ХҒТАР 10.27.23
ӘОЖ 347.78
JEL K24

https://doi.org/10.46914/2959-4197-2026-1-2-403-417

**ТҰРЫСБЕК Ж.Б.,*[1]**
докторант.
*e-mail: miss_zhanara@mail.ru
ORCID ID: 0009-0001-1575-4839
**САРИНА С.А.,[1]**
з.ғ.к., қауымдастырылған профессор.
e-mail: s.sarina@turan-edu.kz
ORCID ID: 0000-0002-1414-027X
**ДАМИАН С.,[2]**
PhD, ассистент-профессор.
e-mail: damian.cyman@pravo.ug.edu.pl
ORCID ID: 0000-0002-1443-8981
**ИСМАИЛОВ А.А.,[3]**
з.ғ.к., аға оқытушы.
e-mail: atahozha@mail.ru
ORCID ID: 0009-0002-1337-5920
[1]«Тұран» университеті,
Алматы қ., Қазақстан
[2]Гданьск университеті,
Гданьск қ., Польша
[3]Оңтүстік Қазақстан зерттеу университеті,
Шымкент қ., Қазақстан

# BIG DATA ЖӘНЕ ЖАСАНДЫ ИНТЕЛЛЕКТ ЭКОЖҮЙЕЛЕРІНДЕГІ ДЕРЕКТЕРДІ ӨҢДЕУДІҢ ҚҰҚЫҚТЫҚ РЕЖИМІ: ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДАҒЫ РЕТТЕУДІҢ ҰЛТТЫҚ МОДЕЛІНІҢ ДАМУЫ

**Аңдатпа**

Big Data технологиялары мен жасанды интеллекттің қарқынды дамуы деректерді өңдеуді құқықтық реттеудің дәстүрлі тәсілдерін түбегейлі өзгертуде. Цифрлық экожүйелер жағдайында дербес деректерді қорғаудың классикалық моделі ақпараттың бүкіл өмірлік циклін толық қамти алмайды; бұл цикл оқыту датасеттерін дайындауды, алгоритмдік өңдеуді, синтетикалық деректерді пайдалануды және жасанды интеллект жүйелерінің жұмыс істеуін қамтиды. Мақалада Қазақстан Республикасында data governance жүйесін ұлттық деңгейде қалыптастыру ерекшеліктері зерттеліп, оның EU AI Act аясында бекітілген Еуропалық Одақтың тәуекелге бағдарланған тәсілімен салыстырмалы талдауы жүргізіледі. Авторлар қазіргі заманғы деректердің құқықтық режимі объектілік, субъектілік, рәсімдік және институционалдық деңгейлерді қамтитын кешенді реттеу жүйесі ретінде құрылуы тиіс екенін негіздейді. Осыған байланысты дербес деректерді, оқыту датасеттерін, синтетикалық деректерді және алгоритмдік өңдеу нәтижелерін ажыратуға негізделген деректердің құқықтық режимінің авторлық интеграцияланған моделі ұсынылады. Зерттеу нәтижесінде жоғары тәуекелді жасанды интеллект жүйелеріне арнайы аудит рәсімдерін енгізу, адам құқықтарына ықпалын бағалау және алгоритмдік ашықтық тетіктерін қалыптастыру қажеттігі туралы қорытынды жасалады. Зерттеудің практикалық маңызы Қазақстан Республикасының жасанды интеллект пен деректер айналымы саласындағы заңнамасын жетілдіруге бағытталған ұсыныстар әзірлеуде көрінеді.

**Тірек сөздер:** Big Data, жасанды интеллект, data governance, алгоритмдік ашықтық, синтетикалық деректер, жоғары тәуекелді жасанды интеллект жүйелері.

## Кіріспе

Цифрлық экономика құқықтық реттеу фокусын жекелеген ақпараттық объектілерден деректер экожүйелеріне қарай ығыстырды, олардың аясында ақпаратты жинау, алмасу және қайта пайдалану процестері үздіксіз жүреді. Дәл осы себепті деректердің құқықтық режимі төңірегіндегі талас бұдан былай дербес деректерді қорғаудың классикалық шеңберімен шектелмейді: ол датасеттерді қайталама пайдаланудың жол берілуін, модельдерді оқыту мен валидациялаудың ашықтығын, синтетикалық контентті бақылауды және ЖИ әзірлеушілері, операторлары мен пайдаланушылары арасындағы жауапкершілікті бөлу мәселелерін қамтиды [1].

Еуропалық Одақ үшін бұған жауап ретінде GDPR, «Data Governance Act», «Data Act» және «AI Act» жиынтығы қалыптасты, мұнда деректерді қорғау, деректерге қолжетімділік және ЖИ-ді реттеу біртұтас цифрлық конституционализмнің элементтері ретінде қарастырылады. «AI Act» тәуекелге бағдарланған тәсілді бекітеді және жоғары тәуекелді жүйелер үшін арнайы талаптарды, соның ішінде тәуекелдерді басқаруды, деректер сапасын, техникалық құжаттаманы, логтарды жүргізуді, ашықтық пен адамның қадағалауын енгізеді [2]. Қазақстан, өз кезегінде, 2025–2026 жж. өзіндік реттеуші пакетін қалыптастырды: ҚР «Жасанды интеллект туралы» Заңы, Цифрлық кодекс және жаңа заңнаманы іске асыру бойынша ілеспе шаралар. Бұл кемелденген еуропалық модель мен қалыптасып жатқан посткеңестік құқықтық тәртіптің ұлттық моделін салыстыруға сирек мүмкіндік береді [3].

Ғылыми мәселе – қазақстандық реттеу ЖИ-ді құқықтық әсер етудің дербес нысаны ретінде танығанымен, доктриналық деңгейде дербес деректерді, иесіздендірілген массивтерді, оқытушы датасеттерді, синтетикалық деректерді және ЖИ жұмысының нәтижелерін біріктіретін деректердің құқықтық режимінің тұтас моделі әлі құрылмағандығында. Мұндай модельсіз заңнама фрагментарлы (үзік-үзік) болып қалу қаупі бар.

Зерттеу жұмысының мақсаты – IMRAD құрылымына негізделген және «data governance» доктринасына сүйенетін Қазақстан үшін деректердің құқықтық режимінің интеграцияланған моделін ұсыну. Зерттеу міндеттері: 1) «data governance» доктриналық концепциясын реконструкциялау; 2) еуропалық «AI/data regulation» моделінің өзегін анықтау; 3) оны қазақстандық режиммен салыстыру; 4) ұлттық заңнама үшін деректердің құқықтық режимінің қолданбалы моделін әзірлеу [4].

Зерттеудің ғылыми жаңалығы авторлардың Қазақстанның заң ғылымында алғаш рет data governance тұжырымдамасына негізделген Big Data және жасанды интеллект экожүйелеріне арналған деректердің құқықтық режимінің кешенді төрт деңгейлі моделін ұсынуымен айқындалады. Қолданыстағы, негізінен дербес деректерді қорғауға бағытталған тәсілдерден айырмашылығы, ұсынылған модель деректердің бүкіл өмірлік циклін қамтиды, соның ішінде оқыту датасеттерін, синтетикалық деректерді, алгоритмдік өңдеуді және жоғары тәуекелді жасанды интеллект жүйелерін аудиттеу тетіктерін құқықтық реттеуді көздейді. Сонымен қатар, авторлар цифрлық реттеу объектілерін ажыратудың критерийлерін тұжырымдап, Еуропалық Одақтың EU AI Act тәуекелге бағдарланған тәсілін Қазақстан Республикасының құқықтық жүйесіне бейімдеу бағыттарын ұсынды.

## Материалдар мен әдістер

Зерттеу цифрлық құқық, ақпараттық құқық және технологияларды реттеу теориясының тоғысында орындалды. Формальды-заңнамалық әдіс (ҚР «Дербес деректер және оларды қорғау туралы» Заңының, ҚР «Ақпараттандыру туралы» Заңының, ҚР «Жасанды интеллект туралы» Заңының және Цифрлық кодекстің нормаларын талдау үшін), салыстырмалы-құқықтық әдіс (қазақстандық тәсілді ЕО-ның «AI Act» құжатымен салыстыру үшін), сондай-ақ деректерді біртұтас объект ретінде емес, өмірлік цикл ретінде қарастыруға мүмкіндік беретін жүйелік әдіс (жинау – сақтау – қолжетімділік – модельдерді оқыту – ендіру – мониторинг – шағымдану) пайдаланылды [5].

Методологиялық тұрғыдан мақала «data governance» доктринасына «data protection»-мен салыстырғанда кеңірек конструкция ретінде сүйенеді. Егер «data protection» негізінен дербес деректер субъектісінің құқықтарына шоғырланса, «data governance» қолжетімділік, сапа,

интероперабельділік, жауапкершілік, аудит және деректер айналымына институционалдық бақылау ережелерін қамтиды. Мұндай тәсіл ЖИ үшін ерекше маңызды, өйткені модельдің сапасы мен заңдылығы тек деректердің бастапқы жиналуына ғана емес, сонымен бірге оларды пайдаланудың бүкіл келесі тізбегіне де байланысты [6].

Эмпирикалық базаға ресми қазақстандық нормативтік құқықтық актілер мен оларды енгізу материалдары, сондай-ақ AI актісінің Еуропалық моделінің ресми және квазиресми сипаттамалары кіреді. Доктриналық қабат 2024–2025 жж. аралығындағы AI басқару және деректерді басқару бойынша ағымдағы зерттеулерге негізделген.

Зерттеудің эмпирикалық базасын күшейту мақсатында Қазақстан Республикасындағы дербес деректерді қорғау және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы құқық қолдану практикасы талданды. Атап айтқанда, Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің Ақпараттық қауіпсіздік комитетінің мәліметтері бойынша, 2023 ж. дербес деректерді қорғау туралы заңнама талаптарын бұзуға байланысты 30-дан астам әкімшілік іс қаралып, жеке және заңды тұлғалар әкімшілік жауаптылыққа тартылған. Бұл жағдай дербес деректерді өңдеу саласындағы құқықтық талаптардың сақталуын мемлекеттік бақылаудың күшейіп келе жатқанын көрсетеді [2].

Сонымен қатар 2024 ж. микроқаржы ұйымдарының клиенттеріне қатысты 2 миллионнан астам дербес деректің интернет желісіне таралу фактісі анықталды. Аталған оқиға азаматтардың жеке мәліметтерін қорғау жүйесінде әлі де болса елеулі тәуекелдердің сақталып отырғанын және Big Data негізінде жинақталатын ақпараттық массивтерді қорғаудың құқықтық тетіктерін жетілдіру қажеттігін көрсетті. Осыған байланысты уәкілетті органдар тексеру жұмыстарын жүргізіп, азаматтарды дербес деректердің жариялануы туралы хабардар ету механизмдерін іске қосты.

Құқық қорғау және бақылау практикасының тағы бір маңызды бағыты – дербес деректер қауіпсіздігінің бұзылуы туралы хабарлау институтының енгізілуі болып табылады. 2024 жылғы заңнамалық өзгерістерге сәйкес дербес деректер операторы ақпараттық қауіпсіздік инциденті анықталған жағдайда уәкілетті органды қысқа мерзімде хабардар етуге міндетті. Бұл өзгерістер деректердің заңсыз таралуына жедел ден қою және азаматтардың құқықтарын қорғау тетіктерін күшейтуге бағытталған.

Практикалық материалдарды талдау нәтижелері көрсеткендей, Қазақстан Республикасында дербес деректерді қорғау саласындағы құқықтық реттеу біртіндеп жетілдіріліп жатқанымен, жасанды интеллект пен Big Data экожүйелерінде өңделетін мәліметтердің көлемінің ұлғаюы жаңа құқықтық тәуекелдерді туындатады. Сондықтан құқық қорғау органдарының практикасы деректерді өңдеудің құқықтық режимін қалыптастыруда маңызды эмпирикалық негіз ретінде қарастырылуы тиіс.

Құқық қорғау және бақылау практикасын талдау Қазақстанда дербес деректерді қорғау мәселесінің ерекше өзектілікке ие екенін көрсетті. Мәселен, 2024 ж. уәкілетті органдар азаматтардың дербес деректерінің заңсыз таралуына байланысты көптеген өтініштерді қарастырды. Қазақстан Республикасы Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің мәліметтері бойынша, микроқаржылық ұйым клиенттерінің деректер базасының жария болуына байланысты Ақпараттық қауіпсіздік комитетіне 1400-ден астам шағым келіп түскен. Сонымен қатар шамамен 2 млн азаматтың дербес деректерінің таралу фактісі бойынша тексеру шаралары жүргізілген. Бұл жағдай цифрлық платформалар мен Big Data жүйелерінде жинақталатын ақпараттық ресурстарды қорғаудың құқықтық кепілдіктерін күшейту қажеттігін айқын көрсетті [2].

Құқық қолдану практикасының дамуын сипаттайтын маңызды жаңалықтардың бірі – дербес деректер қауіпсіздігі бұзылған жағдайда азаматтарды міндетті түрде хабардар ету тетігінің енгізілуі болды. 2024 жылдан бастап дербес деректер операторы қауіпсіздік инциденті анықталған кезден бастап бір жұмыс күні ішінде уәкілетті органға хабарлауға міндетті. Өз кезегінде уәкілетті орган электрондық үкімет инфрақұрылымы арқылы дербес деректер субъектілерін хабардар етеді. Аталған өзгерістер Қазақстанда деректерді өңдеудің құқықтық режимін жетілдіруге, ақпараттық қауіпсіздікті қамтамасыз етуге және азаматтардың цифрлық құқықтарын қорғауға бағытталған заманауи құқықтық тетіктердің қалыптасып келе жатқанын көрсетеді.

**Нәтижелер мен талқылау**

Data governance-тің доктриналық концепциясы.

Тар мағынада «data governance» деректерді кім, қандай негізде, қандай шектеулермен және қандай мақсатта жинай алатынын, сақтай алатынын, бере алатынын және пайдалана алатынын айқындайтын басқарушылық ережелер жүйесі ретінде түсініледі. Кең мағынада – бұл деректер субъектілерінің құқықтарын, иеленушілер мен операторлардың міндеттерін, датасеттер сапасының стандарттарын, деректерге қолжетімділік ережелерін және алгоритмдік өңдеуден келген зиян үшін жауапкершілік механизмдерін біріктіретін нормативтік-институционалдық архитектура [7].

Осы мақаланың мақсаттары үшін data governance-тің төрт деңгейін ажыратуды авторлар ұсынады.

1. Аксиологиялық деңгей: заңдылық, әділдік, пропорционалдылық, қауіпсіздік және адам автономиясын құрметтеу принциптері.

2. Объектілік деңгей: деректер категорияларын саралау (дербес, иесіздендірілген, сезімтал, өнеркәсіптік-технологиялық деректер, оқытушы датасеттер, синтетикалық деректер, ЖИ шығыс нәтижелері).

3. Процедуралық деңгей: деректердің өмірлік цикліне қойылатын талаптар, соның ішінде жинаудың заңды негіздерін верификациялау, сапасы мен репрезентативтілігін тексеру, қайта пайдалануды шектеу және жою немесе мұрағаттау ережелері.

4. Институционалдық деңгей: реттеуші, операторлар, аудиторлар және соттар арасындағы құзыретті бөлу [8].

Мұндай конструкцияның артықшылығы – ол инновациялар мен құқықтарды қорғау арасындағы жалған баламаны еңсеруге мүмкіндік береді. Дұрыс құрылған «data governance» деректер айналымына тыйым салмайды, керісінше оны басқарылатын, қадағаланатын және есеп беруге міндетті етеді [9].

Әрі қарай, біз салыстырмалы талдауға көшуді ұсынамыз: ЕО актісі және Қазақстан (Кесте 1).

Кесте 1 – ЕО және Қазақстан Республикасындағы ai/data реттеу модельдерін салыстырмалы талдау

| Критерий | EU AI Act | Казахстан | Мақала үшін қорытынды |
|---|---|---|---|
| Реттеу моделі | Тәуекелге бағытталған; high-risk AI үшін жеке тыйымдар және арнайы режим | Тәуекелге бағытталған логика да қалыптасады, бірақ егжей-тегжейлердің көп бөлігі заңға тәуелді деңгейге қалдырылады | Қазақстан еуропалық модельге қарай жылжуда, бірақ әзірге нормалардың тығыздығы төмен |
| Тыйым салынған тәжірибелер | Манипуляциялық әдістер, vulnerabilities exploitation of vulnerabilities, social scoring және т. Б. | Манипуляциялық тәжірибеге, осалдықты пайдалануға, әлеуметтік скорингке, деректерді заңсыз жинауға/өңдеуге, эмоцияларды келісімсіз тануға және т. б. тыйым салынады. | Нормативтік жақындасу жоғары; қазақстандық модель тыйым салу логикасының тікелей қарыз алуын көрсетеді |
| Ашықтық/ Мөлдірлік | Жекелеген жүйелер мен генеративті АИ үшін ашықтық жөніндегі міндеттер | Синтетикалық мазмұнды таңбалау және ақпараттық міндеттер заң деңгейінде бекітілген | Қазақстан deepfake / labeling-ке сенімнің практикалық құралы ретінде баса назар аударады |
| Деректер және деректер жиынтығы сапасы | High-risk ai үшін-data governance және quality of training, validation and testing data талаптары | Өңдеудің заңдылығы мен қауіпсіздігіне қойылатын талаптар бар, бірақ сапа/өкілдік стандарттары егжей-тегжейлі қажет | Қазақстанның басты алшақтығы – датасет сапасының дамыған процестік режимінің болмауы |

1-кестенің жалғасы

| | | | |
|---|---|---|---|
| Институционалдық бақылау | ЕО және мүше мемлекеттер деңгейіндегі мамандандырылған қадағалау тетіктері | Ұлттық сәулет жаңа цифрлық институттар мен уәкілетті органның айналасында салынуда | Аудиттің нақты рәсімі және реттеушілер арасында құзыреттілікті бөлу қажет |
| Құқықтарды қорғау құралдары | Ашықтық, құжаттама және нарықтық қадағалау талаптары енгізілген | Құқықтарды қорғау дербес деректердің, ақпараттандырудың және АИ-заңнаманың жалпы тетіктеріне негізделеді | Келесі қадам-алгоритмдік маңызды шешімдерге шағымданудың арнайы процедурасы |
| Ескетрпе: Авторлармен [2, 5, 8] дереккөздер негізінде құрастырылды. | | | |

Авторлардың пікірінше, қазақстандық реттеу моделінің негізгі мәселесі – оқыту датасеттері мен жоғары тәуекелді жасанды интеллект жүйелеріне қатысты data governance саласында дербес процессуалдық құқықтық режимнің болмауы. Деректерге қатысты тек «персоналистік» тәсілді сақтау қазіргі цифрлық экожүйелердің жұмыс істеу логикасына сәйкес келмейді әрі алгоритмдік шешімдерге тиімді бақылау жүргізу мүмкіндіктерін шектейді.

Авторлар деректердің құқықтық режимінің өзара байланысты бес блоктан тұратын моделін енгізу қажеттігін негіздейді.

Бірінші блок – реттеу объектілері. Мыналарды ажырату қажет:

а) дербес деректер;

ә) дербес деректердің арнайы санаттары;

б) иесіздендірілген деректер;

в) ЖИ үшін оқытушы және тестілік датасеттер;

г) синтетикалық деректер;

ғ) өңдеу нәтижелері және ЖИ генерациялаған контент.

Негізгі тезис – бұл санаттар біркелкі реттелмеуі тиіс: тәуекел деңгейі мен міндеттер көлемі адам құқықтары мен қоғамдық мүдделерге тигізетін ықтимал әсеріне байланысты өзгеріп отыруы қажет [10].

Екінші блок – реттеу субъектілері. Деректердің классикалық иеленушісі мен операторынан бөлек, ЖИ үшін алгоритм әзірлеушіні, модельді жеткізушіні, ендіруші ұйымды, кәсіби пайдаланушыны және соңғы пайдаланушыны бөліп көрсету қажет. Дәл осы рөлдерді бөлу датасет сапасына, нәтижені таңбалауға, логтарды сақтауға және тәуекелдер туралы хабарлауға кім жауапты екенін анықтайды [11].

Үшінші блок – деректердің өмірлік циклінің процедуралары. Жинау кезеңінде заңды негіз бен мақсаттарды шектеу; датасетті дайындау кезеңінде – толықтығын, репрезентативтілігін және жүйелік ауытқулардың («bias») жоқтығын тексеру; оқыту кезеңінде – дереккөздерді, модель параметрлері мен шектеулерін құжаттандыру; ендіру кезеңінде – тәуекелдерді бағалау, адамның қадағалауы және эскалация механизмдері; пайдалану кезеңінде – логикалық тіркеу (логирование), мониторинг, аудит және инциденттерге әрекет ету процедуралары талап етіледі [12].

Төртінші блок – деректер субъектілері құқықтарының кепілдіктері. Бұған ақпарат алу құқығы, қолжетімділік құқығы, түзету құқығы, автоматтандырылған өңдеудің белгілі бір түрлеріне қарсылық білдіру құқығы, қолайсыз шешімге шағымдану құқығы және тиімді қорғану үшін жеткілікті көлемде түсініктеме алу құқығы жатады [13].

Бесінші блок – қадағалау және жауапкершілік. Жоғары тәуекелді жүйелер үшін міндетті аудит, ал генеративті ЖИ үшін синтетикалық контентті таңбалау презумпциясы қажет. Жауапкершілік сараласуы тиіс: деректерді заңсыз жинағаны үшін, датасет сапасының ақауы үшін, ашықтық талаптарын орындамағаны үшін және алгоритмдік маңызы бар шешімнен келген зиян үшін [14].

Қазақстандық модельдің ерекшеліктері мен дефициттері

Қазақстан айтарлықтай алға қадам басты: ҚР «Жасанды интеллект туралы» Заңы негізгі принциптерді, тыйымдар мен ашықтық бойынша міндеттерді енгізді, ал Цифрлық кодекс ЖИ-

ді кеңірек цифрлық реттеу жүйесіне кіріктірді. Дегенмен, дәл «data governance» деңгейінде бірнеше құрылымдық дефициттер сақталып отыр [2].

1. Дербес деректер мен ЖИ-ді оқытуға арналған датасеттерді нормативтік тұрғыдан ажырату қажет. Әрбір оқытушы массив дербес дерек болып табылмайды, бірақ әрбір мұндай массив шығу тегінің заңдылығы, сапасы, пайдалану мақсаты және кейінгі аудит мүмкіндігі бойынша ең төменгі талаптарға сай болуы тиіс.

2. Синтетикалық деректер мен синтетикалық контент режимін егжей-тегжейлі сипаттау керек. Олардың құқықтық мәртебесі тек таңбалаумен ғана шектелмеуі керек; модельдерді қосымша оқыту (fine-tuning) үшін пайдаланудың жол берілуі, тұлғаға еліктеу (имитация) үшін жауапкершілік және дербес деректер туралы ережелерді айналып өтудің алдын алу мәселелері маңызды.

3. Қоғамдық секторда (сот ісін жүргізу, денсаулық сақтау, білім беру, әлеуметтік көмек және құқық қорғау қызметі) жоғары тәуекелді ЖИ жүйелерін ендіру кезінде құқықтар мен бостандықтарға әсерін бағалаудың арнайы процедурасын бекіту қажет [15].

4. Ұлттық модель процессуалдық кепілдіктерге мұқтаж. Түсініктеме алу құқығы алгоритмнің бастапқы кодын ашу міндеті ретінде түсінілмеуі тиіс; шешім қабылдау логикасын және қолжетімді шағымдану құралдарын түсінікті сипаттап беру жеткілікті.

Тұжырым

EU AI Act-пен салыстыру Қазақстанның қалыпты тәуекелге бағдарланған тәсілді таңдағанын көрсетеді. Бұл инновацияларды қолдауды ең қауіпті практикаларға тыйым салумен ұштастыруға мүмкіндік береді. Алайда, ЕО-мен салыстырғанда, қазақстандық модель әзірге жоғары тәуекелді ЖИ жүйелеріне қатысты data governance-ке қойылатын процедуралық талаптармен аз толықтырылған [8, 7 б.].

Доктриналық тұрғыдан алғанда, көптеген құқықтық тәртіптердің негізгі қателігі – ЖИ-ді реттеуді тек дербес деректер призмасы арқылы немесе тек техникалық қауіпсіздік арқылы құруға тырысуында. Сонымен қатар, ЖИ деректер сапасының, тәуекелдерді басқарудың, нарықтық қадағалаудың және сот қорғауының қиылысында жұмыс істейді. Сондықтан «data governance» құпиялылық құқығы (privacy law) мен ЖИ құқығы («AI law») арасындағы байланыстырушы көпір болуы тиіс [7, 21 б.].

Қазақстан үшін цифрлық егемендік мәселесі ерекше маңызды. Трансшекаралық бұлттық сервистер мен шетелдік модельдерді белсенді пайдалану жағдайында ұлттық деректер режимі технологияларды жіберу ережелерін, сезімтал деректер массивтерін локализациялауды және инфрақұрылымдық тәуелділікті бақылауды анықтауы тиіс.

Ұсынылып отырған деректердің құқықтық режимінің моделі тек теориялық емес, сонымен қатар қолданбалы маңызға ие. Ол практикалық сұрақтарға жауап беруге мүмкіндік береді: ауытқулары бар (“biased”) датасет үшін кім жауапты; синтетикалық контентті пайдалануды қалай квалификациялау керек; қай жағдайда міндетті аудит талап етіледі; пайдаланушы жасанды интеллектінің айтарлықтай қатысуымен қабылданған шешімге қалай дауласа алады.

Жасанды интеллект пен Big Data технологияларын құқықтық реттеу мәселелерін зерттеуге арналған соңғы ғылыми еңбектер Қазақстандағы цифрлық трансформация жағдайында ерекше өзектілікке ие болып отыр. Бұл бағыттағы зерттеулердің маңызды бөлігі мемлекеттік саясатты қалыптастыру, дербес деректерді қорғау, цифрлық құқықтар мен жасанды интеллект жүйелерінің құқықтық мәртебесін айқындау мәселелеріне арналған.

Қазақстан Республикасында жасанды интеллектті құқықтық және институционалдық дамыту бағыттары Қазақстан Республикасы Үкіметінің 2024–2029 жж. арналған Жасанды интеллектті дамыту тұжырымдамасында көрініс тапқан [16]. Аталған құжатта ұлттық деректер инфрақұрылымын қалыптастыру, мемлекеттік деректер қорларын интеграциялау, жасанды интеллект жүйелерін оқыту үшін сапалы деректер массивтерін қалыптастыру және оларды қауіпсіз пайдалану мәселелері айқындалған. Тұжырымдама Қазақстанда Big Data және жасанды интеллект экожүйелерін құқықтық реттеудің стратегиялық негізін қалыптастыратын маңызды нормативтік бағдар болып табылады.

Ережепқызының зерттеуінде экологиялық көші-қонды құқықтық реттеу тетіктері цифрлық басқару құралдарымен өзара байланыста қарастырылады [17]. Автор халықаралық құқық нормаларын талдай отырып, цифрлық технологиялардың мемлекеттік басқару тиімділігін

арттырудағы рөлін негіздейді. Бұл зерттеу деректерді жинау мен талдаудың құқықтық маңызын көрсетіп, мемлекеттік шешімдер қабылдау үдерісінде үлкен деректерді пайдалану мәселелерінің құқықтық қырларын жанама түрде ашады.

Нұрғалым және әріптестерінің еңбегінде цифрлық технологияларды құқықтық реттеу, жасанды интеллектті қолдану және дербес деректерді қорғау мәселелері кешенді түрде зерттелген [18]. Авторлар жасанды интеллект жүйелерінің дамуы азаматтардың жеке өміріне қол сұқпаушылық құқығы мен ақпараттық қауіпсіздігіне жаңа тәуекелдер туғызатынын атап көрсетеді. Осыған байланысты зерттеушілер дербес деректерді өңдеу рәсімдерін жетілдіру және ұлттық заңнаманы халықаралық стандарттарға сәйкестендіру қажеттігін негіздейді.

Амантай, Нұрмағамбетов және Ахпанов жасанды интеллект құралдарын сот төрелігіне қолжетімділікті қамтамасыз етудің инновациялық тетігі ретінде қарастырады [19]. Авторлардың пікірінше, алгоритмдік жүйелер құқықтық ақпаратқа қолжетімділікті кеңейтуге және құқықтық қызметтердің тиімділігін арттыруға мүмкіндік береді. Сонымен қатар зерттеуде алгоритмдердің ашықтығы, шешім қабылдау процестерінің түсіндірмелілігі және құқықтық жауапкершілік мәселелерінің маңыздылығы көрсетілген. Бұл тұжырымдар жасанды интеллект негізінде өңделетін деректердің құқықтық режиміне қойылатын талаптарды айқындауда маңызды ғылыми негіз болып табылады.

Шошаева мен Аманбаева жасанды интеллектті құқықтық категория ретінде қарастырып, оның құқықтық табиғатын анықтау мәселелеріне назар аударады [20]. Авторлар жасанды интеллекттің қоғамдық қатынастарға ықпалының артуы құқықтық реттеудің жаңа тәсілдерін қалыптастыруды талап ететінін көрсетеді. Зерттеуде жасанды интеллект субъектілігі, құқықтық жауапкершілік және цифрлық технологияларды пайдаланудың құқықтық шектері жөніндегі ғылыми пікірлер талданған.

Жоғарыда қарастырылған еңбектер Қазақстандағы жасанды интеллект пен деректерді өңдеуді құқықтық реттеудің әртүрлі аспектілерін қамтығанымен, Big Data және жасанды интеллект экожүйелерінде деректерді өңдеудің бірыңғай құқықтық режимін қалыптастыру мәселесі әлі де жеткілікті деңгейде зерттелмеген. Атап айтқанда, деректерді басқару, алгоритмдік ашықтық, дербес емес деректердің құқықтық мәртебесі, мемлекеттік және жеке сектор арасындағы деректер алмасу тәртібі, сондай-ақ ұлттық цифрлық егемендікті қамтамасыз ету тетіктері бойынша кешенді ғылыми зерттеулердің қажеттілігі сақталуда. Осыған байланысты Қазақстан Республикасында Big Data және жасанды интеллект экожүйелеріндегі деректерді өңдеудің ұлттық құқықтық моделін әзірлеу қазіргі құқықтық ғылымның маңызды бағыттарының бірі болып табылады (кесте 2).

Кесте 2 – Қазақстан Республикасында деректерді қорғау және киберқауіпсіздік саласындағы жекелеген көрсеткіштер

| Көрсеткіш | Жыл | Мәні |
|---|---|---|
| Дербес деректерді қорғау саласындағы жүргізілген тексерулер саны | 2024 | 60 |
| Ақпараттық қауіпсіздік саласындағы жүргізілген тексерулер саны | 2024 | 210 |
| Дербес деректердің таралуына байланысты азаматтардың шағымдары | 2024 | 1400-ден астам |
| Микроқаржы ұйымдары клиенттерінің жария болған дербес деректері | 2024 | 2 млн-нан астам |
| Халықтың киберқауіпсіздік мәселелері бойынша хабардарлық деңгейі | 2024 | 80,4 % |
| Қазақстанның Ғаламдық киберқауіпсіздік индексіндегі (GCI) көрсеткіші | 2024 | 94,04 балл |
| Тіркелген киберқылмыстар саны | 2024 | 14 мыңнан астам |
| Киберқылмыстардан келген материалдық шығын | 2024 | шамамен 6 млрд теңге |
| Ескетрпе: Авторлармен тарапынан ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің, Ақпараттық қауіпсіздік комитетінің және ашық ресми дереккөздердің материалдары негізінде құрастырылды [16]. | | |

Кестеден көрініп отырғандай, Қазақстанда Big Data және жасанды интеллект технологияларының қарқынды дамуы деректерді қорғау мәселелерінің өзектілігін арттыруда. 2024 ж. дербес деректерді қорғау саласында 60 тексеру, ал ақпараттық қауіпсіздік саласында 210 тек-

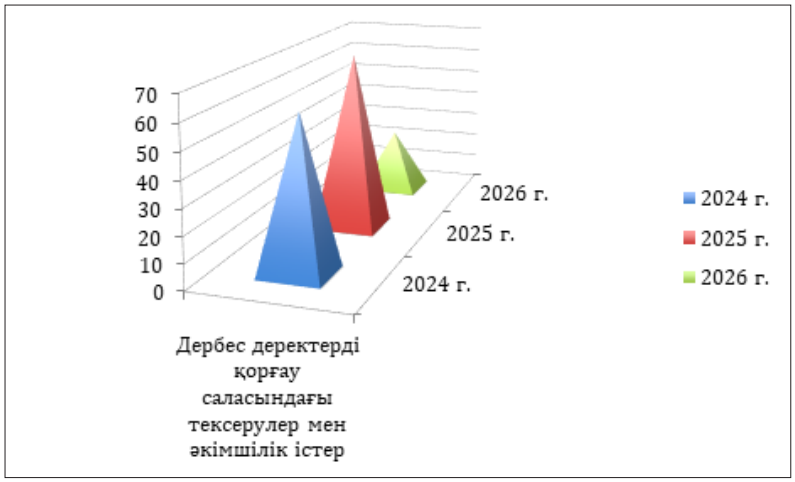
серу жүргізілген. Сонымен қатар дербес деректердің жария болуы фактілері бойынша 1400-ден астам азамат шағым түсірген және 2 миллионнан астам тұлғаның дербес деректерінің таралуы тіркелген. Бұл көрсеткіштер қолданыстағы құқықтық реттеу тетіктерін жетілдіру қажеттігін көрсетеді.

Қазақстанның 2024 жылғы Ғаламдық киберқауіпсіздік индексінде 94,04 балл жинауы және халықтың киберқауіпсіздік бойынша хабардарлық деңгейінің 80,4 %-ға жетуі цифрлық қауіпсіздік саласындағы оң үрдістерді көрсетеді. Сонымен бірге 2024 ж. 14 мыңнан астам киберқылмыстың тіркелуі және олардың нәтижесінде шамамен 6 млрд теңге көлемінде шығын келтірілуі құқықтық және институционалдық қорғау тетіктерін одан әрі жетілдірудің маңыздылығын дәлелдейді (кесте 3).

Кесте 3 – Қазақстан Республикасында деректерді қорғау және киберқауіпсіздік саласындағы құқық қолдану практикасының динамикасы (2024–2026 жж.)

| Көрсеткіш | 2024 | 2025 | 2026 |
|---|---|---|---|
| Дербес деректерді қорғау саласындағы тексерулер мен әкімшілік істер | 60 | 70-тен астам | 25-тен астам |
| Тіркелген интернет-алаяқтық фактілері | 22 870 | 14 000-нан астам (жыл басынан) | өсу үрдісі сақталуда |
| Деректердің ірі жариялану (leak) оқиғалары | бірнеше ірі жағдай | 43 оқиға | 40-тан астам оқиға туралы хабарланған |
| Дербес деректерді заңсыз тарату бойынша анықталған тұлғалар | – | 140-тан астам адам ұсталды | құқық қорғау шаралары жалғасуда |
| Ескертпе: 2026 ж. деректер – есепті кезеңнің алғашқы айлары бойынша. 2025 ж. мәндер құқықтық бақылаудың күшеюі және деректердің жариялану фактілерінің көбеюі негізінде бағаланған. Аралық көрсеткіш. | | | |

Кесте деректері Қазақстанда цифрландыру деңгейінің өсуімен қатар дербес деректерді қорғауға байланысты құқықтық тәуекелдердің де артып отырғанын көрсетеді. 2025 ж. интернет-алаяқтық фактілерінің саны 14 мыңнан асып, киберқылмыстардан келген шығын 16,4 млрд теңгеге жеткен.




Сурет 1 – Деректердің жариялану оқиғалары

Ескертпе: Авторлармен [12, 13, 14] дереккөздер негізінде құрастырылды.

Сонымен қатар 140-тан астам адамның азаматтардың дербес деректерін заңсыз таратуға қатысы бар екені анықталған. 2025 ж. деректердің жариялануына байланысты 43 ірі оқиға тіркелген, бұл Big Data экожүйелеріндегі ақпараттық қауіпсіздік мәселелерінің өзектілігін растайды.

Еуропалық Одақ тәжірибесімен қатар Азия және ТМД мемлекеттерінің тәжірибесін зерттеу де ерекше маңызға ие. Азия елдері арасында Сингапур, Оңтүстік Корея және Қытай деректерді басқарудың институционалдық моделін қалыптастыруда елеулі нәтижелерге қол жеткізді. Мәселен, Сингапурда дербес деректерді қорғау жөніндегі тәуелсіз орган – Personal Data Protection Commission (PDPC) қызмет етеді. Бұл орган деректерді өңдеудің заңдылығын бақылаумен қатар ұйымдарға әдістемелік қолдау көрсетеді және жасанды интеллект жүйелерін жауапты пайдалану қағидаттарын әзірлейді.

Оңтүстік Кореяда мемлекеттік және жеке сектор арасында деректер алмасуды реттейтін кешенді құқықтық механизмдер енгізілген. Елде деректерді қауіпсіз пайдалану және цифрлық инновацияларды дамыту мақсатында «Data 3 Act» заңнамалық пакеті қабылданған. Бұл модель деректерді қорғау мен инновациялық технологияларды дамыту арасындағы теңгерімді қамтамасыз етуге бағытталған.

Қытай Халық Республикасында деректерді басқару жүйесі мемлекеттік бақылаудың жоғары деңгейімен ерекшеленеді. «Data Security Law» және «Personal Information Protection Law» заңдары деректерді жинау, сақтау, өңдеу және трансшекаралық беру тәртібін егжей-тегжейлі реттейді. Сонымен қатар стратегиялық маңызы бар деректерге қатысты арнайы құқықтық режим белгіленген.

ТМД мемлекеттері ішінде Ресей Федерациясы мен Өзбекстанның тәжірибесі назар аударуға тұрарлық. Ресейде дербес деректерді қорғау мәселелері «Персональные данные туралы» федералдық заңмен реттеледі және ақпараттық қауіпсіздік саласында мамандандырылған мемлекеттік бақылау жүйесі қалыптасқан. Өзбекстанда соңғы жылдары цифрлық трансформацияға байланысты деректерді қорғау және ақпараттық қауіпсіздік саласындағы заңнаманы жаңғырту бойынша бірқатар реформалар жүргізілуде. Бұл тәжірибе Қазақстан үшін өңірлік ерекшеліктерді ескере отырып, ұлттық деректерді басқару жүйесін жетілдіру тұрғысынан маңызды.

Жоғарыда қарастырылған халықаралық тәжірибе деректерді басқарудың тиімді жүйесі тәуелсіз қадағалау органдарының қызметіне, нақты құқықтық рәсімдерге және жасанды интеллект жүйелерінің қауіпсіздігін тұрақты бақылауға негізделуі тиіс екенін көрсетеді.

Жүргізілген зерттеу нәтижесінде авторлар Қазақстан Республикасында деректер мен жасанды интеллектті реттеудің ұлттық моделін дамытуға бағытталған негізгі теориялық және қолданбалы тұжырымдарды қалыптастырды.

Біріншіден, тек дербес деректерді қорғауға негізделген дәстүрлі реттеу моделінің қазіргі цифрлық экожүйелердің жұмыс істеу ерекшеліктеріне сәйкес келмейтіні негізделді. Авторлар деректер мен алгоритмдік жүйелердің бүкіл өмірлік циклін қамтитын кешенді data governance моделіне көшу қажеттігін дәлелдейді.

Екіншіден, авторлық деректердің құқықтық режимінің төрт деңгейлі моделі әзірленді, оған объектілік, субъектілік, рәсімдік және институционалдық реттеу деңгейлері кіреді. Аталған модель дербес деректердің, оқыту датасеттерінің, синтетикалық деректердің және алгоритмдік өңдеу нәтижелерінің құқықтық режимін жүйелі түрде ажыратуға мүмкіндік береді.

Үшіншіден, Қазақстан Республикасының қолданыстағы заңнамасында жоғары тәуекелді жасанды интеллект жүйелеріне арналған оқыту датасеттерінің сапасы мен репрезентативтілігін реттеу бөлігінде нормативтік олқылық бар екені анықталды. Авторлар алгоритмдік жүйелердің тәуекелдерін бағалау мен аудиттің міндетті рәсімдерін заңнамалық тұрғыдан бекіту қажеттігі туралы қорытындыға келеді.

Төртіншіден, Қазақстандағы жасанды интеллектті реттеу моделі EU AI Act еуропалық моделіне жақын тәуекелге бағдарланған бағытта дамып келе жатқаны дәлелденді, алайда ұлттық заңнамада деректер субъектілерінің құқықтарын және алгоритмдік шешімдердің адресаттарын қорғауға арналған процессуалдық кепілдіктер әлі де жеткілікті деңгейде дамымаған.

Бесіншіден, авторлар Қазақстан Республикасының заңнамасын жетілдірудің келесі практикалық бағыттарын ұсынды:

- жоғары тәуекелді жасанды интеллект жүйелерінің адам құқықтарына ықпалын міндетті бағалауды енгізу;
- датасеттер сапасының стандарттарын әзірлеу;
- тәуелсіз алгоритмдік аудит рәсімдерін енгізу;

- алгоритмдік маңызы бар шешімдерге дау айту құқығын бекіту;
- синтетикалық контентті таңбалау тетіктерін дамыту.

Зерттеу нәтижелерінің ғылыми маңыздылығы Қазақстанның цифрлық экономикасы үшін деректердің құқықтық режимінің тұтас тұжырымдамасын қалыптастыруда көрінеді. Ал практикалық маңыздылығы ұсынылған ережелерді жасанды интеллект, цифрлық реттеу және адам құқықтарын қорғау саласындағы заңнаманы әзірлеу барысында пайдалану мүмкіндігімен сипатталады.

**Қорытынды**

Зерттеу нәтижелері негізінде Қазақстан Республикасының заңнамасында жоғары тәуекелді жасанды интеллект жүйелерін құқықтық реттеуге бағытталған келесі шараларды енгізу ұсынылады:

1. Жоғары тәуекелді жасанды интеллект жүйелерінің заңнамалық анықтамасын бекіту және оларды тәуекел деңгейіне қарай жіктеу.
2. Денсаулық сақтау, құқық қорғау қызметі, сот төрелігі, қаржы секторы, білім беру және мемлекеттік басқару салаларында қолданылатын жоғары тәуекелді жасанды интеллект жүйелері үшін міндетті мемлекеттік бағалау және сертификаттау рәсімін енгізу.
3. Жасанды интеллект жүйелерін әзірлеушілер мен операторлар үшін алгоритмдердің ашықтығы мен түсіндірмелілігі қағидатын бекіту.
4. Автоматтандырылған шешімдердің нәтижесінде азаматтардың құқықтары мен заңды мүдделеріне зиян келтірілген жағдайда құқықтық жауапкершілік тетіктерін нақтылау.
5. Жоғары тәуекелді жүйелерді пайдаланушылар үшін деректер сапасына, киберқауіпсіздікке және тәуекелдерді басқаруға қатысты міндетті талаптарды белгілеу.
6. Жасанды интеллект жүйелерінің құқықтар мен бостандықтарға ықпалын алдын ала бағалау (AI Impact Assessment) институтын енгізу.
7. Жоғары тәуекелді жасанды интеллект жүйелерінің ұлттық тізілімін қалыптастырып, олардың қызметіне тұрақты мемлекеттік мониторинг жүргізу.

Аталған ұсыныстар Қазақстан Республикасында Big Data және жасанды интеллект экожүйелеріндегі деректерді өңдеудің құқықтық режимін жетілдіруге, азаматтардың құқықтарын қорғауды күшейтуге және цифрлық технологияларды қауіпсіз дамытуға мүмкіндік береді.

Ақпараттық экономикадан деректер экономикасына көшу заңнамалық реттеудің логикасын өзгертуді талап етеді. Жасанды интеллект технологияларының қарқынды дамуы және үлкен деректер массивтерін өңдеу жағдайында тек дербес деректерді қорғауға бағытталған дәстүрлі тәсілдер жеткіліксіз болып табылады. Қазіргі цифрлық экожүйелер деректерді үздіксіз алмасу, қайта пайдалану және алгоритмдік өңдеу негізінде жұмыс істейді. Бұл деректердің жиналуы мен дайындалуынан бастап, олардың алгоритмдік жүйелерде пайдаланылуына және нәтижелердің кейінгі мониторингіне дейінгі бүкіл өмірлік циклін қамтитын кешенді data governance жүйесін қалыптастыруды талап етеді [7, 6 б.].

Еуропалық тәжірибе көрсеткендей, деректерді қорғау тетіктерін, деректерге қолжетімділікті реттеуді және жасанды интеллект жүйелерінің жұмыс істеуін бақылауды біріктіретін интеграцияланған реттеу моделі ең перспективалы болып табылады. Атап айтқанда, EU AI Act тәуекелге бағдарланған реттеу жүйесін бекітеді, оның шеңберінде жасанды интеллект жүйелері адам құқықтары мен бостандықтары үшін ықтимал тәуекел деңгейіне қарай жіктеледі. Жоғары тәуекелді жүйелер үшін тәуекелдерді басқаруды, оқытушы датасеттердің сапасын қамтамасыз етуді, алгоритмдердің ашықтығын, техникалық құжаттаманы жүргізуді, адам тарапынан бақылау тетігін және маркетингтен кейінгі мониторинг процедураларын қоса алғанда, арнайы талаптар енгізіледі [8, 14 б.].

Қазақстан Республикасы 2025–2026 жж. іс жүзінде осыған ұқсас бағытта қозғалысты бастады. Қазақстан Республикасының «Жасанды интеллект туралы» Заңын қабылдау және Цифрлық кодекстің енгізілуі жасанды интеллект пен деректерді реттеудің ұлттық жүйесін қалыптастыруға негіз қалады. Бұл нормативтік-құқықтық актілер ЖИ-ді пайдаланудың базалық принциптерін бекітеді, ең қауіпті практикаларға шектеулер қояды және алгоритмдік

жүйелердің ашықтығы бойынша талаптар енгізеді. Дегенмен, қолданыстағы заңнама деректерді басқаруға, датасеттердің сапасына және алгоритмдік жүйелердің аудитіне байланысты процедуралық механизмдерді одан әрі егжей-тегжейлі пысықтауды қажет етеді [2].

Қазақстан үшін ұсынылып отырған деректердің құқықтық режимінің авторлық моделі инновациялық даму мен адам құқықтарын қорғау арасындағы теңгерімді қамтамасыз ете алатын тұтас реттеу архитектурасын қалыптастыруға бағытталған. Бұл модель бірнеше өзара байланысты элементтерді қамтиды. Біріншіден, деректер объектілерін саралау – бұл дербес деректер, иесіздендірілген ақпарат массивтері, оқытушы датасеттер, синтетикалық деректер және жасанды интеллект жүйелері жұмысының нәтижелері арасындағы айырмашылықты білдіреді. Екіншіден, цифрлық экожүйе субъектілері – алгоритм әзірлеушілер, модель жеткізушілер, деректер операторлары, ендіруші ұйымдар және соңғы пайдаланушылар арасындағы рөлдерді нақты бөлу. Дәл осы рөлдердің бөлінісі деректер сапасына, алгоритмдердің ашықтығына және заңнама талаптарының сақталуына жауапкершілікті айқындайды.

Модельдің үшінші элементі – датасеттің өмірлік циклін процедуралық реттеу. Қазіргі заманғы жасанды интеллект жүйелерінде деректер бірнеше кезеңнен өтеді: жинау, тазалау, құрылымдау, модельді оқыту, тестілеу, ендіру және кейінгі мониторинг. Осы кезеңдердің әрқайсысында деректердің шығу тегінің заңдылығына, олардың сапасы мен репрезентативтілігіне, сондай-ақ модельдерді оқытудың дереккөздері мен параметрлерін құжаттандыруға қатысты арнайы талаптар қолданылуы тиіс. Мұндай тәсіл алгоритмдік дискриминация тәуекелдерін барынша азайтуға мүмкіндік береді және қоғамның жасанды интеллект жүйелеріне деген сенімін арттырады .

Модельдің төртінші элементі деректер субъектілері мен алгоритмдік шешімдердің адресаттарының құқықтарын кепілдендірумен байланысты. Автоматтандырылған шешім қабылдау жүйелерінің таралу жағдайында алгоритмнің қолданылуы туралы ақпарат алу құқығы, деректерге қолжетімділік құқығы, дәл емес мәліметтерді түзету құқығы және жасанды интеллектіні пайдалана отырып қабылданған қолайсыз шешімдерге дауласу құқығы ерекше маңызға ие болады. Бұл құқықтарды іске асыру алгоритмдердің түсіндірілу тетіктерін дамытумен қатар жүруі тиіс, бұл пайдаланушыларға жүйенің бастапқы кодын ашу қажеттілігінсіз шешім қабылдау логикасын түсінуге мүмкіндік береді.

Модельдің бесінші элементі институционалдық бақылау мен жауапкершілікке қатысты. Жоғары тәуекелді жасанды интеллект жүйелері үшін алгоритмдердің қауіпсіздік пен ашықтықтың белгіленген талаптарына сәйкестігін тексеруге мүмкіндік беретін міндетті тәуелсіз аудитті енгізу қажет. Генеративті жасанды интеллект модельдерін пайдаланған жағдайда, синтетикалық контентті таңбалау презумпциясын бекіткен жөн, бұл дезинформация мен манипуляциялық практикалардың таралу тәуекелдерін төмендетуге мүмкіндік береді. Бұл ретте жауапкершілік сараланған болуы және цифрлық экожүйенің әрбір қатысушысының – модель әзірлеушіден бастап жүйе операторы мен соңғы пайдаланушыға дейінгі рөлін ескеруі тиіс.

Қолданбалы тұрғыда Қазақстандағы деректерді реттеудің ұлттық моделін одан әрі дамыту бірнеше негізгі бағыттарды іске асыруды көздейді. Біріншіден, алгоритмдік модельдерді оқыту үшін пайдаланылатын датасеттердің сапасы мен репрезентативтілігінің заңға тәуелді стандарттарын әзірлеу қажет. Екіншіден, қоғамдық секторда жоғары тәуекелді жасанды интеллект жүйелерін ендіру кезінде адам құқықтары мен бостандықтарына әсерін бағалау процедурасын енгізген жөн. Үшіншіден, жасанды интеллектінің айтарлықтай қатысуымен қабылданатын алгоритмдік маңызды шешімдерге тиімді шағымдану құқығын бекіту керек. Соңында, синтетикалық деректердің құқықтық режимін егжей-тегжейлі сипаттап, жасанды интеллектінің генеративті модельдері жасаған контентті таңбалауға қойылатын міндетті талаптарды белгілеу қажет.

Осылайша, толыққанды data governance режимін қалыптастыру цифрлық экономиканың тұрақты дамуының негізгі шартына айналуда. Инновацияларды қолдау мен адам құқықтарын тиімді қорғауды ұштастыратын теңгерімді реттеу жүйесін құру Қазақстан Республикасына алдыңғы қатарлы халықаралық практикалармен салыстыруға келетін деректер мен жасанды интеллектіні реттеудің заманауи ұлттық моделін қалыптастыруға мүмкіндік береді.

Авторлар Қазақстан Республикасының заңнамасын одан әрі дамыту жекелеген цифрлық технологияларды фрагментарлық реттеуге емес, деректерді қорғау, жасанды интеллектті

реттеу және адам құқықтарын қорғау тетіктерін біріктіретін бірыңғай data governance жүйесін қалыптастыруға бағытталуы тиіс деген қорытындыға келеді. Ұсынылған модель технологиялық даму, мемлекеттің цифрлық егемендігі және жеке тұлға құқықтарының кепілдіктері арасындағы тепе-теңдікті қамтамасыз ететін цифрлық реттеудің тұрақты архитектурасын қалыптастыруға мүмкіндік береді.

## ӘДЕБИЕТТЕР

1 Floridi L. The Ethics of Artificial Intelligence. Oxford University Press, 2023. DOI: 10.1093/oso/9780190905033.001.0001

2 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: https://eur-lex.europa.eu (accessed: 10.01.2026)

3 Mantelero A. Artificial Intelligence and Data Protection: Challenges and Opportunities // Computer Law & Security Review. 2024. DOI: 10.1016/j.clsr.2024.105781

4 Kuner C. Transborder Data Flows and Data Governance in the Age of Artificial Intelligence // International Data Privacy Law. 2024. DOI: 10.1093/idpl/ipad035

5 Жасанды интеллект туралы: Қазақстан Республикасының Заңы 2025 жылғы 17 қарашадағы № 230-VIII ҚРЗ. // Информационно-правовая система «Әділет». URL: https://adilet.zan.kz/rus/docs/Z2500000230 (өтініш берілген күн: 10.01.2026)

6 OECD Digital Economy Outlook 2023. OECD Publishing. URL: https://www.oecd.org (accessed: 16.02.2026)

7 Floridi L., Cowls J. A Unified Framework of Five Principles for AI in Society // Harvard Data Science Review. 2022. DOI: 10.1162/99608f92.8cd550d1

8 Veale M., Borgesius F. Demystifying the Draft EU Artificial Intelligence Act // Computer Law Review International. 2021. DOI: 10.9785/cri-2021-0401

9 Bryson J. Artificial Intelligence Governance and the Rule of Law // Science and Engineering Ethics. 2023. DOI: 10.1007/s11948-023-00373-2

10 Crawford K. Atlas of AI. Yale University Press, 2021. DOI: 10.2307/j.ctv1ghv45t

11 Cath C., Wachter S., Mittelstadt B. Artificial Intelligence and the Law // Nature Machine Intelligence. 2024. DOI: 10.1038/s42256-024-00611-z

12 Kitchin R. Big Data, New Epistemologies and Paradigm Shifts // Big Data & Society. 2022. DOI: https://doi.org/10.1177/20539517221082574

13 Hildebrandt M. Smart Technologies and the End(s) of Law. Edward Elgar Publishing, 2022. DOI: https://doi.org/10.4337/9781789908787 (accessed: 23.03.2026)

14 European Commission. EU Justice Scoreboard 2024. URL: https://commission.europa.eu (accessed: 29.03.2026)

15 UNCITRAL Technical Notes on Online Dispute Resolution. URL: https://uncitral.un.org (accessed: 29.03.2026)

16 Қазақстан Республикасы Үкіметінің 2024–2029 жылдарға арналған жасанды интеллектті дамыту тұжырымдамасын бекіту туралы: Қазақстан Республикасы Үкіметінің 2024 жылғы 24 шілдедегі № 592 қаулысы. – Астана, 2024.

17 Ережепқызы Р. Экологическая миграция: международно-правовые основы, цифровые инструменты управления и практика Казахстана // Journal of Actual Problems of Jurisprudence (Хабаршы. Заң сериясы). – 2025. – Т. 116. – № 4. – С. 78–89.

18 Нұрғалым Қ.С. және т.б. Цифрлық технологиялардың құқықтық реттелуі: жасанды интеллект және дербес деректерді қорғау // Вестник КазНПУ имени Абая. Серия: Международная жизнь и политика. – 2026. – Т. 1. – № 84. – Б. 45–57.

19 Amantay A., Nurmagambetov A.M., Akhpanov A.N. Жасанды интеллект құралдарын қолдану тұтынушылардың сот төрелігіне қолжетімділігін қамтамасыз ету әдісі ретінде // Scientific and Legal Journal «Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan». – 2025. – Т. 80. – № 3. – Б. 112–124.

20 Шошаева Л., Аманбаева А. Искусственный интеллект как правовая категория // ҚЭУ Жаршысы: Экономика, философия. – 2023. – № 4. – С. 99–105.

## REFERENCES

1 Floridi L. (2023) The Ethics of Artificial Intelligence. Oxford University Press. DOI: 10.1093/oso/9780190905033.001.0001 (In English)

2 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: https://eur-lex.europa.eu (accessed: 10.01.2026) (In English)

3 Mantelero A. (2024) Artificial Intelligence and Data Protection: Challenges and Opportunities // Computer Law & Security Review. DOI: 10.1016/j.clsr.2024.105781 (In English)

4 Kuner C. (2024) Transborder Data Flows and Data Governance in the Age of Artificial Intelligence // International Data Privacy Law. DOI: 10.1093/idpl/ipad035 (In English)

5 Jasandy intelekt turaly: Qazaqstan Respublikasynyñ Zañy 2025 jylğy 17 qaraşadağy No. 230-VIII QRZ. // İnformasionno-pravovaia sistema «Ädılet». URL: https://adilet.zan.kz/rus/docs/Z2500000230 (ötınış berılgen kün: 10.01.2026) (In Kazakh)

6 OECD Digital Economy Outlook 2023. OECD Publishing. URL: https://www.oecd.org (accessed: 16.02.2026) (In English)

7 Floridi L., Cowls J. (2022) A Unified Framework of Five Principles for AI in Society // Harvard Data Science Review. DOI: 10.1162/99608f92.8cd550d1 (In English)

8 Veale M., Borgesius F. (2021) Demystifying the Draft EU Artificial Intelligence Act // Computer Law Review International. DOI: 10.9785/cri-2021-0401 (In English)

9 Bryson J. (2023) Artificial Intelligence Governance and the Rule of Law // Science and Engineering Ethics. DOI: 10.1007/s11948-023-00373-2 (In English)

10 Crawford K. (2021) Atlas of AI. Yale University Press. DOI: 10.2307/j.ctv1ghv45t (In English)

11 Cath C., Wachter S., Mittelstadt B. (2024) Artificial Intelligence and the Law // Nature Machine Intelligence. DOI: 10.1038/s42256-024-00611-z (In English)

12 Kitchin R. (2022) Big Data, New Epistemologies and Paradigm Shifts // Big Data & Society. DOI: https://doi.org/10.1177/20539517221082574 (In English)

13 Hildebrandt M. (2022) Smart Technologies and the End(s) of Law. Edward Elgar Publishing. DOI: https://doi.org/10.4337/9781789908787 (accessed: 23.03.2026) (In English)

14 European Commission. EU Justice Scoreboard 2024. URL: https://commission.europa.eu (accessed: 29.03.2026) (In English)

15 UNCITRAL Technical Notes on Online Dispute Resolution. URL: https://uncitral.un.org (accessed: 29.03.2026) (In English)

16 Qazaqstan Respublikasy Ükımetınıñ 2024–2029 jyldarğa arnalğan jasandy intelekttı damytu tūjyrymdamasyn bekıtu turaly: Qazaqstan Respublikasy Ükımetınıñ 2024 jylğy 24 şıldedegı No. 592 qaulysy. Astana, 2024. (In Kazakh)

17 Erezhepқyzy R. (2025) Jekologicheskaja migracija: mezhdunarodno-pravovye osnovy, cifrovye instrumenty upravlenija i praktika Kazahstana // Journal of Actual Problems of Jurisprudence (Habarşy. Zañ seriasy). V. 116. No. 4. P. 78–89. (In Russian)

18 Nūrğalym Q.S. jäne t.b. (2026) Sifrlyq tehnologialardyñ qūqyqtyq rettelu: jasandy intelekt jäne derbes derekterdı qorğau // Vestnik KazNPU imeni Abaja. Serija: Mezhdunarodnaja zhizn' i politika. V. 1. No. 84. P. 45–57. (In Kazakh)

19 Amantay A., Nurmagambetov A.M., Akhpanov A.N. (2025) Jasandy intelekt qūraldaryn qoldanu tūtynuşylardyñ sot törelıgıne qoljetımdılıgın qamtamasyz etu ädısı retınde // Scientific and Legal Journal «Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan». Vol. 80. No. 3. P. 112–124. (In Kazakh)

20 Shoshaeva L., Amanbaeva A. (2023) Iskusstvennyj intellekt kak pravovaja kategorija // QEU Jarşysy: Jekonomika, filosofija. No. 4. P. 99–105. (In Russian)

**ТҰРЫСБЕК Ж.Б .,*[1]**
докторант.
*e-mail: miss_zhanara@mail.ru
ORCID ID: 0009-0001-1575-4839
**САРИНА С.А.,[1]**
к.ю.н., ассоциированный профессор.
e-mail: s.sarina@turan-edu.kz
ORCID ID: 0000-0002-1414-027X
**ДАМИАН С.,[2]**
PhD, ассистент-профессор.
e-mail: damian.cyman@pravo.ug.edu.pl
ORCID ID: 0000-0002-1443-8981
**ИСМАИЛОВ А.А.,[3]**
к.ю.н., ст. преподаватель.
e-mail: atahozha@mail.ru
ORCID ID: 0009-0002-1337-5920
[1]Университет «Туран»,
г. Алматы, Казахстан
[2]Гданьский университет,
г. Гданьск, Польша
[3]Южно-Казахстанский исследовательский
университет им. М. Ауэзова,
г. Шымкент, Казахстан

# ПРАВОВОЙ РЕЖИМ ОБРАБОТКИ ДАННЫХ В ЭКОСИСТЕМАХ BIG DATA И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: РАЗВИТИЕ НАЦИОНАЛЬНОЙ МОДЕЛИ РЕГУЛИРОВАНИЯ В РЕСПУБЛИКЕ КАЗАХСТАН

**Аннотация**

Стремительное развитие технологий Big Data и искусственного интеллекта трансформирует традиционные подходы к правовому регулированию обработки данных. В условиях цифровых экосистем классическая модель защиты персональных данных уже не охватывает весь жизненный цикл информации, включающий подготовку обучающих датасетов, алгоритмическую обработку, использование синтетических данных и функционирование систем искусственного интеллекта. В статье исследуются особенности формирования национальной модели регулирования data governance в Республике Казахстан и проводится ее сопоставление с рискориентированным подходом Европейского союза, закрепленным в EU AI Act. Авторами обосновано, что современный правовой режим данных должен строиться как комплексная система регулирования, охватывающая объектный, субъектный, процедурный и институциональный уровни. Предлагается авторская интегрированная модель правового режима данных, основанная на разграничении персональных данных, обучающих датасетов, синтетических данных и результатов алгоритмической обработки. Сделан вывод о необходимости формирования специальных процедур аудита высокорисковых ИИ-систем, оценки воздействия на права человека и внедрения механизмов алгоритмической прозрачности. Практическая значимость исследования заключается в разработке предложений по совершенствованию законодательства Республики Казахстан в сфере искусственного интеллекта и оборота данных.

**Ключевые слова:** Big Data, искусственный интеллект, data governance, алгоритмическая прозрачность, синтетические данные, системы искусственного интеллекта высокого риска.

**TURYSBEK Zh.B.,*[1]**
PhD student.
*e-mail: miss_zhanara@mail.ru
ORCID ID: 0009-0001-1575-4839
**SARINA S.A.,[2]**
c.l.s., associate professor.
e-mail: s.sarina@turan-edu.kz
ORCID ID: 0000-0002-1414-027X
**DAMIAN C.,[3]**
PhD, assistant professor.
e-mail:damian.cyman@pravo.ug.edu.pl
ORCID ID: 0000-0002-1443-8981
**ISMAILOV A.A.,[4]**
c.l.s., senior lecturer
e-mail: atahozha@mail.ru
ORCID ID: 0009-0002-1337-5920
[1]Turan University,
Almaty, Kazakhstan
[2]University of Gdansk,
Gdansk, Poland
[3]M. Auezov South Kazakhstan Research University,
Shymkent, Kazakhstan

# LEGAL FRAMEWORK FOR DATA PROCESSING IN BIG DATA AND ARTIFICIAL INTELLIGENCE ECOSYSTEMS: DEVELOPMENT OF A NATIONAL REGULATORY MODEL IN THE REPUBLIC OF KAZAKHSTAN

**Abstract**

The rapid development of Big Data and artificial intelligence technologies is transforming traditional approaches to the legal regulation of data processing. In the context of digital ecosystems, the classical model of personal data protection no longer covers the entire information lifecycle, including the preparation of training datasets, algorithmic processing, the use of synthetic data, and the functioning of artificial intelligence systems. The article examines the specific features of the formation of the national data governance regulatory model in the Republic of Kazakhstan and compares it with the risk-based approach of the European Union enshrined in the EU AI Act. The study substantiates that the modern legal regime for data should be constructed as a comprehensive regulatory system encompassing objective, subjective, procedural, and institutional levels. An original integrated model of the legal regime for data is proposed, based on the differentiation between personal data, training datasets, synthetic data, and the results of algorithmic processing. It is concluded that there is a need to establish special procedures for auditing high-risk AI systems, assessing their impact on human rights, and implementing mechanisms of algorithmic transparency. The practical significance of the study lies in the development of proposals for improving the legislation of the Republic of Kazakhstan in the field of artificial intelligence and data circulation.

**Keywords:** Big Data, artificial intelligence, data governance, algorithmic transparency, synthetic data, high-risk AI systems.

Мақаланың редакцияға түскен күні: 12,04,2026