ҒТАМР 10.87.27; 81.93.29 https://doi.org/10.26577/JAPJ2025116415

А.А. Утенова, В.Т. Ауешова*, Е.Т. Нұрмағанбет

Ш. Есенов атындағы Каспий технология және инжиниринг университеті, Ақтау, Қазақстан
*e-mail: baueshova@mail.ru

АҚШ, АЗИЯ ЕЛДЕРІНІҢ (МЫСАЛЫ, ЖАПОНИЯ, СИНГАПУР) ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУ ТӘЖІРИБЕСІ

Бұл мақалада АҚШ пен Азия елдеріндегі, соның ішінде Жапония мен Сингапурдағы дербес деректерді қорғау саласындағы құқықтық реттеу тетіктері мен олардың ерекшеліктері салыстырмалы-құқықтық тұрғыдан қарастырылады. Автор дербес деректердің қазіргі цифрлық қоғамдағы рөлі мен жеке өмірге қол сұқпау құқығын қамтамасыз етудің маңыздылығын атап өтеді. АҚШ тәжірибесі бірыңғай кешенді деректерді қорғау заңының болмауымен ерекшеленіп, жеке сектор мен мемлекеттік институттар арасындағы жауапкершілік бөлінісінің әлсіздігі тұрғысынан егжей-тегжейлі талданады. Онда деректерді қорғау негізінен салалық заңдармен (денсаулық, қаржы, білім және т.б.) реттелетіні, ал федералдық деңгейде бірыңғай құқықтық режимнің әлі қалыптаспағаны көрсетіледі.

Сонымен қатар ғылыми мақалада Азия елдерінде, соның ішінде Жапония мен Сингапурда, деректерді қорғау жүйесі халықаралық стандарттарға сәйкестендіріле отырып, ұлттық мәдени және құқықтық дәстүрлермен үйлестірілгендігі айқындалады. Зерттеу барысында деректерді қорғаудың институционалдық құрылымы, реттеуші органдардың рөлі мен корпоративтік жауапкершілік мәселелері талданады. Мақалада сонымен қатар аймақтық ерекшеліктер мен жаһандық интеграциялық үрдістердің өзара ықпалы, халықаралық құқықтық үйлесімділік пен дербес деректердің қауіпсіз айналымын қамтамасыз ету қажеттілігі қарастырылған. Автор жаһандану жағдайында ұлттық заңнамаларды халықаралық стандарттарға үйлестіру қажеттігін және деректерді қорғауда құқықтық, технологиялық әрі мәдени факторлардың өзара байланысын айқындайды.

Түйін сөздер: дербес деректерді қорғау; жекешелік құқығы; АҚШ; Жапония; Сингапур; құқықтық реттеу; цифрлық қоғам; халықаралық стандарттар; деректерді басқару; салыстырмалы талдау.

A.A. Utenova, B.T. Aueshova*, E.T. Nurmaganbet

Sh. Yesenov Caspian University of Technology and Engineering, Aktau, Kazakhstan
*e-mail: baueshova@mail.ru

Experience of personal data protection in the USA and Asian countries (e.g. Japan, Singapore)

This article provides a comparative legal analysis of the mechanisms and specific features of legal regulation in the field of personal data protection in the United States and a number of Asian countries, including Japan and Singapore. The author highlights the role of personal data in the modern digital society and emphasizes the importance of safeguarding the right to privacy. The US experience is examined in detail from the perspective of the absence of a single comprehensive data protection act and the weak allocation of responsibilities between the private sector and public institutions. It is shown that data protection in the United States is mainly governed by sectoral legislation (healthcare, finance, education, etc.), while a unified legal regime at the federal level has not yet been formed.

Furthermore, the article demonstrates that in Asian countries, including Japan and Singapore, data protection systems have been aligned with international standards while being adapted to national cultural and legal traditions. The study analyses the institutional framework of data protection, the role of regulatory authorities, and issues of corporate responsibility. The article also considers the interaction between regional specificities and global integration trends, the need for international legal harmonization, and ensuring the secure cross-border flow of personal data. The author argues that, under conditions of globalization, it is necessary to align national legislation with international standards and to account for the interconnection of legal, technological and cultural factors in the field of data protection.

Keywords: personal data protection; privacy; USA; Japan; Singapore; legal regulation; digital society; international standards; data governance; comparative analysis.

А.А. Утенова, В.Т. Ауешова*, Е.Т. Нұрмағанбет
Каспийский университет технологии и инжиниринга имени Ш. Есенова, Актау, Казахстан
*e-mail: baueshova@mail.ru

Опыт защиты персональных данных в США и странах Азии (на примере Японии и Сингапура)

В данной статье в сравнительно-правовом аспекте рассматриваются механизмы и особенности правового регулирования в сфере защиты персональных данных в США и ряде стран Азии, в том числе в Японии и Сингапуре. Автор подчеркивает роль персональных данных в современном цифровом обществе и важность обеспечения права на неприкосновенность частной жизни. Опыт США подробно анализируется с точки зрения отсутствия единого комплексного закона о защите данных и слабой разграниченности ответственности между частным сектором и государственными институтами. Показано, что защита данных в США в основном осуществляется на основе отраслевого законодательства (в области здравоохранения, финансов, образования и др.), при этом единый правовой режим на федеральном уровне до сих пор не сформирован.

Одновременно в статье отмечается, что в странах Азии, в том числе Японии и Сингапуре, системы защиты данных выстраиваются в соответствии с международными стандартами с учетом национальных культурных и правовых традиций. В ходе исследования анализируются институциональная структура защиты данных, роль регуляторных органов и вопросы корпоративной ответственности. Кроме того, рассматривается взаимовлияние региональных особенностей и глобальных интеграционных процессов, необходимость международно-правовой гармонизации и обеспечения безопасного трансграничного обращения персональных данных. Автор обосновывает необходимость приведения национального законодательства в соответствие с международными стандартами и учета взаимосвязи правовых, технологических и культурных факторов в сфере защиты данных в условиях глобализации.

Ключевые слова: защита персональных данных, частная жизнь, США, Япония, Сингапур, правовое регулирование, цифровое общество, международные стандарты, управление данными, сравнительный анализ.

Кіріспе

XXI ғасырда ақпарат мемлекеттердің саяси, экономикалық және әлеуметтік тұрақтылығын айқындайтын негізгі құндылықтардың біріне айналды. Жеке тұлғаға тән ерекшеліктерді бейнелейтін дербес деректер ерекше маңызға ие стратегиялық ресурс ретінде қарастырылып, олардың қорғалу деңгейі азаматтардың цифрлық технологияларға деген сенімін және құқықтық институттардың заңдылығын қамтамасыз ететін басты факторлардың бірі болып отыр. Алайда цифрлық ортаның қарқынды дамуы, жиналатын деректер көлемінің үздіксіз өсуі мен ақпараттық ағындардың трансшекаралық сипаты әлемдік қауымдастық алдына ұлттық юрисдикциялар дербес деректер қозғалысын бақылау мүмкіндігін жоғалтқан жағдайда жеке өмірдің құпиялылығын тиімді қорғау тетіктерін қалыптастыру міндетін қойды (https://www.un.org/en).

Материалдар мен әдістер

Дербес деректерді қорғау жөніндегі халықаралық тәжірибе адам құқықтары, экономикалық бәсекелестік және технологиялық прогресс тоғысында қалыптасуда. Бір жағынан, жеке өмірді қорғау құқықтары Адам құқықтарының жалпыға бірдей декларациясы (https://rm.coe.int/) мен Еуропа кеңесінің №108 конвенциясы (https://eur-lex.europa.eu/) сияқты әмбебап және өңірлік халықаралық актілерде бекітілген, бұл құпия ақпараттың қорғалуы адамның негізгі құқықтарының бірі ретінде танылғанын білдіреді. Екінші жағынан, деректерге негізделген жаһандық экономика бұзушылықтардың алдын алып қана қоймай, инновацияларды, электрондық коммерцияны және трансшекаралық ынтымақтастықты дамытуға мүмкіндік беретін икемді құқықтық реттеуді талап етеді. Сол себепті қазіргі халықаралық құқықтық жүйе ақпараттың еркін айналымы мен дербес деректерді қорғау құқығын қамтамасыз ету арасындағы тепе-теңдікті табу қажеттілігімен бетпе-бет келіп отыр.

Соңғы жылдары цифрлық реттеу саласында жаңа ықпал орталықтарының қалыптасу үрдісі байқалады. Бұрын бұл салада еуропалық стандарттар үстемдік етіп келсе, бүгінде дербес деректерді қорғау үлгілерін әзірлеу мен іске асыру ісіне АҚШ пен Азия елдері белсенді түрде араласа бастады. Бұл өңірлерде цифрлық нарық еркіндігі мен тұлғаның құқықтық қауіпсіздігі

арасындағы өзара байланысқа қатысты дербес көзқарастар жүйесі қалыптасуда. Олардың тәжірибесін зерделеу қазіргі кезеңдегі жаһандық цифрлық трансформация дәуірінде құқықтық реттеу қағидаттарының қалайша қалыптасып жатқанын түсінуге мүмкіндік береді.

Америка Құрама Штаттары жеке деректерді қорғауда салалық тәсілді қолданады. Елде жеке деректердің құпиялылығы мен қорғалуын қамтамасыз ететін бірыңғай, кешенді федералдық заң жоқ. Оның орнына, федералдық деңгейдегі заңнама деректерді негізінен нақты салалар шеңберінде қорғайды. Еуропалық Одақтың дербес деректерді қорғау туралы кешенді директивасынан айырмашылығы (https://curia.europa.eu/), АҚШ-та федералдық және штаттық деңгейдегі заңдар, әкімшілік реттеу актілері, сондай-ақ салаішілік өзін-өзі реттеу қағидаларының үйлесімі қолданылады. Деректерді қорғау кепілдіктері салаға бағытталған сипатқа ие және олар көптеген заңнамалық актілер мен сот тәжірибесінде қамтылған. Бұл нормалар тек белгілі бір салаларға ғана қатысты, мысалы: денсаулық сақтау, білім беру, байланыс, қаржы қызметтері, сондай-ақ онлайн деректерді жинау жағдайында – балаларға. Алғашқы көзқараста салыстырмалы құқық саласының мамандары АҚШ-тың дербес деректерді қорғау жүйесін Еуропаға қарағанда әлсіздеу деп қабылдауы мүмкін, дегенмен кейбір аспектілер бойынша американдық үлгі еуропалықтан жоғары деңгейде қорғаныс ұсынады.

АҚШ-тағы алғашқы дербес деректерді қорғау туралы заң – «Тұтынушылардың несиелік есептері туралы әділ заң» (Fair Credit Reporting Act, FCRA) – 1970 жылы қабылданды (https://www.consumer.ftc.gov/). Бұл заңның мақсаты тұтынушылардың несиелік есеп беру саласында деректермен алмасуға шектеу қою және, ең бастысы, азаматтарға есептегі қателерді түзетуге мүмкіндік беру болды.

«Тұтынушылардың несиелік есептері туралы әділ заң» кейінгі деректерді қорғау туралы заңнамалар үшін үш құрамдас үлгі орнатты:

- тұтынушыларға олардың нақты деректер жазбалары туралы хабарлау міндетін енгізу;
- мемлекеттік орган басқаратын әкімшілік шағымдану рәсімін орнату;
- құқық қорғау органдарының деректерге қол жеткізу шарттарын әртүрлі дәлелдеу стандарттары негізінде анықтау.

1973 жылы АҚШ-тың Денсаулық сақтау, білім беру және әл-ауқат министрлігі «Компьютерлер және азаматтардың құқықтары» атты есеп жариялады. Онда үкіметке Әділ ақпараттық тәжірибелер кодексін (Fair Information Practices, FIPs) қабылдау ұсынылды. Бұл кодекс барлық ұйымдарды жеке сәйкестендірілетін ақпаратты қорғау ережелерін сақтауға міндеттеуі тиіс еді. Кодекс талаптарына сай келмейтін тәжірибелерге мемлекеттік санкциялар қолданылуы көзделді.

1974 жылы, Уотергейт жанжалынан кейін, Конгресс Құпиялылық туралы заңды (Privacy Act) қабылдады (https://www.justice.gov/). Денсаулық сақтау, білім беру және әл-ауқат министрлігі есебінде бұл заң «барлық автоматтандырылған жеке деректер жүйелеріне» қолданылуы тиіс делінгенімен, соңғы нүсқасы тек федералдық агенттіктердің деректер базаларына қатысты болды. Заңда «құпиялылық құқығы – АҚШ Конституциясымен қорғалатын жеке және іргелі құқық» деп жарияланды. «Құпиялылық туралы заң» АҚШ Бас қызметтер басқармасы жүргізетін жазбалар жүйелерінде сақталатын жеке ақпаратты қорғайды.

Дегенмен, Конгресс 1974 жылы дербес деректердің құпиялылығын қорғауға өз міндеттемесін мәлімдегеніне қарамастан, АҚШ әлі күнге дейін кешенді деректерді қорғау жүйесін қалыптастырған жоқ. Елдегі федералдық және штаттық деңгейдегі тар шеңберлі заңдар мен ережелердің мозаикалық жүйесі үкіметтік органдарға және кей жағдайларда жеке тұлғаларға заңды бұзған ұйымдарға қарсы шағым түсіруге мүмкіндік береді. Алайда, жеке деректерді қорғаудағы Еуропалық Одақтың тәсілімен салыстырғанда – ол көптеген жағынан құпиялылықты қорғаудың «алтын стандарты» болып саналса – АҚШ-тағы басым модель көбіне тұтынушылардың құқықтарын қорғауға бағытталған реттеу шараларына негізделген (Boyne, 2018).

Талқылау

АҚШ пен Азия елдеріндегі, соның ішінде Жапония мен Сингапурдағы дербес деректерді қорғау саласындағы құқықтық реттеу тетіктері мен олардың ерекшеліктері салыстырмалы-құқықтық тұрғыдан қарастырылатындықтан. Дербес деректердің қазіргі цифрлық қоғамдағы рөлі мен жеке өмірге қол сұқпау құқығын қамтамасыз етудің маңыздылығын атап өтеді. Деректер ауқымының экспоненциалды өсуі, жасанды интеллект, бұлттық технологиялар мен Big Data шешімдерінің кең таралуы тұлғаның автономиясы мен құпия өміріне жаңа қауіп-қатерлер туындататыны көрсетіледі.

АҚШ тәжірибесі бірыңғай кешенді деректерді қорғау заңының болмауымен ерекшеленіп, жеке сектор мен мемлекеттік институттар арасындағы жауапкершілік бөлінісінің әлсіздігі түрғысынан егжей-тегжейлі талданады. Онда деректерді қорғау негізінен салалық заңдармен (денсаулық, қаржы, білім және т.б.) реттелетіні, ал федералдық деңгейде бірыңғай құқықтық режимнің әлі қалыптаспағаны көрсетіледі. АҚШ моделінің артықшылықтары ретінде реттеудің икемділігін, инновацияларды тежемеу қағидатын және нарықтық өзін-өзі реттеуге сенімділікті атап өтеді. Сонымен қатар, тұтынушылардың құқықтары мен дербес деректеріне қатысты түсінікті әрі бірізді емес режим азаматтар үшін құқықтық айқындықтың жеткіліксіз болуына әкелетіні, ал әр штат деңгейіндегі түрлі актілер құқық қолдану тәжірибесін күрделендіретіні көрсетіледі.

Азия елдерінде, соның ішінде Жапония мен Сингапурда, деректерді қорғау жүйесі халықаралық стандарттарға сәйкестендіріле отырып, ұлттық мәдени және құқықтық дәстүрлермен үйлестірілгендігі айқындалады. Бұл ретте Жапониядағы Дербес ақпаратты қорғау туралы заң (APPI) мен Сингапурдың Дербес деректерді қорғау туралы заңы (PDPA) үлгілік құқықтық тетіктер ретінде қарастырылады. Зерттеуде аталған заңдарда ашықтық, жауапкершілік, пропорционалдық және мақсатпен шектелу қағидаттары бекітілгені, дербес деректер субъектілерінің құқықтары (қол жеткізу, түзету, жою және өңдеуге шектеу қою) нақты регламенттелгені талданады.

Зерттеу барысында деректерді қорғаудың институционалдық құрылымы, реттеуші органдардың рөлі мен корпоративтік жауапкершілік мәселелері талданады. Жапониядағы Дербес ақпаратты қорғау жөніндегі комиссия мен Сингапурдың Дербес деректерді қорғау жөніндегі комиссиясы сияқты уәкілетті органдардың тәуелсіздігі, қадағалау функциялары және құқық бұзушылықтар үшін санкциялар қолдану өкілеттіктері қарастырылады. Корпоративтік ортада деректерді қорғау әсерін бағалау (DPIA), ішкі комплаенс-жүйелерді енгізу, киберқауіпсіздік стандарттарын сақтау және қызметкерлерді оқыту сияқты практикаға бағытталған құралдардың маңызы айқындалады.

Сонымен қатар аймақтық ерекшеліктер мен жаһандық интеграциялық үрдістердің өзара ықпалы, халықаралық құқықтық үйлесімділік пен дербес деректердің қауіпсіз айналымын қамтамасыз ету қажеттілігі қарастырылған. Азия-Тынық мұхиты өңіріндегі APEC, сондай-ақ Еуропалық Одақтың GDPR нормаларына жақындасу үрдістері трансшекаралық деректер алмасуда ортақ қағидаттар қалыптастыруға ықпал ететіні атап өтіледі. Автор жаһандану жағдайында ұлттық заңнамаларды халықаралық стандарттарға үйлестіру қажеттігін және деректерді қорғауда құқықтық, технологиялық әрі мәдени факторлардың өзара байланысын айқындайды. Бұл түрғыдан алғанда, дербес деректерді қорғау тек тар салалық құқықтық институт қана емес, сонымен бірге цифрлық егемендік, адам құқықтары және тұрақты даму дискурстарымен тығыз байланыста қарастырылатын кешенді феномен ретінде сипатталады.

Сондықтан, АҚШ-та дербес деректердің құпиялылығын қорғаудағы негізгі орган – Федералдық сауда комиссиясы. Бұл тәуелсіз құқық қорғау агенттігі тұтынушылардың құқықтарын қорғау міндетін атқарады. Алайда, Федералдық сауда комиссиясының негізгі өкілеттігі Федералдық сауда комиссиясы туралы актінің 5-бөлімінен туындайды, сондықтан оның құзыреті тек ақпараттық тәжірибелері «алдаушы» немесе «әділетсіз» деп танылған ұйымдарға ғана таралады.

Осы түрғыдан алғанда, «Құпиялылық туралы заң» дербес деректер туралы арнайы заң емес, керісінше жеке ақпаратты жария ету мен оны қорғауға қатысты әділетсіз немесе алдаушы әрекеттерді тыйым салу үшін қолданылатын кең ауқымды тұтынушыларды қорғау жүйесі болып табылады. Сонымен қатар, «Жеке тұлғаның жеке басын ұрлау және алдын алу туралы заң» (Identity Theft Assumption and Deterrence Act) (https://www.govinfo.gov/) Федералдық сауда комиссиясына жеке басын ұрлауға байланысты шағымдарды қабылдайтын және азаматтарды хабардар ететін бірыңғай орталық қызметін құруды, сондай-ақ жеке тұлғаның деректерін ұрлауға қатысты қылмыстық заңнаманы күшейтуді міндеттейді.

2021-2022 жылдардағы АҚШ Конгресінің сессиясында жеке тұлғалардың дербес деректерін қорғау мен құпиялылығын қамтамасыз етуге қатысты бірнеше заң жобасы қарастырылды. Олардың қатарында 2019-2020 жылдардағы алдыңғы сессияда ұсынылған, бірақ сол кезде қабылданбай, кейінгі сессияда қайта енгізілген бастамалар да болды. Аталған бастамалар деректерді қорғауға түрлі тәсілдер ұсынды: кейбірі ауқымды әрі кешенді сипатта болса, басқалары штат деңгейіндегі дербес деректерді қорғау заңдарының күшін жоятын (preemption) норма-

лар енгізуді көздеді. Кейбір заң жобалары жаңа мемлекеттік агенттіктер құруды ұсынса, енді біреулері тергеу мен қадағалау функцияларын атқаруда қолданыстағы мемлекеттік инфрақұрылымға сүйенді. Ең кең ауқымды жобаларда ғылыми зерттеулермен байланысты қызмет түрлеріне белгілі бір жеңілдіктер қарастырылған. Барлық нұсқаларда қолданыстағы федералдық деректердің құпиялылығы мен қорғалуына қатысты заңдардың күші сақталды. Нәтижесінде, сарапшылардың басым бөлігі Конгресс пен Атқарушы билік тарапынан айқын саяси ерік-жігер байқалмағандықтан, бұл заң жобалары қабылданбады деп есептейді (DiPersio, 2022: 9-16).

Сонымен, АҚШ-та дербес деректерді қорғаудың кешенді жүйесін қабылдау мәселесі Конгрессте екі партия тарапынан да белгілі бір дәрежеде қолдауға ие әрі қоғамда кеңінен қолдау табуда. Алайда бүгінгі күнге дейін бұл бағытта айтарлықтай ілгерілеу байқалмай отыр. Дегенмен, жағдай барған сайын өзекті сипат алуда, себебі азаматтар өздерінің жеке деректерінің цифрлық кеңістікте қалай пайдаланылып (және кейде теріс пайдаланылып) жатқанын барған сайын тереңірек түсінуде.

Компаниялар өзін-өзі реттеу шараларын қабылдап жатқанын мәлімдегенімен, бұл әрекеттер көп жағдайда жеткіліксіз болып қалады. Бірқатар штаттар дербес деректерді қорғауға арналған жеке заңдарын қабылдаған, алайда олардың стандарттары мен ережелері арасында айтарлықтай айырмашылықтар бар. Деректердің жария болып кетуі немесе әділетсіз не адастыратын деректермен жұмыс істеу тәжірибелерінен зардап шеккен тұлғалар әртүрлі құқықтық теориялар мен заңдарға сүйене отырып, соттарға және жекелеген мемлекеттік органдарға жүгінуге құқылы. Алайда бұл ретте шешімдердің біркелкі болмау қаупі де сақталады.

Азия елдеріне келетін болсақ, АҚШ-қа қарағанда бұл аймақта дербес деректерді қорғау саласында едәуір жетістіктерге жеткен мемлекеттер баршылық. Сөйтсе де, Азия мемлекеттеріндегі дербес деректерді қорғау тәжірибесі алуантүрлілікпен ерекшелінеді. Себебі Азия бірыңғай құқықтық кеңістік болып табылмайды, керісінше, бұл құрлық жоғары деңгейдегі құқықтық, саяси және мәдени әртектілікпен сипатталады, ал бұл өз кезегінде жеке деректерді қорғау тәсілдеріне тікелей әсер етеді.

Жалпы алғанда, Азия елдеріндегі құпиялылықты түсіну деңгейі көбіне мәдени нормалармен және әлеуметтік құндылықтармен тығыз байланысты. Кейбір қоғамдарда ұжымшылдық көзқарастар мен қоғамдық мүдде үшін деректермен бөлісуге жоғары дайындық байқалады, бұл өз кезегінде жеке деректерге қатысты сақтықты төмендетеді. Ал басқа қоғамдарда, керісінше, тарихи травмалар мен билікке деген сенімсіздік деректерді қорғауға қойылатын талаптардың күшеюіне әкеледі. Спектрдің бір шетінде либералдық дәстүрі бай, жеке құқықтар мен ашықтыққа басымдық беретін юрисдикциялар орналасқан (Шығыс Азияның кейбір елдері мен шағын қаржылық хаб-мемлекеттер). Ал екінші шетінде – қауіпсіздік, экономикалық жаңғырту және ақпараттық бақылау басым рөл атқаратын жоғары орталықтандырылған мемлекеттер тұр. Мұндай ішкі біркелкі еместік «азиялық модельдің» бірыңғай еместігін білдіреді, іс жүзінде бірнеше бағыт қатар өмір сүреді:

- еуропалық үлгідегі жүйелер (GDPR-ден шабыт алған);
- іскерлік болжамдылыққа негізделген прагматикалық азиялық тәсілдер;
- мемлекеттік бақылауға сүйенетін директивалық режимдер (Paulger, 2022).

Азия елдерінің заңнамаларында деректерді қорғауға қатысты әртүрлі басымдықтар мен модельдер қалыптасқан: бір жағында келісім негізгі және егжей-тегжейлі реттелетін құрал болып саналатын консервативті модель, ал екінші жағында басқа заңды негіздерді (мысалы, шарттық міндеттемелерді орындау, заңды мүдделерді қорғау, қоғамдық мақсаттарды жүзеге асыру) мойындайтын икемдірек жүйелер бар (Schwartz & Peifer 2017). Мұндай айырмашылықтың практикалық салдары айқын:

- қатаң келісімге негізделген тәсіл дербес субъектінің өз деректерін бақылау құқығын арттырады, бірақ сонымен бірге деректер операторына жаппай өңдеу кезінде реттеу және әкімшілік жүктемені үлғайтады;
- ал икемді құқықтық негіздерге сүйенген жүйелер бизнестің операциялық процестерін жеңілдетеді, бірақ жеке бақылау мен ашықтық деңгейін төмендетуі мүмкін.

Қазіргі таңда көптеген мемлекеттер осы екі тәсілдің арасынан тепе-теңдік табуға ұмтылуда, атап айтқанда: «сезімтал» деректер санаттары үшін қатаң келісім талаптарын енгізіп, ал күнделікті, техникалық немесе операциялық өңдеу процестері үшін анағұрлым икемді ережелерді қолдануда.

«Ерекше санаттағы деректердің» (денсаулық жағдайы, биометриялық және генетикалық

ақпарат, саяси көзқарастар және т.б.) анықтамасы әр елде әртүрлі түсіндіріледі. Кейбір мемлекеттерде мұндай деректер қатаң шектеулермен қорғалатын ерекше құқықтық режимге жатады, ал басқа елдерде реттеу деңгейі төменірек және салалық ережелер мен стандарттарға делегирленген (https://www.ppc.go.jp/). Жалпы алғанда, соңғы жылдары технологиялық инновацияларға жауап ретінде сезімтал деректер тізбесінің кеңею үрдісі байқалады – мысалы, биометриялық көрсеткіштер мен геодеректердің қосылуы. Бұл өз кезегінде реттеуші органдар мен деректер операторларынан арнайы техникалық және ұйымдастырушылық шараларды (мысалы, шифрлау, псевдонимизация, қатаң қолжетімділік хаттамалары) әзірлеуді және енгізуді талап етеді.

Азия өңірінде дербес деректерді қорғау саласында ерекше жетістіктерге жеткен мемлекеттің бірі әрі бірегейі ретінде Жапонияны атап өтуге болады. Себебі ол – заңнамасын еуропалық үлгімен (GDPR) үйлестірген Азиядағы ең алғашқы мемлекет. 2003 жылы қабылданған Act on the Protection of Personal Information (APPI) заңы (https://www.japaneselawtranslation.go.jp/en/) 2015 және 2020 жылдары түбегейлі жаңартылып, заманауи цифрлық орта талаптарына бейімделді. Осы реформалардың нәтижесінде, 2019 жылы Еуропалық комиссия Жапонияны деректерді қорғау деңгейі бойынша «тиісті ел» деп таныды (https://eur-lex.europa.eu/). Бұл шешім Жапонияның құқықтық жүйесінің Еуропалық стандарттарға сәйкес келетінін және жеке тұлғалардың дербес деректерін қорғауда сенімді деңгейге жеткенін көрсетті. Нәтижесінде Жапония Азия елдері ішінде бірінші болып Еуропамен деректердің еркін және заңды айналымын қамтамасыз еткен мемлекет атанды.

Жапониядағы дербес деректерді қорғау жүйесі біртіндеп, екі басты императивтің тоғысында қалыптасты: бір жағынан – цифрлық экономиканы және ақпарат алмасуды ынталандыру қажеттілігі, екінші жағынан – жеке ақпаратқа қатысты дәстүрлі «конфиденциалдық-әкімшілік» ұстаным мен сақтық мәдениеті. Алғашқы құқықтық негіздер GDPR-ға дейін-ақ пайда болған. Негізгі белес – «Act on the Protection of Personal Information» (APPI) заңы (https://www.japaneselawtranslation.go.jp/en/), ол соңғы жиырма жыл ішінде дамытылып, цифрлық сервистердің жедел дамуы мен халықаралық трансшекаралық деректер алмасуына қойылған жаңа талаптарға сай елеулі түзетулерден өтті.

2017–2020 жылдары заң жүйелі түрде қайта қаралып, негізгі өзгерістер 2022 жылдың сәуірінде күшіне енді. Бұл реформа көбіне Еуропалық Одақ тарапынан «адекваттық деңгей» мәртебесін алу және халықаралық деректер айналымын жеңілдету ниетімен ынталандырылды. Қазіргі таңда құқықтық режимнің негізін жаңартылған APPI заңы құрайды. Оның орындалуына тәуелсіз ұлттық реттеуші – Жеке деректерді қорғау жөніндегі комиссия (Personal Information Protection Commission) жауапты. Заң деректер субъектілерінің құқықтарын қорғау қағидаттарын (ақпараттандырылған келісім, өңдеу мақсаттарының шектеулігі, сақтау мерзімін шектеу), деректерді бақылаушылардың процессуалдық міндеттерін (қауіпсіздікті қамтамасыз ету, үшінші тұлғаларға беру туралы хабарлау, есеп жүргізу) және трансшекаралық беру талаптарын айқындайды.

Жапон заңнамасында «дербес ақпарат» (personal information) ұғымы адамның жеке тұлғасын тікелей немесе жанама түрде айқындауға мүмкіндік беретін кез келген деректерді қамтиды (аты-жөні, туған күні, клиент нөмірі, бейнесі және т.б.). Сонымен қатар, заңда бірнеше дербес категориялар қарастырылған:

- «Арнайы қорғауды қажет ететін ақпарат (special care-required personal information)» – денсаулық жағдайы, нәсілі, діні және басқа да сезімтал деректер; оларды өңдеу үшін алдын ала келісім талап етіледі.

- «Анонимді өңделген ақпарат (anonymously processed information)» -жеке тұлғаны анықтауға болмайтындай етіп өңделген деректер; оларды тек статистикалық немесе ғылыми зерттеу мақсатында пайдалануға рұқсат етіледі (https://eur-lex.europa.eu/).

APPI шеңберінде деректер операторлары жеке тұлғаны хабардар ету және келісім алу, өңдеу мақсатын шектеу, сондай-ақ ақпараттың қауіпсіздігін қамтамасыз ету міндеттерін орындайды. Үшінші тұлғаларға немесе шетелге деректерді беру тек белгілі шарттар орындалған жағдайда ғана мүмкін, мысалы, егер дерек қабылдаушы ел тиісті қорғау деңгейін қамтамасыз етсе немесе дербес келісім алынған болса.

Жапон құқығы шетелге деректер беруді бақылау механизмдерін көздейді және реттеушіге – Жеке деректерді қорғау жөніндегі комиссияға – деректерді алушы тараптың «эквивалентті қорғауды» қамтамасыз етуін талап етуге немесе балама қорғану шараларын қолдануға өкілеттік береді. Сонымен қатар, APPI үшінші

тұлғаларға берілген деректердің есебін жүргізуді және заң бұзушылықтар үшін санкция қолдануды міндеттейді. Жапония үшін қазіргі басты сын-қатер – трансшекаралық деректер ағынының қолайлылығын сақтай отырып, деректерге заңсыз қол жеткізуге қарсы кепілдіктерді күшейту. Сондай-ақ анонимизация стандарттарын жетілдіру, шағын және орта кәсіпорындар үшін түсінікті комплаенс жүйесін қалыптастыру маңызды. APPI мен PPC нұсқаулықтарын жасанды интеллект пен автоматтандырылған шешім қабылдау салаларына бейімдеу, яғни алгоритмдердің ашықтығы мен түсіндірмелілігіне қатысты нақты талаптарды әзірлеу – негізгі даму бағыты болып табылады.

Жапония деректерді қорғау саласында экономикалық даму мен жеке өмір құқығын қорғау арасындағы теңгерімді сақтауға ұмтылады. Елдің стратегиялық мақсаты – цифрлық экономиканың жаһандық жүйесіне тиімді интеграциялану және халықаралық деректер алмасу процесін жеңілдету. Сонымен қатар, Жапонияның саясаты тек экономикалық прагматизммен ғана емес, сонымен қатар этикалық және құқықтық қағидаттармен сипатталады. Бұл тұрғыда дербес деректердің қорғалуы жапондық қоғамдағы үйлесім мен жауапкершілік құндылықтарымен тығыз байланыста. Мемлекет азаматтардың жеке өміріне қол сұқпау мәдениетін заңнамалық деңгейде бекітіп, деректерді пайдалану кезінде ашықтық пен әділдік қағидаттарын басшылыққа алады. Нәтижесінде Жапонияның тәжірибесі басқа Азия елдеріне үлгі бола алатын құқықтық және моральдық модельге айналды.

Жапониядан бөлек, Азия кеңістігінде дербес деректердің қауіпсіздігін қамтамасыз ету мен цифрлық басқару мәдениетін дамыту тұрғысынан Сингапурдың үлгісі ерекше маңызға ие. Жапония дербес деректерді қорғау саласында еуропалық стандарттарға үйлесім орнатып, құқықтық жүйенің транспаренттілігі мен халықаралық сенімділігін арттырса, Азия өңірінде Сингапур бұл салада өз прагматикалық және инновациялық тәсілімен ерекшеленеді. Көптеген азиялық елдер деректердің қозғалысын шектеу немесе мемлекеттік бақылауды күшейтуге бейім болған жағдайда, Сингапур керісінше, жеке өмірдің құпиялылығын қорғау мен экономикалық тиімділікті тең ұстауға ұмтылады. Елдің деректер саясаты ақпараттық технологиялар мен бизнес-инновацияларды ынталандыруды басты мақсаттардың бірі ретінде қарастырады. Осы себепті Сингапурдың тәжірибесі жеке деректерді қорғау мен цифрлық экономиканы дамыту арасындағы теңгерімді үлгі ретінде қарастырылады. Бұл бағытта қабылданған Дербес деректерді қорғау туралы заң (Personal Data Protection Act – PDPA) (https://sso.agc.gov.sg/) өңірлік деңгейде ең дамыған және жүйелі құқықтық тетік болып саналады.

Сингапур дербес деректерді қорғау жүйесін құруды экономикалық сенім мен цифрлық қызметтерге қоғамның сенімін арттырудан бастады. Нәтижесінде 2012 жылы «Дербес деректерді қорғау туралы заң» қабылданып, кейін кезең-кезеңмен толықтырылып отырды. Ел билігі «икемді, бірақ жауапты» реттеу тәсілін таңдады: бизнеске еркіндік бере отырып, жеке деректердің негізгі кепілдіктерін сақтау. «Дербес деректерді қорғау туралы заң» мен оны іске асыратын орган – Дербес деректерді қорғау комиссиясы – технологиялық өзгерістерге жедел бейімделетін, прагматикалық және пропорционалды реттеу қағидатына негізделген (https://www.pdpc.gov.sg/).

Қорытынды

«Дербес деректерді қорғау туралы заң» субъектілерді хабардар ету, келісім алу, деректердің дұрыстығын қамтамасыз ету, қауіпсіздік шараларын енгізу және маңызды бұзушылықтар туралы реттеушіге хабарлау міндеттерін белгілейді. Заңның ерекшелігі – дербес деректерді қорғау комиссиясы тарапынан шығарылатын егжей-тегжейлі нұсқаулық ұсынымдар, бақылау тізімдері мен бағалау құралдарының кең қолданылуы. GDPR-дан айырмашылығы, Сингапурдың заңы ерекше деректер санаттарын соншалықты егжей-тегжейлі бөлмейді және айналымнан пайыздық айыппұлдар салу тәртібі жоқ. Алайда комиссия елеулі бұзушылықтар үшін миллиондаған сингапур долларына дейін жететін әкімшілік айыппұлдар салуы мүмкін.

Дербес деректерді қорғау комиссиясы өз шешімдерін ашық жариялап, оларды салалық бағдар ретінде пайдаланады. Ең белгілі мысал 2018 жылғы – SingHealth деректерінің ірі көлемде жария болып кетуі (https://www.pdpc.gov.sg/). Бұл оқиға медициналық деректердің қауіпсіздігін күшейту қажеттілігін көрсетті және комиссия 1 млн SGD көлемінде айыппұл салып, реттеуші ұстанымының қаталдығын көрсетті. PDPC сонымен қатар алдын ала келісім алу және шекарааралық беру жөнінде кеңес беру тетіктерін ұсынады, бизнес қауымдастығымен диалог орнатуға басымдық береді.

Жапония мен Сингапурдың тәжірибесі прагматикалық және тепе-тең тәсілді көрсетеді: мемлекеттер цифрлық сенімді сақтау мен инновацияны тежеуден сақтану арасында баланс табуға ұмтылады. Екі елде де тәуелсіз мәртебесі бар реттеуші органдар қызмет атқарады. Екеуі де трансшекаралық аспектіні ерекше назарда ұстайды. Басты айырмашылық – формализация деңгейі мен «жеке тұлға құқықтарына» бағытталу дәрежесі. Жапония соңғы реформалар нәтижесінде Еуропалық стандарттарға барынша жақындаса, Сингапур моделі «азиялық прагматизмге» негізделген: бизнес үшін ыңғайлылық пен құқықтық икемділік басты орында.

Қорытындылай келе, Азиядағы жеке деректерді қорғау ерекшеліктері аймақтың саяси-құқықтық икемділігі, технологиялық амбициялары және экономикалық басымдықтарының өзара тоғысуынан туындайды. Кейбір елдерде халықаралық үйлесімділік пен жеке құқықтарды қорғауға ұмтылыс басым болса, басқаларында цифрлық экономиканы дамытуға бағытталған прагматикалық көзқарас басымдыққа ие; ал жекелеген мемлекеттерде жоғары деңгейдегі мемлекеттік бақылау тән.

Әдебиеттер

United Nations. Universal Declaration of Human Rights. – 1948. URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Council of Europe. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). – Strasbourg, 28 Jan. 1981. URL: https://rm.coe.int/1680078b37

European Parliament & Council. Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR). – Official Journal of the European Union, 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

Court of Justice of the European Union. Case C-311/18 – Data Protection Commissioner v Facebook Ireland & Schrems II. Judgment, 16 July 2020. URL: https://curia.europa.eu/juris/liste.jsf?num=C-311/18

U.S. Congress. Fair Credit Reporting Act (FCRA), Pub. L. No. 91-508; 15 U.S.C. § 1681 et seq., 1970. URL: https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf

U.S. Congress. Privacy Act of 1974, Public Law 93-579; 5 U.S.C. § 552a. URL: https://www.justice.gov/opcl/privacy-act-1974

Boyne S. Data Protection in the United States // The American Journal of Comparative Law. – 2018. – 66. – p. 299-343.

U.S. Congress. Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318. URL: https://www.govinfo.gov/link/plaw/105/public/318

DiPersio D. Data Protection, Privacy and US Regulation. – In: Proceedings of the Workshop on Ethical and Legal Issues in Human Language Technologies and Multilingual De-Identification of Sensitive Data in Language Resources within the 13th Language Resources and Evaluation Conference, 9-16 June 2022, Marseille, France. – Marseille: European Language Resources Association, 2022. – p. 9-16.

Paulger D. Balancing Organizational Accountability and Privacy Self-Management in Asia-Pacific: Comparative review. Future of Privacy Forum (APAC), 2022. – 34 p.

Schwartz P.M., Peifer K.N. Transatlantic Data Privacy Law // Yale Law Journal. – 2017. – Vol. 126(4). – p.102-145.

Personal Information Protection Commission (Japan). Amended Act on the Protection of Personal Information (APPI) – English translation, June 2020. URL: https://www.ppc.go.jp/files/pdf/APPI_english.pdf

Japan Act on the Protection of Personal Information (official Japanese-law-translation). URL: https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en

European Commission. Commission Implementing Decision (EU) 2019/419 of 23 January 2019 – Adequacy decision for Japan. – OJ L 76, 19.3.2019. URL: https://eur-lex.europa.eu/eli/dec_impl/2019/419/oj

Personal Data Protection Act (PDPA) 2012 (as amended). – Singapore Statutes Online. URL: https://sso.agc.gov.sg/Act/PDPA2012

Personal Data Protection Commission (PDPC) Singapore – Advisory Guidelines and decisions (including SingHealth decision Jan 15, 2019). URL: https://www.pdpc.gov.sg/all-commissions-decisions/2019/01/breach-of-the-protection-obligation-by-singhealth-and-ihis

SingHealth / IHiS PDPC decision materials and enforcement summary (2019). URL: https://www.pdpc.gov.sg/

Авторлар туралы мәлімет:

Утенова Айгуль Айдарбаевна – заң ғылымдарының магистрі, Ш. Есенов атындағы Каспий технология және инжиниринг университеті (Ақтау, Қазақстан, e-mail: aigul.utenova@mail.ru);

Ауешова Багдат Тлектесовна (корреспондент авторы) – заң ғылымдарының кандидаты, Ш. Есенов атындағы Каспий технология және инжиниринг университетінің қауымдастырылған профессоры (Ақтау, Қазақстан, e-mail: baueshova@mail.ru);

Нұрмаганбет Ермек Талантұлы – заң ғылымдарының кандидаты, PhD докторы, EMBA, қауымдастырылған профессор, Ш. Есенов атындағы Каспий технология және инжиниринг университетінің атқарушы вице-президенті (Ақтау, Қазақстан, e-mail: yermek.nurmaganbet@yu.edu.kz).

Information about authors:

Utenova Aigul Aidarbayevna – Master of Law, Sh. Yesenov Caspian University of Technology and Engineering (Aktau, Kazakhstan, e-mail: aigul.utenova@mail.ru);

Aueshova Bagdat Tlektesovna (corresponding author) – Candidate of Law, Associate Professor, Sh. Yesenov Caspian University of Technology and Engineering (Aktau, Kazakhstan, e-mail: baueshova@mail.ru);

Nurmaganbet Yermek Talantuly – Candidate of Law, PhD, EMBA, Associate Professor, Executive Vice-President of Sh. Yesenov Caspian University of Technology and Engineering (Aktau, Kazakhstan, e-mail: yermek.nurmaganbet@yu.edu.kz).

Сведения об авторах:

Утенова Айгуль Айдарбаевна – магистр юридических наук, Каспийский технологический и инженерный университет им. Ш. Есенова (Актау, Казахстан, e-mail:aigul.utenova@mail.ru);

Ауэшова Багдат Тлектесовна (автор для корреспонденции) – кандидат юридических наук, ассоциированный профессор Каспийского технологического и инженерного университета им. Ш. Есенова (Актау, Казахстан, e-mail: baueshova@mail.ru);

Нурмаганбет Ермек Талантулы – кандидат юридических наук, EMBA, доцент, исполнительный вице-президент Каспийского технологического и инженерного университета им. Ш. Есенова (Актау, Казахстан, e-mail: yermek.nurmaganbet@yu.edu.kz).

Тіркелді: 26 қыркүйек 2024 жыл.
Қабылданды: 20 желтоқсан 2025 жыл.