесе тексеру мақсатында биологиялық сипаттамаларды өлшеуге, талдауға және түсіндіруге арналған технологиялар жиынтығы» деп түсіндіреді. [5]

Ал халықаралық ISO/IEC 19794: 2005 стандартына сәйкес, биометрика адамның физикалық, физиологиялық немесе мінез-құлық сипаттамаларын өлшеу және талдау нәтижесінде алынған ақпаратты атайды, оны жеке тұлғаны автоматты түрде анықтау үшін пайдалануға болады деп анықтама береді [8]. Бұл анықтама биометриялық жүйелерді жобалау мен бағалауда қолданылатын ресми сипаттаманы береді. Халықаралық стандарттағы анықтамалар халықаралық нормативтік құқықтық актілерге қолдану кезінде негіз болады. Жоғары да көрсетілген анықтамалар биометрия терминінің жалпы идеясын көрсетеді. Биометрия автоматтандырылған жүйелерді қолдану арқылы сәйкестендіруге немесе аутентификациялауға мүмкіндік беретін адамның бірегей сипаттамаларын өлшеуге негізделген сипаттама десекте болады. Жоғарыда аталған еңбектерден басқа, биометрияның дамуына айтарлықтай үлес қосқан француз криминалисті Альфонс Бертильон. Ол денені дәл өлшеуді, саусақ іздерін және алақан іздерін қамтитын қылмыскерлерді есепке алу және каталогтау жүйесін әзірледі, бұл биометриялық сәйкестендіру әдістерін дамытудағы маңызды кезең болды [9]. Негізінен тарихқа көз жүгіртсек саусақ іздерін алу ең алдымен осы қылмысты ашу және қылмыскерлерді тану үшін ең кеңінен қолданылған әдіс. Адамдардың қолдарының саусақ іздері бір біріне ұқсамайтыны ғылыми дәлелденген соң, бұл әдіс криминалистика саласында кеңінен қолданысқа енгізілді.

«Towards a general Definition of Biometric Systems» мақаласында авторлар Маркус Шаттен, Мирослав Бака және Мирко Цубрило биометриялық жүйелердің тұжырымдамасын ұсынады, биометриялық деректерді тексеру, сәйкестендіру және жіктеу арасындағы нақты айырмашылықты жасайды және биометриялық жүйелердің қосымша кластарын енгізеді [10]. Бұл жұмыстар биометрияны адамның жеке басын анықтау және сәйкестендіру үшін оның ерекше сипаттамаларын өлшеу және талдау әдістерін зерттейтін ғылым ретінде зерттеу түсінігін кеңейтеді. Ғылыми жұмыстар мен кітаптардан бөлек биометрия және биометриялық деректер әр түрлі заңнамалық актілерде және халықаралық конвенцияларда келесідей тұжырымдалады.

Заңнамалық актінің қайнар көзі ретінде Еуропалық Одақтың деректерді қорғаудың жалпы ережесі (GDPR) бірінші бастау алады. GDPR 4(14) бабына сәйкес, биометрика — бұл жеке тұлғаның физикалық, физиологиялық немесе мінез-құлық ерекшеліктеріне қатысты және сол жеке тұлғаның бір мәнді сәйкестендіруін жасауға немесе растауға мүмкіндік беретін арнайы техникалық өңдеуден алынған жеке деректер [11]. GDPR регламентіне сәйкес биометриялық деректер деп танимыз: саусақ іздерін, бет суреттері (тану үшін қолданылатын фотосуреттер / бейнелер), ирис (немесе торлы қабық)үлгілері, дауыстық үлгілер, тамырлардың суреті (мысалы, алақан), қолтаңба (егер сәйкестендіру үшін пайдаланылса), пернелерді басу динамикасы немесе теру әрекеті, жаяу жүру (жүру үлгісі). Ескере кететін маңызды ерекшелік биометриялық деректер жеке тұлғаны бірегей сәйкестендіру үшін пайдаланылған жағдайда ғана «жеке деректердің арнайы санаттарына» (sensitive data) айналады. Мысалы: кәдімгі фотосурет биометриялық дерек емес, бірақ егер ол бетті тану үшін қолданылса онда биометриялық дерек болып танылады. Қазақстандық заңдарда

биометриялық деректерге жататын мәліметтердің толық тізімі ұсынылмаған. Біздің заңнамаға сәйкес саусақ іздері, бет суреттері (мысалы, тану үшін), ирис суреттері, дауыстық үлгілер жатады. Пернелерді басу динамикасы немесе жүру сияқты мінез-құлық ерекшеліктері Қазақстандық заңнамаға сәйкес биометриялық деректер болып саналмайтынын атап өту маңызды. Бұл құқықтық олқылық — инновациялық биометриялық технологияларды реттеуде құқықтық белгісіздік тудырады және жеке тұлғалардың дербес деректерін қорғауға қатысты құқықтық қауіптерге әкелуі мүмкін. Сондықтан Қазақстан Республикасының «Дербес деректер және оларды қорғау туралы» заңына биометриялық деректердің кеңейтілген және нақты тізбесін енгізу, сондай-ақ мінез-құлыққа негізделген биометриялық деректерді (мысалы, пернелерді басу динамикасы, жүріс-тұрыс үлгілері) жеке тұлғаны сәйкестендіруге пайдаланылған жағдайда — арнайы санаттағы дербес деректер ретінде тану қажет. Қазақстан Республикасының заңнамасында биометриялық деректерді арнайы (сезімтал) дербес деректер санатына жатқызу жөнінде құқықтық бос кеңістік бар. Бұл мәселе GDPR-мен салыстырғанда маңызды кемшілік болып табылады, себебі Еуропалық заңнамада биометриялық деректер — ерекше қорғалатын (special category of personal data) ретінде белгіленген және оларды өңдеуге негізінен тыйым салынған, тек арнайы шарттар орындалғанда ғана рұқсат беріледі (мысалы, келісім, қауіпсіздік мақсаттары, т.б.). ҚР да биометриялық деректерді арнайы санаттағы (сезімтал) дербес деректер ретінде заңда белгілеу және оларды өңдеу шарттарын қатаңдату қажет. «Дербес деректер және оларды қорғау туралы» заңда арнайы санаттағы дербес деректер деп бап немесе тармақ енгізу, сол нормаға нәсілдік және этникалық тегі; саяси көзқарастары; діни немесе философиялық наным-сенімдері; денсаулық жағдайы; биометриялық деректер; генетикалық деректер; соттылығы туралы мәліметтерді заңда айқындап көрсету керек. Сонымен қатар, 6-бапқа мынадай толықтыру енгізу ұсынылады: «Биометриялық деректерді өңдеу тек субъектінің айқын және нақты келісімімен жүзеге асырылады немесе заңда белгіленген ерекше жағдайларда ғана рұқсат етіледі.» Қазақстан Республикасының Әкімшілік құқық бұзушылық туралы кодексі (ӘҚБтК) 79-бапқа (Дербес деректер заңнамасын бұзу) қосымша толықтыру онда: «Егер бұзу биометриялық деректерге қатысты болса, айыппұл мөлшерін екі еселендіру қажет.» Ал қылмыстық кодексте 147-бапта «Биометриялық деректерді субъектінің келісімінсіз жинау, өңдеу немесе жария ету — ауырлататын мән-жай ретінде қарастырылады.» деп толықтыру енгізу қажет.

Дербес деректерді автоматтандырылған өңдеу кезінде жеке тұлғаларды қорғау туралы Еуропа Кеңесінің жаңғыртылған Конвенциясының 6-бабында адамды бірегей сәйкестендіретін биометриялық деректер заңда көзделген тиісті кепілдіктер болған кезде ғана өңдеуге жол берілетін деректердің арнайы санаттарына жатқызылған деп көрсетеді. [12]

Биометриялық технологиялар - бұл бірегей биологиялық немесе мінез-құлық сипаттамаларына негізделген тұлғаны сәйкестендіру және аутентификациялау әдістері мен құралдарының жиынтығы. Бұл технологиялар жеке тұлғаны тану кезінде жоғары дәлдік пен сенімділікті қамтамасыз етеді,

өйткені биометриялық параметрлер уақыт бойынша жоғарғы дәлдік пен тұрақтылыққа ие. ISO/IEC 19795-1:2021 сияқты халықаралық стандарттарға сәйкес биометриялық жүйе «тұлғаны тану немесе тексеру үшін биологиялық немесе мінез-құлық сипаттамаларын өлшеуді қолданатын автоматтандырылған жүйе» ретінде анықталады. Биометриялық технологиялар қол жеткізуді бақылау және басқару жүйелерінде, қаржылық қызметтерде, мобильді құрылғыларда, мемлекеттік басқару жүйелерінде, криминалистикада және жеке тұлғаны сенімді сәйкестендіру кезінде қолданылады.

Биометриялық технологиялар биометрияға негізделген — жеке адамның ерекше сипаттамаларын өлшеу. Бұл оның туғаннан алған ерекше белгілері (бет, ДНҚ, саусақ іздері, ирис), сондай-ақ уақыт өте келе алынған немесе сыртқы әсеріне (қолжазба, дауыс немесе жүріс) өзгеруге қабілетті сипаттамалары болуы мүмкін [13]. Биометриялық технологиялар биометриялық деректерді қолдану арқылы жұмыс жасайды. Биометриялық жүйелер әртүрлі белгілерге, соның ішінде қолданылатын сипаттамаларға, жұмыс істеу тәсіліне және қолдану саласына қарай жіктеледі. Биометриялық жүйелердің қолданылатын сипаттамалары бойынша негізгі екі санаты бар.

а) физиологиялық биометриялық жүйелер - бұл жүйелер адамның ерекше анатомиялық ерекшеліктерін пайдаланады. Оған;

- Саусақ іздері: саусақтағы сызықтардың үлгісін талдау.
- Бетті тану: бет геометриясын талдау.
- Иристі тану: иристің ерекше үлгісін ескеру.
- Торлы қабықты тану: торлы қан тамырларының құрылымын сканерлеу.
- Қол геометриясы: қолдың өлшемдері мен пішінін есепке алу.
- Тамырларды тану: алақандағы немесе саусақтардағы тамырлардың орналасуын талдау.
- ДНҚ талдауы: генетикалық кодты салыстыру.[14]

б) мінез-құлық биометриялық жүйелері - бұл жүйе адамның қимылдары мен мінез-құлқының ерекше ерекшеліктеріне негізделген. Оған;

- Дауысты тану: сөйлеу тембрін, жиілігін және динамикасын талдау.
- Қолтаңбаны талдау: қол қою кезінде қолжазбаны, жылдамдықты және басу күшін тексеру.
- Жүрісті тану: жүру стилі мен аяқтың орналасуын талдау.[15]

Биометриялық технологиялар жұмыс тәсіліне қарай екіге бөлінеді.

Аутентификациялық биометриялық жүйелер - адамның жеке басын растау үшін қолданылады. Биометриялық жүйелерде бір-бірден (1:1) адамның биометриялық сипаттамалары жүйеде сол адам үшін сақтаған бар деректермен салыстырылады. Бұл жағдайда адам өзінің биометриялық ақпаратын болашақ аутентификация мақсатында бұрын берген. Аутентификация үшін қолданылатын биометриялық жүйелердің көпшілігі адамнан оның биометриялық сипаттамасын белсенді түрде қамтамасыз етуді талап етеді, содан кейін ол дерекқордағы бар биометриялық ақпаратпен салыстырылады. Мысалы ұялы телефонға қол жеткізу үшін саусақ ізін немесе бетті тану немесе әуежайдың

ақылды шығуларында бетті тану технологиясын қолдану жатады.

Сәйкестендіру биометриялық жүйелер - жеке тұлғаны анықтау үшін адамның биометриялық деректерін мәліметтер базасымен салыстырады. Бұл белгісіз адамның биометриялық сипаттамасын дерекқордағы сол типтегі басқа сипаттамалармен салыстыруды білдіреді (мысалы, адамның саусақ іздері және дерекқордағы басқа саусақ іздері). Бұл жүйенің мақсаты - ықтимал сәйкестік және осылайша сол адамды анықтау. Сәйкестендіру биометриялық жүйеге мысалы көпшіліктің ішіндегі адамды анықтау үшін бетті тану технологиясын қолдану. Бұл жүйелер құқық қорғау органдарының контекстінде жиі қолданылады, мысалы қылмыс орнында табылған ДНҚ-ны жәбірленушіні немесе қылмыскерді анықтау мақсатында дерекқордағы басқа үлгілермен салыстыру. Биометриялық жүйелер әдетте автоматтандырылған, кейде тану процесін орындау үшін жасанды интеллектте қолданылады.

Барлық биометриялық технологияларды қолдану төрт негізгі кезеңнен тұрады олар:

- идентификаторды тіркеу - физиологиялық немесе мінез-құлық сипаттамалары туралы мәліметтер компьютерлік технологияларға қол жетімді формаға айналады және биометриялық жүйенің жадына енгізіледі;
- таңдау - жаңадан ұсынылған идентификатордан жүйе талдайтын бірегей белгілер ерекшеленеді;
- салыстыру - жаңадан ұсынылған және бұрын тіркелген идентификатор туралы мәліметтер салыстырылады;
- шешім - жаңадан ұсынылған және бұрын тіркелген идентификатордың сәйкес келетіні немесе сәйкес келмейтіні туралы қорытынды енгізіледі. [9]

Сәйкестендіргіштердің сәйкестігі немесе сәйкес келмеуі туралы қорытынды бұдан әрі алынған ақпарат негізінде әрекет ететін басқа жүйелерге (қол жеткізуді бақылау, ақпаратты қорғау және т.б.) таратылуы мүмкін.

1.2 Даму тенденциялары, интеграция, өмірдің әртүрлі салаларында, процестерде, қызметтерде инновациялар мен биометриялық технологияларды пайдалану тәуекелдері

Азаматтардың биометриялық деректерін өңдеу арқылы және сол деректерді жадында сақтау арқылы дамып, қолданылып жатқан биометриялық технологиялардың саны күн сайын артуда. Әсіресе мобильді құрылғылардың үздіксіз жаңаруымен бұл технология әр салада кеңінен қолданыста. Атап айтқанда мемлекеттік қызмет салаларында, мемлекеттік секторларда, құқық қорғау органдары, банк қызметтерінде және халықтың технологияға деген сұранысы жоғары. Биометриялық жүйелер нарығын зерттеп қарасақ биометриялық технологияның түрлерін (иристі тану, қол геометриясы, бетті тану, қолтаңбаны тексеру, саусақ ізі, дауысты тану, алақан венасы) әлемнің кез келген жерінде қолдануға болады. Биометриялық технологиялар сенімді сәйкестендіру және аутентификация әдістеріне сұраныстың артуына байланысты тұрақты түрде күн сайын өсуде.

Mordor Intelligence мәліметтері бойынша, 2024 жылы әлемдік биометрия

нарығының көлемі 51,15 миллиард АҚШ долларын құрайды. Бұл көрсеткіш 2029 жылға қарай 104,22 миллиард АҚШ долларына жетеді деп күтілуде, орташа жылдық өсу қарқыны (CAGR) 2024 және 2029 жылдар аралығында 15,30% құрайды деген зерттеу болжамы бар.[16] Биометрия нарығы айтарлықтай қарқынмен өсуі ұлттық қауіпсіздікке қатысты алаңдатушылық туғызады деп болжамдайды. Бұл өз кезегінде лаңкестік әрекеттердің көбеюіне және маңызды деректер мен ақпаратты ұрлау оқиғаларының көбеюіне алып келеді. Сондықтанда мобильді құрылғылардағы қосымшалардың қауіпсіздік деңгейін арттыру керек деп есептейді.

Spherical Insights есебі бойынша 2033 жылға қарай әлемдік биометриялық технологиялар нарығы 171,98 миллиард АҚШ долларына жетеді деп болжайды, бұл CAGR өсімі 2023 жылдан 2033 жылға дейін 13,97% құрайды. Биометриялық технологиялардың әлемдік нарығының көлемі 2023 жылы 46,52 миллиард долларға бағаланды. Нарық көлемі 2023 жылдан 2033 жылға дейін 13,97% - ға өсуде. Азия-Тынық мұхиты аймағы болжамды кезеңде ең жылдам өседі деп күтілуде [17]. Болжамды кезеңде Солтүстік Америка әлемдік биометриялық технологиялар нарығында ең үлкен үлеске ие болады деп күтілуде. АҚШ - та биометриялық технология әдістері қорғаныс, ұлттық қауіпсіздік, сауда, сот төрелігі және мемлекеттік істерді қоса алғанда, әртүрлі бөлімдерде кеңінен қолданылады. Сонымен қатар, Индонезияның e-KTP электрондық сәйкестендіру бағдарламасы және бет-әлпетті тану, саусақ ізін сканерлеу және ирис сканерлеу сияқты биометриялық технологияларды қолданатын үнділік UIDAI жобасы сияқты бастамалар биометриялық нарықта жаңа мүмкіндіктер жасайды деп күтілуде. Бұл жобалар озық биометриялық әдістерді біріктіру арқылы ұлттық сәйкестендіру жүйелерін жетілдіруге бағытталған, осылайша жеке тұлғаны тексеру процестерінің дәлдігі мен тиімділігін арттырады. Осы ауқымды биометриялық бастамалар енгізілген сайын олар биометриялық технологияларды қабылдауды кеңейту және әртүрлі секторларда инновациялар мен қолданбалар үшін жаңа мүмкіндіктер ашу арқылы нарықта айтарлықтай өсуді ынталандырады деп күтілуде. [17]

TADVISER мәліметтері бойынша, биометриялық жүйелердің әлемдік нарығы 2023 жылы 33,18 миллиард АҚШ долларын құрады, бұл өткен жылдармен салыстырғанда айтарлықтай өсуді көрсетеді [18]. Географиялық тұрғыдан алғанда, Солтүстік Америка 2023 жылы жетекші орынға ие болды, оның үлесі шамамен $0,705 миллиард кірісті құрады. Қарастырылып отырған саланың негізгі жүйесі бетті тану мүмкіндіктері бар қауіпсіздік пен бейнебақылау құралдарына деген қажеттіліктің артуы. Аймақтың үстемдігіне денсаулық сақтаудың дамыған инфрақұрылымы, озық технологияларды ерте енгізу ықпал етеді. Одан кейін Еуропа мен Азия-Тынық мұхиты аймағы, онда биометриялық қауіпсіздік жүйелеріне мемлекеттік инвестициялардың өсуі байқалады. Market Research Future сарапшылары бұдан әрі қаралып отырған нарықтағы күрделі пайыздардағы (CAGR көрсеткіші) орташа жылдық өсу қарқыны 10,94% құрайды деп есептейді. Нәтижесінде, 2032 жылға қарай жаһандық ауқымдағы шығындар 5,9 миллиард долларға дейін өсуі мүмкін. [18]

Биометриялық технологиялардың бұлай қарқынды өсуіне ықпал ететін

бірнеше факторлар бар. Биометриялық технолгияны пайдаланатын секторлар мен ұйымдар кибершабуылдар мен қауіпсіздік қатерлерінен сақтану үшін биометриялық жүйелер сияқты сенімді аутентификация әдістерін қолданады. Жасанды интеллект пен машиналық оқытуды қоса алғанда, технологияларды дамыту биометриялық жүйелердің дәлдігі мен тиімділігін арттырады, оларды әртүрлі салаларда қолдануды кеңейтеді. Бет пен саусақ іздерін тану сияқты биометриялық әдістер дәстүрлі аутентификация әдістерімен салыстырғанда жүйелер мен қызметтерге жылдам әрі ыңғайлы қол жеткізуді қамтамасыз етеді. Қазақстандағы биометриялық технологиялар нарығы экономиканың түрлі секторларында инновациялық шешімдердің белсенді енгізілуіне байланысты өскен. Ағымдағы көрсеткіштер мен болжамдарға шолу жасайтын болсақ. 17 жыл бойы өзінің жасанды интеллектін дамытып келе жатқан 3iTech IT-компаниясының деректері бойынша Қазақстанда дауыстық талдау және биометрия жүйесі, чат-боттар және ірі деректерді талдау қызметтері нарығының әлеуетті көлемі 112 млрд теңгені құрайды. Бұл нарық корпоративті және мемлекеттік сектордың тапсырыс берушілері арасында бірдей бөлінеді.[19]

Fortune Business Insight аналитикалық компаниясының есебіне сәйкес, 2021 жылдың қорытындысы бойынша биометриялық технологиялар нарығының көлемі 29 млрд құрады, 2022 жылы нарық бір миллиардқа өсті, ал 2029 жылға қарай 76 млрд дейін өседі деп күтілуде. Бұл Alaqan стартапын құрған Берік Нұрымбетов, Александр Мусин, Қанат Сәрсенбаев және Айғазы Жүнісбектің осы нарық бойынша келтірген болжамы. Alaqan стартапы екі шешімді ұсынады: алақанның қан тамырларының үлгісі бойынша адамды анықтайтын құрылғы, сонымен қатар үнемі оқытылатын және өзінің мәліметтер базасын кеңейтетін алгоритм. «Алақан» старт ап жүйесі қазіргі кезде биометриялық технологияның алғашқы сәтті жобаларының бірі Қазақстандағы. Қытай мен Сингапур елдері алақан жобасын қолдану бойынша серіктестік жасалды. Негізгі үш бағытта жұмыс жасайды: мектеп (балаларға қамқорлық), бизнес (карталар мен кілттер орнына) және төлем жасау [21]. Бұл старт ап жүйесінде алақан қол тамырлары биометриялық жүйесін қолданады. Қазіргі кезде мектеп саласында алақан жобасын түрлі қызметтерге қосып қойған. Соның бірі балалар қауіпсіздігін қамтамасыз етеді. Сонымен қатар Президент тапсырмасына сәйкес 2025-ші жылы Alem.AI халықаралық жасанды интеллект орталығы ашылады. «AI-Sana» бағдарламасы аясында биыл 100 мың студент экономика салаларына жасанды интеллектті енгізудің қолға алмақ. Сонымен қатар, Ұлттық жасанды интеллект платформасы «Ұлттық ақпараттық технологиялар» АҚ әзірлеп жатқан және Қазақстанның мемлекеттік мекемелеріне генеративті мәтіндік жасанды интеллекттің мүмкіндіктерін пайдалануға қолдау көрсететін орталықтандырылған инфрақұрылым болып табылады. Ұлттық жасанды интеллект платформасын құрудың басты мақсаттары – жасанды интеллектті дамытуға арналған бірыңғай экожүйе қалыптастыру, деректерді жинау мен талдауды автоматтандыру, сондай-ақ мемлекеттік басқару тиімділігін арттыру. Бұл жоба қызмет көрсету сапасын жақсартып, Қазақстанның жасанды интеллект саласындағы халықаралық беделін күшейтуге бағытталған.

Елімізде биометриялық технологиялардың өсуіне әсер ететін фактор ол

мемлекеттің бастауымен Қазақстанда барлық салаларды қамтитын қашықтықтан биометриялық сәйкестендірудің орталықтандырылған ұлттық жүйесін құру жоспарлануда. Жүйенің негізгі мақсаты-мемлекеттік қызметтерді алу және банктік қызметтерді пайдалану үшін азаматтарды толық сәйкестендіруді қамтамасыз ету. Ұлттық жүйе биометриялық ақпараттың эталондық мемлекеттік базасын құруға, сондай-ақ азаматтардың биометриялық деректерінің өзектілігі мен сақталуын қамтамасыз етуге бағытталған. «Жеке тұлғалар» Мемлекеттік деректер қоры бұл Қазақстан Республикасының жеке тұлғалары туралы ақпаратты тіркеу мен сақтаудың азаматтық хәлді сәйкестендіру және айқындау үшін жеткілікті бірыңғай жүйесі. «Заңды тұлғалар» мемлекеттік деректер қоры (бұдан әрі - ЗТ МДҚ) - ақпараттық жүйе бизнес-сәйкестендіру нөмірлерінің ұлттық тізілімін жүргізуге арналған және ҚР Стратегиялық жоспарлау және реформалар агенттігінің және ҚР ҚМ МКК Ұлттық статистика бюросының ведомстволық жүйелерімен өзара іс-қимыл жасай отырып, заңды тұлғаларға, филиалдар мен өкілдіктерге БСН беруді қамтамасыз етеді. [23]

2023 жылы қазақстандық банктер мен мемлекеттік корпорациялар әртүрлі IT-шешімдердің бұрын-соңды болмаған даму деңгейін атап өтті. Еліміздегі барлық мемлекеттік қызметтердің 90%-дан астамы онлайн-режимде, ал электрондық үкіметтің даму деңгейі бойынша БҰҰ электрондық үкіметінің жаһандық даму индексіне сәйкес Қазақстан 193 елдің ішінен 28-ші орында тұр [19]. Бұл еліміздегі биометриялық технологиялардың даму қарқынын жоғарғы екенін көрсетеді. Жоғарыда айтылып өткен бірыңғай сәйкестендірудің орталықтандырылған ұлттық жүйесін құру биометриялық технологияның Қазақстандағы даму тенденциясының бір көрінісі. 2024 жылы Қазақстанда қашықтықтан биометриялық сәйкестендірудің орталықтандырылған ұлттық жүйесін құру жоспарлары жарияланды. Жобаны цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің басқаруымен "Ұлттық ақпараттық технологиялар" АҚ мен "BTS Digital" ЖШС арасында бірлескен кәсіпорын құру арқылы іске асыру жоспарлануда. Жүйенің негізгі аспектілерінің бірі-балалар биометриясына қол жеткізу. Кәмелетке толмағандардың заңды өкілдерінің олардың дербес деректеріне қол жеткізуге келісім беру мәселесі қауіпсіздік талаптарына ерекше назар аудара отырып, ұлттық жүйе шеңберінде пысықталатын болады. Айта кетейік, мемлекеттік органдардың ақпараттық жүйелерімен интеграцияланған Digital ID жүйесін пилоттық пайдалану 70 миллионнан астам сәйкестендіруді жүргізуге мүмкіндік берді. Бұл жүйенің қызметтерін 11 миллионнан астам азамат пайдаланған.

Ең көне және ең кеңінен қолданылатын технологияның бірі ол саусақ ізін тану. Бұл жүйеде басып шығаруды оқу сенсорлары өте арзан болады, алгоритмдері тиімді және жылдам жұмыс жасайды. Бұл технология мобильді құрылғыларда, банк терминалдары мен банкоматтарда, кеңселер мен тұрғын үй кешендеріндегі кіруді бақылау жүйелерінде үздік қолданыста. Бірқатар зерттеулерге сәйкес, саусақ ізіне негізделген жүйелер биометриялық аутентификация нарығының шамамен 50% алады, әсіресе тұтынушылық электроника сегментінде.

Екінші кең қолданыстағы түрі ол бетті тану технологиясы. Бетті тану бейнебақылау, қол жеткізуді бақылау жүйелерінде, сондай-ақ маркетингтік және бөлшек сауда қызметтерінде белсенді түрде енгізілуде. Бұл технологияның артықшылығы - "қашықтықта" жұмыс істеу мүмкіндігін сыйлайды. Әуежайлардағы, стадиондардағы және сауда орталықтарындағы қауіпсіздік жүйелері, мобильді құрылғылар, мінез-құлықты талдауға арналған интеллектуалды бейне жүйелерінде қолданыста. Әлемдік нарықтағы бетті тану үлесі шамамен 25-30% деп бағаланады. Келесі түрі иристі тану бірегейліктің өте жоғары дәрежесіне ие және оны қолдан жасау мүмкін емес. Технология сәйкестендірудің ең жоғары дәлдігі қажет болған жағдайда қолданылады, және оны жасанды интеллект көмегімен алдауда мүмкін емес. Технология аса жоғарғы қорғалған объектілерде (үкіметтік және әскери) қолданылады. Жабдықтың жоғары құны мен нақты жұмыс жағдайларына байланысты бұл техника биометрия нарығының шамамен 5-10% алады.

Дауыстық биометрия дауыстық сипаттамаларды талдау арқылы аутентификация үшін қолданылады. Оның артықшылығы- дауыстардың жанаспауы және дауыстық көмекшілер мен call-орталық жүйелеріне интеграциялау мүмкіндігі. Дегенмен, нәтижелер дыбыс сапасына және айналадағы шуларға байланысты болуы мүмкін. Банктік және қаржылық қызметтерде, мобильді құрылғылар мен виртуалды көмекшілерде, қашықтан аутентификация жүйелерінде қолданылады. Бірқатар аналитикалық есептерге сәйкес, дауыстық биометрия технологиялары нарықтың шамамен 10-15% құрайды. Саусақ ізі мен бетті тану қолжетімділіктің, ыңғайлылықтың және жеткілікті дәлдіктің үйлесімі арқасында ең танымал шешім болып қала береді. Алайда, қауіпсіздік талаптары мен идентификаторлардың бірегейлігі иристі тану немесе дауыстық биометрия сияқты технологияларға деген қызығушылықты арттырады. Биометриялық технологияның соңғы пайда болған түрі ол мутьтимодальды биометриялық жүйе. Бұл тәсіл технологияларды сыртқа шабуылдардан және деректердің ұрлануынан қорғайтын сенімді жүйе ретінде ұсынылды.

Мультимодальды биометриялық жүйелер жеке тұлғаны анықтау немесе аутентификациялау үшін бір уақытта екі немесе одан да көп биометриялық сипаттамаларды қолданатын шешімдер болып табылады. Бір модальды жүйелерден айырмашылығы мультимодальды жүйелер әртүрлі ақпарат көздерін біріктіруге мүмкіндік береді. Бір модальды жүйе деп жоғарғыда айтылған саусақ ізі немесе бетті тану сияқты тек бір технологияны қолдануды айтсақ. Ал мультимодальды жүйеде бірден саусақ іздері, бетті тану, ирис, дауысты тану сияқты технологияларды қатар қолдануды айтамыз. Бұл тәсіл сәйкестендіру дәлдігінің жоғарылауы, жалғандыққа төзімділігін, икемділік пен ыңғайлылық және қауіпсіздіктің сенімділігін арттырады.

Қазақстанда биометриялық технологияларды қолданудың негізгі бағыттарының бірі азаматтарды сәйкестендіру жүйесін жаңғырту болып табылады. Азаматтардың биометриялық төлқұжаттары мен жеке куәліктерін халықаралық қауіпсіздік стандарттарына сәйкес келетін биометриялық паспорттарға көшіруді бастады. Биометриялық паспорт-мемлекеттердің

шекараларын кесіп өту және шетелде болу кезінде иесінің жеке басын және азаматтығын куәландыратын мемлекеттік құжат. Биометриялық төлқұжат әдеттегіден ерекшеленеді, өйткені оған иесінің фотосуреті, сондай-ақ оның деректері бар арнайы чип салынған: тегі, аты, әкесінің аты, туған күні, төлқұжат нөмірі, берілген күні және жарамдылық мерзімі, сондай-ақ иесі туралы кез келген қосымша ақпарат болуы мүмкін. Стандарттар чипте арнайы биометриялық ақпаратты сақтау мүмкіндігін қарастырады, мысалы, ирис немесе саусақ іздері. Биометриялық төлқұжаттың әдеттегіден айырмашылығы-оның иесіне қол жетімді емес ақпараттың болуы және оны қашықтан оқу мүмкіндігі. Биометриялық төлқұжаттар алғаш рет Малайзияда 1998 жылы шығарыла бастады.

Жаңа биометриялық паспорттар Қазақстан азаматтарына 2009 жылдан бастап беріле бастады. 2013 жылдың қаңтар айынан бастап Қазақстан азаматтарына жаппай беріле бастаған паспорттарға "ұлты" деген баған қайтарылды. Үкімет басшысы Кәрім Мәсімов еліміздің Әділет министрлігіне тиісті тапсырма берді. Әділет министрі Зағипа Балиева бұл баған енді "барлық төлқұжаттарда" қамтылатынын растады. Бұл ретте ол Қазақстан Конституциясының азаматтарға ұлттық тиесілі екенін көрсету құқығын беретін ережесіне сілтеме жасады, қазіргі уақытта ұлты иесінің тілегі бойынша ғана көрсетіледі [19]. Қазіргі таңда көптеген мемлекеттерде азаматтар осы биометриялық паспорттарды қолданады. Бұл құжаттарды қолдан жасау мүмкіндігін едәуір қиындатады және ішкі шекараларда да, халықаралық сапарларда да жеке тұлғаны автоматтандырылған тексеруге мүмкіндік береді. Электрондық жеке куәліктер жүйесін әзірлеу мемлекеттік қызметтерді цифрландырудың маңызды элементі болып табылады. Биометриялық деректерді құжаттарға біріктіру азаматтарға интернет-порталдар арқылы қызметтерге қол жеткізуге мүмкіндік береді, сондай ақ бұл қауіпсіздік деңгейін арттырады және мемлекеттік мекемелердегі кезектерді азайтады. Азаматтар өздеріне қажетті құжаттар мен қызметтерді алу үшін тіпті мемлекеттік органға бармай ақ қашықтықтан өзіне қажетті қызмет түрін ала алады. Бұл ең алдымен халыққа ең тиімді әрі қолайлы жүйе болды. Қазақстан Республикасының электрондық үкіметі (портал egov.kz) өтініш беруден бастап мемлекеттік алымдарды төлеуге дейінгі қызметтердің кең спектрін ұсынады, бұл ретте пайдаланушылардың аутентификациясы биометрия көмегімен жүзеге асырылады. Қазақстан Республикасында электрондық үкіметті «қалыптастырудың 2005-2007 жылдарға арналған мемлекеттік бағдарламасы туралы» Қазақстан Республикасы Президентінің 2004 жылғы 10 қарашадағы №1471 Жарлығында «электрондық үкімет» порталын құру туралы тапсырма береді. Бұл жобаны іске асыру үшін «Ұлттық ақпараттық технологиялар» АҚ «электрондық үкімет» порталын басқаруға және сүйемелдеуге тікелей қатысады. «Электрондық үкімет» порталы 2006 жылдан бастап жұмыс істейді. Электрондық үкімет-бұл мемлекет пен азаматтардың, сондай-ақ мемлекеттік органдардың бір-бірімен өзара іс-қимылының ақпараттық технологиялардың көмегімен олардың келісімділігін қамтамасыз ететін бірыңғай тетігі [25]. Қазіргі таңда электрондық үкімет барлық

мемлекеттік секторларда қолданыста және ол жақтан алынатын барлық құжаттар заңды болып есептеледі.

Биометриялық технологиялар шекаралық бақылауды ұйымдастыру үшін белсенді қолданады. 2024 жылдан бастап Қазақстан азаматтарының жеке куәліктері мен паспорттарына дактилоскопиялық ақпараты бар микросхема (чип) енгізіле бастады. Бұл тек Қазақстан азаматтарына ғана емес, шетелдіктерге, сондай-ақ азаматтығы жоқ адамдарға да қатысты. Ол шет елдерде шекара бекеттерінен өту кезінде биометриялық деректерді беру міндетті болып табылады. Мысалы, Еуропалық Одақ елдерінде 2024 жылдың соңында Шенген аймағының 29 еліне қатысты Entry/Exit system (EES) жұмыс істей бастайды. Алғаш кірген кезде туристерден саусақ іздерін тапсырып, суретке түсіру сұралады. Бұл деректер базада сақталады және қайта шекарадан өту кезінде адамды тез анықтауға мүмкіндік береді дейді. Ал АҚШ- тың әуежайларында барлық келушілер үшін тұлғаны тану технологиясы қолданылады. Сондай-ақ, виза алу немесе визасыз кіру бағдарламасына (ESTA) қатысу үшін саусақ іздерін тапсыру қажет. АҚШ бұл тексерісті терроризмнен қорғаумен байланыстырады, бірақ құқық қорғаушылар биометрияны азаматтарды бақылау сияқты басқа мақсаттарда қолдануы мүмкін деп болжайды. Биометриялық технологияларды қолдану кезінде дербес деректерді қорғау және этикалық нормаларды сақтау сияқты тәуекелдердің көптігіне қарамастан, «Цифрлық Қазақстан» бағдарламасы шеңберінде биометриялық жүйелерді одан әрі дамыту мемлекеттік ресурстарды тиімді басқару және азаматтар үшін заманауи, қорғалған және ыңғайлы сервис құру үшін мемлекет тарапынан кең перспективалар жасалуда.

Қазақстанда медициналық қызметтердің ашықтығын арттыру және бұрмалануын болдырмау мақсатында Денсаулық сақтау саласында биометриялық технологиялар белсенді енгізілуде. Денсаулық саласында ем алушылардың дербес деректері мен биометриялық деректері кеңінен ашық түрде қолданылады. «Атамекен» ҚР ҰКП алаңында медициналық мекемелерде ем алушыларды биометриялық сәйкестендіруді енгізу презентациясы талқыланды. 2024 жылдың қазан айынан бастап Астанада пациенттерді биометриялық сәйкестендіру бойынша «тіркеулер» деп аталатын пилоттық жоба басталды [27]. Пилоттық жобаның негізгі мақсаты- биометриялық сәйкестендіру ем алушының жеке басын дәл растауды және жүйеге енгізілетін деректермен сәйкестендіруді қамтамасыз етуі керек. Бұл бұрын пациенттің қатысуынсыз жасалуы мүмкін медициналық қызметтер мен «тіркемелерді» бұрмалау мүмкіндігін жояды.
Пилоттық жоба пациенттерді анықтаудың екі негізгі әдісін қолданады:

1. Face ID: медицина қызметкері пациенттің суретін түсіреді, содан кейін ол мемлекеттік дерекқормен тексеріледі.
2. Сандық құжат: Пациент EGOV қосымшасында немесе банктік қосымшаларда алты таңбалы кодты жасайды, ол сәйкестендіру үшін денсаулық сақтау маманына беріледі. Пилоттық жоба іске қосылған соң алғашқы екі аптасында қабылдаулардың шамамен 46% Face ID арқылы, 48% цифрлық құжаттар арқылы, ал 6% ғана сәйкестендірусіз мекемелерден өткен [27]. Осылайша, Қазақстанның денсаулық сақтау саласында биометриялық

технологияларды қолдану медициналық қызмет көрсетудің ашықтығы мен тиімділігін арттыруға, сондай-ақ қаржылық бұзушылықтардың алдын алуға бағытталған.

Қазақстандағы қарқынды дамып келе жатқан бағыттардың бірі қаржы секторында биометриялық технологияларды қолдану болып табылады. Онлайн-банк және мобильді қосымшалардағы биометриялық жүйе клиенттерді сәйкестендіру процесін жеңілдетуге және операциялық шығындарды азайтуға көмектеседі. Клиенттер мобильді қосымшалар мен жеке кабинеттерге саусақ іздері немесе бетті тану арқылы кіре алады. Бұл авторизация процесін жылдамдатып қана қоймайды, сонымен қатар дәстүрлі парольдерді қолданумен байланысты алаяқтық әрекеттер қаупін айтарлықтай азайтады. Мысалы, елдегі ең ірі банктердің бірі Kaspi Bank мобильді қосымшасы өз клиенттеріне бет пен саусақ іздерін тану арқылы авторизациялау мүмкіндігін ұсынады. Мұндай функционалдылық операцияларды орындау кезінде қорғаудың жоғары деңгейін қамтамасыз етеді және алаяқтық жағдайларының санын азайтуға мүмкіндік береді. Сондай-ақ, транзакцияларды растау және тұтынушыларды анықтау үшін биометриялық технологияларды енгізу қарапайым аутентификациядан асып түседі. Банктер "Know Your Customer" (KYC) жүйелерін біріктіреді, мұнда биометриялық деректер келісімшарттар жасасу, ақша аударымдарын жүргізу және шоттарды төлеу кезінде клиенттің жеке басын жедел растау үшін пайдаланылады. Қазақстан Республикасы Ұлттық Банкінің деректері бойынша сәйкестендіру процестерінде биометрияны пайдалану алаяқтық деңгейін төмендетуге және клиенттер тарапынан банкке деген сенімді арттыруға ықпал етеді. Десе де, банктерде кибер шабуылдар басқа салаларға қарағанда өте көп орын алатынын және алаяқтық іс әрекеттердің кеңінен жүзеге асырылатынын ескерген жөн. Биометриялық технологиялар денсаулық сақтау мен қаржы секторында ғана емес, сонымен қатар білім беру мекемелері мен бөлшек сауда және қызмет көрсету саласында да қолданыста. Білім беру процестерін басқарудың тиімділігін арттыру үшін кейбір мектептер мен жоғары оқу орындары биометриялық сәйкестендіру жүйелерін енгізген.

Балалар биометриясын балабақшалар мен мектепке енгізу бойынша оқу-ағарту министрлігінің өкілі Манара Адамова: «мектепке дейінгі білім деңгейіндегі биометрия міндетті емес, ұйымдарда биометрияны немесе Face-ID технологиясын енгізу бойынша талаптар жоқ сияқты. Оны тек табельдеу үшін қолдануға болады. Бірақ табельдеуді басқа да жолдармен жасауға болады. QR бар, id карталары бар, басқа да көптеген жолы бар», — деп қосты Адамова. Сондай-ақ Қазақстанның кейбір өңірлерінде Face-ID пилоттық режимде енгізілгенін мәлімдеді. Оның пікірінше, бұл рәсім ереже бұзушылықтармен жүргізілген. Мәселен мұғалімдердің телефондарына ақпараттық жүйе қосымшасын орнатып, балалар биометриясы бойынша сынақ жүргізген, бұл анық заң бұзушылық мұғалім балаларды суретке түсіріп, жалпы жүйеге деректерді жібере алмайды. Тәжірибе жүргізілсе де, электронды есеп беру жүйесі енгізілсе де, ең алдымен ата-ананың келісімі қажет”, — деді Манара Адамова.

Қазақстандағы балалар биометриялық деректерін құқықтық тұрғыдан

қорғау - бүгінгі цифрлық дәуірде аса өзекті мәселе. Қазіргі заңнамада балалардың дербес деректері туралы арнайы норма жоқ, ал биометриялық деректер - жоғары қауіп төндіретін дерек түрі болып саналады. Осыған орай төменде заңнамалық тұрғыдан нақты әрі ғылыми негізделген ұсыныстар бар. Заңға жаңа бап немесе жеке тармақ енгізу онда: 14 жасқа дейінгі балалардың биометриялық деректерін өңдеу - тек заңды өкілдерінің жазбаша келісімімен, нақты көрсетілген мақсат пен мерзіммен жүзеге асырылады. Бұл келісім кез келген уақытта кері қайтарылуы мүмкін. Мемлекеттік органдар немесе жеке компаниялар балалардың биометриялық деректерін өңдеген жағдайда міндетті дербес деректерді қорғау жөніндегі ереже мен қамтамасыз ету тетіктері болуы тиіс. Баланың құқықтары мен мүдделеріне қауіп төндіретін кез келген биометриялық өңдеу - тыйым салынған. Оқу ұйымдары балалардың биометриялық деректерін (бет-әлпетті тану, саусақ іздері, т.б.) тек ата-анасының (заңды өкілінің) жазбаша келісімімен ғана жинауға құқылы және оларды үшінші тұлғаларға беруге қатаң тыйым салынады. ӘҚБтК және Қылмыстық кодекске толықтырулар енгізу қажет. ӘҚБтК (79-бап) – жаңа бөлік: «Кәмелетке толмағандардың биометриялық деректерін заңсыз жинау, сақтау немесе тарату - ауырлататын мән-жай ретінде бағаланып, жоғары мөлшерде айыппұл салуға негіз болады. Қылмыстық кодекс (147-бап) «Егер заңсыз биометриялық дерек жинау кәмелетке толмағандарға қатысты жасалса - жеке жауапкершілік қарастырылады, оның ішінде бас бостандығын шектеу жазасын қосу» сынды нормалармен толықтыру. Халықаралық тәжірбиеде GDPR (ЕО Регламенті), 8-бап: 16 жасқа дейінгі балалардың деректерін өңдеу үшін ата-ананың келісімі міндетті болып табылады. UNICEF нұсқаулары (2021): балалардың биометриялық деректерін жинау - тек шектеулі, нақты қажеттілік болған жағдайда рұқсат етіледі.

Биометриялық технологиялардың әр қызмет салаларда қолданылып жатқанын және даму тенденцияларын, болашақта жүзеге асырылатын перспективаларын зерттеп қарадық. Алайда, оларды енгізу жеке деректерді қорғауға, техникалық шектеулерге және құқықтық аспектілерге байланысты бірқатар тәуекелдермен бірге жүреді. Енді осы жүйелер мен қызметтерді іске асыру кезінде туындайтын бірнеше тәуекелдерге тоқталсақ.

Біріншіден, биометриялық ақпарат сезімталдықтың жоғары деңгейіне ие, өйткені ол әр адам үшін ерекше және тұрақты жасалады. Биометриялық мәліметтер базасы бұзылған жағдайда, бастапқы параметрлерді қалпына келтіру мүмкін емес, бұл ағып кетудің салдарын ерекше ауыр етеді және қайта қалпына келтіру ұзақ уақытты талап етеді. Екіншіден, деректерді тану кезінде техникалық қателер орын алуы. Бұл бетті тану кезінде жарықтың түсуі немесе физикалық өзгерістер (мысалы, терінің зақымдануы) тану сапасына теріс әсер етуі мүмкін. Үшіншіден, кейбір зерттеулер бетті және басқа биометриялық деректерді тану алгоритмдері әртүрлі этникалық топтардың немесе жас санаттарының өкілдерімен жұмыс істеу кезінде қателерді көрсетуі мүмкін екенін көрсетеді. Қазақстан көпұлтты мемлекет болғандықтан кемсітушілік қателіктер азаматтардың белгілі бір топтары үшін мемлекеттік және коммерциялық қызметтерге қолжетімділікке теріс әсер етуі мүмкін. Егер сәйкестендіруде

қайталанатын қателіктер болса, мемлекеттік құрылымдар мен коммерциялық қызметтерге деген сенім төмендеуі мүмкін. Ауқымды тәуекелдердің бірі Қазақстандағы дербес деректерді қорғау және биометриялық ақпаратты пайдалануды реттеу саласындағы заңнаманың әлсіздігі мен жеткіліксіздігі. Қолданыстағы заңдарда биометриялық өңдеудің барлық ерекшеліктерін ескермеген, сондай ақ деректер ағып кеткен немесе дұрыс пайдаланылмаған жағдайда, кімнің жауапты екендігін анықтау қиын. Жауапкершілікке тарту жөніндегі санкциялар әлсіз. Биометриялық жүйелер қауіпсіздікті арттыру үшін ғана емес, сонымен қатар азаматтарды жаппай бақылауды жүзеге асыру үшін де қолданылуы бәріне аян. Деректерді ашық реттеу болмаған жағдайда азаматтардың жеке бас бостандығын шектейтін жаппай бақылау тетіктерін құру қаупі бар. Мемлекеттік билік немесе жеке ұйымдар биометриялық ақпаратты саяси немесе коммерциялық мақсатта қолдана алады, бұл құпиялылық принциптерін бұзады және азаматтардың бостандығына қол сұғу болып табылады. Ашық дереккөздерден қарасақ Қазақстанда дербес деректердің кейбір шетелдік компаниялардағы ағып кетулермен салыстыруға келетіндей ауқымды ағындары тіркелмеген. Дегенмен, деректерді қорғау мәселелері мен ақпаратқа рұқсатсыз қол жеткізу тәуекелдері туралы бұқаралық ақпарат құралдарында жиі көтеріліп, сарапшылардың талқылауында жүр. Мәжіліс депутаты Екатерина Смышляева азаматтардың биометриялық деректерін жинау және сақтау заң нормаларын бұза отырып жүргізілетінін атап өтті. «Биометриялық деректердің ағуы адамның цифрлық тұлғасына тұрақты зақым келтіруі мүмкін. Бұл өткен жылы дактилоскопиялық ақпаратты міндетті түрде жинау туралы Заңның нормасын депутаттардың алып тастауын түсіндірді. Биометрияны жасанды интеллект арқылы алаяқтар пайдаланады, дәл осы деректер банк жүйелерін алдау үшін де қолданылады», – деді Смышляева.[28]

ОЦИБ PS CLOUD SERVICES басшысы Александр Пушкиннің айтуынша, биометриялық деректерді жинау, сақтау және пайдалану процесінің барлық қатысушыларын мемлекеттік деңгейде анықтау маңызды. «Біз бұл мәселеге стратегиялық тұрғыдан қарауымыз керек және мемлекет деңгейінде анықтауымыз керек: бұл деректерді кім сақтайды, кім қорғайды, осы деректердің операторы кім болады. Яғни, мысалы, бұл деректерді мемлекет сақтай алады, бірақ бұл деректердің операторы қаржы ұйымдары, банктер, медициналық мекемелер және жеке бизнес иелері бола алады. Ал биометриялық мәліметтер базасын пайдаланушылар қарапайым азаматтар. Бұл процеске кем дегенде үш тарап қатысуы керек. Бұл жерде жауапкершілік аймағын анықтау өте маңызды», – дейді [29]. Сарапшылар мұндай оқиғалар туралы қоғамды хабардар ету үшін міндетті талаптардың болмауына байланысты ағып кету жағдайлары туралы егжей-тегжейлі ақпарат жиі қол жетімді емес екенін атап өтті. Сондықтан да Қазақстан Республикасында дербес деректер мен биометриялық технологияларды пайдалануды реттейтін құқықтық нормаларды жаңарту қажет.

2 Қазақстан Республикасында биометриялық технологияларды пайдалануды регламенттеудің құқықтық- нормативтік негіздері

2.1 Биометриялық деректерді жинау, сақтау, өңдеу және қауіпсіздікті қамтамасыз етудің заңнамалық негіздері

Қазіргі таңда адамдар әртүрлі қызмет салаларында, әлеуметтік желілерде, қоғамда биометриялық деректерге негізделіп жасалған мобильді құрылғыларды соның ішінде биометриялық технологияларды жиі пайдаланады. Биометриялық дербес деректер дегеніміз -жеке тұлғаны анықтау немесе растау үшін қолданылатын адамның бірегей физиологиялық және биологиялық сипаттамалары. Олар қазіргі заманғы қауіпсіздік жүйелерінің ажырамас бөлігі болып табылады, өйткені олар дәлдік пен сенімділіктің жоғары деңгейін қамтамасыз етеді. Биометриялық деректерді пайдалану арқылы адамның толық сұлбасын құрастыра алады, сонымен қатар оның өміріне тікелей қатысты ақпараттарға қол жеткізе алады. Қазақстан Республикасының "Дербес деректер және оларды қорғау туралы" Заңында «биометриялық деректер - дербес деректер субъектісінің физиологиялық және биологиялық ерекшеліктерін сипаттайтын дербес деректер, олардың негізінде осы субъектінің жеке басын анықтауға болады» - деп анықтама береді [30]. Ал халықаралық ISO/IEC 2382-37 стандартта «биометриялық деректерді жеке тұлғаның аутентификациясы үшін қолданылатын биологиялық сипаттамалардан алынған ақпарат» ретінде анықтайды. Бұл биометрияны сәйкестендіру жүйелерін құрудың негізгі элементіне айналдырады [31]. ISO. Биометриялық деректер өте көп қолданыста пайдаланып жатса да, оларды реттейтін және қорғайтын арнайы нормалар қарастырылмаған. Ал GDPR регламентінің 4-бабында (14-тармақ) «биометриялық деректер - жеке тұлғаның физикалық, физиологиялық немесе мінез-құлық сипаттамаларына қатысты арнайы техникалық өңдеуден алынған жеке деректерді білдіреді, бұл жеке тұлғаның бірегей сәйкестенуіне мүмкіндік береді немесе растайды, мысалы: бет суреттері немесе саусақ іздері» - деп анықтама береді [11]. Сонымен қатар, GDPR кіріспесінде фотосуреттерді өңдеу әрқашан жеке деректердің арнайы санаттарын өңдеу болып саналмайтындығы көрсетілген. Фотосуреттер жеке тұлғаны бірегей сәйкестендіруге немесе аутентификациялауға мүмкіндік беретін арнайы техникалық құралдарды пайдалана отырып өңделетін жағдайларда ғана биометриялық деректердің анықтамасына жатады деп жазылған. Басқа заң актілеріне қарағанда GDPR регламентінде биометриялық деректерге арнайы мән берген. Деректерді қорғаудың жалпы регламентіне (GDPR) сәйкес, биометриялық деректер белгілі бір жағдайларды қоспағанда, өңдеуге тыйым салынған жеке деректердің арнайы санаттарына жатады. Бұл туралы GDPR 9-бабында былай дейді: «жеке тұлғаны, жеке тұлғаның денсаулығына, жыныстық өміріне немесе жыныстық бағдарына қатысты деректерді бір мәнді сәйкестендіру мақсатында нәсілдік немесе этникалық шығу тегін, саяси көзқарастарын, діни немесе философиялық нанымдарын, кәсіптік одаққа мүшелігін ашатын дербес деректерді өңдеуге, сондай-ақ генетикалық деректерді, биометриялық деректерді өңдеуге тыйым

салынады»[11]. Регламент халықаралық заңды акті болып табылатындықтан, тұлғаларға қатысты тікелей жеке деректерге осы тұрғыдан қатаң бақылау орнатқан. Дегенмен, GDPR биометриялық деректерді өңдеуге рұқсат етілген ерекшеліктерді де қарастырады.

Мұндай ерекшеліктерге мыналар жатады:

- Деректер субъектісінің бір немесе бірнеше нақты мақсаттар үшін оның биометриялық деректерін өңдеуге нақты келісімін алу.
- Еңбек заңнамасы, әлеуметтік қамсыздандыру және әлеуметтік қорғау туралы заңнама саласындағы бақылаушының немесе деректер субъектісінің міндеттемелерін орындау және арнайы құқықтарын жүзеге асыру үшін өңдеу қажеттілігі.
- Егер деректер субъектісі физикалық немесе заңды түрде келісім бере алмаса, деректер субъектісінің немесе басқа жеке тұлғаның өмірлік мүдделерін қорғау.
- Қордың, қауымдастықтың немесе басқа коммерциялық емес органның саяси, философиялық, діни немесе кәсіподақ мақсатындағы тиісті кепілдіктерімен заңды қызмет шеңберінде өңдеу, егер өңдеу тек осындай органның мүшелеріне немесе бұрынғы мүшелеріне немесе оның мақсаттарына байланысты онымен үнемі байланыста болатын адамдарға қатысты болса және дербес деректер болмаса деректер субъектілерінің келісімінсіз осы органның шегінен тыс жерде ашылады.
- Деректер субъектісінің өзі анық жариялаған дербес деректерге қатысты өңдеу.
- Құқықтық талаптарды белгілеу, жүзеге асыру немесе қорғау үшін немесе соттардың сот төрелігін жүзеге асыруы кезінде өңдеу қажеттілігі.
- Профилактика немесе еңбек медицинасы, қызметкердің еңбекке қабілеттілігін бағалау, медициналық диагностика, денсаулық сақтау немесе әлеуметтік қамсыздандыру жүйелері сияқты медициналық мақсаттар негізінде немесе медициналық қызметкермен келісім бойынша.
- Денсаулыққа елеулі трансшекаралық қауіп-қатерлерден қорғау немесе денсаулық сақтау мен медициналық өнімдердің немесе медициналық өнімдердің жоғары сапасы мен қауіпсіздік стандарттарын қамтамасыз ету сияқты қоғамдық денсаулық сақтау мүдделері.

Қоғамдық мүддедегі мұрағаттық мақсаттар, сондай-ақ GDPR 89(1) - бабына сәйкес ғылыми немесе тарихи зерттеу мақсаттары немесе статистикалық мақсаттар үшін қолданылады. Осылайша, GDPR биометриялық деректерді ерекше сезімтал деп таниды және деректер субъектілерінің құқықтары мен бостандықтарын қорғауды қамтамасыз ете отырып, оларды өңдеудің қатаң шарттарын белгілейді.

Заңда дербес деректерді мемлекеттік органдар, заңды және жеке тұлғалар жүзеге асыратын дербес деректерді өңдеуге байланысты қызметтің мақсаттарын, міндеттерін, қағидаттары мен құқықтық негіздерін ғана айқындайды. Ал дербес деректердің өзі өте ауқымды зерттелетін объект және оның өзі бірнеше түрлерге бөлінеді. Соның ішінде биометриялық деректердің

өзі жеке зерттеуді қажет етеді. Деректерді дұрыс емес және заңсыз пайдаланудың өзі қаншама құқықтық салдарға әкеп соғады.

Қазақстанда биометриялық деректерді пайдалану оларды жинау, өңдеу және сақтаудың құқықтық негіздерін, сондай-ақ қорғау шараларын белгілейтін нормалар бірқатар заңнамалық актілермен реттелген. Бұл құқықтық тетік инновациялық технологияларды пайдалану мен азаматтардың құқықтарын қорғау арасындағы тепе-теңдікті қамтамасыз етуге бағытталған. Қазақстанның биометриялық деректері туралы негізгі заңнамалық акті ол «Дербес деректер және оларды қорғау туралы» заң. Бұл заң жеке деректермен қатар, соның ішінде биометриялық мәліметтермен жұмыс істеуді реттейтін негізгі ереже болып табылады.

Дербес деректерді жинау, өңдеу, қорғау ол заңда көрсетілген негізгі қағидаттарға сәйкес жүзеге асырылады. Заңның 6- бабында «дербес деректер қол жетімділігі бойынша жалпыға бірдей қолжетімді және қол жетімділігі шектеулі болып бөлінеді» - деп көрсетілген [30]. Биометриялық деректер қай түріне жататыны белгісіз, десе де олар қол жетімділігі шектеулі деректер болып қорғалу керек. Себебі, биометриялық дерек арқылы адамның жеке басын анықтауға және жасанды интеллект көмегімен оның сұлбасын жасауға болады. Бұл дегеніміз бір адамның екінші көшірмесін жасап өзінің бас пайдасына пайдалануына әкеп соғуы мүмкін. Сонымен қатар, заңның 11- бабында дербес деректердің құпиялығы жайлы қол жетімділігі шектеулі дербес деректерге қол жеткізе алатын меншік иелері және (немесе) операторлар, сондай-ақ үшінші тұлғалар субъекті оларды таратуға жол бермеу талаптарын сақтау арқылы олардың құпиялылығын қамтамасыз етеді делінген. Дәл осы баптың үшінші тармағында биометриялық деректердің құпиялығы Қазақстан Республикасының заңнамасында белгіленеді деп көрсетілген, бірақ нақты қай заңнамада екені жазылмаған. Заңның 25-бабында биометриялық деректерді қоса алғанда, дербес деректерді жинаудың, сақтаудың және өңдеудің құқықтық негіздерін айқындайды. Жалпы деректер ол тікелей субъектінің немесе оның заңды өкілінің келісімімен ғана жинауға, сақтауға, өңдеуге және басқа да әрекеттер жасауға рұқсат етіледі. Деректермен жұмыс жасайтын операторлар және үшінші тұлғалар деректер құпиялығы қағидатын ұстана отырып мемлекет бекіткен ережелерге сай ғана жұмыс жасайды. Биометриялық деректерді жинау, сақтау, өңдеу осы заң аясында іске асырылады. Биометриялық деректерді жинау және өңдеу заңнамада көзделген жағдайларды қоспағанда, деректер субъектісінің жазбаша келісімі негізінде жүзеге асырылады. Субъект өзінің келісімін қайтарып алуға, сондай-ақ өзінің биометриялық деректерін жоюды талап етуге құқылы.

Қазақстан Республикасы цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2020 жылғы 27 қазандағы № 406/НҚ бұйрығымен «Мемлекеттік қызметтер көрсету кезінде жеке тұлғалардың биометриялық аутентификациясы үшін биометриялық деректерді жинау, өңдеу және сақтау қағидалары» бекітілді [34]. Осы Ережелерге сәйкес:

- Биометриялық деректерді жинау 18 жасқа толған жеке тұлғаларда ерікті негізде және олардың жазбаша келісімі болған кезде жүзеге асырылады.

•Деректерді жинамас бұрын жеке басын куәландыратын құжаттар бойынша жеке басын сәйкестендіру жүргізіледі.

•Деректерді жинау екі қолдың саусақ іздерін сканерлеу арқылы бояусыз әдіспен жүзеге асырылады.

•Биометриялық деректер ақпаратты криптографиялық қорғау құралдарын пайдалана отырып, дерекқорда сақталады.

•Субъект өзінің биометриялық деректерін жою туралы өтінішпен жүгінген кезде олар дерекқордан жойылуға жатады.

Жиналған биометриялық деректердің қауіпсіздігін қамтамасыз ету мақсатында деректерді базада сақтау мерзімдері бойынша негізгі ережелер бар. Мақсатты сақтау ол биометриялық деректер олар жиналған мақсаттарды іске асыру үшін қажетті кезең ішінде ғана сақталуы керек (мысалы қандай да бір мемлекеттік қызмет көрсету кезінде жеке тұлғаны аутентификациялау үшін). Биометриялық деректерге заңда жазылған арнайы сақтау мерзімі көрсетілмеген, яғни тек қолданыс кезінде ғана ол жүзеге асырылуы қажет. Барлық ақпарат рұқсатсыз кіруді болдырмау үшін қатаң қауіпсіздік шараларын, соның ішінде криптографиялық қорғауды қолдану арқылы өңделуі керек. Бұл талаптар заңнамада бекітілген.

Қазақстан Республикасында биометриялық деректерді жинау, сақтау және өңдеу бірнеше мемлекеттік органдар мен ұйымдармен реттеледі, олардың әрқайсысы осы салада белгілі бір функцияларды орындайды. Бірінші мемлекеттік жоғарғы тұрған орган Қазақстан Республикасының цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі. Бұл мемлекеттік орган цифрлық технологиялар, инновациялар және ақпараттық қауіпсіздік саласындағы мемлекеттік саясатты әзірлейді. Биометриялық деректерді қоса алғанда, дербес деректерді жинау, сақтау және өңдеу мәселелерін реттейтін нормативтік-құқықтық актілерді және ережелерді дайындайды. Сонымен қатар, ақпаратты кешенді қорғауды қамтамасыз ету үшін басқа мемлекеттік органдар мен жеке ұйымдармен жұмыс жасайды. Екінші орында «Азаматтарға арналған үкімет» мемлекеттік корпорациясы, бұл коммерциялық емес акционерлік қоғам. Азаматтарға арналған үкімет өз кезегінде мемлекеттік қызметтерге биометриялық жүйелерді енгізу бойынша жобаларды практикалық іске асыруды жүзеге асырады. Пилоттық жобаларды жүзеге асырады. Сәйкестендіру және аутентификация мақсатында азаматтардың биометриялық деректерін жинауды, өңдеуді және сақтауды ұйымдастырады. Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі әзірлейтін бекітілген нормативтік құжаттар шеңберінде жұмыс істейді. «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының Заңына сәйкес елімізде арнайы уәкілетті орган жұмыс істейді. Орган жалпы дербес деректерді, оның ішінде биометриялық деректерді өңдеуді бақылайды және қадағалайды. Азаматтардың жеке ақпаратты қорғау құқықтарының сақталуын қамтамасыз етеді. Жеке деректерді өңдеу саласындағы бұзушылықтарды анықтау кезінде тексерулерге бастамашылық жасайды және шаралар қабылдайды. Қазақстанда биометриялық деректерді жинау, сақтау және өңдеу жөніндегі функциялар цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі, "Азаматтарға арналған үкімет"

мемлекеттік корпорациясы және дербес деректерді қорғау саласындағы уәкілетті орган арасында бөлінген. Осы органдардың әрқайсысы азаматтардың биометриялық деректерімен тиімді және қауіпсіз жұмыс істеуін қамтамасыз етуде өз рөлін атқарады.

Қазақстанда биометриялық деректерді жинау және өңдеу кезінде олардың қауіпсіздігін, тұтастығын және құпиялылығын қамтамасыз етуге бағытталған кешенді техникалық шаралар қолданылады. Бірінші деректерді шифрлау биометриялық ақпарат тасымалдау кезінде де, сақтау кезінде де деректер арнайы алгоритммен шифрланады. Деректерді ұстап қалудан және рұқсатсыз кіруден қорғау үшін заманауи криптографиялық алгоритмдер (мысалы, AES, RSA) және протоколдар (SSL/TLS) қолданылады. Екінші желілік инфрақұрылымды қорғау, жіберілетін деректерді қорғау үшін брандмауэрлер (firewalls), кіруді анықтау және алдын алу жүйелері (IDS/IPS) және виртуалды жеке желілер (VPN) қолданылады. Бұл шаралар күдікті әрекеттерді бақылауға және деректерге рұқсатсыз қол жеткізу әрекеттерін блоктауға мүмкіндік береді. Биометриялық деректер сақталатын деректер орталықтары мен серверлік үй-жайлар бейнебақылау, қол жеткізуді бақылау, дабыл беру жүйелерімен және басқа да қорғау құралдарымен жабдықталған. Нысандарды физикалық қорғау жабдыққа рұқсатсыз кіру қаупін азайтады. Мемлекеттік бақылаушы органдар деректер базасындағы жүйелерді үнемі жаңартып және тексеріп отыру қажет. Қауіпсіздік аудиттері, ену тестілері және инфрақұрылымның қауіпсіздігін бағалау жүргізіледі, бұл ықтимал қауіптерге жедел ден қоюға мүмкіндік береді. Деректердің сақтық көшірмесін жасау және қалпына келтіру. Биометриялық деректер шифрланған арналар арқылы үнемі сақталады және қорғалған қоймаларда сақталады. Сақтық көшірмелердің болуы оқиғалар немесе ақаулар болған жағдайда деректерді жылдам қалпына келтіруге мүмкіндік береді. Бұл техникалық шаралар Қазақстан Республикасы заңнамасының, атап айтқанда «Дербес деректер және оларды қорғау туралы» Заңның, сондай-ақ тиісті нормативтік актілердің талаптары шеңберінде іске асырылады. Оларды қолдану биометриялық деректерді қорғаудың жоғары деңгейін қамтамасыз етеді және азаматтардың құқықтары мен құпиялылығын сақтауға ықпал етеді.

Қазақстанда цифрлық технологияларды дамыту және оны қоғамның әртүрлі салаларында оның ішінде мемлекеттік қызмет салаларында пайдалану қарқынды дамып жатыр. Президентіміз Қасым-Жомарт Тоқаев 2023 жылғы 1 қыркүйектегі «Әділетті Қазақстанның экономикалық бағдары» атты Қазақстан халқына Жолдауында Қазақстанды IT-мемлекетке айналдыруды тапсырды [32]. Мемлекеттік органдар бұл бағытта тез жұмыс жасауда және цифрлық технологияларға тез бейімделуде, десе де осы саладағы заңнамалар өзгеріссіз артта қалуда. Оған дәлел биометриялық дерек туралы тек анықтама ғана бар заңда, ал оны қалай жинау, сақтау, өңдеу, пайдалану жөнінде нормалар жекеше қарастырылмаған.

Қазақстан Республикасы 2021 жылы 1 қаңтардан бастап «Дактилоскопиялық және геномдық тіркеу туралы» Заң геномдық тіркеу бөлігінде қолданысқа енгізілді. Дактилоскопиялық тіркеу бөлігіндегі заң нормалары 2024 жылы 1 қаңтардан бастап күшіне енді [33]. Бұл заң 2016 жылы

шыққанымен, ол кезде тек арнайы санаттағы адамдардың ғана саусақ іздерін жинақтайтын. Мемлекеттік дерекқорларда адамдардың дактилоскопиялық және геномдық ақпараттың болуы табиғи апаттар, белгісіз мәйіттер, ашылмаған қылмыстар, жедел іздестіру кезінде адамның жеке басын анықтау және растау кезінде рәсімдерді жеңілдетуге мүмкіндік береді. Дактилоскопиялық және геномдық тіркеу туралы Заңның 6- бабында «дактилоскопиялық және (немесе) геномдық тіркеу саласындағы уәкілетті мемлекеттік органдардың өз құзыреті шегінде дактилоскопиялық ақпаратты жинауға, өңдеуге немесе геномдық ақпаратты жинауға, өңдеуге, қорғауға, биологиялық материалды іріктеуге, сақтауға, пайдалануға және жоюға құқығы бар» делінген [33]. Қазақстан азаматтарынан мемлекеттік базаға енгізу үшін саусақ іздерін жинайды. Жеке тұлғаны анықтау, қылмыспен күресу және ұлттық қауіпсіздікті қамтамасыз ету үшін осы биометриялық деректерді пайдаланады. Азаматтар осы заң нормаларына сәйкес өзінің дактилоскопиялық және (немесе) геномдық ақпаратымен танысуға және ақпаратты алуға, шағым жасауға құқығы бар. Осы заңның 8- бабында дактилоскопиялық және геномдық ақпарат қол жетімділігі шектеулі дербес деректерге жататыны жазылған. Дактилоскопиялық және геномдық ақпаратты жинау және өңдеу оны қорғау заңмен қамтамасыз етілген жағдайларда ғана жүзеге асырылады. Дактилоскопиялық және геномдық ақпаратты қорғау Қазақстан Республикасының ақпараттандыру туралы, дербес деректер және оларды қорғау, мемлекеттік құпиялар туралы заңнамасына сәйкес жүзеге асырылады делінген. Азаматтардың деректері арнайы мемлекеттік дерекқорда тұрады және тек мемлекеттік орган ғана ол деректерді пайдаланып жұмыс жасайды. Бұл деректердің қорғалуына және таралып кетпеуіне тікелей мемлекет кепілдік береді.

Жеке тұлғаның бет бейнесін сканерлеу арқылы қосымшаға кіруге және қызметтер алуға, сонымен қатар камера арқылы электронды қол қоюға болады. Банктерде және микроқаржы ұйымдарда азаматтардың дербес деректерімен қатар биометриялық деректері де бар. Деректер банк базасында жиналады, өңделеді және бөгде шабуылдардан қорғалады. Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасы 2024 жылы 16 тамызда банктердің, банк қызметтерінің жекелеген түрлерін жүзеге асыратын ұйымдардың және микроқаржы ұйымдарының биометриялық сәйкестендіруді жүргізу қағидалары туралы № 56 қаулысын бекітті [35]. Бұл қаулыда қысқаша биометриялық сәйкестендіруді жүргізу тәртібін белгілейді олар: биометриялық деректерді пайдалану және қорғау принциптері; бет бейнесі бойынша биометриялық сәйкестендіру тәртібі; сәйкестендіру деректерін алу және кескіннің дұрыстығын тексеру процедуралары; сәйкестендіру деректерін беру кезінде байланыс арналарын шифрлауды қамтамасыз ету жөніндегі талаптар; биометриялық деректерді жинау, сақтау және жою процестерін құжаттау тәртібі жазылған. Қаулының 2- тарауында идентификаттау өткізілетін адамның бет бейнесі бойынша биометриялық идентификаттау процесін жүргізу және қандай кезеңдерден тұратыны жайлы баяндалған. Әрбір сәтті өткен идентификатталау процесінен кейін тағы да биометриялық деректерді тексеру үшін қаулыға сәйкес электронды құжаттар жасалады. Бұл банк базасындағы

ақпараттардың шынайы және дәлдігі үшін жасалады. Десе де қазіргі таңда азаматтардың артынан алаяқтық жасау арқылы несие рәсімдеу, қаражаттарды ұрлау, басқада банк саласымен қатысты құқықбұзушылықтар өте көп орын алуда. Сондықтан азаматтардың жеке деректерін қорғау банк ұйымдары үшін бірінші орында болуы қажет. Қаулының 1- тарауында «бейнелердің мемлекеттік дерекқоры – жеке тұлғалардың идентификаттау деректерін, сондай-ақ оларға сәйкес келетін адамның эталондық бейнелерін қамтитын мемлекетке тиесілі дерекқор» деп анықтама көрсетілген [35]. Бұл дегеніміз жекеменшік банк және басқа да микроқаржы ұйымдарында жиналған, сақталған, өңделген биометрикалық деректердің барлығы мемлекеттік дерекқорда мемлекеттің қарауында болады деген сөз. Банк тұтынушыларының биометриялық деректерін тарап кетуден қорғайды. Қаулының мақсаты қаржы нарығындағы биометриялық сәйкестендіру процесінің ақпараттық қауіпсіздігін регламенттеу, құжаттау және қамтамасыз ету болып табылады.

Биометриялық деректерді жинау, өңдеу, сақтау жоғарыда жазылған заң нормаларымен реттеледі және қорғалады. Биометриялық деректерді пайдалану жоғарғы қауіпсіздік пен азаматтарға қолдануға ыңғайлы артықшылықтар береді, бірақ ол бірқатар құқықтық тәуекелдерді де қамтиды. Бұл тәуекелдер азаматтардың құқықтарына, деректер қауіпсіздігіне және қоғамдық нормаларға әсер етуі мүмкін, сондықтан оларды анықтау, алдын алу және басқару өте маңызды. Қазақстанда 2024 жылы 5 наурызда мемлекеттік техникалық қызмет ZAIMER.KZ микроқаржы ұйымының клиенттері болып табылатын 2 миллионнан астам Қазақстандықтардың дербес деректерінің таралып кеткенін анықтады. Robo.finance платформасында жұмыс істейтін микроқаржы клиенттерінің 36 миллионнан астам жазбалары анықталды олардың ішінде (РФ - 23,6 млн. (zaimer.ru – 16.8 млн., adengi.ru -6.8 млн.); Филиппин-5 млн. (digido.ph); Вьетнам - 2 млн. (vietloan.vn) деректері де бар [36]. Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі осы жағдайды жедел шешу үшін азаматтарға eGov порталы арқылы қарыз алудан ерікті түрде бас тартуды белгілеуді және егер олар осы ұйымға өз деректерін өңдеуге келісім бермеген жағдайда ақпараттық қауіпсіздік комитетіне жүгінуді ұсынды. Дербес деректердің таралып кетуі сияқты істер жеке компанияларда да және мемлекеттік органдарда да жиі орын алуда, Цифрлық даму министрлігі әрбір жағдайды өздері бақылауына алуда.

Биометриялық технологияларды, әсіресе бейнебақылау және жаппай сәйкестендіру жүйелерінде биометриялық деректерді қолдану азаматтардың жеке өмірге деген құпиялылық құқығының бұзылуына әкеп соғады. Қазіргі кезде бетті тану функциясы бар камералар қоғамдық орындарда, көшелерде, жеке меншік ұйымдарда жаппай қолданыста және бұл халықты заңсыз бақылауға алып келеді. Бұл дегеніміз мемлекеттік сектор немесе жеке компаниялар азаматтардың келісімінсіз биометриялық деректерді жинауда және өңдеуде. Ал деректер туралы заңнамада барлық дербес деректер оның ішінде бетті тану биометриялық дерек, барлығы тек субъектінің жазбаша келісімімен ғана жинап сақталуы қажет. Алайда, биометрияны жаппай қолдану жағдайында мұндай тәуекелдер заңнаманы одан әрі жетілдіруді талап етеді.

Сонымен қатар тағы да бір биометриялық деректерді жинаудағы тәуекел ол теріс мақсатта пайдалану. Мемлекеттер тұлғаны тану жүйелері арқылы сөз бостандығын жаппай бақылау немесе қоғамдық белсенділікті бақылау үшін азаматтардың биометриялық деректерін қолдана алады. Ал жеке компаниялар азаматтардың келісімінсіз маркетинг үшін биометриялық ақпаратты пайдалана алады. Бұл нағыз заң бұзушылық себебі, жеке тұлғаның деректерін басқарып, оны заңсыз пайдалану оның өміріне қауіп төндіруі де мүмкін. Адам құқықтарын қорғау бойынша қоғамдық ұйымдардың назарында жүретін сауалда осы. Ата заңымызда жазылғандай әркімнің жеке басына қолсұғылмауына, өмірінің құпия болуына заңмен кепілдік берілген. Мәселен қоғамдық орындар мен көшелердегі орналасқан «Сергек» бейнебақылау жүйесі. Ол адамдардың бет бейнесін сканерлеп азаматтың жеке басын анықтайды. Бұл жазбалар ішкі істер органдарының бақылауымен қаралады, десе де бейнебақылаудың өзі жеке меншік компанияға тиесілі. Биометриялық деректерді қорғаудағы негізгі заң «Дербес деректер және оларды қорғау туралы» Заңның болуына қарамастан, Қазақстандағы құқықтық нормалар технологияның дамуына әрдайым ілесе бермейді артта қалуда. Биометриялық ақпаратты өңдеуді бақылаудың қатаң тетіктерін заңда көздемейді. Бірыңғай ұлттық сенімді жүйе жоқ. Жоғарыда келтірілген нормативтік актілерде биометриялық деректердің тек саусақ ізі және бет бейнені аутентификациялау бойынша ғана нормалар қарастырылған. Ал басқа деректер туралы заң нормаларында анықтама да атыда келтірілмеген. Сонымен қатар, Қазақстан заңнамасы биометриялық деректердің трансшекаралық берілуін жеткілікті түрде реттемеген, бұл олардың деректерді қорғау деңгейі төмен елдерге беріліп кету қаупін тудырады. Қазақстандықтардың көпшілігі биометриялық деректерге қатысты өз құқықтары туралы білмейді. Бұл өз кезегінде деректердің таралып, сақталмауына тәуекелдерді арттыра түседі.

2.2 Дербес деректер субъектілерінің құқықтары: дербес деректер туралы заңнама және оны биометриялық ақпаратқа қолдану

Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы. «Дербес деректер және оларды қорғау туралы» заңы кез келген басқа заң сияқты, ақпараттарды қамтиды және жеке деректерді қорғау бойынша жұмыстың негізгі бағыттарын жүзеге асырады. Дербес деректер туралы Заңның кіріспесі дербес деректер саласындағы қатынастарды реттейтінін, сондай-ақ дербес деректерді жинауға, өңдеуге, қорғауға байланысты қызметтің мақсаттарын, қағидаттарын, негіздерін көздейді. Дегенмен, «Дербес деректер туралы» Заңда оны қолданудың ҚР аумағына шектелгені нақтыланбайды. Сәйкесінше, «Дербес деректер туралы» Заң шетелдік заңды тұлғаға қатысты да болуы мүмкін, бірақ шетелдік заңды тұлғаға қатысты тиісті санкциялар мен айыппұлдар іс жүзінде қаншалықты қолданылуы мүмкін екенін заң анықтайды. Заңның негізгі мақсаты - адамның және азаматтың дербес деректерін жинау және өңдеу кезінде оның құқықтары мен бостандықтарын қорғауды қамтамасыз ету болып табылады. Заңның 1-бабында «дербес деректер – мәліметтер негізінде айқындалған немесе

айқындалатын дербес деректер субъектісіне қатысты, электрондық, қағаз және (немесе) өзге де материалдық жеткізгіште тіркелген сол мәліметтер» - деп анықтама береді [30]. Дербес деректер - жеке тұлға туралы, оның ішінде аты, жасы, жеке сәйкестендіру нөмірі , телефон нөмірі, жынысы, жұмыс орны және басқа да жеке адамға қатысты ақпаратты қамтитын мәліметтер. Анықтаманың өзінен ақ біз бұл мәліметтердің өте құнды ақпарат екенін және тиісінше қорғалмаса, оның салдары көптеген құқықбұзушылықтарға әкеп соғатынын көріп отырмыз. Бұл заң он екі жылдан бері қолданыста, десе де әлі күнге дейін заң өзгертулер мен толықтырулардан өтуде.

Дербес деректер өздерінің қолжетімділігіне қарай жалпыға бірдей қолжетімді және қолжетімділігі шектеулі болып бөлінеді. Бірақ мәліметтердің нақты қайсы түрі қалай ажыратылатыны заңда жазылмаған. Осы заң аясында дербес деректерімізді жинау – дербес деректерді алуға бағытталған іс әрекеттер, дербес деректерді өңдеу – дербес деректерді жинақтауға, сақтауға, өзгертуге, толықтыруға, пайдалануға, таратуға, иесіздендіруге, бұғаттауға және жоюға бағытталған іс-әрекеттер, дербес деректерді пайдалану – меншік иесінің, оператордың және үшінші тұлғаның қызмет мақсаттарын іске асыруға бағытталған дербес деректермен жасалатын іс-әрекеттер туралы нормаларды бекітеді. Заңның 2- бабында дербес деректерді жинау, өңдеу және қорғаудың негізгі принциптері жайлы жазылған. Дербес деректермен жоғарыда көрсетілген іс- әрекеттерді жүзеге асыру үшін: адам мен азаматтың конституциялық құқықтары мен бостандықтарын сақтауға, заңдылық принципін ұстауға, қол жетімділігі шектеулі дербес деректердің құпиялылығын сақтауға (оның ішінде мемлекеттік құпияға жататын деректер), субъектілердің, меншік иелерінің және операторлардың құқықтарының теңдігі принципі, жеке адамның, қоғамның және мемлекеттің қауіпсіздігін қамтамасыз ету қажет. Бұл орайда мемлекет азаматтардың бостандығы мен жеке өміріне деген қолсұғылмаушылықты бірінші орынға қойып отыр. Сонымен қатар дербес деректерді жинау және өңдеу заңда көзделген жағдайларды қоспағанда, тек қана субъектінің келісімімен жүзеге асырылады. Азаматтың жеке дерегін жинап, өңдеу үшін оның немесе оның заңды өкілінің жазбаша келісімі болуы қажет. Субъект дербес деректерді жинауға және өңдеуге берген өзінің келісімін қайтарып алуға да құқылы. Қазақстан Республикасының Үкіметі, орталық және жергілікті атқарушы органдар дербес деректер саласында реттеу мен бақылауды жүзеге асырады. Уәкілетті орган дербес деректер және оларды қорғау туралы заңнаманың сақталуы мен жүзеге асуына жауапты. Сәйкесінше, дербес деректер туралы заңнамада келтірілген нормаларды бұзғаны үшін Қазақстан Республикасының әкімшілік және қылмыстық заңдарына сәйкес жауаптылыққа тартылады. Ұлттық заңнама мен халықаралық заңдардың дербес деректер мен олардың субьектілерінің құқықтарын қорғау туралы нормаларына салыстырмалы талдау жасайық.

Еуропалық Одақта дербес деректерді қорғаудың біріңғай «Деректерді қорғаудың жалпы регламенті» (ағылш. General Data Protection Regulation, GDPR; 2016/679) атты Қаулысы бар. Қаулы Еуропалық Одақтағы (ЕО) барлық тұлғалардың дербес деректерін қорғауды күшейтеді, реттейді және

трансшекаралық беруді қамтамасыз етеді. Бұл қаулы көптеген елдерде қолданыста әрі халықаралық деректерді реттейтін ең күшті заңнама болып табылады. GDPR, ең алдымен, азаматтарға өздерінің жеке деректерін бақылауға мүмкіндік беруге және ЕО шеңберіндегі реттеуді біріздендіру арқылы халықаралық экономикалық қатынастар үшін нормативтік-құқықтық базаны жеңілдетуге бағытталған.

GDPR регламентінің 4-бабында «Дербес деректер» - белгілі бір немесе анықталған жеке тұлғаға (деректер субъектісіне) қатысты кез келген ақпарат [11]. Жеке тұлға, егер оны тікелей немесе жанама түрде анықтауға болатын болса, атап айтқанда идентификатор арқылы (мысалы: аты, сәйкестендіру нөмірі, орналасқан жері туралы деректер, онлайн идентификатор) немесе оның физикалық, физиологиялық, генетикалық, психикалық, экономикалық, мәдени немесе әлеуметтік сәйкестігіне тән бір немесе бірнеше факторлар бойынша анықталатын мәліметтер дербес деректер болып саналады деп анықтама береді. GDPR регламенті дербес деректердің әрбір түріне жеке тоқталып мән береді, жалпылама ұғым ретінде ғана қарап қоймайды. Бұл оның басқа мемлекеттердің заңдарынан ерекшелендіре түседі. Бұл регламентте де азаматтардың дербес деректерін өңдеу, жинау, сақтау және пайдалану арнайы принциптермен іске асырылады.

GDPR регламентінің 5-бабы кез-келген дербес деректерді өңдеуге сәйкес келетін келесі принциптерді белгілейді:

- Заңдылық, әділдік және ашықтық: деректерді өңдеу барысында субъектілерге өңдеу тәсілдері мен мақсаттары туралы нақты хабардар ете отырып, заңды негіздерде жүзеге асырылуы тиіс.
- Мақсаттарды шектеу: дербес деректер нақты, айқын және заңды мақсаттар үшін жиналады және бұдан әрі осы мақсаттарға сәйкес келмейтін тәсілдермен өңделмейді.
- Деректерді азайту: өңделетін деректер барабар, тиісті және өңдеу мақсаттары үшін қажетті көлеммен шектелуі тиіс.
- Дәлдік: деректер дәл және қажет болған жағдайда өзекті болуы керек. Дәлсіздіктер анықталған кезде деректер субъектісі оларды түзетуге құқылы.
- Сақтауды шектеу: дербес деректер субъектілерін сәйкестендіруге мүмкіндік беретін нысанда өңделу мақсаттарына қол жеткізу талап еткеннен кейін артық сақталмайды.
- Тұтастық және құпиялылық (қауіпсіздік): рұқсатсыз немесе заңсыз кіруден, жоғалудан немесе бүлінуден қорғауды қоса алғанда, деректердің қауіпсіздігін қамтамасыз ету үшін тиісті техникалық және ұйымдастырушылық шаралар қабылдануы керек.

Қаулы осы негізге алған принциптермен жұмыс жасай отырып, дербес деректерді қорғаудың көшбасшы заңнамасы болып отыр.

Дербес деректер субъектісі немесе оның заңды өкілі кез келген уақытта, егер деректерді жинау және (немесе) өңдеу заңнаманы бұза отырып жүзеге асырылса, субъектінің дербес деректерін жалпыға қолжетімді дербес деректер көздерінен алып тастауды талап етуге құқылы. Дербес деректердің иесі яғни

субъект оның заң алдында арнайы өзіне тиесілі құқықтары бар. GDPR жеке тұлғалардың жеке деректеріне қатысты құқықтарын айтарлықтай кеңейтеді. Негізгі құқықтарға мыналар жатады:

•Деректерге қол жеткізу құқығы (15 – бап): деректер субъектісі оның дербес деректері өңделіп жатқандығы туралы растау алуға және оларды өңдеу кезінде – осы деректерге қол жеткізуге құқылы. Бұл жағдайда ұйым жеке тұлға туралы қолда бар жеке деректердің көшірмесін және қосымша ақпаратты беруге міндетті, оның ішінде: өңдеу мақсаты, жеке деректердің қандай категорияда өңделеді; деректер кімге беріледі (үшінші елдер немесе халықаралық ұйымдар), ұйым деректерді қанша уақыт сақтайды (сақтау мерзімі) туралы толық ақпаратты алуға және сұрауға құқығы бар.

•Түзету құқығы (16-бап): Субъект дұрыс емес немесе толық емес деректерді түзетуді талап етуі мүмкін. Түзету құқығы жеке тұлғаларға ұйымнан олар туралы кез келген дұрыс емес немесе толық емес деректерді жаңартуды сұрауға мүмкіндік береді. Егер ұйым деректердің дұрыс еместігін растаса, сұрауға жауап берудің заңды мерзімі-бір ай. Сұраныс бойынша ұйым деректердің шынымен дұрыс емес екеніне көз жеткізіп, оларды түзетуі керек. Бұл құқық ұйымдар үшін жаңа операциялық проблемаларды тудырады, өйткені бір деректер жиынтығын түзету бүкіл дерекқорға үлкен әсер етуі мүмкін. Сондықтан әр дерек қатаң тексерілуден өтеді.

•Жою құқығы ("ұмыту құқығы", 17-бап): белгілі бір жағдайларда субъект өзінің жеке деректерін жоюды талап етуге құқылы. Ұмыту құқығы өшіру құқығы ретінде де белгілі . Бұл құқық жеке тұлғаларға жеке деректерін жоюды талап етуге мүмкіндік береді, егерде: жеке деректер енді қажет емес, тұлға келісімді қайтарып алады, дербес деректер заңсыз өңделеді, өңдеуге жеке қарсылықтар бар және деректер контроллерінде өңдеуді жалғастыруға негіз жоқ кезде. Деректерді жою заңды міндеттемені (Еуропалық Одақ заңнамасы немесе ұлттық заңнама) сақтау үшін қажет. Ұйым жалпы деректерді алған кез-келген үшінші тарапқа хабарлауы керек және егер ол сұраныстың пропорционалды емес күш-жігерді қажет ететіндігін немесе мүмкін еместей дәлелдей алмаса, оны жоюды сұрауы керек.

•Өңдеуді шектеу құқығы (18-бап): белгілі бір жағдайларда субъект өз деректерін өңдеуді шектеуді талап етуі мүмкін. Жеке тұлғалар ұйымнан жеке деректерді пайдалануды шектеуді талап етуі мүмкін, дегенмен ұйым оларды автоматты түрде жоюға міндетті емес. Алайда олар белгілі бір жағдайларда өңдеуден бас тартуы керек: деректер дәл емес (тексеру процесінде), өңдеу заңсыз болып табылады, бірақ адам деректердің жойылуын қаламайды және шектеуді талап етеді (бұл жою құқығынан өзгеше), ұйымға енді деректер қажет емес, бірақ адам заңды талаптарды қою үшін деректердің сақталуын қалайды. Ұйым деректерді жою туралы сұранысты тексеру үшін шаралар қабылдайды. Егер деректер шектеулі болса, ұйым оны келісімсіз өңдеуге құқылы емес оларға бұл сот процестері немесе басқа адамдардың құқықтарын қорғау үшін қажет болып табылады.

•Деректердің тасымалдану құқығы (20- бап): Субъект өз деректерін

құрылымдық, жалпы қабылданған және машинада оқылатын форматта алуға және оны басқа контроллерге беруге құқылы. Жеке тұлғалар өз деректерін тікелей басқа ұйымға жіберуді сұрай алады. Дегенмен, оны жеке тұлға ұйымға келісім немесе шарт бойынша берген деректерге ғана қолдануға болады және өңдеу автоматтандырылған болса. Бұл адамның мінез-құлқына қатысты деректерге де қатысты және іздеу сұрауларын, орналасқан мекен жай деректерін, веб-сайт тарихын және т.б. қамтуы мүмкін.

•Қарсылық білдіру құқығы (21-бап): Субъект өзінің ерекше жағдайына байланысты негіздер бойынша өз деректерін өңдеуге қарсылық білдіруге құқылы. Қарсылық білдіру құқығы жеке тұлғаларға кез келген уақытта және белгілі бір жағдайларда жеке деректерді өңдеуге қарсылық білдіруге мүмкіндік береді және бұл өңдеу мақсатына және өңдеу үшін құқықтық негізге байланысты болады. Жеке тұлғалар сонымен қатар заңды мүдделер немесе қоғамдық мүддедегі міндеттер негізінде деректерді өңдеуге қарсылық білдіруі мүмкін. GDPR белгілеген субъектілердің құқықтары жеке тұлғалардың мүмкіндіктерін кеңейтуге, құпиялылықты қорғауды күшейтуге және цифрлық ортада олардың жеке деректерінің ашықтығы мен бақылауын қамтамасыз етуге бағытталған.

Қазақстан Республикасының Дербес деректерді қорғау туралы заңнамасының 24- бабында субъектінің құқықтары мен міндеттері туралы жазылған. Бұл заң құқықтың мына түрлерін қарастырады:

1) меншік иесінде және (немесе) операторда, сондай-ақ үшінші тұлғада өз дербес деректерінің болуы туралы білуге, сондай-ақ: дербес деректерді жинау және өңдеу фактісін, мақсаттарын, көздерін, тәсілдерін растауды; дербес деректердің тізбесін; дербес деректерді өңдеу мерзімдерін, оның ішінде оларды сақтау мерзімдерін қамтитын ақпаратты алуға;

2) тиісті құжаттармен расталған негіздер болған кезде, меншік иесінен және (немесе) оператордан өз дербес деректерін өзгертуді және толықтыруды талап етуге;

3) дербес деректерді жинау, өңдеу шарттарының бұзылғаны туралы ақпарат болған жағдайда, меншік иесінен және (немесе) оператордан, сондай-ақ үшінші тұлғадан өз дербес деректерін бұғаттауды талап етуге;

4) меншік иесінен және (немесе) оператордан, сондай-ақ үшінші тұлғадан Қазақстан Республикасының заңнамасын бұза отырып жиналған және өңделген өз дербес деректерін, сондай-ақ осы Заңда және Қазақстан Республикасының өзге де нормативтік құқықтық актілерінде белгіленген өзге де жағдайларда жоюды талап етуге;

5) дербес деректерді жинауға, өңдеуге, жалпыға бірдей қолжетімді көздерде таратуға, үшінші тұлғаларға беруге және трансшекаралық беруге келісімін кері қайтарып алуға;

6) меншік иесіне және (немесе) операторға дербес деректердің жалпыға бірдей қолжетімді көздерінде өз дербес деректерінің таратылуына келісім беруге (бас тартуға);

7) өз құқықтарының және заңды мүдделерінің қорғалуына, оның ішінде моральдық және материалдық зиянның өтелуі үшін арыз беруге;

8) басқада заңнамаға сәйкес өз құқықтарын жүзеге асыруға құқық.[25]

Бұл құқықтарды субъектілер бейтарап және тәуелсіз іске асыра алады, мемлекеттік ұйымдарда, соттарда өз деректерін қорғау үшін толық заңда көрсетілген құқықтарын талап ете алады. Сонымен қатар Қазақстандағы дербес деректер субъектілерінің құқықтарына қосымша төмендегідей құқықтарды енгізсе жақсы болатын еді. Иесіздендіру құқығы: дербес деректер субъектісі, егер мұндай өңдеу енді қажет болмаса, оны белгілі бір адаммен байланыстыру мүмкін болмайтындай етіп, өз деректерін иесіздендіруді талап етсе және сәйкесінше бұл деректердің нақты кімдікі екенін белгісіз етіп қалдырса. Дербес деректер субъектілеріне олардың дербес деректерінің ағып кету немесе оларға рұқсатсыз қол жеткізу жағдайлары туралы хабарлануы тиіс. Бұл құқық азаматтардың ықтимал тәуекелдер туралы хабардар болуын қамтамасыз етеді. Еліміздегі қолданыстағы электрондық портал жүйесі арқылы немесе басқа ұйымдар бірден дербес дерек субъектісіне хабарландыру жіберсе, онда дерек иесі бірден қауіпсіздікті күшейте алады. Егер дербес деректер субъектісі оның деректерінің мұрағатта екенін анықтаса, ол мұндай мұрағаттық жазбалардың көшірмесін алуға немесе оларды сақтаудың заңды негіздері болмаған кезде жоюды сұрауға құқық берсе. Осы құқықтардың барлығы дербес деректерді өңдеудің ашықтығын, қауіпсіздігін және бақылауын қамтамасыз етуге бағытталған.

Биометриялық ақпарат қауіпсіздік нормалары мен арнайы қорғау шараларын қатаң сақтауды талап ететін ерекше сезімтал жеке деректер ретінде қарастырылады. Биометриялық деректер дербес деректердің бір түрі ретінде қаралады. Қазақстан заңнамасында биометриялық ақпараттарға қатысты нақты нұсқаулық жоқ, бірақ дербес деректер заңымен реттеледі. Сондықтанда, жоғарыда талқыланған дербес деректерді жинау кезінде қойылатын принциптер мен олардың субъектілеріне берілетін құқықтар биометриялық деректерге де қолданылады.

Биометриялық ақпаратты жинамас бұрын оператор өңдеу мақсаттары, әдістері, сақтау мерзімі, үшінші тұлғаларға берілуі мүмкін және қауіпсіздік шаралары туралы субъектіге ақпарат беруге міндетті. Субъектінің сезімтал деректерді өңдеумен байланысты тәуекелдер туралы хабардар болуына ерекше назар аудару қажет. Егер субъект биометриялық ақпаратты дәл емес, толық емес немесе ескірген жағдайда түзетуді немесе толықтыруды талап етсе, оператор берілген мерзімде ақпараттарға өзгеріс енгізуі қажет. Субъект биометриялық ақпаратты өңдеуге бұрын берілген келісімді кері қайтарып ала алады, бұл оны өңдеуді тоқтатуға және өзге заңды негіздер болмаған кезде деректерді жоюға әкеп соғуы мүмкін. Келісімді қайтарып алу ерікті түрде жүзеге асырылады және оператор деректерді сақтаудың басқа негіздері болмаса (мысалы, белгілі бір мақсаттар үшін заңнамада көзделген) деректерді өңдеуді тоқтатуы керек. Деректер жойылған жағдайда субъект оларды жою фактісін растауға құқылы. Субъект өзінің биометриялық деректерін өңдеуге қарсылық білдіруге құқылы. Қарсылықтар болған кезде оператор деректерді өңдеудің заңдылығын қайта қарауға және заңды мүдделерді негіздеу мүмкін болмаған жағдайда оны тоқтатуға міндетті. Субъектінің биометриялық ақпаратты өңдеуге байланысты құқықтары бұзылған жағдайда, ол қорғауға мемлекеттік органдарға немесе сотқа

жүгінуге құқылы. Субъект келтірілген залал үшін өтемақы талап ете алады, сондай-ақ операторды заңнаманы сақтамағаны үшін жауапқа тартуды сұрай алады.

Биометриялық деректерді Қазақстан Республикасынан тыс жерлерге беру кезінде оператор қорғау деңгейінің Қазақстан заңнамасының талаптарына сәйкес келуін қамтамасыз етуге міндетті. Бірақ қазіргі таңда биометриялық деректерді тыс жерлерге трансшекаралық беру нормалары әлі толық қарастырылмаған. Биометриялық деректерді өңдеуге заңдарда тікелей көзделген жағдайларды қоспағанда (мысалы, ұлттық қауіпсіздікті қамтамасыз ету, қылмыстарды тергеу және т.б.) субъектінің анық және ақпараттандырылған келісімі болған кезде ғана жол беріледі. Қазақстанда биометриялық ақпаратқа қатысты дербес деректер субъектілерінің құқықтарын қолдану азаматтардың өздерінің сезімтал деректерін бақылауды қамтамасыз етуге бағытталған. Мұндай ақпаратты өңдеуді жүзеге асыратын операторлар: деректерді жинау және өңдеу кезінде ақпараттың ашықтығы мен толықтығын қамтамасыз ету, субъектінің талабы бойынша деректерге қол жеткізу, өзгерту, шектеу немесе жою мүмкіндігіне кепілдік беру, деректерді рұқсатсыз кіруден немесе жоғалтудан қорғау үшін қажетті техникалық және ұйымдастырушылық шараларды қабылдау. Осы талаптарды сақтау міндетті болып табылады және цифрландыру қоғамында биометриялық технологияларды белсенді пайдалану жағдайында азаматтардың жеке өмірі мен құқықтарын қорғауға зор ықпал етеді.

2.3 Құқық қолдану және дербес деректерді қорғау туралы заңнаманы іске асыру мәселелері

Қазіргі ақпараттық қоғамда дербес деректерді қорғау мемлекеттінде, бизнестінде негізгі міндеттерінің біріне айналуда. Цифрлық технологиялардың қарқынды дамуы, өңделетін ақпарат көлемінің өсуі және электрондық сервистерді кеңінен енгізілуі, азаматтардың жеке ақпаратының қауіпсіздігін қамтамасыз етуге қабілетті құқықтық реттеудің сенімді жүйесін құру қажеттілігін көздейді. Осыған байланысты Қазақстанда құқық қолдану және дербес деректерді қорғау туралы заңнаманы іске асыру мәселелері ерекше өзектілікке ие болуда. Біріншіден, цифрлық экономика мен ақпараттық технологиялардың серпінді дамуы дербес деректердің коммерциялық құрылымдар үшін ғана емес, мемлекеттік органдар үшін де негізгі қызығушылық объектілерінің біріне айналуына алып келеді. Банктік операциялар мен сақтандыру қызметтерінен бастап онлайн-сауда мен әлеуметтік желілерге дейін қазіргі өмірдің кез – келген саласы жеке ақпаратты өңдеумен байланысты. Деректерге ағып кету немесе рұқсатсыз қол жеткізу елеулі қаржылық, моральдық және тіпті беделді шығындарға әкелуі мүмкін жағдайларда, жеке деректерді сенімді қорғауды қамтамасыз ету стратегиялық маңызды міндетке айналып отыр. Екіншіден, Қазақстанда дербес деректерді қорғау мәселелерін реттейтін нормативтік-құқықтық базада белгілі бір заңнамалық актілер бар, алайда оларды іс жүзінде іске асыру процесі кезінде бірқатар қиындықтарға тап болады. Заңнамада тұжырымдамалардың түсініксіздігімен байланысты

олқылықтар бар, бұл нормаларды іс жүзінде біркелкі қолдануды қиындатады. Нақты құрылған сот практикасы мен жүйелі бақылау тетіктерінің болмауы әртүрлі жағдайларда бірдей құқық бұзушылықтарды әртүрлі бағалауға әкеледі. Бұл тұрғыда жаңа құқықтық нормаларды қабылдау ғана емес, оларды қолдану әдістерін жетілдіру, сондай-ақ бұзушылық фактілеріне жедел ден қою тетіктерін әзірлеу де маңызды болып отыр. Үшіншіден, Қазақстанда дербес деректерді қорғау туралы заңнаманың сақталуын қадағалау жүйесі өкілеттіктердің бөлінуімен сипатталады, өйткені бақылауды бірнеше мемлекеттік органдар жүзеге асырады. Бұл әрекеттерді тиімсіз үйлестіруге жағдай жасайды, бұл өз кезегінде деректердің ағып кетуіне немесе дұрыс өңделмеуіне байланысты оқиғаларға жауап берудің тиімділігін төмендетеді. Бірыңғай мамандандырылған реттеушіні құру немесе ведомстволар арасындағы өзара іс-қимыл тетіктерін жетілдіру дербес деректерді қорғау деңгейін едәуір арттыруға қабілетті болатын еді.

Сонымен қатар, азаматтардың дербес деректерді қорғау саласындағы құқықтары туралы хабардар болмау мәселесін атап өтуге болмайды. Көптеген деректер субъектілерінде жеке ақпаратты қорғау мүмкіндіктері және олардың құқықтары бұзылған жағдайда заң көмегіне жүгіну тәртібі туралы толық ақпарат жоқ. Халықтың құқықтық сауаттылығын арттыру және өз деректерін қорғау мүмкіндіктері туралы белсенді хабардар ету тұрақты қорғау жүйесін қалыптастыруда маңызды рөл атқарады, өйткені бұл бұзушылық фактілеріне уақтылы жауап бере алатын және өз құқықтарының сақталуын талап ететін білімді азаматтар. Сонымен, халықаралық стандарттарды бейімдеу (мысалы, Еуропалық Одақтың GDPR) және Қазақстанның әлемдік ақпараттық кеңістікке кіруі сияқты жаһандық үрдістер ұлттық заңнаманы халықаралық нормалармен үйлестіру қажеттілігін талап етеді. Бұл дербес деректерді қорғау деңгейін арттырып қана қоймай, ақпараттық қауіпсіздік саласындағы заманауи сын-қатерлерге дайындығын көрсете отырып, елдің халықаралық аренадағы позициясын нығайтады.

Осылайша, Қазақстанда құқық қолдану және дербес деректерді қорғау туралы заңнаманы іске асыру мәселелерінің өзектілігі мынадай факторларға байланысты:

1. Цифрлық технологиялардың жылдам өсуі және өңделетін ақпарат көлемінің ұлғаюы, бұл жеке деректердің қауіпсіздігіне қосымша қауіп төндіреді.
2. Нормативтік-құқықтық базада олқылықтар мен түсінбеушіліктердің болуы, бұл заңды іс жүзінде біркелкі қолдануды қиындатады.
3. Қадағалауға жауапты мемлекеттік органдар арасындағы өкілеттіктерді бөлшектеу, бұл бұзушылықтарға жауап берудің тиімділігін төмендетеді.
4. Азаматтардың өз құқықтары туралы хабардар болмауы, бұл олардың деректерін заңсыз өңдеуге әкеп соғады.
5. Заңнаманы халықаралық стандарттарға бейімдеу қажеттілігі, бұл жаһандық ақпараттық кеңістікке интеграциялаудың маңызды факторы болып табылады.

Аталған проблемаларды шешу заңнаманы жетілдіруді, техникалық

инфрақұрылымды дамытуды, мамандардың біліктілігін арттыруды және барлық мүдделі тараптардың – мемлекеттің, бизнестің және азаматтық қоғамның белсенді қатысуын қамтитын кешенді тәсілді талап етеді. Жүйенің барлық элементтері үйлесімді жұмыс істеген жағдайда ғана дербес деректерді сенімді қорғауды қамтамасыз етуге және Қазақстанда цифрлық экономиканы дамыту үшін қолайлы жағдайлар жасауға болады.

Цифрлық технологиялардың қарқынды дамуы және өңделетін ақпарат көлемінің ұлғаюы жағдайында Қазақстанда дербес деректерді қорғау туралы заңнаманы құқық қолдану мәселелері өте өзекті болып қала береді. Нормативтік-құқықтық базаның болуына қарамастан, іс жүзінде құрылымдық, процедуралық, ақпараттық, сондай-ақ техникалық және ұйымдастырушылық аспектілерге бөлуге болатын маңызды проблемалар бар. Дербес деректерді қорғау туралы заңнаманың сақталуын бақылауды Әділет министрлігі, цифрлық даму және байланыс министрлігі сияқты бірнеше мемлекеттік органдар, сондай-ақ өзге ведомстволар шеңберіндегі мамандандырылған бөлімшелер жүзеге асырады. Бірыңғай реттеушінің болмауы бұзушылықтарға ден қою шараларының сәйкес келмеуіне әкеледі, бұл бірыңғай сот практикасын қалыптастыруды қиындатады және шешім қабылдаудың жеделдігін төмендетеді. Іс жүзінде дербес деректерді қорғау саласында сот практикасының дамымағандығы байқалады. Сот шешімдерінің материалдарына шектеулі қол жетімділік және мұндай істерді жүйелейтін мамандандырылған органның болмауы сот органдарының кейде бірдей заңнама нормаларына әртүрлі түсіндірулер беруіне әкеледі. Бұл дербес деректер операторлары үшін белгісіздік туғызады және азаматтардың өз құқықтарын қорғауға деген сенімін төмендетеді. Қазақстанда дербес деректерді қорғау саласындағы сот практикасы қалыптасу сатысында тұр. Банктерден, телекоммуникациялық операторлардан және онлайн-сервистерден ақпараттың ағып кетуіне байланысты істердің, сондай-ақ жұмыс берушілердің деректерді заңсыз пайдалануына қатысты даулардың мысалдары бар. Сот жүйесінің ресми порталында жарияланған сот шешімдері соттардың жекелеген жағдайларда моральдық және материалдық залалды өтей отырып, азаматтардың пайдасына шешімдер қабылдайтынын, сондай-ақ операторларға ақпараттық қауіпсіздікті күшейту бойынша шаралар қабылдауға нұсқау беретінін көрсетеді.

2022 жылдан бастап мемлекеттік органдар немесе мемлекеттік заңды тұлғалар тарапынан тиісті ақпаратқа қол жеткізу кезінде міндетті болып табылатын және жүйелік проблемаларды анықтайтын дербес деректерге қол жеткізуді бақылаудың мемлекеттік сервисі жұмыс істейтіні нақтыланды. Мемлекеттік сервиске 125 ақпараттық жүйе біріктірілген (47 – і мемлекеттік органдарға, 24 – і квази мемлекеттік секторға, 54-і жеке секторға тиесілі). Сонымен қатар, 2023 жылы қазақстандықтардың жеке ақпаратты қорғауға қатысты өтініштерінің саны екі есеге дейін өскен. Қазақстандықтардың шағымдары негізінде 2020 жылдың маусым айынан бастап осы саладағы заңнама талаптары бойынша жоспардан тыс 37 тексеру жүргізілді. Нәтижесінде 31 лауазымды және заңды тұлға жауапқа тартылған. 5,3 млн теңгеден астам айыппұл салынған. Барлығы 76 әкімшілік іс қозғалды және 2020 жыл – 7, 2021 жыл – 13, 2022 жыл – 20, 2023 жыл – 25 қаралған [39]. Анықталған

проблемаларға байланысты дербес деректер субъектілерінің құқықтарын қорғаудың жаңа тетіктері әзірлеу, әкімшілік құқық бұзушылық туралы кодекске түзетулер енгізу бойынша жұмыстар жүргізілуде.

2024 жылдың ақпанында кибершабуылдарды талдау және тергеу орталығы қытайлық iSOON киберқауіпсіздік жеткізушісінің GitHub ресурсында пайда болуы туралы есеп жариялады. Компания сонымен қатар Қытайдың қоғамдық қауіпсіздік департаментінің (MPS) мердігері болып табылады. Біріктірілген файлдарда Қазақстан туралы жазбалар табылды, олардың көлемі мен сапасы белгісіз, кем дегенде бір хакерлік топ екі жылдан астам уақыт бойы байланыс операторларының инфрақұрылымына қол жеткізу арқылы деректерге қол жеткізген. Материалдарда telecom.kz, kcell.kz, tele2.kz, beeline.kz базалары болған[40]. Бұл жерде байланыс операторларының да өз қызметтерін жүзеге асыру кезінде қауіпсіздікті сақтамағанын көруге болады. Хакерлік топтар бір базаны ұзақ уақыт бойы бағдарда ұстайды және мүмкіндік туындағанда бірден шабуыл жасайды. Мұндай жағдайда субъектіде және операторда үнемі қауіпсіздікті сақтауда мұқият болғаны дұрыс.

Қазақстан Республикасы Бас прокуратурасының «Qamqor» Құқықтық статистика және арнайы есепке алу жөніндегі комитеті әкімшілік құқық бұзушылықтар туралы жариялаған статистикасына сәйкес, Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі (бұдан әрі-ҚР ЦДИАӨМ) жинағының 2024 жылдың 12 айы бойынша «Уәкілетті органдармен әкімшілік құқық бұзушылықтар жөніндегі істерді қарау нәтижелері туралы» №1-ӘІ нысанды статистикалық есебінің дерегіне сәйкес, ҚР ӘҚБтК 79-бабы «Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасын бұзу» бойынша 387 әкімшілік құқық бұзушылық тіркелген, 78 731 900 тенге айыппұл салынған. 2025 жылдың 1 квартлдағы статистикалық есебі бойынша 24 әкімшілік құқық бұзушылық ісі тіркелген, 1 769 400 тенге айыппұл салынған [26]. Сондай-ақ, Қазақстан Республикасының электрондық құжат және электрондық цифрлық қолтаңба саласындағы заңнамасының талаптарын бұзғаны үшін әкімшілік жауапкершілікке тарту бойынша жұмыс жалғасуда. 2024 жылдың басынан бастап ҚР ӘҚБтК-нің 640-бабы бойынша 8 әкімшілік іс жүргізілді, нәтижелері бойынша 249 210 теңге сомасына 8 лауазымды тұлға әкімшілік жауапкершілікке тартылды [23]. Орын алатын бұзушылықтардың негізгі түрлері: дербес деректерді жинау және өңдеу үшін келісімнің не заңды негіздердің болмауы; дербес деректерді заңсыз тарату; дербес деректерді өңдеуді ұйымдастыруға жауапты тұлғаның болмауы; қолжетімділігі шектеулі дербес деректерді шифрлау үшін МҚЗИ пайдаланбау, пайдаланушылардың және ДҚБЖ іс-әрекеттерін логиялаудың болмауы және т.б. болып табылады. Құқықбұзушылықтың алдын алу үшін келесідей әрекет жасау қажет. Дербес деректер бойынша тұрақты оқыту және сертификаттау жүйесін енгізу. Барлық мемлекеттік қызметкерлер мен деректермен жұмыс істейтін жеке ұйым қызметкерлері дербес деректерді қорғау бойынша міндетті оқу курстарынан өтуі қажет. Бұл Еуропалық GDPR жүйесіндегі Data Protection Officer (DPO) институтына ұқсас, профилактикалық рөл атқарады. ҚР ӘҚБтК 79-бабы бойынша қазіргі санкциялар айыппұлмен шектеледі, бірақ бұл әрдайым

ескерту немесе тоқтату шарасы ретінде тиімді бола бермейді. Сондықтанда санкцияны қатаңдату қажет. Бірінші рет бұзғандарға – ескерту немесе төмен айыппұл, қайталанған бұзушылыққа – айыппұлды 2–3 есеге арттыру, қызметтен шеттету не лицензияны уақытша тоқтату сынды санкция. Дербес деректердің ауқымы мен салдарына қарай санкцияны күшейту. Егер бұзушылық жаппай деректерді (мысалы, 1000+ азаматтың) заңсыз таратуға қатысты болса — бұл ауырлататын мән-жай ретінде бағаланып, қылмыстық жауапкершілікке дейін баруы қажет (қазіргі ҚК 147-баппен байланыстыра отырып). Дүниежүзілік тәжірибе (мысалы, ЕО-ның GDPR жүйесі) құқық бұзушыны алдын ала ескертуге бағытталған кешенді жүйені қалыптастырған. Мәселен, 2022 жылы Meta (Facebook) компаниясына 1,2 миллиард еуро айыппұл салынғаны — дербес деректердің құндылығы мен қоғам алдындағы жауапкершілікті көрсетеді. ҚР Жоғарыдағы негіздерді ұстана отырып ӘҚБтК 79-бабына мынадай нақты өзгеріс енгізу ұсынылады «Қайталанған немесе көп мөлшердегі дербес деректерге қатысты бұзушылықтар үшін айыппұл мөлшерін екі есеге арттыру және заңды тұлғаларға — қызметін уақытша тоқтата тұру шарасын қолдану көзделсін.»

BestProfi.com ақпараттық жүйеде Дербес деректер және оларды қорғау туралы заңы бойынша 643 сот ісі табылды. Оның ішінде дербес деректер субъектісінің құқығын бұзу фактісі бойынша 53 іс табылды, бірақ істерге қолжетімділік шектеулі. BestProfi.com ақпараттық жүйеде Дербес деректер және оларды қорғау туралы заңында биометриялық деректерге қатысты 7 азаматтық ісі табылды. Қаралған сот істерінде азаматтар өздерінің дербес және биометриялық деректерін қорғау мақсатында сотқа талап арызбен жүгінген.

№7113-20-00-2/842 іс бойынша талапкер: Жақыпов А.Б., жауапкер: "Азаматтарға арналған үкімет" мемлекеттік корпорациясы " АҚ директор туралы мәліметтерді дерекқордан шығарудан бас тарту заңсыз деп танылсын және директор туралы мәліметтерді дерекқордан алып тастауды міндеттеу туралы талаппен сотқа жүгінеді. Сот Азаматтық кодекстің 15-бабы, 8-тармағы бойынша егер азаматтың есімін негізсіз пайдаланса онда тыйым салуды талап етуге құқылы, бірақ сот бұл бапты назарға алған жоқ, өйткені мемлекеттік тізілімде Жақыпов есімін пайдалану бұрын ЖШС арқылы ресімделген ресми өкілеттіктермен байланысты және оның құқықтарын бұзбайды деп есептейді, Дербес деректерді қорғау туралы заңның 25-бап 2-тармағының 1-тармақшасына сәйкес дербес деректер оларды сақтау үшін негіздер болмаған кезде жойылуы тиіс. Сот деректерді алып тастау жеке тұлғаның емес, ЖШС өтініші бойынша ғана мүмкін екенін атап өтті. Сондықтан жою тәртібі сақталмайды-алып тастауға негіз жоқ деп уәждейді. Заңды тұлғаларды мемлекеттік тіркеу және филиалдар мен өкілдіктерді есептік тіркеу туралы заңның 14-2-бап, 2-тармағына сай заңды тұлғаның басшысы туралы мәліметтерге өзгерістер тек заңды тұлғаның (ЖШС) бастамасы бойынша енгізіледі делінген. Сот жоғарғы нормаларға сілтеме жасап талапты қанағаттандырмады.

6001-23-00-3гп/121 Жоғарғы сотының қаулысында талапкер Есшанова. Г көршісі Сариева. Ж пәтер есігінің үстінде орнатқан бейнебақылау камерасын алып тастауды талап етті, бұл камера оның жеке өміріне қол сұғылмаушылық құқығын бұзады деп есептейді. Талап бірінші және апелляциялық сатыда

қаралды, сот дербес деректерді қорғау туралы заңның 1, 2-баптары дербес деректерді келісімсіз жинау жеке адамның құқықтарын бұзады, 7 және 8-баптары дербес деректерді жинау деректер субъектісінің келісімімен жүргізілуі тиіс деп талапты қанағаттандырады. Іс Жоғарғы сотта қаралып, онда бейнебақылау дербес деректерді жинамады (ЖСН, ТАӘ, Биометрия және т.б. жоқ). Камера жеке өмірді бұзатыны дәлелденбеген пәтердің ішіне бағытталмаған, баспалдақ алаңының бір бөлігін ғана қамтиды. Жасырын бақылау болған жоқ. "Тұрғын үй қатынастары туралы" ҚР Заңының 2-бабының 14-тармағына сай баспалдақ алаңы-бұл жалпыға ортақ мүлік және оны жеке аумақ деп санауға болмайды. "Рұқсаттар және хабарламалар туралы" ҚР Заңының 28-бабы бейнекамераларды орнату лицензияланбайды және рұқсатты қажет етпейді. Жоғарғы сот осы нормаларға сүйене отырып бірінші және апелляциялық сот шешімдерін жойып, бейнекамераны қалдыру туралы шешім шығарады.

№ 7517-22-00-2/5469 сот ісінде талапкер мен үшінші тұлғалар жауапкер Пылаевтан Facebook-тегі олардың фотосуреттері мен аты-жөні бар жазбаны жоюуын және моральдық зиянды өндіріп алу туралы талап қояды. Жауапкер Пылаев банк қызметкерлеріне сын-ескертпелер жазып, "Одноклассники" ашық профилінен олардың фотосуреттерін жариялайды. Сот келесі заңдарға сілтеме жасайды: Азаматтық кодекс 145-бабы егер заңда өзгеше көзделмесе, адамның бейнесін оның келісімінсіз пайдалануға тыйым салады, ДД заңында 7- бап деректерді жинау/өңдеу субъектінің келісімін талап етеді, 20-бап деректер қорғалуға тиіс, сондай ақ Бұқаралық ақпарат құралдары туралы Заңы 14 – баптың 1-1 тармағы суреттерді келісімсіз жариялауға рұқсат береді, егер ақпарат қоғамдық/қызметтік қызметпен байланысты және сурет бұрын беттің өзі ашық дереккөзде орналастырылған болса. Ақпараттандыру туралы заңда әлеуметтік желілер (Facebook) — бұл интернет-ресурстар, бұқаралық ақпарат құралдарына теңестірілетіндігін анықтайды. Сот талаптарын қанағаттандырудан бас тартты.

Алматы қалалық сотының 2023 жылғы 20 сәуірдегі "Еуразиялық банк" АҚ-ға қарсы Мұқаева Айнұр талабы бойынша №7599-23-00-2а/2730 сот қаулысының мәтіні негізінде талапкер А.С. Мұқаева Еуразиялық банкпен 2022 жылғы 24 тамызда жасалған кредит беру туралы шартты жарамсыз деп тануды талап етті. Ол несиені рәсімдемегенін және келісімшартты алаяқтар оның қатысуынсыз жасағанын мәлімдеді. Сот АК 157-бабы-мәмілелердің жарамсыздығы бойынша шарт ерік білдіруді растайтын биометриялық сәйкестендіруді пайдалана отырып жасалған, алаяқтық фактісі дәлелденбеген сот үкімі жоқ, осы бап бойынша мәмілені жарамсыз деп тануға негіз жоқ. Биометрияны қолдану талапкердің қатысуын растайды. ДД заңның 1-бабы биометриялық мәліметтер-бұл жеке тұлғаны анықтауға мүмкіндік беретін мәліметтер. Несиені рәсімдеу кезінде осындай деректерді пайдалану қарыз алушының жеке басын растайды бұл жағдайда А.С. Мұқаева соттағы ұстанымын әлсіретеді. Сот талапты қанағаттандырмайды.

№ 7514-21-00-2/1793 азаматтық ісі бойынша талапкер Кадетов. Р жауапкер "Alldata" ЖШС- на өзінің дербес деректерін бұзды деген және азаматтық құқықтарды қорғау туралы талаппен сотқа шағымданады. 2020 жылғы 10

желтоқсандағы ЦДИАӨМ №12 қорытындыға сәйкес, интернет-ресурсты зерттеу нәтижесінде жеке және заңды тұлғалардың өз деректер базасының болу белгілері анықталды. "Alldata" ЖШС интернет-ресурсты пайдалана отырып "adata.kz" азаматтардың жеке мәліметтерін өз базасында жариялаған. Ақпараттық қауіпсіздік комитеті 2020 жылғы 30 желтоқсандағы қаулысымен жауапкер ӘҚБтК 79-бабының 1-бөлігінде көзделген әкімшілік құқық бұзушылық жасағаны үшін кінәлі деп танылды және айыппұл түрінде әкімшілік жазаға тартылған. Судья Азаматтық кодексі 115, 951-бабы, Дербес деректер және оларды қорғау туралы" заң 1, 6, 20-баптары, Ақпараттандыру туралы заң 36-баптарын уәждеп, АІЖ дын 76 бабына сай күшіне енген әкімшілік қаулы азаматтық салдарларды қарау кезінде қайта дәлелдеуді талап етпейтінін алға тартып, талапты қанағаттандырмады.

2023 жылғы 6 сәуірдегі №7599-23-00-2a/1760 іс бойынша талапкер Демьяненко Е. С. соттан 30.05.2022 жылғы шағын несие шарты мен 30.03.2022 жылғы жария шартты жарамсыз деп тану туралы талап арыз түсіреді. Сот бірінші сатыда және апелляциялық сатыда қаралады. Сот талапты қанағаттандырудан бас тартады, оған негіз несие биометриялық сәйкестендіру арқылы рәсімделген, талапкердің қатысуын растайтын адамның фотосуреті/видеосы тіркелген, алаяқтық фактілері анықталмаған, жауапкер банк әрекеттерінде заң бұзушылықтар анықталған жоқ. ҚР АІЖК 424, 423, 425, 426-баптар-апелляция рәсімі бойынша, ҚР Ұлттық Банкінің № 217 қаулысы онлайн-кредит беру ережелеріне сүйене отырып шешім шығарады.

Қостанай қалалық сотының 2021 жылғы 30 қарашадағы №3910-21-00-2/4821 бұл сот шешімі талапкер Гаврилова. С Қостанай қаласының білім бөліміне өз қызметіне қайтаруға және моральдық зиян төлеуін талап етті. №18 мектеп-гимназиясының директоры Гаврилова Светлана Витальевна дербес деректерді қорғау туралы заңнаманы бұзғаны үшін тәртіптік жазаға тартылды (қатаң сөгіс) атап айтқанда, прокуратура қызметкерлеріне білім бөлімінің қазіргі басшысы Г.А. Уразбаеваның бұрынғы еңбек қызметі туралы ақпарат бергені үшін. Сот бұл тәртіптік жазаны заңсыз деп таныды. Гаврилова ұсынған ауызша ақпарат жеке деректер туралы заңды бұзу болып табылмайды, өйткені: ол тек фактіні растады Оразбаеваның мектептегі жұмысы ешқандай құжаттар (бұйрықтар, көшірмелер, жеке істер және т. б.) прокуратураға берілмеді, ақпарат өзімшілдік мақсатта пайдаланылмаған, еңбек қызметі фактісі құпия емес және құпия дербес деректердің анықтамасына жатпайды.

Қазақстанда дербес деректердің кибер сақтандыру қауіпсіздігін іске асыратын КИБ ЦДИАӨМ құрылымдық бөлімшесі болып табылады және нормативтік актілерді әзірлеуге, ақпараттық қауіпсіздік талаптарының сақталуын бақылауға, сондай-ақ мемлекеттік электрондық ресурстарды қорғау жөніндегі бағдарламаларды іске асыруға жауапты. «Қазақстанның кибер қауіпсіздігі» атты тұжырымдама 2017 жылы бекітілген. Бұл тұжырымдама ақпараттық жүйелер мен инфрақұрылымды ішкі және сыртқы қауіптерден қорғаудың жоғары деңгейін қамтамасыз етуге бағытталған. Ол кибершабуылдардың алдын алу және елдегі ақпараттық қауіпсіздікті нығайту жөніндегі шараларды көздейді [22]. Қазақстан киберқауіпсіздік бойынша

жаһандық индексте 31 орынды алады. Халықтың киберқауіпсіздік қаупі туралы хабардар болу деңгейі 78% қамтиды. Ақпараттық қауіпсіздік саласындағы қызметкерлермен қамтамасыз етілуі 46% ды қамтиды. Ақпараттық қауіпсіздік жөніндегі 12 жедел орталықтары жұмыс жасайды. Қазақстанның кибер қауіпсіздігі» атты тұжырымдамасының жеке деректерді қорғау бойынша іс-шаралардан күтілетін нәтижесі: дербес деректерді өңдеу саласын үздік әлемдік практикалардың талаптарына сәйкес келтіру (GDPR), азаматтар мен бизнес үшін сандық экономиканың тартымдылығын арттыру, ақпараттық қауіпсіздік саласының дамуына жәрдемдесу, азаматтар мен бизнес тарапынан мемлекетке деген сенімді арттыру. Екінші орталық кибер сақтандыру бойынша KZ-CERT-компьютерлік инциденттерге әрекет етудің ұлттық қызметі деп аталады. KZ-CERT Ұлттық ақпараттық жүйелердегі киберқауіптерге мониторинг, талдау және оларға ден қою жөніндегі бірыңғай орталық ретінде жұмыс істейді. Қызмет кибершабуылдардың алдын алу және жою бойынша ұсыныстар береді.

Төменде Қазақстанда дербес деректерді қорғау туралы заңнаманы құқық қолдану тиімділігін арттыруға бағытталған ұсынымдар келтірілген.

1. Құқықтық нормаларды нақтылау:

Қолданыстағы нормативтік актілерді қайта қарау және толықтыру, нормаларды біркелкі түсіндіруді қиындататын түсініксіздіктер мен белгісіздіктерді жою ұсынылады. Деректер операторларының міндеттерін және заңнаманы бұзғаны үшін жауапкершілікті нақты тұжырымдау сот дауларының санын азайтуға мүмкіндік береді. Ұлттық заңнаманы халықаралық стандарттарға сәйкес бейімдеу. Еуропалық Одақтың GDPR-ге ұқсас қағидаттар мен талаптарды енгізу қорғаныс деңгейін арттырып қана қоймай, халықаралық ынтымақтастық пен шетелдік инвесторлардың сеніміне жағдай жасауға мүмкіндік береді.

2. Бірыңғай мамандандырылған реттеуші органды құру.

Дербес деректерді қорғау туралы заңнаманың сақталуын бақылау мен қадағалауға жауапты бірыңғай реттеуші мемлекеттік органның моделін әзірлеу қажет. Мұндай орган әртүрлі ведомстволардың (оның ішінде Әділет министрлігі, цифрлық даму және байланыс Министрлігі, электрондық үкімет порталы және т.б.) жұмысын орталықтан үйлестіре алады, бұл бұзушылықтарға жедел ден қоюға мүмкіндік береді. Мемлекет тарапынан бақылау және қадағалау жүйесін күшейту. Ақпараттық жүйелер мен қауіпсіздік шараларын сертификаттаудың тәуелсіз тетіктерін құру және дамыту ұйымдарда деректерді қорғау сапасын арттыруға мүмкіндік береді. Тұрақты аудиттер мен тексерулер нормативтік талаптардың сақталуына ықпал етеді.

3.Заңнаманы тиімді қолдану үшін судьяларға, құқық қорғау органдарының қызметкерлеріне және ақпараттық қауіпсіздік саласындағы мамандарға арналған мамандандырылған курстар мен тренингтер ұйымдастыру қажет. Бұл деректерді қорғаудың техникалық және құқықтық аспектілерін терең түсінуге мүмкіндік береді. Ақпараттық қауіпсіздік жөніндегі халықаралық конференцияларға, семинарлар мен форумдарға қатысу отандық мамандарға озық тәжірибелермен танысуға және оларды ұлттық жүйеге сай біріктіруге көмектеседі. Азаматтардың құқықтық сауаттылығын арттыру және жұртшылықты ақпараттандыру, түсіндіру науқандарын өткізу, ақпараттық материалдарды жариялау және

консультациялық орталықтарды ұйымдастыру азаматтарға дербес деректерді қорғау саласындағы өз құқықтары және оларды іске асыру тәсілдері туралы білуге көмектеседі.

4. Заманауи техникалық инфрақұрылымға инвестициялар жасау. Заңнаманың талаптарын іске асыру үшін ақпараттық жүйелерді жаңартуға және жаңғыртуға, деректерді шифрлау мен қорғаудың озық технологияларын енгізуге инвестициялау қажет. Бұл ағып кету және жеке ақпаратқа рұқсатсыз қол жеткізу тәуекелдерін азайтуға мүмкіндік береді. Қауіпсіздік стандарттарын әзірлеу қажет, қазіргі заманғы сын-тегеуріндерге бейімделген ақпараттық қауіпсіздік саласында ұлттық стандарттарды құру дербес деректерді өндейтін ұйымдарға бірыңғай талаптар белгілеуге мүмкіндік береді. Қазақстанның Халықаралық ұйымдарға белсенді қатысуы және шетелдік әріптестермен тәжірибе алмасу үздік тәжірибелерді енгізуге және дербес деректерді қорғаудың ұлттық жүйесінің тиімділігін арттыруға ықпал етеді.

Құқық қолдануды жетілдіру жөніндегі ұсынымдар халықаралық стандарттарды ескере отырып, нормативтік базаны жетілдіруді, бірыңғай мамандандырылған реттеушіні құруды, сот практикасын дамытуды, мамандардың біліктілігін арттыруды және азаматтарды өз құқықтары туралы белсенді хабардар етуді қамтиды. Бұдан басқа, заманауи техникалық шешімдерді енгізу және халықаралық ынтымақтастықты нығайту дербес деректерді қорғау туралы заңнаманы бұзуға қарсы іс-қимылдың тиімді жүйесін құруға мүмкіндік береді. Осылайша, Қазақстанда дербес деректерді сенімді қорғауды қамтамасыз ету үшін қолданыстағы жүйені кешенді реформалау қажет, бұл мемлекеттік органдардың, бизнес пен азаматтық қоғамның өзара іс-қимылын көрсетеді. Ұсынылған шараларды іске асыру бұзушылықтарға ден қоюдың жеделдігін арттырып қана қоймай, азаматтар мен инвесторлардың сенімін нығайтуға ықпал ете отырып, цифрлық экономиканы одан әрі дамыту үшін қолайлы жағдайлар жасауға мүмкіндік береді.

3 Қазақстандағы және шет елдердегі биометриялық технологияларды құқықтық реттеу тәсілдерін салыстырмалы талдау

3.1 Дербес деректерді қорғау және биометриялық технологияларды пайдалану саласындағы халықаралық стандарттар

Халықаралық деңгейде жеке деректерді қорғау және биометриялық технологияларды қолдануды реттеу барған сайын маңызды бола түсуде. Адам құқықтарының жалпыға бірдей декларациясы және азаматтық және саяси құқықтар туралы халықаралық пакт сияқты негізгі құжаттар әр адамның жеке өміріне қол сұғылмаушылық құқығын бекітеді, бұл осы салада мамандандырылған құқықтық тетіктерді әзірлеуге негіз болады. Осыған байланысты дербес деректерді қорғауға бағытталған бірінші халықаралық шарт №108 Еуропа Кеңесінің Конвенциясын, сондай-ақ оның цифрлық дәуірдің сын-тегеуріндеріне бейімделген №108 Конвенциясының жаңғыртылған нұсқасын қабылдау маңызды кезең болды. Бұдан басқа, құқықтық реттеудің дамуына экономикалық ынтымақтастық және даму ұйымының (ЭЫДҰ) ұсынымдары мен қағидаттары, сондай-ақ Еуропалық Одақтың нормативтік актілері, атап айтқанда, деректерді қорғау жөніндегі жалпы регламент (GDPR) айтарлықтай әсер етті. Жаһандық маңызы бар GDPR биометриялық деректерді сезімтал ақпарат категориясы ретінде өңдеуге баса назар аудара отырып, жеке ақпаратты қорғаудың эталонына айналды. Бұл жұмыс дербес деректерді қорғау және биометриялық технологияларды қолдану мәселелерін реттейтін халықаралық нормативтік құқықтық актілерді жан-жақты талдауға арналған. Халықаралық аренадағы осы нормативтік- құқықтық актілерге жеке-жеке талдау жасайық.

Еуропалық Одақтың деректерді қорғау жөніндегі жалпы регламенті (GDPR) (2016/679 ЕО регламенті) құпиялылықты, қауіпсіздікті және адам құқықтарын қамтамасыз ету мақсатында биометриялық деректерді қоса алғанда, дербес деректерді өңдеуді реттейді. Биометрика ең сезімтал болып саналады, сондықтан GDPR оларды өңдеудің қатаң ережелерін белгілейді. GDPR регламенті биометриялық деректерді арнайы категория ретінде жіктеп қарайды. GDPR 9-бабында биометриялық деректер қатаң өңдеу ережелері орнатылған деректердің арнайы санатына жатады. Жеке тұлғаны анықтау үшін қолданылатын биометрикаға арнайы шектеулер қойылған. «Жеке тұлғаны біржақты сәйкестендіру мақсатында нәсілдік немесе этникалық шығу тегін, саяси көзқарастарын, діни немесе философиялық нанымдарын, генетикалық деректерін, биометриялық деректерін ашатын дербес деректерді өңдеуге тыйым салынады». Осылайша, биометриялық деректерді өңдеу маңызды құқықтық негізді қажет етеді. Регламенттің бұл келтірген нормасын азаматтардың жеке бас бостандығы мен өміріне қолсұғылмауы үшін жазылған десек те болады. Биометриялық деректерді өндейтін ұйымдар қосымша талаптарды сақтауы керек:

Деректерді қорғауға әсерді бағалау: биометриялық деректерді өңдеу кезінде деректер субъектілерінің құқықтары үшін тәуекелдерді бағалауды жүргізу және осы тәуекелдерді азайту шараларын қолдану қажет.

Деректерді қорғауға жауапты адамды тағайындау: егер ұйым биометрияны

белсенді түрде өндейтін болса, GDPR принциптеріне сәйкестігін бақылау үшін жауапты адам тағайындауы керек.

Бұзушылықтар туралы хабарлама: биометриялық деректер ағып кеткен жағдайда ұйым қадағалау органына 72 сағат ішінде хабарлауға міндетті. GDPR биометриялық деректерді ерекше қорғауды талап ететін дерек ретінде санайды, сондықтанда қауіпсіздіктің жоғарғы шараларын жүзеге асырады. Сонымен қатар, биометриялық деректер үшін арнайы қауіпсіз техникалық және ұйымдастырушылық шараларды қолдануды талап етеді: деректерді шифрлау; бүркеншік ат (биометриялық идентификаторларды кездейсоқ мәндермен ауыстыру); кіруді шектеу және көп факторлы аутентификация; қауіпсіздік жүйелерін жүйелі түрде тестілеу. GDPR биометриялық деректерді қорғау үшін қатаң құқықтық негіз жасайды, оларды өңдеу ережелерін белгілейді және деректер субъектілерінің құқықтарын қамтамасыз етеді.

Еуропа Кеңесінің № 108 конвенциясы (1981 жылы қабылданған) дербес деректерді автоматтандырылған өңдеу кезінде жеке тұлғалардың құқықтарын қорғауға бағытталған алғашқы халықаралық құқықтық құрал болды. Оның негізгі принциптері – заңдылық, адалдық, мақсаттарды шектеу, деректерді азайту, дәлдік және қауіпсіздікті қамтамасыз ету – ЕО деректерді қорғаудың жалпы ережесі (GDPR) сияқты ережелерге негіз болды. Конвенцияны қабылдау кезінде "биометриялық деректер" ұғымына жеке тоқталмаған еді. Себебі, ол кезде биометриялық технологиялар әлі қалыптасу кезеңінде болған, адамның бірегей физиологиялық және мінез-құлық сипаттамаларын автоматтандырылған өңдеумен байланысты заманауи қауіптер жаңа технологиялар аясында қолданыстағы принциптерді одан ары жетілдіруді талап етеді.

Биометриялық деректерге №108 Конвенция қағидаттарын қолдануға да болады. Мұнда деректерді қорғаудың жалпы принциптерін қолданады. №108 Конвенция жеке тұлғаны сәйкестендіруге мүмкіндік беретін ақпараттың барлық түрлеріне қолданылатын жеке деректерді өңдеуге қойылатын жалпы талаптарды белгілейді [41]. Бұл талаптар биометриялық мәліметтерге де қатысты, тіпті түпнұсқа мәтінде "биометрия" термині болмаса да. Осылайша:

- Заңдылық және келісім. Биометриялық деректерді өңдеу заңды түрде жүргізілуі керек және мұндай деректерді пайдалану үшін, әдетте, субъектінің жеке келісімі қажет.
- Мақсатты шектеу және азайту. Биометриялық деректерді жинау белгілі бір және заңды мақсатпен шектелуі керек (мысалы, қорғалған ресурстарға қол жеткізу үшін сәйкестендіру) және жиналған ақпарат көлемі аз болу қажет.

Соңғы жылдары биометриялық технологиялардың қарқынды дамуын ескере отырып, сарапшылар конвенцияны жаңа шындыққа бейімдеу қажеттілігін атап өтті. Кейбір бастамалар мен аналитикалық құжаттар (кейде "№108+ Конвенция" деп аталады) Конвенцияның бастапқы принциптерін биометрияға қолдануды кеңейтеді. Сонымен, қазіргі заманғы зерттеулер биометриялық деректерді қорғауға, өңдеудің ашықтығына және автоматтандырылған өңдеуге негізделген шешімдерге шағымдану мүмкіндігіне барабар кепілдіктер болған жағдайда ғана рұқсат етілетінін көрсетеді [41]. GDPR сияқты заманауи нормалар биометриялық деректердің қосымша қорғаныс шараларын қажет ететін арнайы деректер

санатына жататынын анықтайды. №108 Конвенция биометрияны жаппай қолдану дәуіріне дейін қабылданғанымен, оның принциптері осындай ережелердің негізін қалады. Бұл дербес деректерді қорғаудың негізгі талаптарының әмбебаптығын көрсетеді, олар қазіргі заманғы технологияларға бейімделген жағдайда деректердің жаңа түрлеріне де қолданылады. Бірақ дербес деректерді өңдеудің неғұрлым қорғалған және транспарентті жүйесін құруға ықпал ете отырып, №108 Конвенцияда нақтыланған базалық принциптерді дамыту арқылы биометриялық ақпаратты қорғауды күшейте аламыз.

Экономикалық ынтымақтастық және даму ұйымы (ЭЫДҰ) нұсқаулықтары 1969 жылы жеке деректерді қорғау және құпиялылық құқықтарын сақтай отырып, ақпараттың еркін трансшекаралық ағынын қамтамасыз ету үшін жалпы стандарттарды белгілеуге бағытталған "жұмсақ құқық" ретінде әзірленді. Қосымша сипатқа қарамастан, олар ұлттық заңнамалар мен деректерді қорғау саласындағы халықаралық келісімдер үшін маңызды сілтеме болып табылады. 1970 жылдардың аяғында ақпараттық технологиялардың қарқынды дамуымен жеке ақпаратты жинау, өңдеу және беру тәсілдерін біріздендіру қажеттілігі туындады. Нұсқаулар 1980 жылы 23 қыркүйекте ЭЫДҰ Кеңесінің 523-ші отырысында ұсыныс ретінде қабылданғаннан кейін күшіне енді. Құжат бес бөлімнен тұрады. Бірінші бөлімде бірқатар анықтамалар бар және нұсқаулықтардың қолданылу аясын анықтайды. Екінші бөлімде басшылық қағидаттардың өзегін құрайтын сегіз негізгі ереже (7-14-тармақтар) бар: 1) мақсатты шектеу; 2) деректер сапасын анықтау; 3) мақсатты анықтау; 4) пайдалануды шектеу; 5) қауіпсіздік кепілдігі, 6) ашықтық; 7) жеке қатысу; 8) жауапкершілік. (ЭЫДҰ) нұсқаулары мемлекет, бизнес және азаматтардың мүдделері арасындағы тепе-теңдікті ұсына отырып, экономиканың жаһандануы мен ақпараттық ағындардың сын-тегеуріндерін шешуші негіз болды.[43] Принциптер ұсынымдық сипатта болғанымен, олар ұлттық заңдардан бастап еуропалық Регламентке (GDPR) дейінгі әртүрлі юрисдикциялардағы ережелерді әзірлеуге айтарлықтай әсер етті. Қазіргі заманғы деректерді қорғау туралы заңдардың көптеген ережелері дәл осы принциптерден көрінеді.

ЭЫДҰ нұсқаулары бірқатар негізгі ережелерден тұрады, олардың әрқайсысы жеке деректерді өңдеуге қойылатын негізгі талаптарды көрсетеді:

- Деректерді жинауды шектеу (collection Limitation Principle).

Мәні: деректерді жинау тек осы мақсаттар үшін қажетті мәліметтермен шектеліп, заңды, әділ әдістермен жүзеге асырылуы керек.

Талдау: бұл принцип жеке ақпараттың артық жиналуын болдырмауға және рұқсатсыз пайдалану қаупін азайтуға көмектеседі. Ол ұйымдардан нақты деректерді жинау қажеттілігінің нақты негіздемесін талап етеді.

- Деректер сапасы (Data Quality Principle).

Мәні: Дербес деректер мәлімделген мақсаттарға жету үшін қажет шамада дәл, толық және жаңартылған болуы тиіс.

Талдау: мемлекеттік басқару немесе коммерциялық қызмет болсын, олардың негізінде қабылданған шешімдердің дұрыстығын қамтамасыз ету үшін деректердің сапасын сақтау маңызды. Бұл ереже сонымен қатар ескірген ақпаратты түзету немесе жою жауапкершілігін білдіреді.

- Мақсаттарды анықтау (Purpose Specification Principle).

Мәні: деректерді жинауға дейін немесе жинау кезінде ұйымдар оларды пайдалану мақсаттарын нақты анықтап, құжаттауы керек.

Талдау: мақсаттарды ашық көрсету пайдаланушылардың сенімін қамтамасыз етеді және ақпарат субъектілерінің құқықтарын бұзуы мүмкін деректерді пайдалану аясын кеңейтуден аулақ болады.[43]

ЭЫДҰ нұсқаулары дербес деректердің субьектісіне қатысты құқықтық нормаларды да қамтиды. Дербес деректерді маңызды ақпарат ретінде көрсетеді. Деректер субъектісі өз келісімін берген немесе басқа да құқықтық негіз болған жағдайларды қоспағанда, жеке деректер бастапқыда мәлімделгенге сәйкес келмейтін мақсаттар үшін пайдаланылмауы керек дейді. Бұл қағида «функционалды ауысуды» болдырмай, жеке тұлғаның құқықтарын қорғауға ықпал етеді. Дербес деректерді өндейтін ұйымдар мақсаттарды, әдістерді және қауіпсіздік шараларын қоса, деректерді өңдеуге қатысты саясаттары мен тәжірибелері туралы ақпарат беруі керек. Бұл ашықтық принципі деректер субъектілеріне өз мәліметтерін беру туралы негізделген шешімдер қабылдауға мүмкіндік береді, сонымен қатар ұйымдар мен мемлекеттік институттарға деген сенімділікті арттыруға ықпал етеді. Сонымен қатар, басқа да халықаралық актілер сияқты деректер субъектілері өз ақпаратына қол жеткізе алуы, оны нақтылауы, түзетуі немесе жоюға құқығы бар. Азаматтарға өз ақпаратын бақылауды ұсыну жеке деректерді қорғаудың негізгі элементі болып табылады және жеке сектордың мүдделері мен жеке тұлға құқықтары арасындағы тепе-теңдікті нығайтады. Жеке деректерді жинайтын және өндейтін ұйымдар осы принциптердің сақталуына жауап береді және қабылданған стандарттарға сәйкестігін көрсетуге дайын болуы керек. Бұл қағида ішкі және сыртқы бақылау тетіктерін құруды, сондай-ақ нормаларды бұзғаны үшін жауапкершілікті білдіреді. Бұл азаматтар тарапынан да, халықаралық қоғамдастық тарапынан да сенім деңгейін арттыруға ықпал етеді. ЭЫДҰ нұсқауларының басқа құқықтық актілерден ең негізгі ерекшелігі ол дербес деректердің трансшекаралық ағыны болып табылады. Мұндағы негізгі ереже басшылық қағидаттарына сай деректерді алушы ел жеке ақпаратты қорғаудың жоғарғы деңгейін қамтамасыз еткен жағдайда дербес деректерді трансшекаралық беру мүмкіндігіне ие бола алады. Әйтпесе, деректер халықаралық контексте азаматтардың құқықтарын қорғауға кепілдік бере отырып, субъектінің келісімі немесе басқа құқықтық негіздер негізінде ғана берілуі мүмкін. Нұсқаулықтар деректерді қорғаудың бірыңғай халықаралық тәсілін құруға зор ықпал етеді, бұл әсіресе трансұлттық корпорациялар мен халықаралық ұйымдар үшін өте маңызды. Кейбір жағдайларда мемлекеттер ЭЫДҰ талаптарын өздерінің келісім шарттарына енгізеді, бұл трансшекаралық ақпарат алмасу процедурасын жеңілдетеді және әкімшілік кедергілерді азайтады. Көптеген елдердің жеке деректерді қорғау туралы ұлттық заңдарын әзірлеу кезінде ЭЫДҰ талаптарына назар аударады. Мысалы, Еуропалық GDPR негізінен жинауды шектеу, ашықтық және жауапкершілік талаптарындағы идеяны осы нұсқаулықтардың әмбебаптығы мен өзектілігінен көрсетеді.

2017 жылғы маусымда Қазақстан Экономикалық ынтымақтастық және

даму ұйымының (бұдан әрі – ЭЫДҰ) Инвестициялар жөніндегі комитетінің қауымдастырылған мүшесі болды және ЭЫДҰ Халықаралық инвестициялар және көпұлтты кәсіпорындар туралы декларациясына қосылған 48-ел болды [45]. ЭЫДҰ-ның басшылық қағидаттары адам құқықтары, еңбек құқықтары, қоршаған орта, парақорлық және сыбайлас жемқорлық, тұтынушылардың мүдделері, ақпаратты ашу, ғылым мен технология, бәсекелестік және салық салуды қоса алғанда, іскерлік жауапкершіліктің барлық негізгі салаларын қамтиды. Құпиялылықты қорғау және дербес деректердің трансшекаралық ағыны бойынша ЭЫДҰ нұсқаулары деректерді қорғау саласындағы халықаралық реттеудің іргетастарының бірі болып қала береді. Олардың әмбебап сипаты мен ақпарат бостандығы мен жеке құқықтар арасындағы тепе-теңдікке бағдарлануы қазіргі заманғы стандарттардың қалыптасуына ықпал етті, соның ішінде GDPR сияқты міндетті ережелердің дамуына әсер етті. Өзінің ұсынымдық сипатына қарамастан, бұл қағидаттар дербес деректерді қорғаудың ұлттық және халықаралық тәсілдерін үйлестіруде маңызды рөл атқаруды жалғастыруда, сондай-ақ қоғамның цифрлық трансформациясы жағдайында нормативтік базаны одан әрі жетілдіруді ынталандырады.

APEC Privacy Framework - бұл жеке деректерді қорғау мен Азия-Тынық мұхиты елдері арасындағы ақпараттың еркін қозғалысы арасындағы тепе-теңдікті қамтамасыз етуге арналған принциптер мен ұсыныстар жиынтығы. Бұл құжат жеке ақпараттың барлық түрлерін қамтығанымен, оның принциптері биометриялық идентификаторлар (саусақ іздері, бетті тану, дауыстық деректер және т.б.) сияқты жоғары сезімтал деректермен жұмыс істеу кезінде ерекше маңызға ие. Қазіргі цифрлық әлемде биометриялық деректерді қорғау әсіресе маңызды болып табылады, өйткені оларды бұзу қайтарымсыз салдарға әкелуі мүмкін. APEC Privacy Framework қатаң міндетті ереже емес, керісінше APEC Privacy Framework -ке мүше мемлекеттер үшін ұсыныстар мен ең жақсы тәжірибелерді көздейді. Оны қолдану өңірдегі деректерді қорғау саласында бірыңғай стандарттарды әзірлеуге ықпал етеді, бұл трансшекаралық ынтымақтастықты жеңілдетеді және цифрлық экономиканың дамуына ықпал етеді. APEC Privacy Framework жеке ақпараттың барлық түрлеріне қолданылатын бірнеше негізгі принциптерге сүйенеді:

- Хабарлама принципі: деректерді жинауды жүзеге асыратын кез келген ұйым субъектіні өңдеу мақсаттары мен тәсілдері, сондай-ақ биометриялық ақпаратты өңдеумен байланысты ықтимал тәуекелдер туралы хабардар етуге міндетті.
- Жинауды шектеу принципі: деректерді жинау нақты, заңды мақсаттарға жету үшін қажетті көлемде ғана жүзеге асырылуы керек. Бұл ереже биометрика үшін өте маңызды, өйткені оны шамадан тыс пайдалану құпиялылықтың бұзылуына әкелуі мүмкін.
- Қауіпсіздікті қамтамасыз ету принципі: деректерді өңдеу және сақтау шифрлау, қол жеткізуді бақылау және қауіпсіздік жүйелеріне тұрақты аудит жүргізу сияқты заманауи қорғаныс шараларын қолдануды талап етеді. Биометриялық мәліметтер үшін бұл ереже олардың бірегейлігі мен сезімталдығына байланысты өте маңызды.

•Қол жеткізу және түзету принципі: деректер субъектілері олардың деректері қалай және қандай мақсатта пайдаланылатыны туралы ақпарат ала алуы керек, сонымен қатар қателер болған жағдайда түзетулер енгізуді талап етуі керек.[46]

APEC Privacy Framework биометриялық деректерді бөлек санатқа бөлмегенімен, оның принциптері оларға да қатысты. Биометриялық мәліметтермен жұмыс істейтін компаниялар пайдаланушыларға ақпаратты жинау мақсаттары мен өңдеу әдістері туралы нақты ақпарат беруге міндетті. Бұған бетті тану деректері немесе саусақ іздері сияқты қалай және не үшін қолданылатыны туралы егжей-тегжейлі сипаттама ақпараттары кіреді. Ұйымдар көп факторлы аутентификация, деректерді шифрлау және қауіпсіздікті үнемі бақылау сияқты заманауи қорғаныс әдістерін қолдануы керек. Бұл шаралар биометриялық ақпарат үшін маңызды болып табылатын рұқсатсыз кіру мен ағып кетудің алдын алуға көмектеседі. Биометриялық деректерді жинау тек көрсетілген функцияларды орындау үшін қажет көлеммен шектелуі керек. Бұл деректер бұзылған жағдайда ықтимал зиянды азайтуға көмектеседі. Нақты принциптерге қарамастан, APEC Privacy Framework биометриялық деректерге қолдану бірқатар мәселелермен қатар жүреді. Олар технологиялық күрделілік заманауи қорғаныс шараларын жүзеге асыру технологиялар мен инфрақұрылымға қомақты инвестицияларды, сондай-ақ қауіпсіздік жүйелерін үнемі жаңартуды талап етеді. APEC елдерінде дербес деректерді қорғау туралы заңнамада ұлттық айырмашылықтар байқалады, бұл ақпаратты трансшекаралық беру кезінде жаңа мәселелердің туындауына себеп болады. APEC Privacy Framework жеке деректерді, соның ішінде биометриялық деректерді қорғаудың кешенді негізін ұсынады. Оның принциптерін қолдана отырып, ұйымдар биометриялық ақпаратты өңдеу кезінде қауіпсіздік пен ашықтықтың жоғары деңгейін қамтамасыз ете алады, бұл Азия-Тынық мұхиты аймағында пайдаланушылардың сенімін сақтауға және цифрлық экономиканың тұрақты дамуына ықпал етеді.

Халықаралық стандарттар ақпараттық технологиялар, қауіпсіздік, денсаулық сақтау, өнеркәсіп және басқа салаларды қоса алғанда, әртүрлі қызмет салаларында маңызды рөл атқарады. Олар өнімнің, қызметтердің және процестердің сапасына, қауіпсіздігіне, үйлесімділігіне және тиімділігіне бірыңғай талаптар қояды. Биометриялық деректер мен биометриялық технологиялар саласында стандарттардың да әсері маңызды, өйткені олар сәйкестендіру жүйелерінің сенімділігін, қауіпсіздігін және бірізділігін қамтамасыз етеді. Стандарттар биометриялық технологиялардың қауіпсіздігін, тиімділігін және үйлесімділігін қамтамасыз ету үшін қажет. Олар тәуекелдерді азайтуға, алаяқтықтың алдын алуға және жаһандық деңгейде қолдануға болатын сенімді сәйкестендіру жүйелерін құруға көмектеседі. Биометриялық жүйелердің үйлесімділігін, сенімділігі мен қауіпсіздігін қамтамасыз ету үшін ISO (халықаралық стандарттау ұйымы) және IEC (Халықаралық электротехникалық комиссия) сияқты жетекші ұйымдардың ұсыныстарына негізделген халықаралық стандарттар әзірленді. Бұл стандарттар деректер алмасу

форматтарынан бастап өнімділігін бағалауға және ақпаратты қорғауға дейінгі көптеген мәселелерді қамтиды.

ISO/IEC сериясы 19794 – биометриялық алмасу форматтары. ISO/IEC 19794 сериясы биометриялық ақпаратты сақтау мен бөлісудің бірыңғай форматтарын анықтауға арналған. Ол әртүрлі биометриялық жүйелерді (мысалы, саусақ іздері, бет суреттері, қолмен жазылған қолтаңба деректері және т.б.) қамтиды және биометриялық деректермен бірге құрылымға, өңдеуге қойылатын талаптарды белгілейді[47]. Оның ішінде стандарт әртүрлі өндірушілердің құрылғылары мен жүйелері арасындағы үйлесімділікті қамтамасыз етеді, бұл масштабталатын және бір-бірін алмастыратын шешімдер жасауға мүмкіндік береді. Бұл әсіресе биометриялық деректерді жаһандық сәйкестендіру жүйелеріне біріктіру кезінде маңызды. Деректерді пішімдеу сериясы бұл белгілі бір форматтар жүйелерге жіберілген деректерді біржақты түсіндіруге мүмкіндік береді, бұл ақпарат алмасу кезінде қателіктер қаупін азайтады. Дегенмен, бұл стандарт негізінен тасымалдау немесе сақтау қауіпсіздігі шараларына емес, кодтаудың техникалық аспектілеріне бағытталған қызмет атқарады. Бұл стандарт деректерді құрылымдауға және бөлісуге бағытталғандықтан, қорғау және құпиялылық мәселелері көбінесе оның пәндік саласынан тыс. Бұл дегеніміз, осы форматтарды қолданатын ұйымдар деректерді рұқсатсыз кіруден қорғау үшін қосымша шаралар қабылдауы керек. ISO / IEC 19794 биометриялық мәліметтерді ұсынуды біріктіруде іргелі рөл атқарады, бұл өзара байланысты жүйелердің дамуына ықпал етеді. Бұл ретте ақпараттың толық қорғалуын қамтамасыз ету үшін басқа да стандарттар мен қауіпсіздік шараларын кешенді қолдану қажет.

ISO/IEC сериясы 19795 – биометриялық жүйелердің өнімділігін бағалау стандарты. ISO/IEC 19795 сериялы стандарттары биометриялық жүйелердің тиімділігін объективті бағалауға арналған. Олар тестілеу әдістерін, бағалау критерийлерін (мысалы, жалған оң және жалған теріс позитивтердің көрсеткіштері) және сынақ процедураларын анықтайды [48]. Негізгі аспектілерінің бірі стандарттар бақыланатын жағдайларда әртүрлі жүйелердің тиімділігін салыстыруға мүмкіндік беретін тестілеудің әмбебап тәсілдерін сипаттайды. Бұл биометриялық технологиялар нарығында сенімді шешімді таңдау үшін өте маңызды. Жақсы анықталған көрсеткіштермен (мысалы, FAR және FRR) пайдаланушылар мен әзірлеушілер жүйенің мәлімделген өнімділік пен қауіпсіздік талаптарына қаншалықты сәйкес келетінін объективті түрде бағалауға мүмкіндік алады. Стандарттар жүйелерді салыстыруға ғана емес, сонымен қатар технологияны жетілдіру бағыттарын анықтауға көмектеседі. Алайда, жасанды интеллект әдістерінің қолданылуы мен жаңа биометриялық технологиялардың қарқынды дамуымен қолданыстағы әдістер мерзімді жаңартуды қажет етеді.

ISO/IEC 24745 – биометриялық ақпаратты қорғау стандарты. Бұл стандарт биометриялық деректерді жинау мен сақтаудан бастап, беру мен өңдеуге дейінгі барлық кезеңдерінде қауіпсіздік пен қорғау мәселелеріне бағытталған. Ол криптографиялық қорғау әдістерін, қол жетімділікті бақылауды және ағып кетуге немесе биометриялық ақпаратты рұқсатсыз пайдалануға байланысты

тәуекелдерді басқаруды қарастырады [49]. ISO / IEC 24745 биометриялық деректерді қорғаудың техникалық және ұйымдастырушылық шараларын қамтиды. Ол криптографиялық алгоритмдерді таңдау, аутентификация жүйелеріндегі деректерді қорғау әдістері және қол жеткізуді басқару механизмдері бойынша ұсыныстар береді. Стандарт дербес деректерді қорғау туралы заңнаманың заманауи талаптарын ескереді. Бұл ұйымдарға құпия ақпаратты қорғаудың халықаралық және ұлттық ережелеріне сәйкес шешімдерді әзірлеуге көмектеседі. ISO / IEC 24745 биометриялық өңдеумен айналысатын кез келген адам үшін негізгі құжат болып табылады, өйткені ол техникалық ұсыныстарды ақпаратты қорғаудың құқықтық және этикалық аспектілерімен біріктіреді.

ISO/IEC 30107 сериясы – биометриялық жүйелерге шабуылдарды анықтау стандарты. ISO/IEC 30107 сериясы шабуылдаушылар жалған немесе өзгертілген үлгілерді (мысалы, фотосуреттер, маскалар, кескін құрылғыларында ойнатылған басып шығарулар) пайдаланып биометриялық жүйелерді алдауға тырысатын шабуылдарды анықтау әдістерін әзірлеуге бағытталған [50]. Серия стандарттары жүйелердің алдау әрекеттерін анықтау қабілетін бағалау үшін критерийлер мен сынақ әдістерін белгілейді. Бұл аутентификацияның сенімділігін қамтамасыз ету үшін өте маңызды, өйткені қазіргі таңда жасанды интеллекттің пайда болуымен шабуылдардың түрлері де күрделене түсуде. Стандартты тестілеу параметрлерін анықтау әзірлеушілерге манипуляция әрекеттеріне тұрақты жауап бере алатын жүйелерді құруға және пайдаланушыларға таңдалған шешімнің қауіпсіздігін бағалауға көмектеседі.

Қарастырылған стандарттардың әрқайсысы биометриялық мәліметтермен жұмыс істеудің белгілі бір аспектісіне әсер етеді. Алмасу форматтары (ISO/IEC 19794) деректердің құрылымдық көрінісі мен үйлесімділігін қамтамасыз етеді. Өнімділікті бағалау (ISO/IEC 19795) жүйелерді сенімділік пен тиімділік бойынша объективті салыстыруға мүмкіндік береді. Деректерді қорғау (ISO/IEC 24745) ақпараттың кешенді қауіпсіздігі мен құпиялылығына бағытталған. Шабуылдарды анықтау (ISO/IEC 30107) алаяқтық жүйені айналып өту әрекеттеріне қарсы тұруға бағытталған. Біріктірілген бұл стандарттар қауіпсіздік пен функционалды талаптарына жауап беретін заманауи биометриялық жүйелерді әзірлеу, енгізу және пайдалану үшін негіз болады. Сонымен қатар, бірнеше стандарттардың интеграциясы әр жеке құжаттың қиындықтарын өтеуге және биометриялық технологиялардың кешенді қорғанысы мен тиімділігін қамтамасыз етуге мүмкіндік береді. Бұл халықаралық стандарттар дербес деректерді қорғаудың жалпы регламенті GDPR мен қатар қолданыста жүреді. Мемлекеттік секторлар, банк қызмет саласы, денсаулық сақтау және басқада техникаларды қолдану кезінде осы стандарттарға сай жасайды. Осы стандарттардың қолданылуын мысалдармен қарастырсақ. Citibank және HSBC сияқты ірі банктер бет пен саусақ ізін сканерлеу арқылы клиенттерге биометриялық аутентификацияны енгізді. 2023 жылы HSBC Ұлыбританиядағы клиенттердің 55% - ы жалған биометриялық шабуылдардан қорғану үшін ISO/IEC 30107 стандартына сәйкес келетін биометрия арқылы мобильді банкке кіруді таңдайтынын хабарлады.[50]

Стандарттар қалай қолданылады ? GDPR регламентіне сәйкес клиенттердің биометриялық деректері қорғалған, пайдаланушылар оларды өңдеуге нақты өзінің келісімін береді. ISO/IEC 27001: Банк қауіпсіздікті басқару жүйелерін, соның ішінде көп факторлы аутентификацияны дамытады. ISO/IEC 30107: жүйені айналып өту үшін жалған саусақ іздері мен фотосуреттерден қорғау әдістері қолданылады.[50]

Стандарттардың мемлекеттік секторда қолданылуы мысалы, 2021 жылдан бастап Еуропалық Одақ елдері ISO/IEC 19794-5 (бет биометриялық бейнелеу стандарты) стандартына сәйкес саусақ іздері мен бет сканерлеуі бар биометриялық төлқұжаттарды беруге міндетті [47]. Мұнда ISO / IEC 19794: биометриялық төлқұжаттар деректерді сақтаудың бірыңғай форматтарын қолданады, бұл оларды халықаралық мәліметтер базасында тексеруге мүмкіндік береді. ISO / IEC 30107: жалған саусақ іздерін анықтау алгоритмдерін әзірлейді. Ал GDPR регламенті бойынша азаматтар төлқұжатының күші жойылған жағдайда деректерді жоюды сұрауға құқылы.

Apple және Samsung құрылғыларына қауіпсіз кіру үшін биометриялық аутентификация жүйелерін (бетті сканерлеу, саусақ ізі) сияқты технологияларды қолданады. Бұл жерде мына стандарттар қолданылады. ISO/IEC 30107: жалған фотосуреттер мен 3D маскалардан қорғаудың кіріктірілген механизмдерін пайдаланады. ISO/IEC 27001: пайдаланушы деректері шифрланады және құрылғыны қорғалған чипте сақталады. GDPR регламентіне сәйкес пайдаланушы биометрияны өшіріп, деректерін жоя алады. Бұл мысалдар стандарттар жеке деректерді қорғауды қамтамасыз етіп қана қоймай, қауіпсіз цифрлық технологияларды дамытуға ықпал ететінін көрсетеді.

GDPR, ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 19794, ISO/IEC 30107, ISO/IEC 24745 сияқты халықаралық стандарттар жеке деректер мен биометриялық ақпаратты қорғау үшін сенімді негіз жасайды. Алайда оларды қолдану кезінде бірқатар құқықтық, техникалық, этикалық және ұйымдастырушылық мәселелер туындайды. Мәселен ұлттық заңдар мен халықаралық стандарттар арасындағы сәйкессіздіктер туындауы. Әр түрлі елдер стандарттарды ұлттық заңнамаға сай бейімдейді. Мысалы, GDPR Еуропалық Одақ елдерінде жұмыс істейді, бірақ АҚШ-та GDPR-ге ұқсас бірыңғай федералды заң жоқ. Сонымен қатар, биометриялық деректерді өңдеуге келісім беру мәселесі ауқымды. Стандарттар биометриялық деректерді тек нақты келісіммен жинауды талап етеді (GDPR, ISO/IEC 27701). Алайда, мемлекеттік жүйелерде (мысалы, биометриялық төлқұжат алған кезде) азаматтар деректерді өңдеуден бас тарта алмайды, келісімсізде өңделетін жағдайлар орын алады. Тағы бір өткір мәселе, GDPR биометрияны негізсіз өңдеуге тыйым салады, бірақ Қытай сияқты елдерде бетті танудың жаппай бейнебақылау жүйелері жұмыс жасайды. 2023 жылы Amnesty International зерттеуі бойынша Қытайдағы қалалардың 75% -да GDPR-ге сәйкес келмейтін биометриялық бетті тану камералары бар екенін анықтады. Бұл азаматтардың құқығын тікелей бұзу және жаппай бақылау болып табылады. GDPR (ЕО деректерді қорғаудың жалпы ережесі), ISO/IEC 24745 (Ақпараттық технологиялар – биометриялық ақпарат), Еуропа Кеңесінің №108 конвенциясы және ұлттық заңнамалық актілер сияқты

халықаралық стандарттар биометриялық ақпаратты қауіпсіз жинауға, өңдеуге және сақтауға құқықтық негіз береді. Бұл стандарттар деректердің бұзылу, биометриялық ақпаратты теріс пайдалану және адам құқықтарын бұзу қаупін азайтуға бағытталған. Олар деректерді өңдеу принциптерін, түпнұсқалықты, тұтастықты және құпиялылықты қамтамасыз етуді және рұқсатсыз кіруден қорғау механизмдерін қоса алғанда, негізгі аспектілерді реттейді.

3.2 Қазақстандағы және шет елдердегі биометриялық технологияларды пайдалануды салыстырмалы құқықтық талдау

Қазақстанда биометриялық технологиялар мемлекеттік қызметтер, қаржы институттары, күзет және қауіпсіздік қызметтері, денсаулық сақтау және көлік жүйелерінде кеңінен қолданылады. 2015 жылы Қазақстан Республикасы электрондық үкімет (eGov) жүйесінде азаматтарды аутентификациялау үшін саусақ іздері мен бет-әлпетті тану технологияларын енгізе бастады. Сонымен қатар, 2020 жылдан бастап банктер мен мобильді операторлар қашықтықтан сәйкестендіру үшін Face ID, дауысты тану және биометриялық деректерді қолдану арқылы қызмет көрсетуге көшті. Алайда, биометриялық деректердің құпиялылығы, деректерді қорғау, жеке өмірге қол сұғылмаушылық, сондай-ақ олардың құқықтық негіздері мәселелері әлі де өзекті. Қазақстан Республикасында биометриялық деректерді қоса алғанда, дербес деректерді өңдеуге байланысты мәселелерді реттеу бірінші кезекте "дербес деректер және оларды қорғау туралы" Заңның негізінде жүзеге асырылады. Бұл заңда дербес деректерді өңдеу, жинау, сақтау, пайдалану қалай жүзеге асырылатыны, сонымен қатар дербес деректер субъектісінің құқықтары мен міндеттері жайлы нормаларды қарастырады. Жоғарыдағы бөлімдерде айтып өткеніміздей, биометриялық деректерге тек анықтама беріліп өткен. Ал оның қорғалуы мен пайдалануы жағынан ешқандай айрықша нормалар қарастырылмаған. Дербес деректер субъектісінің оларды өңдеуге, оның ішінде биометриялық деректерге нақты келісімін алу талабы ашық көрсетілмеген. Қолданыстағы "Дербес деректер және оларды қорғау туралы" Заң биометриялық деректерді өңдеу бойынша толықтай жетілдірілмеген және халықаралық стандарттарға толық сәйкес келмейді. Сондықтан Қазақстанда биометриялық технологияларды қолдануды құқықтық реттеу жүйесін жетілдіру, заманауи қауіптерді ескере отырып заңнаманы жаңарту және азаматтардың жеке деректерінің қауіпсіздігін қамтамасыз ету қажеттілігі туындайды. Қазақстан Республикасында биометриялық технологияларды пайдалану мынадай негізгі нормативтік-құқықтық актілермен реттеледі.

Ең алдымен негізгі заң "Дербес деректер және оларды қорғау туралы" Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы, бұл заң биометриялық деректерді қоса алғанда, дербес деректерді жинауға, өңдеуге және қорғауға байланысты қызметтің құқықтық негіздерін белгілейді. Заң жеке тұлғаға қатысты барлық дербес деректерді өңдеу, жинау және қорғау бойынша жұмыс жасайды. Деректер қолжетімді және қол жетімділігі шектеулі болып екі санатқа бөлінеді. Биометриялық технологиялардың көмегімен алынған

деректерді (саусақ іздері, бет пішіні, көздің ирисі және т.б. туралы деректер) қоса алғанда, жеке тұлғаны сәйкестендіруге мүмкіндік беретін барлық ақпаратты қамтиды. Биометриялық деректерді өңдеуге субъектінің нақты және ақпараттандырылған келісімі болған жағдайда ғана жол беріледі. Бұл дегеніміз, адам өзінің биометриялық деректерін өңдеудің мақсаттары, тәсілдері және ықтимал қауіптері туралы толық хабардар болған кезде және оның келісімі белгіленген тәртіппен рәсімделген кезде оның деректерін пайдалана алады. Заңның 8-бабына сай субъект немесе оның заңды өкілі дербес деректерді жинауға, өңдеуге жазбаша, мемлекеттік сервис, мемлекеттік емес сервис арқылы не келісімді алғанын растауға мүмкіндік беретін өзге де тәсілмен келісім береді және оны кері қайтарып алуға құқығы бар. Мемлекеттік органдардың және мемлекеттік заңды тұлғалардың ақпараттандыру объектілеріндегі дербес деректерді жинау және өңдеу кезінде келісім мемлекеттік сервис арқылы беріледі [30]. Сондықтан да мемлекеттік қызметтерді алу кезінде субъектінің дербес деректерін пайдалану арқылы жүзеге асырылады. Сондай ақ субъект немесе оның заңды өкілі дербес деректерді жинауға, өңдеуге берген келісімді, егер бұл Қазақстан Республикасының заңдарына қайшы келсе не орындалмаған міндеттемесі болған кезде кері қайтарып ала алмайды. Дербес деректер туралы заңы принциптермен қатаң жұмыс жасайды. Заң биометриялық деректерді жинау және пайдалану белгіленген мақсаттар шегінде қатаң түрде жүзеге асырылуы керек деп ұйғарады. Өңдеу заңдылық, қажеттілік және мақсатты шектеу қағидаттарына сәйкес келуі керек деректерді қосымша келісімсіз немесе басқа құқықтық негізсіз басқа мақсаттарда пайдалануға болмайды. Ал қауіпсіздік шараларына келетін болсақ, деректерді сақтауға және оны қорғауға мемлекет өзі кепілдік береді және уәкілетте органдармен жүзеге асырылады делінген. Биометриялық ақпаратты өңдеу кезінде операторлар арнайы техникалық және ұйымдастырушылық қорғау шараларын қолдануға міндетті. Дербес деректер иесінің келісімін алу және деректердің базада болуына да жауапты операторлар. ҚР дербес деректерді бұзғаны үшін әкімшілік және қылмыстық жауапкершілік қарастырылған. ҚР-ның Әкімшілік құқық бұзушылық кодексінің 79 бабына сәйкес егер құқық бұзушылық әрекетінде қылмыстық жазаланатын белгілер болмаған жағдайда, дербес деректерді заңсыз жинау немесе өңдеу жеке тұлғаларға – 10 АЕК, лауазымды адамдарға, жекеше нотариустарға, жеке сот орындаушыларына, адвокаттарға, шағын кәсіпкерлік субъектілеріне немесе коммерциялық емес ұйымдарға – 20 АЕК, орта кәсіпкерлік субъектілеріне – 30 АЕК, ірі кәсіпкерлік субъектілеріне 70 АЕК айыппұл салуға әкеп соғады. Егер дәл осы әрекеттерді меншік иесі, оператор немесе үшінші тұлға өз қызмет бабын пайдалана отырып жасаған кезде – жеке тұлғаларға – 50 АЕК , лауазымды адамдарға, шағын кәсіпкерлік субъектілеріне немесе коммерциялық емес ұйымдарға – 75 АЕК, орта кәсіпкерлік субъектілеріне – 1000 АЕК, ірі кәсіпкерлік субъектілеріне 200 АЕК мөлшерінде айыппұл салуға әкеп соғады[54]. Дәл осы баптың басқада тармақтарымен дербес деректерді қорғау шараларын сақтамау және заңсыз жинау, дербес деректерді жоғалту туралы құқықтық іс әрекеттер кезінде айыппұл мөлшері ұлғайа түседі. Дербес

деректерді пайдалану, жинау, өңдеу кезінде қылмыстық іс әрекет белгілері табылған жағдайда ҚР Қылмыстық кодексімен жауаптылық қарастырылады. Қылмыстық Кодексінің 147-бабы «Жеке өмірге қол сұғылмаушылықты және Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасын бұзу» егер дербес деректерді қорғау жөніндегі шараларды қолдану міндеті жүктелген адамның мұндай шараларды сақтамауы, егер бұл іс-әрекет адамдардың құқықтары мен заңды мүдделеріне елеулі зиян келтірсе, белгілі бір лауазымдарды атқару немесе белгілі бір қызметпен айналысу құқығынан үш жылға дейінгі мерзімге айыра отырып немесе онсыз, 3000 АЕК дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзету жұмыстарына не алты жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не екі жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады. Адамның жеке немесе отбасы құпиясын құрайтын, жеке өмірі туралы мәліметтерді оның келісімінсіз заңсыз жинау не өзге де дербес деректерді заңсыз жинау және (немесе) өңдеу (таратуды қоспағанда) нәтижесінде адамның құқықтары мен заңды мүдделеріне елеулі зиян келтіру – 5000 АЕК дейінгі мөлшерде айыппұл салуға не сол мөлшерде түзету жұмыстарына не сегіз жүз сағатқа дейінгі мерзімге қоғамдық жұмыстарға тартуға не үш жылға дейінгі мерзімге бас бостандығын шектеуге не сол мерзімге бас бостандығынан айыруға жазаланады [55]. Дербес деректер заңнамасындағы нормаларды сақтамағаны үшін және субъектінің деректерін заңсыз игеріп пайдаланғаны үшін, құқықтық салдарына қарай әкімшілік және қылмыстық жауапкершіліктер қарастырылған.

Қазақстандағы биометриялық технологияны іске асыру кезінде қолданылатын екінші заң «Дактилоскопиялық және геномдық тіркеу» туралы 2016 жылғы 30 желтоқсандағы № 40-VI Қазақстан Республикасының Заңы[33]. Құжат саусақ ізі мен геномдық тіркеуді жүргізу тәртібін, сондай-ақ тиісті ақпаратты жинау, өңдеу және қорғау шарттарын айқындайды. Заңның 6-бабында дактилоскопиялық және (немесе) геномдық тіркеу саласындағы уәкілетті мемлекеттік органдардың өз құзыреті шегінде дактилоскопиялық ақпаратты жинауға, өңдеуге немесе геномдық ақпаратты жинауға, өңдеуге, қорғауға, биологиялық материалды іріктеуге, сақтауға, пайдалануға және жоюға құқығы бар делінген, осыдан ақ бұл ақпараттарды жинайтын тек мемлекеттік органдар екенін білеміз. Бұл ақпараттар трансшекаралық беруге жатпайтын, қол жетімділігі шектеулі дерекке жатады. Бұл заң аясында дактилоскопиялық тіркеу және геномдық тіркеу туралы барлық іс шаралар туралы нормалар көзделген. Адамның биологиялық материалдары туралы деректер жатады. Оның ішінде шекарадан өту кезінде және жеке басын куәландыратын куәлік алу кезінде он алты жасқа толған адам өзінің келісімімен дактилоскопиялық тіркеуге жатады. Саусақ іздерін сканерлеу арқылы базаға енгізеді. Дактилоскопиялық және геномдық ақпаратты қорғау Қазақстан Республикасының ақпараттандыру туралы, дербес деректер және оларды қорғау, мемлекеттік құпиялар туралы заңнамасына сәйкес жүзеге асырылады.

Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2024 жылғы 16 тамыздағы № 56 қаулысы [35]. Осы қаулымен

«банктердің, банк қызметтерінің жекелеген түрлерін жүзеге асыратын ұйымдардың және микроқаржы ұйымдарының биометриялық сәйкестендіруді жүргізу қағидалары» туралы нормалар бекітілді. Ережелер қаржы секторында биометриялық сәйкестендіруді қолдану тәртібін белгілейді. Атап айтқанда идентификаттау өткізілетін адамның бет бейнесі бойынша биометриялық идентификаттау тәртібінің барлық кезеңдері және биометриялық деректерді пайдалану мен қорғау қағидаттарын бекітетін ережелерді қамтиды. Бұл Нормативтік-құқықтық актілер дербес деректерді қорғауды қамтамасыз ете отырып және оларды өңдеу мен пайдалану тәртібін айқындай отырып, Қазақстанда биометриялық технологияларды пайдалануды құқықтық реттеу үшін негіз қалыптастырады. Қазақстан Республикасында биометриялық технологияларды құқықтық реттеуге байланысты бірнеше маңызды проблемалар бар. Олардың негізгілері заңнамалық жетілмегендік, деректердің қорғалуының әлсіздігі, азаматтардың жеке өміріне қатысты құқықтық кепілдіктердің жеткіліксіздігі және киберқауіпсіздік тәуекелдері болып табылады.

Біріншіден, құқықтық негіздің жеткіліксіздігі және реттеу нормаларының нақты айқындалмауы мәселесі бар. Қазақстан Республикасының "Дербес деректер және оларды қорғау туралы" заңы биометриялық деректерді қорғау бойынша жалпы ережелерді қамтығанымен, бұл заңдағы нормалар техникалық және құқықтық талаптар деңгейінде толыққанды реттелмеген. Нақтырақ айтқанда, биометриялық деректерді жинау шарттары, оларды сақтау мерзімі және үшінші тұлғаларға беру талаптары туралы құқықтық нормалар әлсіз сипатқа ие.

Екіншіден, мемлекеттік бақылау механизмдерінің әлсіздігі биометриялық деректердің қауіпсіздігін қамтамасыз етуде айтарлықтай қиындықтар туғызуда. Қазақстанда биометриялық деректерді бақылау мен басқару жөніндегі тәуелсіз орган жоқ, бұл жеке компаниялар мен мемлекеттік органдар тарапынан биометриялық ақпаратты заңсыз пайдалануға жол ашуы мүмкін. Азаматтар өздерінің биометриялық деректерін кім, қандай мақсатта өңдеп жатқанын біле алмайды және осыған қатысты заңды шағымдану механизмдері жеткіліксіз.

Үшіншіден, халықаралық тәжірибемен салыстырғанда Қазақстанның биометриялық деректерді қорғау жүйесі айтарлықтай артта қалған. GDPR стандарттарына сәйкес, Еуропада биометриялық деректерді өңдеу үшін азаматтың нақты келісімі қажет және ол деректерді кез келген уақытта жоюға құқылы. Сонымен қатар, АҚШ-та Иллинойс штатының BIPA заңы компаниялардан биометриялық деректерді жинауға рұқсат алуды талап етеді және оларды рұқсатсыз қолданған жағдайда ауыр айыппұлдар қарастырылған. Қазақстанда мұндай нақты тетіктер жоқ, бұл азаматтардың деректерін қорғау деңгейінің төмендігін көрсетеді.

GDPR-дегі деректерді қорғау ережелерін сақтамағаны үшін айыппұлдар бизнес үшін 20 000 000 еуроға дейін немесе компанияның жылдық айналымының 4%-на дейін жетуі мүмкін. Жауапкершілікке тарту жағдайларының басым бөлігі ақпараттық қауіпсіздікке, биометрияға және сақтау мерзіміне байланысты бұзушылықтар шеңберінде шетелдік компанияларға

қатысты. Сондай-ақ, GDPR ЕО-да орналасқан еншілес компаниялардың қызметіне тыйым салуды қоса алғанда, интернет-ресурсты немесе қосымшаны бұғаттау мүмкіндігін қарастыра алады [11]. Бұл GDPR регламентінің қатаң құқықтық санкциясы. GDPR компаниялар жиналған жеке деректер үшін жауап беруі керек екенін анық көрсетеді. Ақпарат шынымен де құнды, сондықтан компаниялар кез келген басқа актив сияқты оның қауіпсіздігін қамтамасыз ету үшін заңды жауапкершілікке ие. Аудит жүргізу арқылы жеке деректердің қалай алынғанын ғана емес, сонымен бірге олардың қалай қорғалғанын да бағалауға болады.

Америка Құрама Штаттарында биометриялық өңдеуді реттейтін бірыңғай федералды заң жоқ, дегенмен бірқатар штаттар өздерінің деректерді өңдеуге қатысты ережелерін қабылдаған. Американың заң жүйесі федералды және штаттық заңдармен бөлінеді. Сондықтан да азаматтардың дербес деректерін өңдеу жөніндегі қызметті реттейтін мемлекеттік органдар осы саладағы компания операторлары үшін екі нормативтік акт қабылдады. Ол Privacy Act of 1974 және Privacy Protection Act of 198 тек федералды органдармен ғана қолданылуға жатады. Оларда деректердің құпиялылық режимін реттейтін техникалық нормалар болғандықтан, компаниялар оларды өз қызметін ұйымдастыру бойынша ұсыныстар ретінде пайдалана алады. Дербес деректерді қорғауға байланысты даулар туындаған жағдайда, сот бұл актілерге емес, негізгі сот практикасына жүгінеді [57]. Федералды деңгейде биометриялық технологияларға қатысты мәселелер бірнеше актілермен қозғалады, бірақ олардың ешқайсысы биометрияға мамандандырылған емес. АҚШ тың көптеген нормативтік ережелері жеке деректерді тұтастай қорғайды, бірақ олар биометриялық ақпарат бойынша арнайы нұсқаулар бермейді.

Биометриялық ақпараттың құпиялылығы туралы Заң (BIPA) 2008 жылы қабылданған Иллинойс Заңы биометриялық деректерге қатысты ең қатаң ережелердің бірі болып табылады. Ол биометриялық деректерді жинайтын компаниялардан (саусақ іздері, бет сканерлері, ирис және т.б.) деректер субъектісінің жазбаша ақпараттандырылған келісімін алуды талап етеді. Заң сонымен қатар ақпаратты қорғау бойынша міндеттемелер жүктейді, сақтау мерзімдерін шектейді және бұзылған жағдайда азаматтардың зиянды өтеу құқығын қарастырады. Сот практикасына көз жүгіртсек BIPA компанияларға қарсы көптеген сот процестерінің негізі болды, нәтижесінде айтарлықтай өтемақы төленді және осы саладағы тәжірибелерді қайта қарауға түрткі болды. Жақында Иллинойс штаты биометриялық ақпараттың құпиялылығы туралы Заңға (BIPA) түзетулер енгізіп, биометриялық деректерді қорғауды айтарлықтай өзгертті. Бастапқыда 2008 жылы қабылданған BIPA компаниялардан көз сканері, бет сканері, саусақ іздері және дауыс іздері сияқты биометриялық деректерді жинауға немесе пайдалануға жазбаша келісім алуды талап етті. Бұзушылықтар орын алған жағдайда бір адамға қатысты әрбір бұзушылық үшін 1000 және 5000 доллар өтемақы төлеуі қажет еді. Алайда 2024 жылғы жаңа түзетуде бір адамның биометрикасына қатысты бірнеше бұзушылықтар енді бір ғана бұзушылық ретінде қарастырылатыны туралы өзгеріс енгізілді [58]. BIPA жеке талап қою құқығын қарастырады, яғни кез-келген азамат өз құқықтары бұзылған жағдайда

сотқа жүгіне алады. Санкциялар нақты зиянға қарамастан қолданылады, бұл заңды дербес деректерді қорғау саласындағы ең қатал заңдардың біріне айналдырады. Жиналған биометриялық деректерді сақтау мерзімі нақты белгіленген. Мәлімделген мақсаттарға қол жеткізгеннен кейін немесе белгілі бір мерзім өткеннен кейін (субъектімен соңғы байланыстан кейін 3 жылдан аспайтын) мерзімде оның деректерін түпкілікті жою рәсімдері орындалу керек. Заң деректер субъектісінің тиісті келісімінсіз биометриялық ақпаратты сатуға, беруге немесе коммерциялық пайдалануға тыйым салады. Бұл ереже осындай сезімтал ақпараттан қаржылық пайда табудың алдын алу үшін жасалған. BIPA Иллинойс штатының заңы болса да, егер олар Иллинойс азаматтарының биометриялық ақпаратын жинаса да, бұл ұлттық және тіпті халықаралық деңгейде жұмыс істейтін компанияларға әсер етеді.

CCPA Калифорнияда қабылданды және 2020 жылдың 1 қаңтарында күшіне енді. Заң штат тұрғындарына өздерінің жеке деректерін бақылауды қамтамасыз етуге бағытталған, бұл компанияларды ашықтық талаптарын сақтауға, пайдаланушыларға деректерді жинау туралы хабарлауға және олардың пайдаланылуын бақылауға мүмкіндік береді. CCPA заңына бағынатын компаниялар ақпараттарға қатысты келесі аспектілерді орындау қажет. Олар деректерді жинау туралы хабарлауға құпиялылық саясатында компаниялар жеке деректердің қандай санаттары жиналатынын, қандай мақсатта және бұл деректер қалай пайдаланылатынын нақты көрсетуі; қол жетімділік пен ашықтықты қамтамасыз ету тұтынушының сұранысы бойынша бизнес дербес деректерді жинау, пайдалану, беру және сату туралы толық ақпарат беруге міндетті; компаниялар тұтынушыларға жеке ақпаратын сатудан бас тартуға мүмкіндік беретін функционалды енгізуге міндетті. CCPA техникалық қорғаныс шараларын тікелей егжей-тегжейлі көрсетпесе де, компаниялар ағып кетудің алдын алу және жеке деректерге рұқсатсыз қол жеткізу үшін ақылға қонымды шаралар қабылдауы керек. Бизнес тексеру және аудит жүргізу мүмкіндігі үшін тұтынушылардың сұраныстары, хабарламалар және қауіпсіздік шаралары бойынша ішкі жазбаларды жүргізіп отыруы тиіс. Заң тек Калифорния компанияларына ғана емес, сонымен қатар штаттан тыс жерде болса да, Калифорния тұрғындарымен бизнес жүргізетін ұйымдарға да қатысты қолданылады.

2021 жылы қабылданған PIPL Қытайдың азаматтардың жеке деректерін қорғауға бағытталған алғашқы кешенді Заңы болды. Заң құпиялылық, ақпарат қауіпсіздігі және деректердің трансшекаралық қозғалысын бақылау мәселелерімен айналысудың жаһандық өсуі жағдайында пайда болды. Ол Еуропалық GDPR сияқты нормативтік актілердің тәжірибесін ескере отырып құрылған, бірақ сонымен бірге ұлттық саясаттың ерекшеліктері мен мемлекеттің басымдықтарын ескереді. PIPL мақсаты деректер субъектілерінің құқықтары мен заңды мүдделерін қорғау. Заңда жеке ақпаратты жинау, сақтау және өңдеу азаматтардың құқықтарын қорғауға бағытталған. Ұлттық қауіпсіздік үшін стратегиялық маңызы бар деректердің елден тыс жерлерге қалай өтетініне ерекше назар аударылады. PIPL дың 28 бабында сезімтал жеке ақпаратты бір рет жария етілгенде (leaked-ағып кеткен) немесе заңсыз пайдаланылғанда жеке

адамның қадір-қасиетіне, жеке басының немесе мүліктік қауіпсіздігіне зиян келтіруі мүмкін ақпарат ретінде анықтайды. Бұл ақпаратқа биометриялық сипаттамалар, діни нанымдар, арнайы мәртебе, денсаулық туралы ақпарат, қаржылық шоттар, орналасқан жерді бақылау және т.б., сондай-ақ 14 жасқа дейінгі балалар туралы ақпарат кіреді [59]. Бұл жағынан GDPR сияқты биометриялық деректерге айрықша санатта қарайды. PIPL Қытай азаматтарының жеке деректерін өңдеудің барлық түрлеріне қолданылады, оны мемлекеттік органдар немесе жеке компаниялар жүзеге асырады. Заң жеке тұлғаны тікелей немесе жанама түрде анықтай алатын ақпараттарды өңдеуді қамтиды. Сезімталдығы жоғары деректерге ерекше назар аударылады (мысалы: биометриялық, генетикалық, қаржылық ақпарат). Оларды өңдеу үшін қосымша қорғаныс шаралары қажет және көбінесе жеке келісім қажет етеді. PIPL заңындағы деректер субъектілерінің құқықтарына тоқталатын болсақ, ақпаратқа қол жеткізу және көшіру құқығы, азаматтар олар туралы қандай ақпарат жиналатынын және қалай пайдаланылатынын білуге құқығы бар. Қателер немесе ескірген ақпарат болған жағдайда, субъектілер өзгертулер енгізуді немесе олардың деректерін толығымен жоюды талап етуі мүмкін. Ерекше жағдайларда азамат мән-жайлар анықталғанға дейін өз деректерін өңдеуді уақытша тоқтата тұруды талап ете алады. PIPL GDPR-мен айқын ұқсастықтарға қарамастан (мысалы, заңдылық, ашықтық, деректерді азайту және субъектілердің кеңейтілген құқықтары) PIPL өз кезегінде бірқатар ерекшеліктерге ие. Қытайдағы ақпаратты мемлекеттік реттеуді күшейту жағдайында PIPL мемлекеттік органдармен тығыз қарым-қатынасты көздейді. Деректерді трансшекаралық беру кезінде Қытай заңы елдің стратегиялық мүдделерін ескере отырып, деректерді экспорттаудың қатаң тәртібін белгілейді.

Қазақстанның және жеке қаралған шет елдердің заңдарына сай құқықтық талдау жасайық. Біріншіден, деректерді анықтау және жіктеуге байланысты Қазақстанда биометриялық мәліметтер жалпы дербес дерек ретінде танылады, бірақ заңнама да түрлері мен оларды өңдеу әдістері бойынша егжей-тегжейлі анықтамаларды жүргізбейді. Ал Еуропалық Одақтың GDPR регламентінде қатаң талаптарға бағынатын сезімтал ақпарат ретінде биометрияны бөліп көрсететін нақты құрылымдалған анықтама бар. АҚШ та BIPA заңымен жұмыс істейтін Штаттарда биометрика маңызды деп жіктеледі, бірақ бірыңғай жүйенің қалыптаспауы қорғаныс тәсілдердің бөлшектенуіне әкеледі. Екіншіден, деректер субъектісінен келісім алу және ақпараттандыру тетіктері бойынша. Қазақстан заңнамасында деректер субъектісінің келісім туралы жалпы ережелер бар, бірақ биометриялық деректерді өңдеудің нақты тәуекелдерін ескеретін процедуралар жоқ қарастырылмаған. GDPR регламенті мақсаттар мен өңдеу әдістері туралы субъектіге хабарлама жібереді және біржақты келісімді талап етеді. АҚШ та Иллинойс сияқты Штаттар ақпараттандырудың қатаң ережелерін ұсынады, бірақ олардың қолданылуы белгілі бір штатқа байланысты өзгеруі мүмкін. Үшіншіден, Қазақстанда бақылау мемлекеттік органдар арқылы жүзеге асырылады, бірақ бұл құрылымдардың өкілеттіктері мен ашықтық дәрежесі жиі шектеледі, бұл бұзушылықтар орын алған кезде уәкілеттер арасында жедел әрекет етуді қиындата түседі. Еуропалық Одақта тәуелсіз қадағалау органдарының кең

өкілеттіктері бар, соның ішінде тексерулер жүргізу және айтарлықтай айыппұлдар салу, бұл нормалардың қатаң сақталуына ықпал етеді. АҚШ та биометриялық құпиялылықты бұзумен байланысты істер бойынша сот практикасы белсенді дамыған, сот практикасы бойынша тәжірбиесі мол, алайда орталықтандырылған реттеушінің болмауы жауапкершілік шараларын біріздендіруде қиындықтарды туғызады. Төртіншіден, заңдардың технологиялық өзгерістер мен жиі жаңарып отыратын салаларда артта қалуы да өзгешеленген. Қазақстанда әлі күнге дейін толыққанды деректерге қатысты барлық құқықтық аспектілерді қамтитын заңның болмауы. Ал ЕО да нормативтік-құқықтық базаны жүйелі түрде бейімдеу (мысалы, GDPR түзетулері арқылы) технологиялық сын-қатерлерге жедел жауап беруге мүмкіндік береді, алайда қатаң талаптар әсерінен кейде жаңа инновацияларды енгізуде қиындай түседі.

Жоғарыдағы салыстырмалы талдау Қазақстанда биометриялық технологияларды пайдалану саласындағы заңнаманы халықаралық тәжірибені ескере отырып, айтарлықтай пысықтау қажет екенін көрсетеді. Қазақстан үшін негізгі міндеттер нормативтік актілерді нақтылау, олардың сақталуын бақылауды күшейту және халықаралық стандарттармен белсенді үйлестіру болып табылады. Бұл шаралар азаматтардың құқықтарын сенімді қорғауды қамтамасыз етуге және сонымен бірге елде инновациялық технологияларды дамыту үшін қолайлы жағдайлар жасауға мүмкіндік береді.

ҚОРЫТЫНДЫ

Биометриялық деректер саласындағы диссертациялық жұмыс биометриялық технологиялардың пайдалануымен туындайтын тәуекелдерді жан-жақты қарастыруға, сот практикасының негізінде құқық қолдану тәжірибесінің негізгі кемшіліктерін анықтауға, шетелдік құқықтық актілер мен халықаралық конвенциялардың ұсынымдарының негізінде заңнаманы жетілдіру бойынша бастамалар дайындауға мүмкіндік берді.

Зерттеу барысында Қазақстан Республикасындағы биометриялық деректердің қорғалуымен қатар оларды өңдеу, жинау, сақтау кезіндегі осы саладағы құқық бұзушылықтар үшін әкімшілік-құқықтық жауапкершіліктің теориялық және практикалық мәселелері қарастырылды. Зерттеуде теориядағы, құқық қолдану практикасындағы және қолданыстағы заңнаманың кемшіліктеріне байланысты бірқатар мәселелерді анықталып, ұсынымдар жасалды. Ұлттық заңнама дербес деректерді қорғау туралы заңнамаға өзгерістер енгізу туралы автордың ұсыныстары жасалды. Биометриялық технологияларды пайдалану кезінде туындайтын мәселелердің алдын алу үшін ұсыныстар айтылды.

Диссертацияның бірінші тарауында биометриялық технологиялардың түсінігі, түрлері мен ерекшеліктерін анықтау және даму тенденцияларын, өмірдің әртүрлі салаларында, қызметтерде пайдаланудың тәуекелдерін анықтау бойынша зерттеу жүргізілді. Биометриялық технологиялардың түрлерін және жіктелу топтарын зерттеп, әрбір түріне жеке тоқталдық. Биометрия бойынша шетелдік авторлардың еңбектерін қарап, биометрия түсінігін қалыптастырған анықтамаларды зерттедік. Биометриялық технологиялардың даму тенденциясы мен қолданылып жатқан салалардағы прогресін зерттеп, туындаған тәуекелдер бойынша мәселелерді шешудің ұсынымдарын келтірдік. Биометриялық жүйелердің дамуы жасанды интеллект, машиналық оқыту және үлкен деректерді өңдеу саласындағы прогреспен тығыз байланысты екендігі анықталды. Қазақстанда мұндай технологиялар цифрлық үкімет шеңберінде, қолжетімділікті бақылау, биометриялық дауыс беру жүйелерінде және қашықтықтан мемлекеттік қызметтер көрсету кезінде қолданылуда. Биометриялық жүйелердің тұжырымдамасы мен жіктелуі тек техникалық ерекшеліктерді ескеріп қана қоймай, сонымен қатар осы технологияларды реттеу объектілері ретінде заңды түсінумен қатар жүруі керек деп санаймын. Қазақстан заңнамасында биометриялық технологияларды қолданудың техникалық ережелері мен оларды қорғаудың арнайы нормалары қарастырылмаған. Осы тұрғыдан мемлекеттік органдар қызмет көрсету кезінде биометриялық технологиялармен іске асырылатын процестер де азаматтарды алдын ала хабардар қылу қажет. Сонымен қатар бірыңғай биометриялық технологияларды қолданылу кезінде пайдаланылатын ереже нұсқаулық түрінде нормативтік акті болуы қажет деп санаймын.

Елімізде мемлекеттік қызмет салаларында 90%-дан астамы онлайн режимде жұмыс жасайды, ал электрондық үкіметті пайдалану жағынан алғашқы орындарды алады. 2024 жылы Қазақстанда қашықтықтан биометриялық

сәйкестендірудің орталықтандырылған ұлттық жүйесін құру жоспарлары жарияланды. Жобаның мақсаты мемлекеттік қызметтерді алу және банктік қызметтерді пайдалану үшін азаматтарды толық сәйкестендіруді қамтамасыз ету. Бұл бірыңғай ұлттық жүйе өз жұмысын бастаса онда қазақстандықтардың дербес деректеріне келетін қауіпте азаяр еді. Жүйенің тағы бір негізгі аспектісі - балалар биометриясына қол жеткізу. Бұл өз кезегінде кәмелетке толмаған азаматтардың биометриялық деректерін қорғау мәселесін шешеді.

Биометриялық технологиялардың интеграциясы қазіргі кезде көптеген салаларды қамтиды:

- мемлекеттік секторда - бұл электрондық паспорттар, жеке куәліктер, «электрондық үкімет» жүйесі (eGov), шекаралық бақылауды автоматтандыру;
- қаржы саласында - клиенттердің биометриялық аутентификациясы, қашықтықтан банктік қызмет көрсету жүйелері, алаяқтықтан қорғау;
- медицинада - медициналық деректерге қауіпсіз қол жеткізу, пациенттерді автоматты түрде сәйкестендіру;
- білім беруде - сабаққа қатысуды бақылау, онлайн емтихандар және жеке тұлғаны ауыстырудан қорғау;
- көлікте - вокзалдар мен әуежайларда, сондай-ақ қоғамдық көлік жүйелеріндегі биометриялық жүйелер.

Кең мүмкіндіктермен қатар, биометрияны қолдану белгілі бір қауіптермен бірге жүреді. Олар: биометриялық деректердің ағып кету қаупі, рұқсатсыз кіру және бақылау қаупі, адамдарды этникалық, жас немесе басқа белгілер бойынша танудағы қателіктер. Ауқымды тәуекелдердің бірі Қазақстандағы дербес деректерді қорғау және биометриялық ақпаратты пайдалануды реттеу саласындағы заңнаманың әлсіздігі мен жеткіліксіздігі. Қолданыстағы заңдарда биометриялық өңдеудің барлық ерекшеліктерін ескермеген, сондай ақ деректер ағып кеткен немесе дұрыс пайдаланылмаған жағдайда, кімнің жауапты екендігін анықтау қиын. Жауапкершілікке тарту жөніндегі санкциялар әлсіз. Биометриялық жүйелер қауіпсіздікті арттыру үшін ғана емес, сонымен қатар азаматтарды жаппай бақылауды жүзеге асыру үшін де қолданылуы бәріне аян. Деректерді ашық реттеу болмаған жағдайда азаматтардың жеке бас бостандығын шектейтін жаппай бақылау тетіктерін құру қаупі бар. Мемлекеттік билік немесе жеке ұйымдар биометриялық ақпаратты саяси немесе коммерциялық мақсатта қолдана алады, бұл құпиялылық принциптерін бұзады және азаматтардың бостандығына қол сұғу болып табылады. Айта кету керек, нормативтік базаның болуына қарамастан, технологиялардың қарқынды дамуы жағдайында оны жетілдіру қажеттілігі байқалады. Заңнама бет — әлпетті тану функциясы бар бейнебақылау жүйелерінде, автоматтандырылған шешім қабылдау платформаларында, сондай-ақ халықаралық трансшекаралық қызметтерде биометрияны пайдалану сияқты жаңа сын-қатерлерге уақтылы жауап беруі тиіс. Биометриялық технологияларды сәтті енгізу инновациялар мен азаматтардың іргелі құқықтарын, соның ішінде жеке өмірге қол сұғылмаушылық құқығын, жеке деректерді қорғауды және қозғалыс еркіндігін қорғау арасындағы тепе-теңдік сақталған жағдайда ғана мүмкін болады.

Диссертацияның екінші тарауында биометриялық деректерді жинау,

сақтау, өңдеу және қорғауды қамтамасыз ететін нормативтік-актілерді талдау міндеті орындалды. Оның ішінде Қазақстандық заңнамалар мен шетелдік GDPR Ережесі деректерді жинау, сақтау, өңдеу кезіндегі нормаларына салыстырмалы талдау жасалды. Дербес деректерді қорғау туралы заңнаманы іске асыру мәселелерін анықтау кезінде сот тәжірбиесі мен мемлекеттік органдардың жұмысына, цифрлық даму және аэроғарыш өнеркәсібі министрлігінің азаматтардың құқықтарын қорғау мәселесі бойынша жасалған жұмыстарына зерттеу жүргізілді. Нәтижесінде деректерді қорғаудың жалпы регламентін де (GDPR) биометриялық деректер белгілі бір жағдайларды қоспағанда, өңдеуге тыйым салынған жеке деректердің арнайы санаттарына жатады. Регламент халықаралық заңды акті болып табылатындықтан, тұлғаларға қатысты тікелей жеке деректерге қатаң бақылау орнатқан. Дегенмен, GDPR биометриялық деректерді өңдеуге рұқсат етілген ерекшеліктерді де қарастырады. Ал Қазақстан заңнамасында дербес деректерді қол жетімділігі бойынша жалпыға бірдей қолжетімді және қол жетімділігі шектеулі деп екі топқа бөледі. Ал биометриялық деректер қай түріне жататыны белгісіз, десе де олар қол жетімділігі шектеулі деректерге жатуы тиіс. Биометриялық деректердің құпиялығы ҚР-ның заңнамасында белгіленеді деп көрсетілген, бірақ нақты қай заңнамада екені жазылмаған. Заңның 25-бабында биометриялық деректерді қоса алғанда, дербес деректерді жинаудың, сақтаудың және өңдеудің құқықтық негіздері жазылған, бірақ биометриялық деректерге айрықша нормалар қарастырылмаған. Қазақстан Республикасы цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2020 жылғы 27 қазандағы № 406/НҚ бұйрығымен «Мемлекеттік қызметтер көрсету кезінде жеке тұлғалардың биометриялық аутентификациясы үшін биометриялық деректерді жинау, өңдеу және сақтау қағидалары» бекітілді. Бұл қағидат мемлекеттік қызметтер алуда ғана қолданылады және ондағы қағидалар санын тағыда күшейту қажет. Биометриялық деректерді қорғаудағы негізгі заң «Дербес деректер және оларды қорғау туралы» Заңның болуына қарамастан, Қазақстандағы құқықтық нормалар технологияның дамуына әрдайым ілесе бермейді артта қалуда. Биометриялық ақпаратты өңдеуді бақылаудың қатаң тетіктерін заңда көздемейді. Бірыңғай ұлттық сенімді жүйе жоқ. Жоғарыда келтірілген нормативтік актіде биометриялық деректердің тек саусақ ізі және бет бейнені аутентификациялау бойынша ғана нормалар қарастырылған. Ал басқа биометриялық деректер туралы заң нормаларында анықтама да атыда келтірілмеген. Осы олқылықтарды қайта қарап жүйелеу қажет, себебі биометриялық технологиялар тек қызмет алуда емес, басқа да салаларда кеңінен қолданыста, оның бірі қоғамдық орындар мен көшелердегі бақылау камералары оларды жүйелеп қарайтын реттейтін арнайы заң нормалары жоқ.

Дербес деректерді қорғау туралы заңның 24-бабында субъектінің құқықтары мен міндеттері туралы жазылған. Осы бапқа субъектінің деректерін қорғау мақсатында мынандай нормаларды енгізсе жақсы болатын еді. Иесіздендіру құқығы: дербес деректер субъектісі, егер мұндай өңдеу енді қажет болмаса, оны белгілі бір адаммен байланыстыру мүмкін болмайтындай етіп, сәйкесінше бұл деректердің нақты кімдікі екенін белгісіз етіп қалдырса. Дербес деректер

субъектілеріне олардың дербес деректерінің ағып кету немесе оларға рұқсатсыз қол жеткізу жағдайлары туралы уақытында хабарландыру. Бұл құқық азаматтардың ықтимал тәуекелдер туралы хабардар болуын қамтамасыз етеді. Еліміздегі қолданыстағы электрондық портал жүйесі арқылы немесе басқа ұйымдар бірден дербес дерек субьектісіне хабарландыру жіберсе, онда дерек иесі бірден қауіпсіздікті күшейте алады. Егер дербес деректер субъектісі оның деректерінің мұрағатта екенін анықтаса, ол мұндай мұрағаттық жазбалардың көшірмесін алуға немесе оларды сақтаудың заңды негіздері болмаған кезде жоюды сұрауға құқық берсе. Осы құқықтардың барлығы дербес деректерді өңдеудің ашықтығын, қауіпсіздігін және субъектінің құқығын қорғауға бағытталған.

Қазақстанда құқық қолдану және дербес деректерді қорғау туралы заңнаманы іске асыру мәселелерінің өзектілігі төмендегі факторларға байланысты.

1.Цифрлық технологиялардың жылдам өсуі және өңделетін ақпарат көлемінің ұлғаюы, бұл жеке деректердің қауіпсіздігіне қосымша қауіп төндіреді.

2.Нормативтік-құқықтық базадағы олқылықтардың болуы, бұл заңды іс жүзінде біркелкі қолдануды қиындатады.

3.Қадағалауға жауапты мемлекеттік органдар арасындағы өкілеттіктердің бөлшектенуі, бұл бұзушылықтарға жауап берудің тиімділігін төмендетеді.

4.Азаматтардың өз құқықтары туралы хабардар болмауы, бұл олардың деректерін заңсыз өңдеуге әкеп соғады. Сонымен қатар, іс жүзінде дербес деректерді қорғау саласында сот практикасының дамымағандығы байқалады. Сот шешімдерінің материалдарына қол жетімділік шектеулі және мұндай істерді жүйелейтін мамандандырылған органның болмауы сот органдарының кейде бірдей заңнама нормаларына әртүрлі түсіндірулер беруіне әкеледі. Бұл дербес деректер операторлары үшін белгісіздік туғызады және азаматтардың өз құқықтарын қорғауға деген сенімін төмендетеді.

Диссертацияның үшінші тарауында Еуропалық Одақтың деректерді қорғау жөніндегі жалпы регламенті (GDPR) (2016/679 ЕО регламенті), Еуропа Кеңесінің №108 конвенциясы, халықаралық биометриялық ақпаратты қорғау, биометриялық жүйелерге шабуылдарды анықтау сынды халықаралық стандарттар зерттеп қарастырылды, Қазақстандағы биометриялық технологияларды пайдалануды шет елдің оның ішінде Америка Құрама Штаттары, Қытай, Калифорния заңнамаларымен салыстырмалы құқықтық талдау жасалды. Дербес деректермен биометриялық технологияларды тиімді пайдалану және тәуекелдердің алдын алу үшін ұсыныстар берілді. GDPR, ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 19794, ISO/IEC 30107, ISO/IEC 24745 сияқты халықаралық стандарттар жеке деректер мен биометриялық ақпаратты қорғау үшін сенімді негіз жасайды. Алайда оларды қолдану кезінде бірқатар құқықтық, техникалық, этикалық және ұйымдастырушылық мәселелер туындайды. Сонымен қатар, биометриялық деректерді өңдеуге келісім беру мәселесі ауқымды. Стандарттар биометриялық деректерді тек нақты келісіммен жинауды талап етеді (GDPR, ISO/IEC 27701). Алайда, мемлекеттік жүйелерде (мысалы, биометриялық төлқұжат алған кезде) азаматтар деректерді өңдеуден бас тарта алмайды, келісімсізде өңделетін жағдайлар орын алады. Тағы бір өткір

мәселе, GDPR биометрияны негізсіз өңдеуге тыйым салады, бірақ Қытай сияқты елдерде бетті танудың жаппай бейнебақылау жүйелері жұмыс жасайды. GDPR (ЕО деректерді қорғаудың жалпы ережесі), ISO/IEC 24745 (Ақпараттық технологиялар – биометриялық ақпарат), Еуропа Кеңесінің №108 конвенциясы және ұлттық заңнамалық актілер сияқты халықаралық стандарттар биометриялық ақпаратты қауіпсіз жинауға, өңдеуге және сақтауға құқықтық негіз береді. Бұл стандарттар деректердің бұзылу, биометриялық ақпаратты теріс пайдалану және адам құқықтарын бұзу қаупін азайтуға бағытталған. Олар деректерді өңдеу принциптерін, түпнұсқалықты, тұтастықты және құпиялылықты қамтамасыз етуді және рұқсатсыз кіруден қорғау механизмдерін қоса алғанда, негізгі аспектілерді реттейді. Қазақстанның және шет елдердің заңдарына құқықтық салыстырмалы талдаудың нәтижесіне көз жүгіртсек. Біріншіден, деректерді анықтау және жіктеуге байланысты Қазақстанда биометриялық деректер заңда жалпы дербес деректер категориясы ретінде танылады, бірақ нақты түрлері мен оларды өңдеу әдістері бойынша егжей-тегжейлі анықтамаларды жүргізбейді. Ал Еуропалық Одақтың GDPR регламентінде қатаң талаптарға бағынатын сезімтал ақпарат ретінде биометрияны бөліп көрсететін нақты құрылымдалған анықтама бар. АҚШ та BIPA заңымен жұмыс істейтін Штаттарда биометрика маңызды деп жіктеледі, бірақ бірыңғай жүйенің қалыптаспауы қорғаныс тәсілдердің бөлшектенуіне әкеліп соғады. Екіншіден, деректер субъектісінен келісім алу және ақпараттандыру тетіктері бойынша Қазақстан заңнамасында деректер субъектісінің келісім туралы жалпы ережелер бар, бірақ биометриялық деректерді өңдеудің нақты тәуекелдерін ескеретін процедуралар жоқ қарастырылмаған. GDPR регламенті мақсаттар мен өңдеу әдістері туралы субъектіге хабарлама жібереді және біржақты келісімді талап етеді. АҚШ та Иллинойс сияқты Штаттар ақпараттандырудың қатаң ережелерін ұстанады, бірақ олардың қолданылуы белгілі бір штатқа байланысты өзгеруі мүмкін. Үшіншіден, Қазақстанда бақылау мемлекеттік органдар арқылы жүзеге асырылады, бірақ бұл құрылымдардың өкілеттіктері мен ашықтық дәрежесі жиі шектеледі, бұл бұзушылықтар орын алған кезде уәкілеттер арасында жедел әрекет етуді қиындата түседі. Еуропалық Одақта тәуелсіз қадағалау органдарының кең өкілеттіктері бар, соның ішінде тексерулер жүргізу және айтарлықтай айыппұлдар салу сияқты, бұл нормалардың қатаң сақталуына ықпал етеді. АҚШ та биометриялық құпиялылықты бұзумен байланысты істер бойынша сот практикасы белсенді дамыған, сот практикасы бойынша тәжірбиесі мол. Ал қазақстанды биометриялық және дербес деректер бойынша сот тәжірбиесі әлі жақсы дамымаған. Төртіншіден, заңдардың технологиялық өзгерістер мен жиі жаңарып отыратын салаларда артта қалуы да өзгешеленген. Қазақстанда әлі күнге дейін толыққанды деректерге қатысты барлық құқықтық аспектілерді қамтитын нормалар жоқ. Биометриялық деректерді қорғау бойынша жалпы ережелерді қамтығанымен, бұл заңдағы нормалар техникалық және құқықтық талаптар деңгейінде толыққанды реттелмеген. Нақтырақ айтқанда, биометриялық деректерді жинау шарттары, оларды сақтау мерзімі және үшінші тұлғаларға беру талаптары туралы құқықтық нормалар әлсіз. Дербес деректерді

бұзғаны үшін әкімшілік және қылмыстық жауапкершілік қарастырылған. Десе де ондағы санкциялар айыппұл мөлшері аз немесе құқық бұзушылар айтарлықтай келтірілген залалды тек айыппұл төлеумен құтылуда. Ал GDPR да деректер қауіпсіздігін бұзғаны үшін өте үлкен көлемде айыппұл салынады, онда биометриялық деректер үшін санкция өте қатал. Құқықтық салыстырмалы талдаудан Қазақстанда биометриялық технологияларды пайдалану саласындағы заңнаманы халықаралық тәжірибені ескере отырып, айтарлықтай пысықтау қажет екенін көреміз. Қазақстан үшін негізгі міндеттер нормативтік актілерді нақтылау, олардың сақталуын бақылауды күшейту және халықаралық стандарттармен белсенді үйлестіру болып табылады.

Зерттеу барысында биометриялық технологиялардың интеграциясы бойынша мәселелері қарастырылып, шетелдік және халықаралық заң актілермен сарапталып, биометриялық деректердің маңыздылығы зерттеліп сот практикасы қарастырылып, осы бағыттағы заңнаманы жетілдіруге қатысты ұсыныстар дайындалып, диссертациялық жұмыстың бастапқыда белгіленген негізгі мақсаттары орындалды. Нәтижесін де келесі негізгі тұжырымдар мен ұсыныстар жасалды:

1. Қазақстан Республикасының "Дербес деректер және оларды қорғау туралы" Заңына биометриялық деректерді арнайы (сезімтал) санаттағы дербес деректер ретінде енгізіп, оларды өңдеуді субъектінің нақты келісіміне немесе заңда көрсетілген ерекше жағдайларға ғана рұқсат ету нормаларын бекіту қажет.
2. Қылмыстық кодексте 147-бапқа «Биометриялық деректерді субъектінің келісімінсіз жинау, өңдеу немесе жария ету - ауырлататын мән-жай ретінде қарастыру» деген тармақпен толықтыру қажет.
3. Қазақстан Республикасының "Дербес деректер және оларды қорғау туралы" Заңының 1-бабына жаңа тармақ енгізілсін: «Биометриялық деректер - жеке тұлғаны бірегей сәйкестендіру үшін пайдаланылатын физиологиялық немесе мінез-құлық сипаттамаларының деректері (мысалы, саусақ ізі, бет бейнесі, көздің тор қабығының үлгілері, дауыстық үлгі, қолтаңба, перне басу динамикасы, жүріс-тұрыс үлгісі және басқа да осыған ұқсас сипаттар).
4. ҚР ӘҚБтК 79-бабына мынадай өзгеріс енгізу ұсынылады: «Қайталанған немесе көп мөлшердегі дербес деректерге қатысты бұзушылықтар үшін айыппұл мөлшерін екі есеге арттыру және заңды тұлғаларға - қызметін уақытша тоқтата тұру шарасын қолдану қажет.»
5. Мемлекеттік қызметтер мен банк секторында азаматтардың шынайы сәйкестендіру деңгейін арттыру және деректер қауіпсіздігін күшейту мақсатында мультимодальды биометриялық сәйкестендіру жүйесін кезең-кезеңімен енгізу ұсынылады.
6. Қазақстан Республикасының "Дербес деректер және оларды қорғау туралы" Заңына балалардың биометриялық деректерін өңдеуге қатысты жеке бөлім енгізіліп, заңды өкілдің нақты келісімінсіз кез келген өңдеуге тыйым салу қажет. ӘҚБтК мен Қылмыстық кодекс нормаларына балалардың деректеріне қатысты бұзушылықтар үшін күшейтілген жауапкершілік енгізу ұсынылады.
7. Дербес деректерді қорғау туралы заңның 24-бабында субъектінің құқықтары нормасына «Иесіздендіру құқығын» қосу және мұрағаттағы

деректерін сұрату және жою құқығын субъектіге беру.

8. Қазақстанда ұлттық бірыңғай деректер базасын құру үшін арнайы заң қабылданып, деректердің жинау мақсаты, сақталу шарттары, азаматтардың құқықтары мен тәуелсіз бақылау тетіктері нақты белгіленуі тиіс, ал биометриялық және балалар деректеріне қатысты - қосымша шектеулер мен қорғау шаралары енгізілуі қажет.

Жалпы, диссертациялық зерттеудің нәтижелері Қазақстан Республикасының Дербес деректер және оларды қорғау саласындағы заңнамаларын жаңа нормалармен толықтыруда, осы саладағы биометриялық деректерде болатын құқық бұзушылықтар үшін жауапкершілікті қатаңдату үшін мемлекеттік органдарда пайдаланылуы мүмкін.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ:

1.Сейданов А.Б., Цифровая трансформация здравоохранения и влияние современных технологий на обеспечение безопасности пациентов в РК. // «Legalitas» ғылыми журнал, №2 (2), 2024.

2.История биометрии // https://www.tadviser.ru

3.Чипигина П.А., Правовое регулирование персональных данных в цифровую эпоху. // Магистерская работа – Томск – 2024.

4.Jain, A. K., Ross, A., & Nandakumar, K. // (2016). Introduction to Biometrics. Springer.

5.Wayman, J., Jain, A. K., Maltoni, D., & Maio, D. // (2017). Biometric Systems: Technology, Design and Performance Evaluation. Springer.

6.Биометрическая идентификация личности. Ворона В.А., 2021.

7.Биометрические системы. Методы и средства идентификации личности человека: Георгий Кухарев., 2001.

8.ISO/IEC 19794-1: 2005, Biometric data interchange formats — Part 1: Framework.

9.Статья «История Биометрии» // https://znanierussia.ru/articles/

10.«Emerging Biometric Modalities and their Use: Loopholes in the Terminology of the GDPR and Resulting Privacy Risks» Tamas Bisztray , Nils Gruschka , Thirimachos Bourlai // https://arxiv.org/abs/0909.2365

11.Общий регламент по защиты персональных данных *General Data Protection Regulation, GDPR* // https://gdpr-info.eu/art-1-gdpr/

12.Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Конвенция 108+)

13.Биометрические технологий // https://idrak.com/ru/technologies/biometricheskaya-identifikaciya/

14.Общая характеристика биометрических технологий // https://www.biolink.ru/technology/biometric.php?utm_source

15.Типы биометрии: полное руководство // https://recfaces.ru/articles/types-of-biometrics.

16.Анализ размера и доли рынка биометрии — тенденции роста и прогнозы (2024–2029 гг.) // https://www.mordorintelligence.com/ru/industry-reports/biometrics-market

17.Глобальный рынок биометрических технологий // https://www.sphericalinsights.com/ru/reports/biometric-technology-market

18.Биометрическая идентификация мировой рынок // https://www.tadviser.ru/

19.Статья: Объем рынка речевой аналитики, биометрии и чат-ботов в Казахстане оценили в 112 млрд тенге в год // автор: Александр Левин. https://2023-06-15/skvr-analytics3i/

20.Асаинова Л.С., Защита персональных данных в контексте использования технологий биометрической аутентификации // АО «Университет КАЗГЮУ им. М.С. Нарикбаева» 2021.

21.Казахстанцы разработали необычный способ биометрической идентификации человека // https://alaqan.kz/main

22.Қазақстандағы Киберқауіпсіздік тұжырмдамасы // https://egov.kz/cms/kk/cyberspace
23.ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Мемлекеттік көрсетілетін қызметтер комитеті сайтынан.https://www.gov.kz/memleket/entities/kgu/activities/9552?lang=kk&par6
24.Биометрический паспорт // https://ru.wikipedia.org/wiki/%D0%9%B8
25.Электрондық үкімет дегеніміз не және ол не үшін қажет ? // https://egov.kz/cms/information/about/help-elektronnoe-pravitelstvo
26.Қазақстан Республикасы Бас прокуратурасының «Qamqor» Құқықтық статистика және арнайы есепке алу жөніндегі комитетінің статистикасы // https://qamqor.gov.kz/crimestat/indicators/administrative
27.Цифровой Казахстан. В Астане стартовал пилотный медицинский проект с использованием Face ID // https://atameken.kz/
28.Депутат заявила о нарушениях при хранении биометрических данных казахстанцев // https://www.zakon.kz/obshestvo/6447374-deputat-zayavila-o-narusheniyakh-pri-khranenii-biometricheskikh-dannykh-kazakhstantsev.html
29.Кража цифровой личности: власти Казахстана призвали защитить взрослых и детей // https://ekaraganda.kz/?id=145020&mod=news_read&utm_sourcecom
30.Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Дербес деректер және оларды қорғау туралы Заңы // https://adilet.zan.kz/kaz/docs/Z1300000094
31.Халықаралық стандарт ISO/IEC 2387-37:2012 // https://cdn.standards.iteh.ai/samples/55194c24033c83b6/ISO-IEC-2382-37-2012.pdf
32.Мемлекет басшысы Қасым-Жомарт Тоқаевтың «Әділетті Қазақстанның экономикалық бағдары» атты Қазақстан халқына Жолдауы 2023 жылғы 1 қыркүйек // https://www.akorda.kz/kz/memleket-basshysy-kasym-zhomart-tokaevtyn-adiletti-kazakstannyn-ekonomikalyk-bagdary-atty-kazakstan-halkyna-zholdauy-18333
33.Қазақстан Республикасының 2016 жылғы 30 желтоқсандағы № 40-VI Дактилоскопиялық және геномдық тіркеу туралы Заңы // https://adilet.zan.kz/kaz/docs/Z1600000040
34.Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрінің 2020 жылғы 27 қазандағы № 406/НҚ Мемлекеттік қызметтер көрсету кезінде жеке тұлғаларды биометриялық сәйкестендіру үшін олардың биометриялық деректерін жинау, өңдеу және сақтау қағидаларын бекіту туралы бұйрығы // https://adilet.zan.kz/kaz/docs/V2000021547
35.Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2024 жылғы 16 тамыздағы № 56 Банк қызметтерінің жекелеген түрлерін жүзеге асыратын ұйымдарды және микроқаржы ұйымдарын биометриялық сәйкестендіруді жүргізу қағидаларын бекіту туралы қаулысы // https://adilet.zan.kz/kaz/docs/V2400034950
36.Микроқаржы ұйымында Қазақстан Республикасы азаматтарының дербес деректерінің жариялануы туралы "zaimer.kz"// https://www.gov.kz/memleket/entities/mdai/press/news/details/

37.ИС BestProfi сайтындағы сот шешімдері // ИС BestProfi
38.Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан ответ от (19.07.2022) на обращение от (20.05.2022) № 740331
39.Чиновников в Казахстане наказали за плохую защиту персональных данных // https://lsm.kz/chinovnikov-v-kazahstane-nakazali-za-plohuyu-zashitu-personal-nyh-dannyh
40.Утечка персональных данных: как теряют сведения о казахстанцах и чем это грозит // https://factcheck.kz/analitika/utechka-personalnyh-dannyh-kak-teryayut-svedeniya-o-kazahstantsah-i-chem-eto-grozit/
41.Конвенция о защите физических лиц при автоматизированной обработке персональных данных ETS от 28.01.1981 № 108 https://rppa.pro/npa/ets108_28.01.1981
42.Биометрические технологии и свобода выражения мнений 2021 // https://www.article19.org/wp-content/uploads/2023/01/Biometric-Report-Russian.pdf
43.Экономикалық ынтымақтастық және даму ұйымы (ЭЫДҰ) нұсқаулықтары // http://cyberpeace.org.ua/files/3_2_2.pdf
44.Руководящие принципы OECD по защите конфиденциальности и трансграничному потоку.
45.Бизнесті жауапты жүргізу мәселелері жөніндегі көпұлтты кәсіпорындар үшін ЭЫДҰ-ның басшылық қағидаттары // https://eri.kz/kz/Nacionalnyj_kontaktnyj_centr/Rukovodjaschie_principyB.
46.APEC cross-border privacy rules system // https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf
47.ISO/IEC сериясы 19794 стандарты // https://meganorm.ru/
48.ISO/IEC сериясы 19795 стандарты // https://meganorm.ru/
49.ISO/IEC 24745 стандарты // https://www.iso.org/ru/standard/75302.html
50.ISO/IEC 30107 сериясы стандарты // https://www.iso.org/ru/standard/.html
51.HSBC Biometric Authentication Report 2023 – https://www.hsbc.com
52.ISO/IEC 30107-3:2017 – Presentation attack detection – https://www.iso.org
53.Еуропалық Комиссия – Биометриялық Төлқұжаттарды Рәсімдеу Ережелері, 2023- https://ec.europa.eu
54.Қазақстан Республикасының 2014 жылғы 5 шілдедегі Әкімшілік құқық бұзушылық туралы Кодексі // https://adilet.zan.kz/kaz/docs/K1400000235
55.Қазақстан Республикасының 2014 жылғы 3 шілдедегі Қылмыстық Кодексі // https://adilet.zan.kz/kaz/docs/K1400000226
56.Защита персональных данных граждан РК vs Европейского союза // https://profit.kz/articles/14832/Zaschita-personalnih-dannih-grazhdan-RK-vs-Evropejskogo-souza/#:~:text
57.Защита персональных данных в США // https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/mezhdunarodnaya-sistema-zashchity-personalnyh-dannyh/v-ssha/

58.Закон о конфиденциальности биометрической информации (BIPA) // https://incognitobrowser.io/ru/illinois-biometric-privacy-law-change/

59.Обзор закона КНР о защите персональной информации (Personal Information Protection Law of the People's Republic of China (PIPL)) // https://zakon.ru/blog/2021/9/17/obzor_zakona_knr_o_zaschite_personalnoj_informaciipersonal_information_protection_law_of_the_peoples

60.Биометрическая защита. Обзор технологии: Антти Суомалайнен., 2019.

61.Дайырбеков Р.Т., Биометрическая идентификация в Казахстане: правовые особенности обработки биометрических данных граждан // https://tis.hse.ru/article/view/13048/13062

62.Терещенко Л.К., Государственный контроль в сфере защиты персональных данных. С 142-161.