ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ
ЗАҢНАМА ЖӘНЕ ҚҰҚЫҚТЫҚ АҚПАРАТ
ИНСТИТУТЫНЫҢ ЖАРШЫСЫ
ҒЫЛЫМИ-ҚҰҚЫҚТЫҚ ЖУРНАЛЫ
ISSN 2788-5283
eISSN 2788-5291
ТОМ 81, НӨМІРІ 1(2026), 359-369

**ӘОЖ 342.723**
**ҒТАМР 10.87.27**
**DOI 10.52026/2788-5291_2026_81_1_359**
**Ғылыми мақала**

**© Ә.М. Көптлеуова[1], 2026**
[1]Қазақстан Республикасының Заңнама және құқықтық ақпарат институты, Астана, Қазақстан
(e-mail: [1]asemaikoptleuova9@gmail.ru)

# ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУ САЛАСЫНДАҒЫ ШЕТЕЛДІК ҮРДІСТЕРДІ ТАЛДАУ

**Аннотация.** Бұл мақалада автор Оңтүстік Корея, Жапония, Сингапур және Канада мемлекеттерінің мысалында дербес деректерді қорғау саласындағы заманауи шетелдік үрдістерге талдау жасайды. Зерттеу барысында дербес деректерді өңдеуді құқықтық реттеу тәсілдері, цифрлық үдерістердің ашықтығын қамтамасыз ету талаптарының дамуы қарастырылады. Атап айтқанда, Оңтүстік Кореяның PIPA, Сингапурдың PDPA, Жапонияның APPI және Канаданың PIPEDA заңдарына талдау жүргізіледі. Осы мақала негізінде аталған елдердің кең өкілеттіктерге ие, тәуелсіз арнайы жұмыс істейтін мемлекеттік органдары мен ұйымдары ерекше назар аударатын негізгі бағыттар анықталады. Ал заңнамаларды талдау дербес деректерді қорғаудың заманауи үрдістерін көрсетеді.

Қазіргі уақытта деректерді қорғауда мінсіз жүйе жоқ. Шетелдік тәжірибе көрсеткендей, дербес деректерді қорғау заңнамасы үнемі өзгерістерге бейімделетін, динамикалық сипатқа ие болып келеді. Құқықтық нормалар технологиялық өзгерістер мен жаңа киберқауіптерге сәйкес үнемі жаңартылып, деректер субъектілерінің құқықтарын тиімді қорғауға мүмкіндік беруі тиіс.

Зерттеу нәтижесі көрсеткендей, белсенді және жүйелі саясат дербес деректерді қорғауда тек құпиялықты сақтаумен шектелмейді. Сонымен қатар, ол пайдаланушылардың цифрлық платформаларға сенімін арттыруға, ақпараттық жүйелердің тұрақтылығын қамтамасыз етуге және технологиялық өзгерістер кезінде цифрлық инфрақұрылымның тиімді жұмысын қолдауға ықпал етеді

Автор дербес деректерді тиісінше қорғауды қамтамасыз ету реттеуші органдар және өзге де мүдделі тараптар үшін басым бағыттардың бірі болуы қажет екенін алға тартады. Өйткені халықаралық және ұлттық стандарттарды жүйелі түрде сақтау қауіпсіз, тұрақты және үнемі дамып отыратын цифрлық экожүйе қалыптастыруға мүмкіндік береді.

**Түйінді сөздер:** дербес деректерді қорғау; халықаралық құқық; цифрлық орта; құпиялылықты сақтау; дербес деректерді өңдеу.

## Кіріспе

Ғаламдық цифрландыру мен ақпараттық технологиялардың қарқынды дамуы өңделетін дербес деректер көлемінің айтарлықтай өсуіне алып келді. Онлайн-сервистердің кеңінен таралуы, жасанды интеллект пен биометриялық технологияларды енгізу жеке тұлғаларға қатысты ақпаратты жинау мен өңдеуді жеделдетіп, оларды құқықтық қорғау мәселесін өзекті етті. GDPR-дің 4-бабының 1-тармағына сәйкес, дербес деректер анықталған немесе анықталуы мүмкін жеке тұлғаға қатысты ақпарат болып табылады[1], бұл мұндай деректерге арнайы құқықтық режим қолдану қажеттігін айқындайды.

Дербес ақпараттың құпиялылығы мен қауіпсіздігін қамтамасыз ету мемлекеттер үшін басым бағыт болып отыр. Деректердің ірі көлемде таралуы және кибершабуылдардың жиілеуі заң шығарушыларды дербес деректерді қорғаудың арнайы тетіктерін әзірлеуге итермелейді. Әрбір мемлекет ұлттық ерекшеліктерді ескере отырып өзіндік реттеу моделін әзірлейді. Қазіргі уақытта қандай да бір ұлттық режимді абсолютті үлгі немесе деректерді қорғаудың мінсіз жүйесі деп тануға негіз болатын ортақ көзқарас қалыптаспаған.

Жеке өмірге қол сұқпаушылық құқығы адам құқықтарының негізгі санатына жатады. Ақпараттық қауіпсіздік шеңберіндегі құпиялылық технологияларды қолданбауды білдірмейді, ол жеке

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union. – 2016. – L 119/33 // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (date of reference:02.01.2026).

адамның деректеріне заңсыз түрде қол сұғылмайтынына кепілдік беріліп, қоғам өміріне белсенді қатысу мүмкіндігін қамтамасыз етеді. Мұндай кепілдіктердің болмауы азаматтар үшін ұзақ мерзімді жағымсыз салдарға әкелуі мүмкін [1]. Аталған құқық адам құқықтары саласындағы іргелі халықаралық актілерде, оның ішінде 1966 жылғы Азаматтық және саяси құқықтар туралы халықаралық пактінің[2] 17-бабында бекітілген, онда жеке және отбасылық өмірге араласуға тыйым салу, сондай-ақ мемлекеттердің тұлғаны осындай қол сұғушылықтардан қорғау міндеті көзделген.

Жеке деректерді қорғау және құпиялылық саласындағы мамандардың халықаралық қауымдастығының бағалауына сәйкес, 2025 жылға қарай әлемнің 144 мемлекетінде жеке деректерді қорғауға бағытталған құқықтық актілер қабылданған. Алайда оларды құқықтық реттеу тетіктері, қолданылу аясы мен қатаңдық деңгейі мемлекеттер арасында елеулі түрде ерекшеленеді[3]. С.К. Жетписов, Г.А.Алибаева, О.Б.Дубовицкаяның зерттеу жұмысында айтылғандай, заң шығарушы дербес деректерді реттеу мен қорғаудың құқықтық құралдарын үнемі жетілдіріп отыруы керек [2]. Сол себепті шетелдік тәжірибені зерттеу қажеттілігі өзектілікке ие.

Мақаланың мақсаты шетелдік тәжірибені талдау арқылы дербес деректерді қорғау саласындағы шетелдік үрдістерді айқындау және тиімді құқықтық элементтерді анықтау. Зерттеу Канада, Сингапур, Жапония және Оңтүстік Кореядағы дербес деректерді өңдеуді құқықтық реттеу тәсілдерін салыстырмалы талдауға негізделеді.

Сонымен бірге зерттеу шеңберінде келесі ғылыми сұрақтар қарастырылады: а) аталған мемлекеттердегі дербес деректерді қорғауды құқықтық реттеудің негізгі модельдері; ә) деректер операторларының міндеттері мен мемлекеттік қадағалау механизмдері; б) деректердің таралып кетуі, жасанды интеллект және биометриялық деректерді өңдеу жағдайында құқық қолдану тенденциялары.

## Зерттеу материалдары мен әдістері

Зерттеу материалдары ретінде Оңтүстік Кореяның PIPA, Сингапурдың PDPA, Жапонияның APPI және Канаданың PIPEDA заңдары, сондай-ақ осы мемлекеттердің реттеуші органдарының ресми есептері, құқық қолдану тәжірибесі, деректердің таралуы жөніндегі статистикалық мәліметтері және нақты істер бойынша шешімдері пайдаланылды. Зерттеу барысында салыстырмалы-құқықтық және құқық қолдану тәжірибесін зерделеу, жалпы ғылыми талдау әдістері қолданылады.

## Нәтижелер мен талқылау

Әлемде дербес деректерді қорғау мемлекеттік маңызды бағыт ретінде танылып, ұлттық деңгейде нормативтік-құқықтық актілер жүйесі арқылы реттеледі. Әр елде дербес деректерді қорғау саласында зерттеулер жүргізетін, саясатты әзірлейтін және оның орындалуын қадағалайтын арнайы мемлекеттік институттар бар. Бұл институттар сондай-ақ дербес деректерді өңдеудегі тәуекелдерді бағалауды бақылау, статистикалық шолулар дайындау және осыған ұқсас басқа да міндеттермен айналысады.

Осы тұрғыда Корея Республикасы 2011 жылғы «Дербес ақпаратты қорғау туралы» заң (PIPA) негізінде Азияда деректерді қорғаудың ең қатаң әрі институционалдық тұрғыдан қамтамасыз етілген режимдерінің бірін қалыптастырған мемлекет ретінде ерекше ғылыми қызығушылық туғызады.

PIPA бастапқыда жеке өмірге қол сұқпаушылық құқығын конституциялық тұрғыдан түсінуге бағдарланған. PIPA-ның[4] 1-бабында дербес деректерді өңдеудің басым бағыты ретінде тұлғаның қадір-қасиетін және адам құқықтарын қорғау тікелей бекітілген.

Кореялық механизмнің ең маңызды ерекшелігі PIPA деректер айналымына бақылаудың «қатаң» моделін институционалдық тұрғыдан орнықтырып, онда операторлардың дискрециясы субъектінің автономиясын кепілдендіру мақсатында саналы түрде

[2] Международный пакт о гражданских и политических правах от 16 декабря 1966 года // URL: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (дата обращения: 02.01.2026).

[3] Aly Apacible-Bernardo, Kayla Bushey «Data protection and privacy laws now in effect in 144 countries», 28 January 2025 // URL: https://iapp.org/news/a/data-protection-and-privacy-laws-now-in-effect-in-144-countries (date of reference: 02.01.2026).

[4] Personal Information Protection Act, Act No. 16930, Feb. 4, 2020 (Republic of Korea) // URL: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=53044&lang=ENG (date of reference: 02.01.2026).

шектеледі. Мысалы, PIPA-ның 15-бабына сәйкес дербес ақпаратты жинау мен пайдалану тек алдын ала, нақты әрі саналы түрде берілген келісім болған жағдайда ғана жол беріледі. Ал арнайы бекітілген оператор өңдеудің мақсаттарын, деректер көлемін, сақтау мерзімдерін және келісім беруден бас тартудың ықтимал салдарын түсіндіруге міндетті. Бұл тетік формальды келісім беру тәуекелін едәуір төмендетіп, артық деректерді беру шартымен қызметтерді мәжбүрлеп ұсыну тәжірибесін болдырмайды.

Кореяда деректерді қорғау белгілі бір процедуралар жиынтығы емес, ықтимал зиянның көлемін динамикалық түрде басқару ретінде танылады.

Сезімтал дербес деректердің құқықтық режимі ерекше маңызға ие. PIPA-ның 23-бабында оларға денсаулық туралы мәліметтер, биометриялық деректер, саяси және діни нанымдар, кәсіподақтарға мүшелік және жеке өмірдің ең осал қырларына әсер етуі мүмкін өзге де деректер жатқызылады. Мұндай деректерді өңдеуге тек деректер субъектісінің айқын келісімі және қатаң түрде айқындалған заңды мақсат болған жағдайда ғана жол беріледі. Мәселен іс-жүзінде практикада заңнаманың жасанды интеллект дәуірдегі олқылықтары мен олардың шектері көрсетілді. 2019–2022 жылдар аралығында Корея Республикасының ӘМ Инчхон халықаралық әуежайында тұлғаларды сәйкестендіру және қадағалау мақсатында жасанды интеллект жүйесін әзірлеген. Осы үдерісте Корея азаматтары мен шетелдіктерді қоса алғанда, 170 миллионнан астам адамның бет бейнелері мен жеке деректері пайдаланылып, олар жүйені әзірлеуге тартылған жеке ұйымдарға қолжетімді болды.

2021 жылғы қазанда KBS News бұл жүйенің PIPA талаптарын бұзуы мүмкін екені туралы хабарлаған, соның нәтижесінде Корея Республикасының Жеке деректерді қорғау жөніндегі комиссиясы 2021 жылғы желтоқсаннан 2022 жылғы сәуірге дейін тергеу жүргізді. Тергеу барысында жүйе жалпы алғанда заңды деп танылғанымен, PIPA-ның жекелеген бұзушылықтары анықталды. Комиссия бет бейнелерін PIPA-ны қолдану туралы Жарлықтың 18-бабына сәйкес конфиденциалды биометриялық ақпарат ретінде бағалады. Сонымен қатар, PIPC жеке ұйымдардың деректерді өңдеудегі құқықтық мәртебесінің айқын болмағанын атап өтіп, бұл жағдайды деректерді үшінші тұлғаларға беру ретінде саралады. Осыған байланысты Әділет министрлігіне PIPA-ның 26-бабының 2-тармағын бұзғаны үшін 1 миллион вон мөлшерінде әкімшілік айыппұл салынды [3].

Инчхон әуежайы ісі Корея Республикасында бет-әлпетті тану технологияларын құқықтық реттеудегі бірқатар олқылықтарды, атап айтқанда Privacy by Design қағидаты мен жасанды интеллект жүйелерін тәуекелге негізделген жіктеу тетіктерінің жеткіліксіздігін көрсетті [3].

Оңтүстік Кореяның дербес деректерді қорғау деңгейінің GDPR талаптарына сәйкестігін тану жөніндегі өтінімдері 2017 және 2020 жылдары да оң нәтиже бермегенін атап өту керек. Бұған негізгі себеп ретінде тәуелсіз қадағалау органының болмауы және жеке деректерді қорғау саласындағы құқықтық реттеудің жеткіліксіз ауқымы көрсетілді. Осыған байланысты Корея Республикасының үкіметі ұлттық құқықтық жүйені халықаралық стандарттар мен заманауи жаһандық үрдістерге сәйкестендіру мақсатында кешенді құқықтық қайта ұйымдастыру жүргізуге мәжбүр болды [4]. Оңтүстік Кореядағы қазіргі кезеңде дербес деректерді реттеу жүйесінің маңызды институционалдық құрамдас бөлігі «Тұлғалық ақпаратты қорғау комиссиясы» (PIPC)[5]. PIPA заңының 7-бабына сәйкес, Комиссия автономды мемлекеттік орган мәртебесіне ие болып, әкімшілік санкциялар қолдану, цифрлық қызметтерді тұрақты бақылау және деректерді өңдеу стандарттарын бекіту сияқты өкілеттіктерге ие. Мысалы, 2024 жылы ақпараттардың таралып кетуі бойынша 307 хабарламалар қабылданған. Олардың негізгі себептері хакерлік шабуылдар (56%, 171 жағдай), қызметкерлердің қателіктері (30%, 91 жағдай) және жүйелік қателіктер (7%, 23 жағдай). Осыған байланысты, тәжірибеде ең үлкен жиынтық айыппұл 21,62 млрд вон көлемінде белгіленген[6]. Бұл әкімшілік санкциялық жүйесінің

[5] Personal Information Protection Commission // URL: https://www.pipc.go.kr/eng/index.do (date of reference: 02.01.2026).

[6] 개인정보위, 2024년 개인정보 유출 신고 동향 분석결과 발표 // URL: https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=11074 (date of reference: 02.01.2026).

превентивтік сипатта екендігін көрсетеді.

Қоғамдық және мемлекеттік процестердің цифрлануы жағдайында дербес деректерді қорғау саласындағы құқық бұзушылықтардың саны Сингапур Республикасында тұрақты түрде артып отыр. Сингапурдың Дербес деректерді қорғау жөніндегі комиссиясының мәліметтеріне сәйкес, 2017–2019 жылдар аралығында жеке ұйымдар тарапынан дербес деректер туралы заңнаманың бұзылуына байланысты келіп түскен өтініштердің саны екі есеге өсіп, 4,5 мың жағдайды құрады. Бұл статистика жекелеген құқық бұзушылықтардың кездейсоқ сипатын емес, мәселенің әкімшілік бақылау мен комплаенс бақылаудың дербес сегменті ретінде институционалданғанын айғақтайды.

Сингапурде жеке деректерді қорғауды құқықтық реттеудің ерекшелігі жеке деректерге қатысты екі түрлі құқықтық режимді белгілейтін екі нормативтік-құқықтық актінің болуы. Бір режим мемлекеттік мекемелер мен ұйымдарға арналған 2018 жылғы «Мемлекеттік секторды басқару туралы» заңға сәйкес бекітілсе, екінші режим жеке сектор үшін «Дербес деректерді қорғау туралы» заңға сәйкес белгіленеді.

2012 жылғы «Дербес деректерді қорғау туралы» заңы (PDPA) жеке өмірге қол сұқпаушылықтың базалық кепілдіктерін сақтай отырып, цифрлық экономиканы қолдауға бағытталған неғұрлым икемді реттеу моделінің қалыптасқанын көрсетеді. Тұжырымдамалық тұрғыдан PDPA дербес деректерді қорғаудың «базалық стандарты» ретінде рәсімделген және бір мезгілде ұйымдардың деректерді «заңды және ақылға қонымды мақсаттарда» өңдеу қажеттілігін мойындайды. Бұл Сингапурдың дербес деректер саласында қатаң тыйым салушы-келісімге негізделген тәсілді толық көлемде қайталамай, режимді деректер субъектісінің құқықтық мәртебесі мен ұйымдардың экономикалық тұрғыдан негізделген мүдделерін теңгеру арқылы құратынын білдіреді.

Сингапурлық зерттеушілердің еңбектерінде ақылға қонымдылық талаптарының «ашық» табиғаты реттеуді өзгермелі технологиялық жағдайларға бейімдеуге мүмкіндік беретіні және акцентті келісімнің формальды рәсімінен ұйымның нақты адалдығы мен тәуекелдерді басқару қабілетін бағалауға қарай жылжытатыны көрсетіледі [5].

2021 жылы заңнамаға айтарлықтай өзгерістер енгізілді, соның нәтижесінде «болжамды келісім»[7] санатымен және бірқатар жаңа ерекше жағдайлармен толықтырылды. Келісімнің болжамды нысанын енгізу және деректер субъектісінің тікелей, айқын келісімінсіз өңдеудің жаңа негіздерінің белгіленуі заңнаманың бизнестің практикалық қажеттіліктеріне бейімделуін білдіреді. Алайда жүргізілген талдау мұндай икемділік деректерді өңдеудің субъектілердің құқықтары мен мүдделеріне ықпалын бағалау жөніндегі операторлардың қосымша міндеттерімен өтелетінін көрсетеді, бұл ерекшеліктерді еркін және негізсіз қолдануға жол бермейді.

Осыған байланысты, жеке өмірге қол сұқпаушылық құқығы абсолютті сипатқа ие емес екенін ескеру қажет. Бұл құқыққа араласудың әрбір жағдайы заңдылық, қажеттілік пен пропорционалдылық қағидаттарына сәйкестігі тұрғысынан мұқият бағалану тиіс [6].

Сингапурдегі жеке деректерді қорғау механизмінің ерекшелігі PDPA заңында қолданылатын ерекше терминологияда жатыр. Мысалы, «деректер операторы» (data controller) деген терминнің орнына «ұйым» (organisation) термині қолданылады. Бұл термин PDPA бойынша міндеттемелерді орындауға жауапты субъектілерді білдіреді және кең мағынада барлық жеке тұлғаларды, заңды тұлғаларды және корпоративтік емес бірлестіктерді қамтиды.

Warren B.Chik пікірінше, Сингапурдың PDPA заңындағы талаптардың сақталуын бағалаудың негізгі өлшемі «ақылға қонымдылық тесті» болып табылады. Бұл тестке сәйкес ұйымның әрекеті нақты жағдайларда объективті түрде орынды әрі тиісінше болған-болмағаны тұрғысынан бағаланады. Аталған стандарт деректерді өңдеу мақсаттарына да, заң талаптарын сақтауға қатысты жалпы міндеттерге де қолданылады және оның мазмұны тиісті міндеттеменің сипатына өзгеріп отырады [5].

Дербес деректерді қорғау жөніндегі

[7] Personal Data Protection Act 2012: 2020 Revised Edition (incorporating amendments up to and including 1 December 2021; comes into operation on 31 December 2021) // URL: https://sso.agc.gov.sg/Act/PDPA2012 (date of reference: 02.01.2026).

жауапты тұлғаны (Data Protection Officer)[8] міндетті түрде тағайындау механизмі арқылы жауапкершіліктің институционалдандырылуын атап өтуге болады. Бұл ұйымішілік деңгейде заңнаманы сақтау тетігін қалыптастырып, сингапурлық модельді еуропалық стандарттарға жақындатады. Сонымен қатар, елеулі деректердің таралып кетуі жағдайлары туралы реттеуші органды және деректер субъектілерін хабардар ету міндеті ашықтықты арттырып, киберқауіпсіздікке инвестиция салуды ынталандырады.

Сингапур құқық қолдану тәжірибесіндегі ең айқын қазіргі үрдіс enforcement шараларының кибертәуекелдермен байланыстырылуы. PDPC-ның 2023–2024 жылдарға арналған деректердің таралып кетуі ландшафты туралы есебінде ірі көлемдегі тараулардың 41%-ға артқаны тіркелген, киберинциденттер реттеуші мәжбүрлеу шараларын қолданған жағдайлардың 82%-ын құраған. Бұл практика PDPC кейстерімен де расталады. «Breach of the Protection Obligation by Payroll2U»[9] ісі бойынша шешімде Protection Obligation міндеттемесінің бұзылуы қорғаныс шараларының жеткіліксіздігімен байланыстырылып, айыппұл тағайындау кезінде PDPA-ның s48J(6) нормасында көзделген факторлар тікелей ескерілген. Бұл санкциялық саясаттың жекешелендірілген сипатқа көшкенін және «ақылға қонымды шаралар» стандартының тәуекелдерді басқару ұғымдары арқылы құқықтық тұрғыдан нақтыланғанын көрсетеді.

Жапонияның «Дербес ақпаратты қорғау туралы» заңының (APPI) талдауы дербес деректерді қорғаудың құқықтық режимі біртіндеп, бірақ жүйелі түрде күшейтіліп келе жатқанын көрсетеді. 2015 және 2020 жылдардағы түзетулердің 2022 жылы күшіне енуі реттеудің фрагменттілігін жойып, мемлекеттік және жеке секторлар үшін бірыңғай құқықтық режимді белгіледі.

APPI-дің негізгі принциптері жаһандық стандарттарға сәйкес келеді. Дербес ақпарат тек нақты және заңды мақсаттар үшін ғана жиналуы тиіс, ал оны кейіннен пайдалану бастапқыда мәлімделген мақсаттарға қайшы келмеуі керек. Деректерді үшінші тұлғаларға беру, жалпы ереже бойынша, тек деректер субъектісінің алдын ала келісімі болған жағдайда ғана мүмкін болады. APPI-де «сезімтал дербес ақпаратқа» 10 нақты анықтама берілген. Оған нәсілдік немесе этникалық тегі мен діни сенімі және денсаулық жағдайы мен соттылығы туралы мәліметтер, сондай-ақ дискриминацияға немесе өзге де жағымсыз салдарға әкеп соғуы мүмкін басқа да деректер жатады. Мұндай жіктеу мәліметтердің ең осал санаттарын күшейтілген түрде қорғауға бағытталған.

Жапондық модельдің ең маңызды ерекшелігі ол құқықтық қорғау құралдарын деректердің экономика үшін «пайдалылығын» сақтауға бағытталған институционалдық тетіктермен ұштастыра отырып, субъектілердің құқықтарын қатар қамтамасыз етуге ұмтылады.

Деректердің таралып кетеуі жөніндегі елеулі инциденттер орын алған жағдайда Дербес ақпаратты қорғау жөніндегі комиссияны (PPC) 11 және зардап шеккен тұлғаларды хабардар ету міндеті ашықтықтың деректер субъектілерінің құқықтарын қорғаудағы негізгі элемент ретінде танылғанын білдіреді. APPI-дің экстерриториялық қолданылуы және дербес деректерді трансшекаралық беру режимі Жапонияның жаһандық реттеу жүйесіне кірігуге ұмтылысын айқын көрсетеді.

Елеулі инциденттер орын алған жағдайда реттеуші органды және зардап шеккен субъектілерді хабардар ету жөніндегі нормативтік міндет ашықтықтың құқықтарды қорғаудың негізгі элементі ретінде танылғанын білдіреді. Бұл міндетті есептіліктің ауқымы арқылы эмпирикалық тұрғыдан да расталады. Реттеушінің 2024 қаржы жылына арналған жылдық есебінде APPI-дің 26(1)-бабы бойынша деректердің таралып кетуі туралы 19 056 хабарлама өңделгені көрсетілген және бұл алдыңғы жылмен (12 120) салыстырғанда өсім бар екені тікелей атап өтіледі. Сонымен

[8] Data Protection Officer // URL: https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers (date of reference: 02.01.2026).

[9] Breach of the Protection Obligation by Payroll2U // URL: https://www.pdpc.gov.sg/all-commissions-decisions/2024/04/breach-of-the-protection-obligation-by-payroll2u (date of reference: 03.01.2026).

[10] Act on the Protection of Personal Information Act No. 57 of 2003 // URL: https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en (date of reference: 03.01.2026).

[11] Personal Information Protection Commission // URL: https://www.ppc.go.jp/en/ (date of reference: 03.01.2026).

бірге хабарламалардың 88,3%-ы зардап шеккендер саны 1000 адамға дейінгі инциденттерге тиесілі, ал аса ірі оқиғалардың үлесі небәрі 0,8% құрайды[12]. Бұл деректер салыстырмалы қорытындылар үшін принципті маңызға ие. Жоғарғы көрсеткіштер режимнің хабардар ету табалдырығының төмендігін және есептелік тәртібінің комплангстік тәртіпке айналғанын білдіреді.

Канадада дербес деректерді қорғау саласында тармақталған заңнама жүйесі жұмыс істейді. Бұл жүйе еуропалық модельге ұқсас, бірақ ұлттық құқықтық жүйенің ерекшеліктеріне бейімделген принциптерге негізделген. 2000 жылы қабылданған және жеке сектордың коммерциялық қызметіне қолданылатын «Жеке ақпаратты қорғау және электрондық құжаттар туралы заң» (PIPEDA)[13] негізгі федералдық акт болып табылады.

PIPEDA-дан бөлек, кейбір провинциялар (Альберта, Британдық Колумбия және Квебек) федералдық заңға «айтарлықтай балама» деп танылған Альбертаның PIPA заңы[14], Британдық Колумбияның PIPA заңы[15] және Квебектің жеке сектордағы жеке ақпаратты қорғау туралы заңы[16] қабылдады. Тиісті провинциялар шегінде PIPEDA-ның орнына дәл осы актілер қолданылады. Жалпы алғанда, бұл нормативтік құжаттар канадалық құпиялылықты қорғау жүйесін қалыптастырады. Мұнда реттеудегі белгілі бір айырмашылықтарға қарамастан жеке ақпаратты жинауға, пайдалануға және ашуға қатысты ортақ тәсіл іске асырылады.

Зерттеуші Teresa Scassa пікірінше, PIPEDA шеңберінде Құпиялылық жөніндегі уәкілдің рөлі көпқырлы сипатқа ие. Ол ұйымдардың заң талаптарын жалпы деңгейде сақтауын арттыруға бағытталған. Екінші жағынан, жеке тұлғалардан түскен шағымдарды тергеп-тексеріп, оларды шешу міндетін атқарады [7].

Канаданың құпиялылық туралы заңнамасы деректерді өңдеудің ашықтығы мен дәлдігінің жоғары стандарттарын қарастырады. Ұйымдар дербес ақпаратты өңдеу саласындағы өз саясаттарын ашық жариялауға, сондай-ақ сақталатын деректердің өзектілігі мен шынайылығын қамтамасыз етуге міндетті. Бұл мәліметтерді жүйелі түрде жаңартып отыруды және дәл емес ақпаратты түзетуді көздейді. Деректер субъектілеріне құқықтардың маңызды кешені берілген:

– ұйымдардағы дербес деректерге қол жеткізу құқығы;

– дәл емес немесе толық емес мәліметтерді түзету құқығы;

– дербес ақпаратты одан әрі өңдеуге берілген келісімді қайтарып алу құқығы.

Бұл құқықтардың іске асырылуы азаматтардың өз жеке ақпаратына тиімді бақылау жасауын қамтамасыз етеді. Аталған қағидаттардың іс жүзінде қалай қолданылатынын Clearview AI компаниясына қатысты іс айқын көрсетеді. 2020 жылы Канаданың Құпиялылық жөніндегі уәкілетті органы аталған компанияның биометриялық деректерді жаппай жинау және пайдалануына байланысты қызметіне федералдық және провинциялық деңгейде бірлескен тергеп-тексеру жүргізуді бастады. Тергеу нәтижесінде Clearview AI дербес деректерді деректер субъектілерінің тиісті келісімінсіз өңдегені, сондай-ақ ашық интернет-көздерде орналастырылған мәліметтерді олар бастапқыда жарияланған контекстке сәйкес келмейтін мақсаттарда пайдаланғаны анықталды. Канадалық уәкілетті орган «жалпыға қолжетімді ақпарат» ұғымы мұндай деректерге қолданылмайтынын атап өтіп, оларды өзара байланысы жоқ әрі жеке тұлғалар үшін ықтимал зиянды мақсаттарда пайдалануға жол берілмейтінін көрсетті. Сонымен қатар жеке тұлғалардың бейнелерін бақылаусыз түрде жаппай көшіру дербес деректерді өңдеудің ақылға қонымды тәжірибесі болып табылмайтыны атап өтілді. Аталған іс Канададағы дербес деректерді қорғау моделінің жеке тұлғаның құқықтары мен бостандықтарының басымдығына бағытталғанын, сондай-ақ

[12] URL: https://www.ppc.go.jp/aboutus/report/annual_report_2024/ (date of reference: 03.01.2026).

[13] Personal Information Protection and Electronic Documents Act // URL: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/ (date of reference: 03.01.2026).

[14] PIPA Alberta // URL: https://www.alberta.ca/personal-information-protection-act (date of reference: 03.01.2026).

[15] Personal Information Protection Act // URL: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00_03063_01 (date of reference: 03.01.2026).

[16] Québec's Act respecting the protection of personal information in the private sector // URL: https://ca.practicallaw.thomsonreuters.com/w-036-3291?transitionType=Default&contextData=(sc.Default)&firstPage=true (date of reference: 03.01.2026).

цифрлық экономика жағдайында дербес ақпаратты шамадан тыс және тәуекелі жоғары өңдеуді шектеуге ұмтылатынын айқын көрсетеді [8].

Зерттеу нәтижелері шетелдік құқықтық жүйелерде дербес деректерді қорғаудың тұрақты моделі қалыптасқанын көрсетеді, ол тұлғаның құқықтық мәртебесінің элементі ретінде деректерді тануға негізделген. Құқықтық жүйелердің айырмашылықтарына қарамастан, Корея Республикасы, Сингапур, Жапония және Канада заңнамалары деректер субъектісінің өз деректері үстіндегі бақылауын күшейтуге, операторлардың жауапкершілігін арттыруға және осы саладағы мемлекеттік қадағалауды институционалдауға бағытталған ортақ үрдісті көрсетеді.

Ең алдымен нәтижелер деректер субъектілерінің құқықтарын кеңейту және тереңдету тенденциясын растайды. Кореяның PIPA заңында, Жапонияның APPI, Сингапурдың PDPA және Канаданың PIPEDA заңдарында қол жеткізу, түзету, жою және өңдеуді шектеу құқықтарының бекітілуі келісімді бір реттік формальды акт ретінде қарастырудан бас тартуды көрсетеді. Шетелдік модельдерде келісім субъект пен деректер операторлары арасындағы үздіксіз құқықтық қатынастың элементі ретінде қарастырылады, бұл тұлғаның автономиясын күшейтіп, құқықтық жүйелерді ақпараттық өзін-өзі анықтау тұжырымдамасына жақындатады.

Екінші негізгі аспект дербес деректер операторларының жауапкершілігін және есептілігін күшейту. Зерттелген мемлекеттерде дербес деректерді қорғау операторлардың алдын алу сипатындағы комплаенс міндеттерімен және кең өкілеттіктерге ие тәуелсіз реттеуші органдардың қызметімен қамтамасыз етіледі. Санкциялық саясаттың ірі әкімшілік айыппұлдармен, міндетті хабарлау рәсімдерімен және ұйымішілік жауапты тұлғаларды тағайындау талаптарымен толықтырылуы деректерді қорғаудың реактивті сипаттан жүйелі тәуекелдерді басқару моделіне ауысқанын көрсетеді.

Үшінші негізгі үрдіс деректердің таралуы, жасанды интеллект және биометриялық деректерді өңдеу жағдайында құқық қолдану тәжірибесінің тәуекелге негізделген тәсілге көшуімен байланысты. Қарастырылған мемлекеттерде биометриялық деректерге қатысты арнайы құқықтық режимдердің қалыптасуы, деректердің таралуы туралы міндетті хабарлау жүйелерінің енгізілуі және киберқауіпсіздік талаптарының күшеюі деректер субъектілерінің құқықтарын қорғаудың институционалдық тетіктерін нақтылай түседі.

Бұл контексте еліміз үшін алынған нәтижелер деректер субъектілерінің құқықтарын нормативтік түрде бекіту ғана емес, оларды жүзеге асырудың процессуалдық механизмдерін дамыту қажеттілігін көрсетеді. Оператордың субъект сұраныстарын орындау жөніндегі нақты міндеттері мен реттеуші органның тиімді бақылауы болмаған жағдайда бұл құқықтар декларативті сипатта қалуы мүмкін. Аталған үрдістер Қазақстандағы жағдаймен салыстырғанда ерекше мәнге ие. 2025 жылғы маусымда 16,3 миллион азаматтың дербес деректерінің ашық қолжетімділікке түсуіне байланысты дербес деректерді қорғау саласындағы институционалдық бақылау және комплаенс тетіктерінің жеткіліксіздігін көрсетті. Бұл жағдай С.К. Жетписовтың цифрландыру жағдайында адам құқықтарын қорғау халықаралық құқық нормалары мен конституциялық кепілдіктердің өзара байланысы арқылы қамтамасыз етілуі тиіс деген ғылыми тұжырымымен сабақтас [2].

Алайда деректердің жаппай таралуы мұндай кепілдіктердің тиімділігі оларды іске асыратын нақты институционалдық және процедуралық механизмдердің болуына тікелей тәуелді екенін айқын көрсетті.

**Қорытынды**

Оңтүстік Корея, Жапония, Сингапур және Канаданы салыстырмалы-құқықтық талдау үшін таңдау бірқатар объективті факторлармен негізделеді. Аталған мемлекеттердің барлығында дербес деректерді қорғаудың орнықты жүйелері қалыптасқан. Бұл жүйелер дамыған цифрлық экономика жағдайында және ақпараттық технологияларды белсенді пайдалану аясында қызмет етеді. Барлық елдерде арнайы заңнама қолданылады және тәуелсіз бақылау органдары жұмыс істейді. Құқық қолдану практикасы тұрақты түрде

жинақталған. Көрсетілген сипаттамалар аталған мемлекеттерді олардың тәжірибесін Қазақстан Республикасының құқықтық жүйесіне бейімдеу мүмкіндіктерін бағалау тұрғысынан үлгілі модельдер ретінде қарастыруға мүмкіндік береді.

Қазақстанда дербес деректер субъектілерінің құқықтарын іске асыру негізінен олардың нормативтік тұрғыда бекітілуімен шектеледі. Бұл ретте рәсімдік тетіктер жеткілікті деңгейде дамымаған. Шетелдік юрисдикцияларда жағдай өзгеше. Атап айтқанда, Канада мен Жапонияда өтініштерді қараудың нақты мерзімдері және уәжделген бас тарту міндеті көзделген. Оңтүстік Корея моделінде тәуелсіз реттеуші органның белсенді қатысуы арқылы қорғау деңгейі күшейтіледі. Сингапурда деректерді қорғауға жауапты тұлғаны міндетті түрде тағайындау қосымша кепілдік ретінде қызмет етеді. Аталған тәжірибе Қазақстанда дербес деректер субъектілерінің құқықтарын институционалдық және рәсімдік тұрғыдан күшейту қажеттігін көрсетеді.

Сезімтал және биометриялық дербес деректерді өңдеу режимі ерекше назар аударуға лайық. Елімізде бұл режим фрагментарлы сипатта қалып отыр және әрдайым технологиялық тәуекелдердің деңгейін толық көлемде көрсете бермейді. Оңтүстік Корея мен Канадада мұндай деректер жоғары қауіп төндіретін деректер ретінде танылады және күшейтілген қорғауға жатады. Жапония моделі сезімтал деректердің нормативтік жіктелуіне негізделсе, Сингапурда өңдеудің жеке тұлғаның құқықтарына ықпалын бағалау тетігі қолданылады. Салыстырмалы талдау биометриялық дербес деректерді реттеудің тәуелсіз құқықтық режимін қалыптастырудың орындылығын растайды.

Зерттеу нәтижесіне сәйкес, дербес деректер операторларының жауаптылығына қатысты тәсілдер де елеулі айырмашылықтармен сипатталады. Қазақстанда жауаптылық шаралары құқық бұзушылықтар анықталғаннан кейін қолданылады. Ал Канадада керісінше accountability қағидатына негізделген превентивтік модель әрекет етеді. Оңтүстік Кореяда бұл тәсіл міндетті техникалық және ұйымдастырушылық шаралар арқылы күшейтілген. Жапония мен Сингапурда комплаенс және тәуекелдерді басқару тетіктері кеңінен пайдаланылады. Мұндай тәжірибе жауаптылық моделін трансформациялау тұрғысынан маңызды болып табылады.

Мемлекеттік қадағалау тетігі де кем емес көрсеткіш болып табылады. Қазақстан Республикасында бақылау функциялары бірнеше орган арасында бөлінген, бұл олардың тиімділігін төмендетеді. Ал талқыланып отырған шетелдік елдерде қадағалау арнайы және институционалды түрде тәуелсіз органдар арқылы жүзеге асырылады, олар нақты санкциялық өкілеттіктерге ие. Бұл дербес деректерді қорғау саласында жүйелі және бірізді бақылауды қамтамасыз етуге мүмкіндік береді.

Жалпы алғанда, шетелдік тенденцияларды талдау оның Қазақстан Республикасында қолданылуының мүмкін екеніндігін көрсетеді. Алайда негізгі механизмдерді ұлттық құқық жүйесіне және құқық қолдану практикасына бейімдеу қажеттігін растайды. Институционалдық, рәсімдік және превентивтік элементтерді жүйелі түрде енгізу дербес деректерді қорғау деңгейін арттыруға, цифрлық технологияларға сенімді нығайтуға және ақпарат қоғамының тұрақты дамуын қамтамасыз етуге мүмкіндік береді.

**Әдебиеттер тізімі:**

1. Серімбетов Н.Н., Жилкайдаров Р.Р. Защита персональных данных в облаках и права физических лиц // ҒЫЛЫМ - НАУКА. Международный научный журнал. 2024. №1 (80). С. 186-192.

2. Жетписов, С.К., Алибаева, Г.А., Дубовицкая, О.Б. Цифрландыру дәуіріндегі дербес деректерді қорғау конституциялық-құқықтық аспект // Қазақстан Республикасының Заңнама және құқықтық ақпарат институтының Жаршысы. 2023. №5 (74). 68 – 76 б.

3. Lee H., Kim E. & Park D.H. Insights from the Incheon Airport Case in South Korea: balancing public safety and individual rights with global scalability analysis // Humanities and Social Sciences Communications. 2025. №12 (1). P.1-11. Available from: https://www.scopus.com/pages/publications/105010714603?origin=resultslist (date of reference: 03.01.2026).

4. Lim S., Oh J. Navigating Privacy: A Global Comparative Analysis of Data Protection Laws // IET Information Security. 2025. №1. P.1-5. Available from: https://www.researchgate.net/publication/388401409_

Navigating_Privacy_A_Global_Comparative_Analysis_of_Data_Protection_Laws/citation/download (date of reference: 02.01.2026).

5. CHIK, Warren B. The reasonableness standard of compliance in the Singapore Personal Data Protection Act // Singapore Academy of Law Journal. 2022. №34. P.352-399. Available from: https://ink.library.smu.edu.sg/sol_research/4588 (date of reference: 02.01.2026).

6. Каирбаева Л.К. Защита персональных данных в международном и европейском праве // Вестник Института законодательства и правовой информации Республики Казахстан. 2020. №5 (63). С. 168–174.

7. Teresa Scassa. Moving on From the Ombuds Model for Data Protection in Canada // Canadian Journal of Law and Technology. 2019. №17 (1). P.90 – 98.

8. Won Kyung Jung and Hun Yeong Kwon. Privacy and data protection regulations for AI using publicly available data: Clearview AI case // ACM International Conference Proceeding Series.2024. №24. P. 48-55. Available from: https://www.scopus.com/pages/publications/85216095961?inward (date of reference: 03.01.2026).

**© Ә.М. Көптлеуова[1], 2026**
[1] Институт законодательства и правовой информации Республики Казахстан, Астана, Казахстан
(e-mail: [1]asemaikoptleuova9@gmail.com)

## АНАЛИЗ ЗАРУБЕЖНЫХ ТЕНДЕНЦИЙ В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

**Аннотация.** В данной статье автор проводит анализ современных зарубежных тенденций в области защиты персональных данных на примере Южной Кореи, Японии, Сингапура и Канады. В ходе исследования рассматриваются методы правового регулирования обработки персональных данных, а также развитие требований к обеспечению прозрачности цифровых процессов. В частности, проводится анализ законодательства Южной Кореи (PIPA), Сингапура (PDPA), Японии (APPI) и Канады (PIPEDA). На основе статьи определяются ключевые направления, на которые обращают особое внимание независимые специализированные государственные органы и организации с широкими полномочиями в этих странах. Анализ законодательства демонстрирует современные тенденции в области защиты персональных данных.

В настоящее время не существует идеальной системы защиты данных. Зарубежный опыт показывает, что законодательство о защите персональных данных постоянно подвержено изменениям и имеет динамичный характер. Нормы права должны регулярно обновляться в соответствии с технологическими изменениями и новыми киберугрозами, обеспечивая эффективную защиту прав субъектов данных.

Результаты исследования показывают, что активная и системная политика в области защиты персональных данных не ограничивается только сохранением конфиденциальности. Она также способствует повышению доверия пользователей к цифровым платформам, обеспечению устойчивости информационных систем и эффективной работе цифровой инфраструктуры в условиях технологических изменений.

Автор подчеркивает, что обеспечение надлежащей защиты персональных данных должно быть одним из приоритетов для регуляторных органов и других заинтересованных сторон. Это связано с тем, что систематическое соблюдение международных и национальных стандартов позволяет формировать безопасную, устойчивую и постоянно развивающуюся цифровую экосистему.

**Ключевые слова:** защита персональных данных; международное право; цифровая среда; обеспечение конфиденциальности; обработка персональных данных.

**© A.M. Koptleuova[1], 2026**
[1]Institute of Legislation and Legal Information of the Republic of Kazakhstan, Astana, Kazakhstan
(e-mail: [1]asemaikoptleuova9@gmail.ru )

## ANALYSIS OF FOREIGN TRENDS IN THE FIELD OF PERSONAL DATA PROTECTION

**Abstract.** This article analyzes contemporary international trends in personal data protection using the examples of South Korea, Japan, Singapore, and Canada. The study examines legal approaches to personal data processing and the development of requirements for ensuring transparency in digital processes. In particular, it analyzes South Korea's PIPA, Singapore's PDPA, Japan's APPI, and Canada's PIPEDA. Based on this analysis, the article identifies the key areas that independent, specialized public authorities and organizations with broad powers in these countries focus on. Furthermore, the legislative analysis highlights modern trends in personal data protection.

Currently, there is no perfect system for data protection. International experience demonstrates that

personal data protection legislation is continuously evolving and inherently dynamic. Legal norms must be regularly updated to respond to technological changes and emerging cyber threats, ensuring effective protection of data subjects' rights.

The study's results indicate that an active and systematic policy in personal data protection extends beyond mere confidentiality. It also contributes to increasing users' trust in digital platforms, ensuring the stability of information systems, and supporting the efficient operation of digital infrastructure amid technological changes.

The author emphasizes that ensuring adequate personal data protection should be a priority for regulatory authorities and other relevant stakeholders. Consistent adherence to international and national standards enables the creation of a secure, stable, and continuously evolving digital ecosystem.

**Keywords:** personal data protection; international law; digital environment; confidentiality; personal data processing.

**References:**

1. Serimbetov N.N., Zhilkajdarov R.R. Zashhita personal'nyh dannyh v oblakah i prava fizicheskih lic // ҒYLYM - NAUKA. Mezhdunarodnyj nauchnyj zhurnal. 2024. №1 (80). S. 186-192.

2. Zhetpisov S.K., Alibaeva G.A., Dubovickaja, O.B. Cifrlandyru dəuirindegi derbes derekterdi qorғau konstitucijalyқ-құқyқtyқ aspekt // Қazaқstan Respublikasynyң Zaңnama zhəne құқyқtyқ aқparat institutynyң Zharshysy. 2023. №5 (74). 68 – 76 B.

3. Lee H., Kim E. & Park D.H. Insights from the Incheon Airport Case in South Korea: balancing public safety and individual rights with global scalability analysis // Humanities and Social Sciences Communications. 2025. №12 (1). P.1-11. Available from: https://www.scopus.com/pages/publications/105010714603?origin=resultslist (date of reference: 03.01.2026).

4. Lim S., Oh J. Navigating Privacy: A Global Comparative Analysis of Data Protection Laws // IET Information Security. 2025. №1. R.1-5. Available from: https://www.researchgate.net/publication/388401409_Navigating_Privacy_A_Global_Comparative_Analysis_of_Data_Protection_Laws/citation/download (date of reference: 02.01.2026).

5. CHIK, Warren B. The reasonableness standard of compliance in the Singapore Personal Data Protection Act // Singapore Academy of Law Journal. 2022. №34. R.352-399. Available from: https://ink.library.smu.edu.sg/sol_research/4588 (date of reference: 02.01.2026).

6. Kairbaeva L.K. Zashhita personal'nyh dannyh v mezhdunarodnom i evropejskom prave // Vestnik Instituta zakonodatel'stva i pravovoj informacii RK. 2020. №5 (63). S. 168–174.

7. Teresa Scassa. Moving on From the Ombuds Model for Data Protection in Canada //Canadian Journal of Law and Technology. 2019. №17 (1). R.90 – 98.

8. Won Kyung Jung and Hun Yeong Kwon. Privacy and data protection regulations for AI using publicly available data: Clearview AI case // ACM International Conference Proceeding Series. 2024. №24. R.48-55. Available from: https://www.scopus.com/pages/publications/85216095961?inward (date of reference: 03.01.2026).

**Автор туралы мәліметтер:**

**Көптлеуова Әсемай Мұхтарқызы –** заң ғылымдарының магистрі, Қазақстан Республикасының Заңнама және құқықтық ақпарат институтының аға ғылыми қызметкері, Жеңіс даңғылы, 15А, 010000, Астана, Қазақстан.

ORCID: https://orcid.org/0009-0008-9506-2971;

E-mail: asemaikoptleuova9@gmail.ru.

**Алғыс.** Автор сарапшылық пікірі мен сындарлы көзқарасы үшін рецензенттерге алғыс білдіреді.

**Дәйексөз келтіру үшін.** Көптлеуова Ә.М. Дербес деректерді қорғау саласындағы шетелдік үрдістерді талдау // Қазақстан Республикасының Заңнама және құқықтық ақпарат институтының Жаршысы. Ғылыми-құқықтық журнал. 2026;81(1): 359-369. DOI – https:// doi.org/10.52026/2788-5291_2026_81_1_359.

**Мүдделер қақтығысы туралы ақпарат.** Автор мүдделер қақтығысының жоқтығын туралы мәлімдейді.

**Қаржыландыру көзі.** Автор зерттеу жүргізу кезінде қаржыландырудың жоқтығын туралы мәлімдейді.

Мақала редакцияға келіп түсті: 14.01.2026; рецензиялаудан кейін келіп түсті: 27.01.2026; басып шығаруға қабылданды: 31.03.2026.

Автор қолжазбаның соңғы нұсқасын оқып, мақұлдады.

**Сведения об авторе:**

**Көптлеуова Әсемай Мұхтарқызы –** магистр юридических наук, старший научный сотрудник Института законодательства и правовой информации Республики Казахстан, проспект Женис, 15А, 010000, Астана, Казахстан.
ORCID: https://orcid.org/0009-0008-9506-2971;
E-mail: asemaikoptleuova9@gmail.ru.

**Благодарности.** Автор выражает благодарность рецензентам за экспертное мнение и конструктивный подход.

**Для цитирования.** Көптлеуова Ә.М. Анализ зарубежных тенденций в сфере защиты персональных данных // Вестник Института законодательства и правовой информации Республики Казахстан. Научно-правовой журнал. 2026;81(1): 359-369. DOI – https:// doi.org/10.52026/2788-5291_2026_81_1_359.

**Информация о конфликте интересов.** Автор заявляет об отсутствии конфликта интересов.

**Источник финансирования.** Автор заявляет об отсутствии финансирования при проведении исследования.

Статья поступила в редакцию: 14.01.2026; поступила после рецензирования: 27.01.2026; принята в печать: 31.03.2026.

Автор прочитал и одобрил окончательный вариант рукописи.

**Information about the author:**

**Koptleuova Assemay Mukhtarkyzy –** Master of Juridicial sciences, senior Research Fellow, Institute of Legislation and Legal Information of the Republic of Kazakhstan, Zhenis Avenue, 15A, 010000, Astana, Kazakhstan.
ORCID: https://orcid.org/0009-0008-9506-2971;
E-mail: asemaikoptleuova9@gmail.ru.

**Acknowledgements.** The author would like to express their gratitude to the reviewers for their expert opinions and constructive feedback.

**For citation:** Koptleuova A.M. Analysis of foreign trends in the field of personal data protection // Bulletin of Institute of Legislation and Legal Information of the Republic of Kazakhstan. Scientific and legal journal. 2026;81(1): 359-369. DOI – https:// doi.org/10.52026/2788-5291_2026_81_1_359.

**Conflict of interest statement.** The author declares that there is no conflict of interest.

**Funding.** The autor received no specific funding for this work.

Received: 14.01.2026; revised: 27.01.2026; accepted for publication: 31.03.2026.

The author has read and approved the final manuscript.