

IT LAW FORUM:

«ЖАСАНДЫ ИНТЕЛЛЕКТ,
ЦИФРЛАНДЫРУ ЖӘНЕ ҮЛКЕН ДЕРЕКТЕР -
ҚҰҚЫҚТЫҢ ЖАҢА ШЕКАРАЛАРЫ»

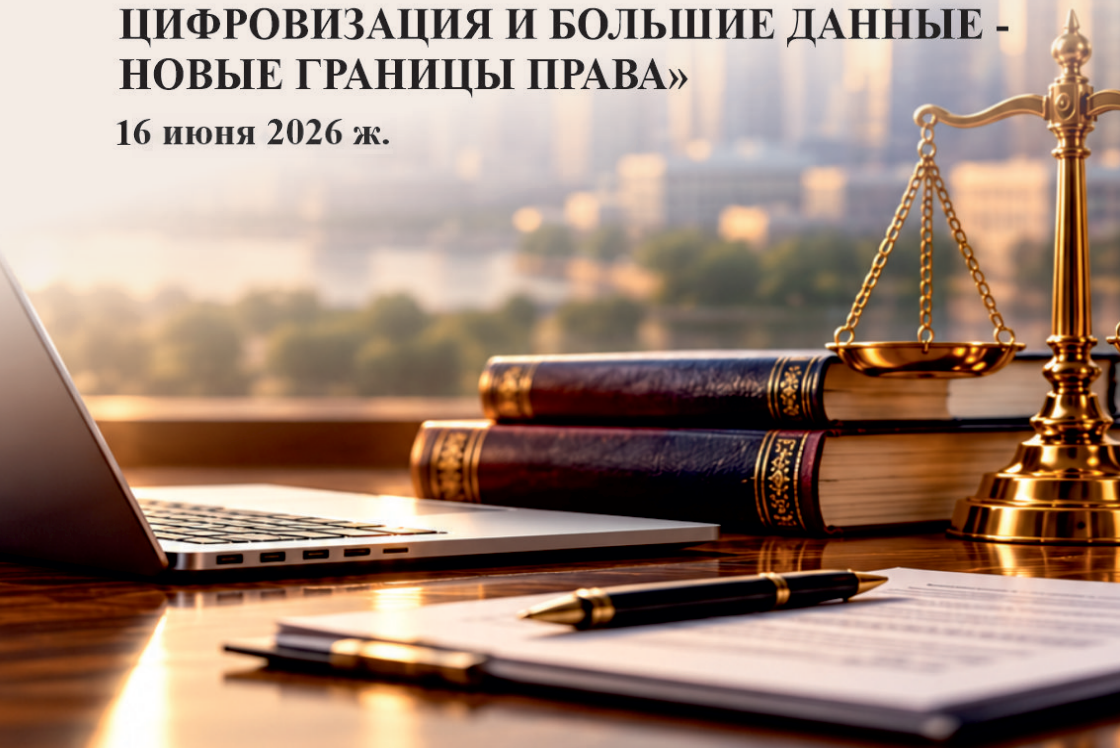
V ЖЫЛ САЙЫНҒЫ ФОРУМ МАТЕРИАЛДАРЫ
2026 ж. 16 маусым

МАТЕРИАЛЫ V ЕЖЕГОДНОГО ФОРУМА

IT LAW FORUM:

«ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ,
ЦИФРОВИЗАЦИЯ И БОЛЬШИЕ ДАННЫЕ -
НОВЫЕ ГРАНИЦЫ ПРАВА»

16 июня 2026 ж.



Университет NARXOZ, Almaty Hub и SDU University

**«IT LAW FORUM: ЖАСАНДЫ ИНТЕЛЛЕКТ,
ЦИФРЛАНДЫРУ ЖӘНЕ ҮЛКЕН ДЕРЕКТЕР -
ҚҰҚЫҚТЫҢ ЖАҢА ШЕКАРАЛАРЫ»**

V ЖЫЛ САЙЫНҒЫ ФОРУМ

МАТЕРИАЛДАРЫ

2026 ж. 16 маусым

МАТЕРИАЛЫ

V ЕЖЕГОДНОГО ФОРУМА

**«IT LAW FORUM: ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ,
ЦИФРОВИЗАЦИЯ И БОЛЬШИЕ ДАННЫЕ -
НОВЫЕ ГРАНИЦЫ ПРАВА»**

16 июня 2026 г.

Алматы,
2026 жыл

УДК 004.8:34 (063)
ББК 32.973.26-018.2
I-10

З.ғ.к., профессор А.Б. Омарованың жалпы редакциясымен/Под общей редакцией к.ю.н., профессора А.Б. Омаровой/Under the general editorship of Doctor of Law, Professor A.B. Omarova

Редакциялық алқа: А. Мағауия, А.А. Сейтжан (жинақтың жауапты хатшысы)
Редакционная коллегия: Мағауия А., Сейтжан А.А. (отв. секретарь сборника)
Editorial Board: Magauia A, Seitzhan A. (executive secretary of the collection)

IT Law Forum: ЖИ, цифрландыру және үлкен деректер - құқықтың жаңа шекаралары: V жыл сайынғы форум материалдары (16 маусым 2026 ж.) / Жауапты ред. А.Б. Омарова. – Алматы: Нархоз Университеті КЕАҚ, 2026. – 368 б.

IT Law Forum: ИИ, цифровизация и большие данные - новые границы права: Материалы V ежегодного форума (16 июня 2026 г.) / отв. ред. А.Б. Омарова – Алматы: НАО «Университет Нархоз», 2026. – 368 с.

IT Law Forum: AI, Digitalization and Big Data - New Frontiers of Law: Proceedings of the 5th Annual Forum / ed. by A.B. Omarova – Almaty: Narхоз University, 2026. – 368 p.

ISBN 978-601-222-181-7

Жинаққа Нархоз Университеті, Almaty Hub және SDU University бірлесіп ұйымдастырған «IT Law Forum: Жасанды интеллект, цифрландыру және үлкен деректер - құқықтың жаңа шекаралары» атты V жыл сайынғы форумының материалдары енді. Басылым қоғамның қарқынды цифрлық трансформациясы жағдайындағы қазіргі заманғы заң ғылымы мен құқық қолдану тәжірибесінің өзекті теориялық және практикалық мәселелерін жан-жақты қамтиды. Жинақ зерттеушілер, оқытушылар, тәжірибелі заңгерлер, судьялар, адвокаттар, сондай-ақ IT-құқық және ақпараттық қауіпсіздік саласының мамандары үшін ғылыми және практикалық тұрғыдан үлкен қызығушылық тудырады.

Жинақ ЖТН AP23489796 «Үлкен деректердің (Big Data) құқықтық режимін реттеу мәселелері: отандық және халықаралық тәжірибе» жобасы бойынша Қазақстан Республикасы Ғылым және жоғары білім министрлігінің ғылым комитеті қаржыландырған 2024-2026жж. арналған ғылыми және ғылыми-техникалық бағдарламаларды қаржыландыру шеңберінде дайындалды.

В настоящем сборнике представлены материалы V ежегодного форума «IT Law Forum: AI, цифровизация и большие данные - новые границы права», организованного Университетом Нархоз совместно с Almaty Hub и SDU University. Издание освещает широкий спектр актуальных теоретических и практических проблем современной юридической науки и правоприменительной практики в условиях стремительной цифровой трансформации общества. Сборник представляет научный и практический интерес для исследователей, преподавателей, практикующих юристов, судей, адвокатов, а также специалистов в сфере IT-права и информационной безопасности.

Сборник подготовлен в рамках реализации проекта ИРН AP23489796 «Проблемы регламентации правового режима больших данных (Big Data): отечественный и международный опыт» (2024-2026), финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан.

This collection features materials from the 5th Annual Forum "IT Law Forum: AI, Digitalization and Big Data - New Frontiers of Law," organized by Narхоз University in cooperation with Almaty Hub and SDU University. The publication addresses a wide range of pressing theoretical and practical issues in modern legal science and law enforcement amid rapid digital transformation. The collection is of academic and practical interest to researchers, educators, practicing lawyers, judges, attorneys, and professionals in the fields of IT law and information security.

The collection was prepared within the framework of funding for scientific and (or) scientific and technical programs for 2024-2026, aimed at the implementation of the IRN project AP23489796 "Problems of regulating the legal regime of big data: domestic and international experience", funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan.



УДК 004.8:34 (063)
ББК 32.973.26-018.2

© Нархоз Университеті, 2026 ж

МАЗМУНЫ / СОДЕРЖАНИЕ / CONTENT

Научные доклады

<i>Абдухамитов В.А.</i> Экстремистские проявления в молодежной среде Таджикистана: проблемы профилактики.	5
<i>Айнакулова Д.Б.</i> Характеристика убийства по законодательству Республики Казахстан.	10
<i>Акпаева Ж.</i> Цифровая сделка и пределы упрощенного производства: Требуется ли переосмысление стандартов судебного доказывания?	16
<i>Акболатова М.Е.</i> Уголовные правонарушения, связанные с миграцией населения.	23
<i>Алдабек Е.А., Сапарбекова Ж.</i> Доказывание нарушений при использовании больших данных и выбор способов судебной защиты.	26
<i>Алимкулов Е.Т.</i> Депонирование показаний – как один из основных полномочий следственного судьи.	41
<i>Арын А.А.</i> Криминалістік одорология және оның қылмыстарды ашу мен тергеудегі маңызы.	45
<i>Әбдіразақ Б.</i> Зарубежные модели правового режима больших данных: международные подходы к ответственности, защите и законодательным решениям.	52
<i>Abdirazak B.</i> The legal regime of de-identified data in big data applications	67
<i>Базилова А.А.</i> Организационно-правовые меры борьбы с компьютерными преступлениями.	81
<i>Жәнібеков А.К.</i> Қорғаушының қылмыстық іс жүргізудегі құқықтық мәртебесін арттыру мәселелері.	86
<i>Казбекова А.</i> Ответственность при использовании искусственного интеллекта: киберриски в Республике Казахстан. Почему это важно прямо сейчас.	96
<i>Калиев Ж.А.</i> Пробелы правового регулирования больших данных (big data) в Республике Казахстан: отечественный и зарубежный опыт.	101
<i>Қуандықова Э.С.</i> Қазақстанның қылмыстық құқығындағы лингвистикалық коллизиялар: терминологиялық алшақтықтардың іс-әрекеттерді саралауға әсері.	114
<i>Қуандыкова Э.С.</i> Қазақстан республикасының қылмыстық заңнамасындағы терминологиялық дәлдік мәселелері: цифрландыру жағдайындағы құқық қолдану тәжірибесі.	126
<i>Қубанова Н.Б.</i> Жасанды интеллектті кибершабуылдарға қарсы іс-қимыл жүйесінде құқықтық реттеу.	137
<i>Kussainova A.</i> Harmonization of Legal Terminology and Linguistic Authenticity in the Criminal Law of Kazakhstan.	146
<i>Қусаинова А.К.</i> Юридикто-лингвистические проблемы формирования и гармонизации уголовно-правовой терминологии Республики Казахстан.	155

Yeerkenbieke Zh. Criminological Characteristics of the Causes and Conditions of Juvenile Delinquency (Based on the Experience of the Republic of Kazakhstan and the People's Republic of China)	165
Yeerkenbieke Zh. Criminological Characteristics of the Causes and Conditions of Juvenile Delinquency (Based on the Experience of the Republic of Kazakhstan and the People's Republic of China)	169
Маликова Ш.Б. Разграничение уголовной, административной и гражданско-правовой ответственности за неправомерное использование больших данных.	173
Маликова Ш.Б. Қазақстанның қылмыстық құқығындағы лингвистикалық коллизиялар: терминологиялық алшақтықтардың іс-әрекеттерді саралауға әсері.	188
Мағауия А., Сейтжан А.А. Распределение прав, обязанностей и ответственности между участниками обработки больших данных.	199
Мукашева А.А. Разграничение компетенции государственных органов при защите прав в сфере больших данных.	213
Нұрмағанбет Е.Т. Дәлелдемелерді жинау бойынша адвокат-қорғаушы қызметінің дербестігін жүзеге асыру құқығының мәселесі.	227
Нурмуханов Ж.Б. Некоторые вопросы самоубийства.	236
Омарова А.Б. Соотношение защиты коммерческой тайны и персональных данных в спорах об использовании клиентских баз.	241
Омарова А.Б. Доказывание режима коммерческой тайны при защите массивов цифровых данных.	257
Иноятова С. Ф. Правовые механизмы защиты женщин от притеснения и насилия и расширения их возможностей в предпринимательской деятельности.	273
Иноятова С.Ф. Современные тенденции защиты новых объектов гражданских прав в условиях цифровизации и развития искусственного интеллекта	286
Петрова А. К. Алгоритмические доказательства в судебном процессе: правовые риски и перспективы регулирования в условиях цифровизации.	295
Рузиназаров Ш.Н. Парадигма частного права в цифровую эпоху: соотношение цифрового и гражданского права.	306
Сейтжан А.А. Жасанды интеллект негізінде Қазақстан Республикасының қылмыстық заңнамасының терминологиялық деректер базасын құру.....	330
Смагулова Т.С., Порохов Е.В. Уклонение от уплаты алиментов как форма экономического насилия: позитивные обязательства государства и роль налоговых органов в их реализации.....	337
Гленбергенев О.Н. Ұлттық құқықтық сана, рухани даму және қылмыстан сақтандырудың өзара сұрақтары жайлы.	360

ЭКСТРЕМИСТСКИЕ ПРОЯВЛЕНИЯ В МОЛОДЕЖНОЙ СРЕДЕ ТАДЖИКИСТАНА: ПРОБЛЕМЫ ПРОФИЛАКТИКИ

В современных условиях особую угрозу представляют экстремистские проявления в поведении молодежи, что чревато опасностью для Республики Таджикистан в целом, наносит ощутимый вред ее территориальной целостности, конституционным правам и свободам граждан, особенно на фоне обострения национальных и конфессиональных противоречий в мире. В этой связи глобальной международной проблемой становится борьба с религиозным экстремизмом.

Закон РТ «О борьбе с экстремизмом» от 8 декабря 2003 г. №69 [1] впервые в истории Таджикистана закрепил легальную дефиницию понятия «экстремизм» в форме экстремистской деятельности. Однако, признат, что Закон РТ «О борьбе с экстремизмом» как принципиально новое в законодательстве Таджикистана, значит, преувеличивать его роль, так как нормативно-правовые акты в той или иной мере затрагивающее меры борьбы с экстремизмом в РТ была уже действующими до его принятия.

Так, законы, направленные на борьбу с экстремизмом в РТ, до принятия Закона РТ «О борьбе с экстремизмом», являются: 1. Конституция РТ [2]. 2. Закон РТ «О религии и религиозных организациях» от 1 декабря 1994 года (по состоянию на 12 мая 2001 г.), утратившим силу с ведением в действие 26 марта 2009 г. нового Закона РТ «О свободе совести и религиозных объединениях» [3] 3. Уголовный кодекс РТ от 21 мая 1998 года [4]. 4. Закон РТ «Об общественных объединениях» от 23 мая 1998 года (по состоянию на 12 мая 2007), утративший силу с ведением в действие 12 мая 2007 г. нового Закона РТ «Об общественных объединениях» [5]. 5. Закон РТ «О политических партиях» от 13 ноября 1998 г [6]. 6. Закон РТ «О борьбе с терроризмом» от 16 ноября 1999 года [7]. 7. Шанхайская

конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 15 июля 2001 года (в редакции протокола от 5 сентября 2003 г.) [8]. 8. Постановление Парламента РТ о ратификации договора [9] о совместных действиях по борьбе с терроризмом, политическим и религиозным экстремизмом, транснациональной организованной преступностью и иными угрозами стабильности и безопасности.

Противодействие с экстремизмом в РТ в основном сводится к пресечению террористической деятельности, в то время как главным направлением этой деятельности должна стать профилактика терроризма, поскольку государственная власть, опирающаяся только на силовой аппарат противодействия террору, не использующая в полной мере разнонаправленные политико-правовые механизмы его предупреждения и пресечения, не имеет будущего.

Экстремизм выступает по отношению к терроризму как понятие родового плана, а терроризм является разновидностью экстремизма (по крайней мере, оба характеризуются радикализмом).

Проведенное исследование позволило выявить ряд значимых тенденций и детерминант социального развития молодежи. На их основе можно сделать общий вывод об изменении вектора ее развития.

Исследование подтвердило, что в изменении социального положения и мотивационной сферы сознания молодежи определяющую роль играют объективные изменения, происходящие в обществе. Переход от неопределенности к устойчивому развитию связан с разрешением одних противоречий, но одновременно порождает другие. Их природа носит внешний по отношению к молодежи характер и определяется более широкими социальными детерминантами, а конкретные проявления среди молодежи зачастую приобретают непредсказуемый, спонтанный характер. В связи с этим возникает необходимость в постоянном мониторинге изменений в молодежной среде.

Остается стабильно высокой и даже имеет тенденцию роста доля нуждающейся молодежи. Решение этих проблем находится в непосредственной связи с мероприятиями по повышению жизненного уровня населения в целом. При этом необходимы

дополнительные меры. Поддержка работающей молодежи должна осуществляться посредством широкого комплекса мер по расширению возможностей ее самореализации в сфере труда, а также путем повышения уровня ее социальной и правовой защищенности. Дополнительную материальную помощь учащейся молодежи целесообразно в большей мере связывать с расширением доступа к образованию. Материальную поддержку молодых семей следует в первую очередь осуществлять путем решения их жилищных проблем.

Основой обеспечения эффективной организации противодействия экстремизму в Таджикистане, по мнению большинства исследователей, являются, создание эффективной системы взаимосвязанных мер по выявлению, предупреждению, профилактике и пресечению экстремизма, разработка и реализация общегосударственной комплексной программы, включающей политический, социальный, экономический, правовой, идеологический, специальный (оперативный, розыскной, технический, охранный) и другие аспекты. Эта программа должна основываться на следующих основополагающих принципах и стратегических установках: уяснение содержания экстремистской деятельности (ее субъектов, целей, задач, средств, а также типологии современного экстремизма, его причин, социальной базы, специфики и форм подготовки и проведения оперативных операций); нормативно-правовое обеспечение антиэкстремистских действий; анализ и учет зарубежного опыта борьбы с экстремизмом, различных моделей антиэкстремистской деятельности по предупреждению и пресечению экстремизма; преимущество превентивных мероприятий, позволяющих осуществлять выявление намерений проведения экстремистских акций, оперативное пресечение экстремистских действий на стадии их реализации, обеспечение правомочий и ресурсов; всестороннее обеспечение осуществляемых военных, специальных и идеологических мероприятий; воспитательно-идеологическое дифференцированное воздействие на население, экстремистов, субъектов их поддержки и противников, всестороннее информационно-психологическое обеспечение антиэкстремистской деятельности; обеспечение

взаимодействия и координации действий антиэкстремистских сил в международном, межгосударственном масштабе; неуклонное обеспечение неотвратимости наказания за экстремистские преступления в соответствии с законом.

Необходимыми мерами являются: повышение юридической компетентности граждан, правовой культуры, образования отдельных социальных групп, создание условий для развития традиционной и самобытной культуры; усиление пропагандистской работы среди населения, разъяснение сути антиэкстремистских идей; создание эффективной системы просвещения граждан в части культурного и конфессионального многообразия и исторического единства жителей страны, истории религиозной нетерпимости, геноцида и других преступлений, порожденных экстремизмом; обеспечение системы мер, направленных на противодействие пропаганде экстремистской идеологии, насилия в средствах массовой информации, усиление контрпропаганды, переориентации СМИ на внедрение в социальную практику норм толерантного поведения и др.

Проводимые мероприятия по улучшению демографической ситуации в стране пока не дали желаемых результатов. Сохраняется тенденция роста незарегистрированных браков, продолжается тенденция распада молодых семей. Становится очевидным, что меры, предусмотренные в существующих государственных программах, недостаточны. Прежде всего, они не решают проблему отложенного родительства, которая, в свою очередь, определяет весь комплекс демографических проблем. Необходима корректировка намеченных мер в соответствующем национальном проекте.

Сохраняется на высоком уровне процент незанятой молодежи. К ней относятся безработные и те, кто по разным причинам нигде не работает и не учится. Причем подавляющее большинство среди них имеют образование и профессию и мотивируют незанятость нежеланием работать задарма. При очевидном различии этих форм незанятости последствия их для молодых людей одинаково опасны. Поэтому нужны специальные региональные программы

трудоустройства этих категорий молодежи, в которых учитывалась бы специфика различной мотивации незанятости.

Выявленные тенденции снижения качества образования и уровня квалификации в самооценке молодежи имеют общую причину. Она отражает последствия накопившихся противоречий в затянувшемся процессе реформирования данной сферы. Учитывая значимость этой проблемы для расширенного воспроизводства образовательного и профессионально-квалификационного потенциала в стране, важно предусмотреть комплекс специальных мер по повышению качества образования и профессиональной подготовки в рамках соответствующего национального проекта. Особое внимание следует обратить на заочные формы обучения в связи с ростом их популярности среди молодежи.

Наименьшими возможностями в получении образования располагает сельская молодежь. Недоступность многих форм образования по месту жительства, в том числе и профессионального, для сельских юношей и девушек дополняется низким качеством образовательных услуг в средней школе, снижающих уровень их конкуренто-способности по сравнению с молодежью из крупных городов. Поэтому проблема доступности и качества образования для сельской молодежи должна быть выделена в самостоятельную государственную программу.

Не реализуется до настоящего времени в полном объеме правос воспитательная функция государства, которая, на наш взгляд, очевидна, должна стать самостоятельной функцией государства. Представляется оправданной также разработка специальной региональных программ повышения правовой культуры молодежи, изучение опыта, накопленного за рубежом.

Список использованных источников

- 1 Закон РТ «О борьбе с экстремизмом» от 8 декабря 2003 года //Ахбори Маджлиси Оли РТ. –2003. –№12. – Ст.697.
- 2 Конституция РТ. – Душанбе: Матбуот, 2004.
- 3 Закон РТ «О свободе совести и религиозных объединениях» от 26 марта 2009 года //Ахбори Маджлиси Оли РТ. –2009 г. –№489. – Ст.739.
- 4 Уголовный кодекс РТ от 21 мая 1998 года. - Душанбе: Конуният, 2004.
- 5 Закон РТ «Об общественных объединениях»от 12 мая 2007 года //Ахбори Маджлиси Оли РТ. – 2007. –№5. – Ст.363.

6 Закон РТ «О политических партиях» от 13 ноября 1998 года //АхбориМаджлиси Оли РТ. –1998. –№22. – Ст.300.

7 Закон РТ «О борьбе с терроризмом» от 16 ноября 1999 года //АхбориМаджлиси Оли РТ. –1999. –№11. – Ст.275.

8 Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом от 15 июля 2001 года // Сборник международных актов по борьбе с терроризмом. – Душанбе, 2003.

9 Договор между Республикой Таджикистан, Республикой Казахстан, Кыргызской Республикой и Республикой Узбекистан о совместных действиях по борьбе с терроризмом, политическим и религиозным экстремизмом, транснациональной организованной преступностью и иными угрозами стабильности и безопасности // АхбориМаджлиси Оли РТ. – 2000. –№10. – Ст.442.

Айнакулова Д.Б.

*Казахского национального университета имени аль-Фараби,
Республика Казахстан, г. Алматы*

E-mail: dari92@bk.ru

ХАРАКТЕРИСТИКА УБИЙСТВА ПО ЗАКОНОДАТЕЛЬСТВУ РЕСПУБЛИКИ КАЗАХСТАН

Как известно, преступления против личности на протяжении столетий и тысячелетий приковывали к себе внимание юристов и философов психологов, писателей, художников и историков. С истоков уголовного права вопрос о преступлениях против личности выходит на первое место, а именно: преступления против жизни.

Наиболее опасное преступление против жизни – это убийство. В уголовном законодательстве РК убийство определено как «противоправное умышленное причинение смерти другому человеку» (статья 99 УК РК). Ранее действовавшее уголовное законодательство не содержало определения «убийства», поскольку неосторожное причинение смерти также признавалось убийством. Действующим уголовным кодексом Республики Казахстан причинение смерти по неосторожности не относится к убийству. Наряду с этим, в отличие от российского Уголовного кодекса, казахстанский законодатель определил убийство, как «противоправное умышленное причинение смерти».

Противоправность в данном случае выделено для устранения недоразумений, так как в законе имеет место и узаконенное причинение смерти, такое как исполнение приговора суда о высшей мере наказания, причинения смерти при задержании лица совершившего преступление, причинении смерти при необходимой обороне.

Перечень «узаконенных» убийств в различные исторические эпохи претерпевал изменения. Так, исторический анализ уголовно - правового законодательства показывает, что убийство, одно из тех преступлений, которые в различные исторические эпохи, как законами, так и моралью расценивались различно [1, с. 42].

Вышеизложенное объясняется разными социальными и религиозными взглядами на различных этапах развития общества, что в свою очередь приводило к неадекватной оценке общественной опасности убийства.

Статья 3 Всеобщей декларации прав человека устанавливает, что каждый человек имеет право на жизнь, на свободу и на личную неприкосновенность [2]. Это положение воспроизведено в ст. 15, 16 Конституции Республики Казахстан. Всемирная охрана жизни и здоровья человека – важнейшая задача уголовного законодательства. центре внимания борьбы с преступностью на современном этапе стоят преступления против жизни и здоровья человека, которые занимают особое место как в системе наук уголовного права и процесса, так и в других юридических науках – криминологии, исправительно трудовом праве и т. д. В настоящее время, преступные посягательства на жизнь и здоровья являются все более нетерпимы, и решительная борьба с ними составляет важнейшую задачу правоохранительных и правоприменительных органов. Однако, как свидетельствует следственная и судебная практика, преступления против жизни и здоровья (в особенности Убийство) относятся к числу тех преступлений, которые наиболее часто вызывают большие трудности при расследовании и квалификации.

Предусмотренные уголовным законом преступления против жизни - это группа общественно - опасных деяний, направленных против основных личных прав человека. В этой связи правильная квалификация этих преступлений, большая часть которых

относится к категории особо тяжких преступлений, включает не только его правовую, но и более широкую социальную, информационную оценку. Правильная квалификация рассматриваемых преступлений является важной гарантией осуществления правосудия в строгом соответствии с действующим процессуальным законодательством.

Преступлениями против жизни признаются такие действия, непосредственно направленные на жизнь человека, при совершении которых лишение жизни или доведение до самоубийства другого лица считается основанием уголовной ответственности.

По действующему УК к преступлениям против жизни относятся: убийство (ст. 99 УК); убийство матерью новорожденного ребенка (ст. 100 УК); убийство, совершенное в состоянии аффекта (ст. 101 УК); убийство, совершенное при превышении пределов необходимой обороны (ст. 102 УК); убийство, совершенное при превышении мер, необходимых для задержания лица, совершившего преступление (ст. 103 УК); причинение смерти по неосторожности (ст. 104 УК); доведение до самоубийства (ст. 105 УК). Все перечисленные преступления против жизни, за исключением последних двух, относятся к убийству.

Убийство (ст. 99 УК РК). Уголовные кодексы РСФСР 1926г и 1990г. не содержали определения убийства, и лишь предусматривали составы умышленного и неосторожного убийства (ст. ст. 102 - 103, 109, 106, УК РСФСР). Отсутствие определения убийства породило неоднозначные суждения относительно содержания и формы деяния при убийстве, что не могло не сказаться на судебной практике.

Пробел в законе восполняли «ученые». Они предлагали несколько «определений» убийства. По мнению Н.И. Загородникова убийство есть противоправное умышленное или неосторожное лишение жизни другого лица, когда лишение жизни является основанием уголовной ответственности [3, с. 79]. В этом определении противоправность названо, конкретно. Такое определение позволяло, террористический акт назвать убийством. Кроме того, введение в определение убийства умысла и неосторожности противоречило ст. 7 УК РК.

С.Б. Бородин определял убийство как предусмотренное Особенной частью УК виновное деяние, посягающее на жизнь другого человека и причиняющее ему смерть [1, с. 13].

Согласно ст. 99 УК убийство – это умышленное причинение смерти другому человеку. Введение в УК понятие убийства является значительным шагом вперед в развитие законодательства о преступлениях против жизни. Указание на умышленный характер действия четко привело границу между убийством и другими преступлениями, сопряженными с неосторожным причинением смерти.

Определение убийства в определенной мере согласуется с определением преступления, данным ст. 9 УК и имеющим общий характер.

Убийство – наиболее тяжкое преступление против личности. Часть первая статьи 99 УК определяет, что убийством является противоправное умышленное причинение смерти другому человеку. Жизнь человека представляет собой важнейшую, природой данную социальную ценность, которая принадлежит каждому от рождения.

В уголовно-правовом смысле понятие убийства более узкое, так как для наступления уголовной ответственности за убийство необходимо наличие определенных признаков, которые свидетельствовали о совершении данного преступления.

Понятие «убийство» неразрывно связано с жизнью и смертью человека, поэтому без выяснения содержания понятие жизни и смерти нельзя говорить об определении убийства.

Известно, что жизнь человека, с биологической точки зрения, состоит в непрерывном обмене веществ, питании и выделении. С прекращением этих функции прекращается и жизнь человека. Человеческая жизнь в биологическом смысле этого слова имеет значение для определения границ жизни человека. Возникновение жизни связано с началом процесса родов. Естественным и неизбежным завершением жизни является физиологическая смерть человека вследствие старения организма.

Вопрос о моменте наступления смерти человека в медицинской литературе является дискуссионным. Одни авторы полагают, что

смерть человека наступает с момента прекращения дыхания и сердцебиения. Другие считают сердцебиение не абсолютным доказательством жизни. Но признается бесспорным наступление смерти с момента органических изменений в головном мозге и центральной нервной системе. До наступления этих изменений смерть человека называют клинической.

Встречаются случаи, когда после наступления клинической смерти удастся восстановить дыхание и сердцебиение и вернуть человека к жизни. Особенно в последние годы достижение медицинской науки и практики в области реаниматологии способствовали изменению отношения к смерти как одномоментному явлению.

О наступлении смерти человека свидетельствует только биологическая смерть, то есть состояние необратимой гибели организма как целого, когда остановлена сердечная деятельность исчезла пульсация в крупных артериях, прекращено дыхание, утрачены функции центральной нервной системы.

Некоторая часть людей умирает в результате патологической, преждевременной смерти, вызванной болезнью или насильственными действиями. К патологической смерти относится и убийство, которая является родом насильственной смерти.

Следовательно, насильственный характер смерти – один из признаков убийства. Но насильственная смерть, может носить и правомерный характер (например, приведение в исполнение приговора к смертной казни). Кроме того, насильственная смерть может свидетельствовать не только об убийстве, но и о несчастном случае и самоубийстве. В связи с этим возникает вопрос об их разграничении.

В отличие от правомерного лишения жизни, несчастного случая и самоубийства, убийство преследуется как противоправное деяние, предусмотренное Особенной частью Уголовного кодекса Республики Казахстан. Чтобы исключить отнесение к убийству правомерного лишения жизни и случайного причинения смерти, совершаемых при отсутствии вины. Как считает С.В. Бородин, необходимо при определении убийства указать на виновное лишение жизни [1, с. 14]. Наконец для отграничения от

самоубийства, указывается, что, речь идет о лишении жизни другого человека.

Исходя из указанных признаков в отечественной литературе с теми или другими небольшими различиями убийство определялось как противоправное умышленное или неосторожное лишение жизни другого человека. В части 1 статьи 99 Уголовного кодекса дано определение понятия убийства, которое существенно уточняет понятие этого преступления по данной статье под убийством признается противоправное умышленное причинение смерти другому человеку. Из данной формулировки следует, что убийством является умышленное причинение смерти другому человеку. Тем самым из категории убийств исключается причинение смерти по неосторожности, но это не означает исключения последнего из числа преступлений против жизни.

М.Д. Шаргородский также относит к убийству только умышленное причинение кому-либо смерти, неосторожное же причинение смерти он оставляет за пределами этого понятия [4, с.57].

Следует отметить, что некоторые авторы считают неполным определение убийства. Так, Бородин С.В. пишет: «в законодательном определении убийства, с нашей точки зрения не достаёт указания на противоправность и виновность деяния» [1, с.97]. Заметим, что в определении убийства в Уголовного кодекса Российской Федерации отсутствует указание на противоправность, в отличии от нас. Не вливаясь в баталии, нужно отметить, что наш законодатель наверное счел вполне полным и определенным понятие убийства дав ему такое определение, которое указано в части 1 статьи 99 Уголовного кодекса Республики Казахстан.

Уголовный кодекс Республики Казахстан предусматривает только умышленные убийства. Причинение смерти по неосторожности действующим Уголовным кодексом не относится к убийству.

Умышленные убийства делят на следующие три вида:

1) убийство без отягчающих и смягчающих обстоятельств (часть 1 статьи 99 Уголовного кодекса);

2) убийство при отягчающих обстоятельствах (часть 2 статьи 99 Уголовного кодекса);

3) убийство при смягчающих обстоятельствах (статьи 100-103 Уголовного кодекса).

Убийство предусмотренное частью 1 статьи 99 Уголовного кодекса или «простое» убийство является так называемым основным составом данного вида преступлений.

Убийство предусмотренное частью 2 статьи 99 Уголовного кодекса, является квалифицированным составом данного вида преступлений. Данная часть статьи содержит пятнадцать пунктов отягчающих обстоятельств.

Убийство при смягчающих обстоятельствах относится к привилегированному составу данного вида преступлений. К данному виду убийства относятся убийства предусмотренные статьями 99, 100, 101, 102, 103 Уголовного кодекса.

Список использованных источников

- 1 Бородин С.В. Преступления против жизни. – Москва, 1999. – 136 с.
- 2 Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10 декабря 1948 г.) // Российская газета. – 1998. - 10 декабря.
- 3 Загородников Н.И. Преступления против жизни по Советскому уголовному праву. – Москва, 1961. - 102 с.
- 4 Шаргородский М.Д. Ответственность за преступления против личности. - Москва, 1953. - 96 с.

Акпаева Ж.

*Судья районного суда №2 Алмалинского района
города Алматы, магистр права*

ЦИФРОВАЯ СДЕЛКА И ПРЕДЕЛЫ УПРОЩЕННОГО ПРОИЗВОДСТВА: ТРЕБУЕТСЯ ЛИ ПЕРЕОСМЫСЛЕНИЕ СТАНДАРТОВ СУДЕБНОГО ДОКАЗЫВАНИЯ?

В юридическом сообществе Казахстана все чаще обсуждаются вопросы цифровизации гражданского оборота, электронных договоров, дистанционной идентификации личности, применения

искусственного интеллекта и платформенной экономики (цифровые сервисы).

Крупные платформы аккумулируют колоссальные объемы данных и могут диктовать свои условия продавцам, что вынуждает государства обновлять антимонопольное законодательство. Возникновение «гиг-экономики» (фриланс) заставляет законодателей пересматривать трудовое законодательство, разрабатывать механизмы предоставления таким работникам социальных гарантий и пенсионного обеспечения. Государства вводят новые требования к цифровым платформам, включая маркетплейсы, в части возврата товаров, ответственности за их качество и прозрачности ценообразования. Одновременно формируются новые налоговые режимы, учитывающие особенности платформенной занятости и цифровой экономики.

В Казахстане планируется внедрение полноформатной системы электронного Парламента (e-Parliament). Об этом заявил Глава государства Касым-Жомарт Токаев, выступая на совместном заседании палат Парламента. В эпоху тотальной цифровизации и искусственного интеллекта Курултаю придется работать в ускоренном темпе для оперативной адаптации национального законодательства к стремительно меняющимся реалиям в цифровой матрице, - подчеркивал Президент [1].

Цифровая эволюция требует безусловного совершенствования материального права. Вместе с тем, не менее существенные изменения необходимы и в сфере процессуального права, поскольку цифровизация затронула формы возникновения, исполнения и доказывания гражданско-правовых обязательств. В этих условиях закономерно возникает вопрос о соответствии существующей модели гражданского процесса природе цифровых правоотношений и ее способности обеспечить эффективную судебную защиту их участников.

Наиболее отчетливо этот вопрос проявляется при рассмотрении споров, возникающих из электронных договоров займа (о предоставлении микрокредита).

Именно эта категория дел стала своеобразным испытанием для гражданского процесса, поскольку требует оценки

дистанционной идентификации личности, электронного волеизъявления, цифровых следов совершения сделки и иных электронных доказательств, которые нередко являются единственным подтверждением возникновения обязательства.

В последние годы количество таких споров увеличилось многократно. Вместе с ростом цифрового кредитования произошло и стремительное увеличение количества судебных дел о взыскании задолженности. При этом значительная часть подобных споров рассматривается в порядке упрощенного производства. Превалирующая масса таких дел разрешается на уровне районных судов.

Цифровая форма сделки сохраняет сущность обязательственных отношений. Под цифровой сделкой следует понимать сделку, совершаемую в электронной форме посредством электронного документа и цифровых средств идентификации, подтверждающих волю сторон.

Способна ли существующая процессуальная модель обеспечить тот уровень судебной проверки, которого требуют цифровые доказательства?

В момент принятия главы 21-1 Гражданского процессуального кодекса Республики Казахстан об упрощенном (письменном) производстве предполагалось, что подобные дела обладают очевидностью. Но цифровизация изменила объект доказывания. Законодатель создавал институт упрощенного производства для бесспорных требований. Однако цифровая трансформация гражданского оборота изменила характер таких споров. Сегодня цена иска далеко не всегда отражает сложность установления юридически значимых обстоятельств.

Достаточна ли существующая процессуальная форма для исследования электронной сделки?

Особенность действующего процессуального регулирования заключается в том, что значительная часть подобных дел одновременно рассматривается в упрощенном порядке и не подлежит кассационному пересмотру.

Следовательно, именно практика судов первой и апелляционной инстанций фактически формирует окончательный стандарт оценки электронных доказательств.

При отсутствии единообразных подходов различия в судебной практике перестают быть локальной проблемой отдельных дел и начинают непосредственно влиять на уровень судебной защиты тысяч граждан.

Цена иска перестала быть критерием сложности дела.

Независимо от размера исковых требований спор может потребовать исследования биометрической идентификации/аутентификации, журналов событий, IP-адреса, ОТП-код с подтверждением собственника абонентского номера, серверных логов, электронной цифровой подписи, последовательности действий пользователя.

Электронный заем - лишь первая стадия цифровизации гражданского оборота.

Уже сегодня появляются сделки, совершаемые с использованием искусственного интеллекта, автоматизированных платформ, цифровых агентов.

Если процессуальное законодательство не выработает специальных стандартов исследования цифровых доказательств уже сейчас, аналогичные проблемы неизбежно возникнут и в иных категориях гражданских дел.

Цифровизация не снижает значение судебной защиты. Напротив, чем сложнее становятся технологии заключения сделок, тем выше должны становиться требования к судебному доказыванию.

Сейчас как никогда настало время для профессиональной дискуссии о новой модели судебного доказывания по цифровым гражданским спорам.

Очевидно, что цифровой спор требует переосмысления критериев выбора процессуальной формы и стандарта судебного доказывания.

Цифровая трансформация изменила экономику, способы заключения сделок и формы взаимодействия граждан с финансовыми организациями.

Институт упрощенного производства создавался как эффективный механизм разрешения дел, не требующих сложного исследования доказательств. Но электронная сделка поставила перед судом принципиально новые задачи. Сегодня предметом судебного исследования становятся цифровые данные.

Современная экономика объективно невозможна без цифровых сервисов, дистанционного кредитования и электронного документооборота. Стало очевидно, что цифровая трансформация изменила природу доказательств, которыми эти сделки подтверждаются в суде.

Может ли гражданский процесс оставаться неизменным, если кардинально изменился объект судебного познания? Если юридически значимые факты все чаще подтверждаются цифровыми следами, журналами событий, электронными сообщениями, биометрической идентификацией, логами информационных систем и иными электронными доказательствами, то неизбежно требует пересмотра и процессуальная модель их судебной оценки.

Это означает необходимость нового осмысления критериев, распределения бремени доказывания и стандарта достаточности и оценки цифровых доказательств.

Значение этого вопроса выходит далеко за пределы судебной практики по вышеуказанной категории дел. Линейка категорий споров стремительно растет.

По существу, речь идет о способности гражданского процесса обеспечить **конституционное право на судебную защиту** в условиях цифровой экономики и сохранить доверие общества к судебной власти.

Поэтому главный вопрос заключается в том, какие первоочередные шаги следует предпринять, чтобы гражданский процесс смог уже сегодня адаптироваться к новой цифровой реальности, обеспечив при этом законность.

В этих условиях на суд возлагается новая задача - суд должен установить, какое обязательство возникло в действительности и какими цифровыми параметрами подтверждается воля человека.

Современная научная литература подчеркивает, что электронные доказательства представляют собой результат

функционирования информационных систем, а не самостоятельный объект доказательства. Поэтому при их оценке необходимо исследовать надежность системы, которая сформировала цифровой след [4].

По мнению Стивена Мейсона, одного из ведущих исследователей электронных доказательств, суд обязан оценивать не только сам цифровой файл, но и технологическую среду его создания, включая систему регистрации действий пользователя и механизмы защиты данных [4].

Даниэль Сэнг обращает внимание на то, что цифровые доказательства могут быть созданы как человеком, так и автоматически информационной системой. Это требует различного подхода к их доказательственной оценке, поскольку автоматические данные отражают работу алгоритма, а не непосредственное волеизъявление лица [5].

В этих условиях традиционная модель доказывания, основанная на материальных носителях, демонстрирует свои пределы. Цифровому доказательству присущи такие свойства, как абстрактность, опосредованность, интерпретируемость, технологическая зависимость и трансграничность.

К общепризнанным международным стандартам оценки цифровых доказательств относятся требования целостности данных, проверяемости источника, неизменности информации, аутентичности цифрового следа [6].

Как отмечает Джордж Пол, цифровые доказательства позволяют осуществлять реконструкцию событий на основе анализа цифровых следов - логов, метаданных, временных отметок и сетевых идентификаторов [7].

Однако наличие данных само по себе еще не означает установление юридически значимого факта. Техническая фиксация события и правовое доказательство относятся к различным категориям.

Цифровая сделка существует для суда лишь постольку, поскольку установлены ее обязательные элементы (субъект, факт выражения воли, способ идентификации, неизменность данных и

причинная связь между действием и возникновением обязательства).

В теории гражданского процесса доказывание рассматривается как центральный элемент судебной деятельности, направленный на установление юридически значимых фактов. Как отмечает профессор З.Х. Баймолдина, доказательства приобретают юридическое значение лишь тогда, когда позволяют суду сформировать внутреннее убеждение относительно наличия обстоятельств, входящих в предмет доказывания [2].

Личные наблюдения за судебной практикой показывают, что понимание стандартов доказывания в цифровых делах остается фрагментарным. скриншоты, цифровые sms-коды нередко принимаются судами как достаточные доказательства без проверки их подлинности и источника происхождения.

В цифровую эпоху судья остается главным носителем ответственности за справедливость решения.

В этой связи представляется необходимым:

- разработать единые методические рекомендации по оценке цифровых доказательств;
- внедрить дифференцированные стандарты доказывания для цифровых дел;
- развивать судебную экспертизу в сфере цифровых технологий;
- рассмотреть возможность создания специализированных цифровых судов (Smart court).

Право должно адаптироваться к цифровой реальности, не утрачивая своего гуманистического содержания.

Список использованной литературы

1. Токаев К.К. Выступление Главы государства. - Режим доступа: <https://www.akorda.kz/ru/vystuplenie-glavy-gosudarstva-kasym-zhomarta-tokaeva-na-sovmestnom-zasedanii-palat-parlamenta-3054921>

2. Баймолдина З.Х. Гражданское судопроизводство в Республике Казахстан: новеллы и тенденции развития. - Режим доступа: <https://cyberleninka.ru/article/n/grazhdanskoe-sudoproizvodstvo-v-respublike-kazahstan-novelly-i-tendentsii> (дата обращения: 2023).

3. Mason S., Seng D. Electronic Evidence. 4th ed. - London: Institute of Advanced Legal Studies, University of London Press, 2017. - 421 p. Открытый доступ: <https://books.uolpress.co.uk/10.14296/517.9781911507079.pdf>

4. Mason S. Electronic Signatures in Law. 4th ed. - London: Institute of Advanced Legal Studies, University of London Press, 2016. - 476 p. Открытый доступ: <https://sas-space.sas.ac.uk/6518/>

5. Mason S., Seng D. (eds.). Electronic Evidence and Electronic Signatures. 5th ed. - London: University of London Press, 2021. - 604 p. Открытый доступ: <https://library.oapen.org/handle/20.500.12657/55755>

6. Paul G. L. Foundations of Digital Evidence. - Chicago: American Bar Association, 2008. - 450 p.

7. Murdoch S., Seng D., Schafer B., Mason S. The Sources and Characteristics of Electronic Evidence and Artificial Intelligence. In: Mason S., Seng D. (eds.) Electronic Evidence and Electronic Signatures. - London: University of London Press, 2021. - P.1–50.

Акболатова М.Е.

Казахский национальный университет имени аль-Фараби,

Республика Казахстан, г. Алматы

E-mail: m_akbolatova@mail.ru

УГОЛОВНЫЕ ПРАВОНАРУШЕНИЯ, СВЯЗАННЫЕ С МИГРАЦИЕЙ НАСЕЛЕНИЯ

Миграция населения является одним из важных факторов динамики численности населения, а также структуры населения, как во всей стране в целом, так и в отдельных ее регионах.

Миграция в целом является положительным показателем, так как влияет на развитие государства в целом. Ведь по миграционной политике можно определить политические, экономические, демографические процессы, происходящие в стране. Однако проведение миграционной политики требует принятия ряда нормативных правовых актов, возможности их исполнения на практике, а также возможности выявления и устранения проблем, связанных с миграцией.

С начала становления Казахстана как независимого государства, а также вступления его на международную арену происходили различные изменения. В начале своей независимости

наблюдалось активное перемещение в большей части квалифицированной рабочей группы населения в другие страны, в особенности в страны Европы, где внутреннее положение было стабильным, законодательство было упорядоченным и больших изменений в политической сфере не наблюдалось.

На сегодняшний день в Казахстане за 20 с лишним лет установились более устойчивые направления развития, в особенности в части миграции населения как внутри страны, так и внешней миграции. Однако до сих пор существуют некоторые проблемы, связанные с этим. Одним из таких проблем является совершение различных правонарушений мигрантами (административных, уголовных), в данном случае, имеется ввиду про мигрантов из других стран. Это связано с различными факторами.

Нахождение территории Казахстана в центре Евразии делает страну своеобразным пунктом, через который проходят различные пути из одних стран в другие.

Отсутствие правовой базы в области миграционной политики после распада СССР.

Мигранты ищут работу, в основном, в больших городах страны. Однако в этих регионах также есть свой уровень безработицы для населения самого региона. Это создает условия для совершения различных правонарушений в целях дохода в свои руки.

Нестабильность в государствах, находящихся поблизости. Так, политические события на Украине повлекли отток граждан той страны в различные страны, в том числе и в Казахстан;

Несильный пограничный контроль в стране, а также не совсем сильная исполнительная власть в области миграции.

Приведенные причины являются одними из важных. Но кроме них существуют и различные другие причины, связанные также с внутренними и внешними процессами.

При незаконной миграции ответственность несут не только мигранты, но и лица, которые организовали и участвовали в данном правонарушении. Организация незаконной миграции является не просто уголовным правонарушением, а именно преступлением, за которое предусмотрено такое наказание, как штраф в размере до

двух тысяч месячных расчетных показателей либо исправительные работы в том же размере, либо ограничение свободы на срок до двух лет, либо лишение свободы на тот же срок [1].

В новом Уголовном кодексе Республики Казахстан, вступившем в силу в 2015 году, этот вид наказания ужесточен, тогда как в старом Уголовном кодексе был предусмотрен такие виды наказания, как штраф в размере от двухсот до пятисот месячных расчетных показателей либо лишением свободы на срок до двух лет [2].

Кроме того, ч. 2 ст. 330-2 старого Уголовного кодекса РК, которая звучала как: «те же деяния, совершенные организованной группой либо с использованием своих служебных полномочий» была изменена. Теперь же в ч. 2 ст. 394 Нового Уголовного кодекса говорится «деяние, совершенное лицом с использованием своих служебных полномочий или группой лиц по предварительному сговору». К тому же существует и часть 3, которая звучит как «Деяние, предусмотренное частью первой настоящей статьи, совершенное преступной группой».

Заключение соглашений между странами, создание законодательной базы в области миграции, указание ответственности за нарушения норм права не решает полностью всех проблем миграции. Необходимо осуществление ее на деле, а также постоянное обновление базы данных, создание статистики наиболее часто совершаемых правонарушений, выявление, изучение и устранение этих правонарушений.

Мигранты, в особенности временные, совершают различные уголовные правонарушения, среди которых участие в бандитских или террористических группировках, осуществление перевозки наркотиков, оружия и иной контрабанды, занятие иной нелегальной деятельностью и т. д. Известно, что продажа наркотических веществ является одним из распространенных видов преступлений. В особенности этот вид правонарушения распространен среди правонарушений, совершаемых мигрантами. Многие населенные пункты Казахстана является пунктами для переправки наркотических веществ в другие страны.

Одним из известных происшествий в данной области было громкое дело - совершение убийства целой семьи в 2013 году. Гражданин Узбекистана, который являлся трудовым мигрантом и был нанят для ремонта квартиры, задушил семью своего хозяина из четырех человек в Алматы. Преступление было совершено летом 2013 года. Впоследствии было выяснено, что в преступлении участвовали 3 человека в главе с гражданином Узбекистана [3].

Мигранты за совершение различных правонарушений несут ту ответственность, которая предусмотрена Уголовным кодексом Республики Казахстан, Кодексом об административных правонарушениях Республики Казахстан, если иное не предусмотрено международными соглашениями и договорами, ратифицированными нашим государством.

Список использованных источников

- 1 Уголовный кодекс Республики Казахстан от 3 июля 2014 года
- 2 Уголовный кодекс Республики Казахстан от 16 июля 1997 года, утративший силу введением нового Уголовного кодекса.
- 3 http://tengrinews.kz/kazakhstan_news/sud-ostavil-prigovor-ubiysam-semi-v-almaty-bez-izmeneniy-251442/.

Алдабек Е.А.

*Судья специализированного межрайонного суда
по административным правонарушениям г.Алматы*

Сапарбекова Ж.

старший преподаватель КазНУ им. аль-Фараби

ДОКАЗЫВАНИЕ НАРУШЕНИЙ ПРИ ИСПОЛЬЗОВАНИИ БОЛЬШИХ ДАННЫХ И ВЫБОР СПОСОБОВ СУДЕБНОЙ ЗАЩИТЫ

В споре о больших данных выражение «защитить информацию» еще не определяет ни содержание требования, ни необходимые доказательства. Гражданин может добиваться исправления относящейся к нему записи, а организация - прекращения неправомерного извлечения коммерчески ценного

массива. Требование раскрыть сведения об обработке также отличается от требования компенсировать ее последствия. Пока эти цели не разграничены, возникает риск исследовать масштаб информационного инцидента вместо обстоятельств, от которых зависит разрешение конкретного иска.

М.К. Сулейменов отделяет материально-правовые способы защиты от процессуальных форм их осуществления и рассматривает ответственность как часть, а не синоним защиты гражданских прав [1]. Применительно к данным это разграничение позволяет поставить вопрос о прекращении нарушения без подмены его вопросом о размере компенсации. Пункт 1 статьи 9 ГК РК предусматривает пресечение нарушающих действий, восстановление прежнего положения и исполнение обязанности в натуре наряду с денежными требованиями [2]. Поэтому доказывать уже возникшие убытки для любого требования об исправлении или прекращении обработки было бы неправильно.

Специальное регулирование также дифференцирует основания требований. Подпункты 1)-4) пункта 1 статьи 24 Закона «О персональных данных и их защите» закрепляют получение сведений об обработке, изменение данных при документальном подтверждении оснований, блокирование и устранение незаконно обрабатываемой информации. Подпункты 15) и 16) пункта 37 статьи 1 Закона от 24 июня 2026 года № 326-VIII уточнили положения статей 24-25, включая удаление данных [3; 4]. Это действующие средства, а не институты, которые еще предстоит впервые предложить законодателю.

Научная проблема состоит в несоответствии между принадлежностью права заявителю и нахождением доказательств его нарушения у другого лица. Предлагается анализировать не массив вообще, а связку «требование - юридически значимое обстоятельство - источник сведений - способ получения - защитное ограничение». Изменяемость базы и распределение операций между участниками учитываются при определении источника и периода фиксации. Техническая сложность не освобождает от обычных требований к относимости, допустимости и достоверности, но требует их содержательной конкретизации.

Используются формально-юридический, сравнительно-правовой методы и анализ опубликованной практики. Нормативная часть учитывает доступные редакции по состоянию на 27 сентября 2026 года. Новые положения не применяются ретроспективно к событиям 2023-2024 годов. Полные зарубежные решения, официальное сообщение регулятора и журналистское описание казахстанского спора имеют различную доказательственную ценность для самого исследования. Отобранные эпизоды проверяют отдельные конструкции; они не образуют репрезентативной выборки всех споров о Big Data.

Выбор судебной процедуры определяется природой оспариваемого отношения. При частноправовом требовании к оператору предметом могут быть нарушение договора, неправомерная передача сведений или неисполнение обязанности исправить запись. При оспаривании публичного решения требуется установить соответствующий административный акт либо действие. Статьи 132-134 АППК различают иски об оспаривании, принуждении и совершении действия [5]. Само участие государственного органа или использование государственного сервиса не превращает любое информационное разногласие в административный спор.

Особенно важно правильно соединять требования. Части 3-4 статьи 107 АППК предусматривают рассмотрение связанных с административным актом или действием убытков административным судом, тогда как моральный вред взыскивается в гражданском судопроизводстве. Статья 160 допускает требование о связанных убытках одновременно с исками, предусмотренными статьями 132-135 [5]. Следовательно, формула «вся компенсация - только отдельным гражданским иском» неточна. Необходимо различать имущественные потери, моральный вред и самостоятельное требование к частному обработчику.

Общее правило статьи 72 ГПК возлагает на стороны доказывание обстоятельств их требований и возражений. Части 4-5 статьи 73 позволяют просить суд об истребовании: заявитель указывает доказательство, его значение, препятствия самостоятельному получению и место нахождения [6]. Для

цифрового спора это означает необходимость описать искомую запись через систему, событие и период. Предлагать суду «проверить всю деятельность оператора» вместо определенного доказательственного запроса - значит смешивать рассмотрение иска с общей надзорной проверкой.

В административном процессе распределение иное, но также не безусловное. Подпункт 1) части 2 статьи 129 АПК возлагает доказывание законности обременяющего акта на ответчика; подпункты 2)-3) разграничивают основания отказа и факты, необходимые для благоприятного акта или действия. По части 1 истец участвует в собирании доказательств и независимо от вида иска подтверждает время получения сведений о нарушении и размер заявленных убытков [5]. Поэтому активная роль административного суда не заменяет доказательств индивидуальных последствий.

Практическое значение разграничения показывает опубликованное Верой Александровой описание спора с Home Credit Bank. По ее сведениям, банк ошибочно передал следствию выписку постороннего человека, затем направил исправление, однако гражданина вызвали на допрос. Автор сообщает о взыскании Медеуским районным судом Алматы 5 июля 2024 года 300 тысяч тенге морального вреда и о представлении банком переписки, подтверждавшей ошибку [7]. Полного решения в публикации нет: изложенное используется как атрибутированное описание дела, а не как непосредственно исследованная судебная мотивировка.

Этот эпизод позволяет выделить три разных предмета проверки: содержание первоначальной передачи, факт и момент исправления, последующее использование ошибочной записи получателем. Исправленный файл у источника еще не показывает, какие сведения находились у адресата в момент совершения им действия. Для доказывания поэтому существенно сохранять последовательность версий и уведомлений, а не только окончательное состояние базы. Такой вывод относится к методике исследования доказательств; он не устанавливает виновность неназванных участников или содержание не опубликованных судебных выводов.

Подпункт 1) пункта 1 статьи 24 Закона о персональных данных позволяет выяснить факт, цели, источники и способы обработки; подпункт 5) пункта 2 статьи 25 возлагает на собственника или оператора представление доказательства получения согласия в установленных законом случаях [3]. Отсюда не следует универсальная презумпция неправомерности любой обработки без предъявленного согласия: могут применяться иные законные основания. Но ссылка ответчика именно на согласие требует установить содержание разрешенной операции, относимость подтверждения к субъекту и действовавшую редакцию условий.

По предлагаемой доказательственной модели фиксации одного нажатия кнопки недостаточно, когда оспаривается объем предоставленного разрешения. Истребуемый материал должен позволять сопоставить действие пользователя с тем текстом и назначением обработки, к которым оно относилось. Это не требование заранее раскрыть всю внутреннюю документацию оператора. Определению подлежит необходимый комплект сведений для проверки конкретного возражения: содержание, момент выражения воли и связь с последующей операцией.

Различие между исходными сведениями и информацией об операциях раскрыто в решении Суда ЕС от 22 июня 2023 года по делу C-579/21 Pankki S. При толковании статьи 15 GDPR Суд признал значение дат и целей обращений к данным; пункты 60-66 связывают такой доступ с проверкой законности обработки. При этом пункт 83 не устанавливает общего права знать имена сотрудников, действовавших по указаниям контролера: необходимо учитывать существенность этой информации для осуществления прав и права работников [8; 9]. Значит, предоставить объяснение операций и открыть все журналы всем заявителям - не одно и то же.

А. Хойзельманн и Б. Кастерс исследуют трудности исправления производных сведений: прогноз, субъективная оценка и запись об установленном факте не обладают одинаковой проверяемостью [10]. Для выбора требования это принципиально. Неверно отнесенная к человеку задолженность может проверяться первичными документами; неблагоприятный прогноз сам по себе не доказывает ложности исходной информации. В последнем случае

предметом исследования должны стать использованные данные, примененные факторы и соблюдение гарантий принятия решения, а не требование заменить любой неудобный результат желаемым.

Казахстанское регулирование уже содержит право на объяснение. Подпункты 1)-3) пункта 4 статьи 43 Цифрового кодекса предусматривают в установленных законодательством случаях и порядке информирование, разъяснение ключевых факторов и критериев полностью автоматизированного решения, а также пересмотр с участием специалиста. Объяснение отделено от раскрытия алгоритмов, исходных кодов и иной охраняемой информации [11]. Поэтому исследовательская задача - не повторно провозгласить право, а определить достаточность объяснения для проверки конкретного результата.

В деле C-203/22 Dun & Bradstreet Austria, решение от 27 февраля 2025 года, спор возник после отказа в договоре мобильной связи вследствие оценки кредитоспособности. Пункты 58-62 требуют понятного объяснения реально примененных процедур и принципов: одна математическая формула его не заменяет. По пунктам 73-75 ссылка на коммерческую тайну предполагает передачу спорной информации компетентному органу или суду для оценки, а не автоматический отказ в защите [12]. Это толкование GDPR не создает прямого требования к казахстанскому оператору, но позволяет сопоставить объяснение заявителю и судебное исследование конфиденциального материала.

Предлагается оценивать объяснение по способности связать использованные сведения с оспариваемым результатом. Общее перечисление факторов работы модели не доказывает, что именно они и в такой версии применялись к заявителю. Одновременно выдача исходного кода не гарантирует понятности решения. Надлежащая конкретизация требует указать относящиеся к спору данные, версию примененной процедуры, существенные факторы и причину отказа, сохраняя отдельный процессуальный порядок для исследования защищенных технических сведений.

Части 1-2 статьи 69 ГПК позволяют обеспечить доказательства при риске последующей невозможности или затруднительности их представления; часть 3 отсылает досудебное обеспечение к

законодательству о нотариате [6]. Статьи 98-99 Закона «О нотариате» предусматривают соответствующие действия нотариуса, включая осмотр электронных доказательств, но исключают обеспечение по делу, уже находящемуся в производстве суда или другого компетентного органа [13]. Следовательно, обращаться к сохранению записей желательно до их утраты, выбирая надлежащую процедуру по стадии спора.

Нотариальная фиксация доступного содержания не равнозначна принудительному обследованию чужой системы и не подтверждает автоматически истинность опубликованного сообщения. Ее назначение следует отделять от экспертного исследования и судебной оценки. Получение протокола осмотра также не является универсальной предпосылкой допустимости любых электронных доказательств. Для конкретного материала необходимо объяснить, что именно зафиксировано: отображение страницы, содержание сообщения, состояние файла либо последовательность действий при обращении к ресурсу.

Части 1-2 статьи 99 ГПК допускают соответствующие электронные и цифровые материалы и требуют указать условия их получения; положение о подписанном электронном документе в части 6 статьи 100 не превращает цифровую подпись в обязательный реквизит каждого снимка экрана или журнала операций [6]. Отсутствие подписи и недостоверность содержания - разные вопросы. В то же время снимок экрана без сведений о происхождении не должен получать доказательственное преимущество только вследствие своей наглядности.

Для распределенного массива предлагается фиксировать источник, время, способ извлечения, отбор записей и сведения о последующих преобразованиях. Рекомендации NIST IR 8387 связывают сохранение цифровых материалов с документированием происхождения и контролем целостности; раздел 3.2 отдельно рассматривает хеширование и риски изменения материала до вычисления хеша [14, с. 7, 11]. Поэтому контрольная сумма помогает проверять неизменность копии, но не устанавливает истинность первоначально внесенных сведений. Существенно также сохранять пояснение структуры загрузки: одинаковое

обозначение поля в разных системах не гарантирует тождества его содержания. Эти сведения предназначены для воспроизводимой проверки, а не для замены правовой оценки технической экспертизой.

Истребование и обеспечение не следует смешивать с обеспечением иска. Статьи 155-156 ГПК направлены на предупреждение затруднений исполнения будущего решения; часть 3 статьи 156 требует соразмерности и учета публичных интересов и прав третьих лиц [6]. Поэтому сохранение журнала операций и временное ограничение обработки имеют разные цели. Приостановление всей платформы нуждается в самостоятельном обосновании: одного довода о необходимости получить доказательства для него недостаточно.

Сравнительный ориентир содержит правило 37(е) Федеральных правил гражданского процесса США. Оно относится к утрате электронных сведений, подлежавших сохранению в связи с ожидаемым или ведущимся процессом, если разумные меры не приняты и восстановление либо замена невозможны. Подпункт (1) связывает корректирующие меры с возникшими препятствиями для другой стороны, а подпункт (2) допускает наиболее тяжелые последствия при намерении лишить ее возможности использовать сведения [15]. Этот режим не действует в Казахстане; его значение - в разграничении доказанной утраты, причин ее возникновения и соразмерного процессуального ответа.

Для отечественного регулирования предлагается отдельно исследовать ситуацию уничтоженного материала и удержания существующего доказательства. Само отсутствие записи не объясняет, существовала ли она, кто обязан был ее сохранять и когда возникла возможность предвидеть спор. Автоматическая обязанность хранить все массивы бессрочно противоречила бы цели ограничения обработки. Более определенным решением является адресное сохранение относящихся к спору записей на установленный срок с запретом их использования вне доказательственной цели.

Часть 9 статьи 73 ГПК уже предусматривает последствия удержания стороной истребованного судом доказательства:

сведения предполагаются направленными против ее интересов и признанными ею [6]. Поэтому предложение впервые переложить неблагоприятные последствия сокрытия журналов на их держателя было бы неточным. Практическая проблема - установить, какое доказательство истребовано, какие обстоятельства оно подтверждает и выполнены ли предусмотренные нормой условия. Нельзя объявлять признанными все элементы иска исключительно потому, что ответчик не раскрыл неопределенный массив.

З.Х. Баймолдина разграничивает освобождение от доказывания и случаи принятия фактов без исследования доказательств, в том числе вследствие процессуального поведения стороны [16, с. 64-72]. Это различие позволяет отделить преюдицию от последствий удержания и от разрешения неустраненной неопределенности по правилам бремени доказывания. Для цифровых споров оно особенно важно: недоказанность согласия, признание содержания удержанного журнала и установленная вступившим в силу судебным актом виновность не являются одним основанием судебного вывода.

Часть 2 статьи 76 ГПК связывает обязательность обстоятельств прежнего гражданского дела с участием тех же лиц. Часть 5 предусматривает освобождение от повторного доказывания виновности, установленной вступившим в силу постановлением суда по административному правонарушению, при рассмотрении гражданских последствий того же нарушения тем же лицом [6]. Следовательно, сообщение министерства, материалы проверки и судебное постановление необходимо оценивать раздельно. Наличие административного реагирования еще не означает наличия судебного акта с предусмотренным этой нормой эффектом.

В официальном сообщении о ТОО «МФО Робокэш.кз» указаны обнаружение утечки 5 марта 2024 года, результаты проверки, административное взыскание по части 4 статьи 79 КоАП и уведомление граждан [17]. Из текста не следует, что вопрос разрешен именно постановлением суда. В гражданском споре следует истребовать относящиеся к требованию материалы и установить форму итогового акта. Нельзя придавать самой

публикации эффект преюдиции либо считать ее доказательством состава утекших сведений каждого обратившегося гражданина.

Вместе с тем ограниченность сообщения не делает материалы проверки бесполезными. Они могут подтверждать общие для инцидента обстоятельства, тогда как связь с заявителем и содержание индивидуального требования требуют дополнительной проверки. При взыскании убытков отдельно устанавливаются потери и причинная связь; при требовании исправить запись - ее относимость к истцу, ошибка и обязанность ответчика устранить ее. Такая дифференциация предотвращает обе крайности: повторное доказывание каждого технического факта с нуля и автоматическое удовлетворение всех требований после одного штрафа.

Обладатель коммерчески ценного массива заинтересован получить доказательства неправомерного извлечения, не раскрывая оставшуюся часть ресурса. В статье 43(1) Соглашения ТРИПС истребование конкретизированных доказательств у противоположной стороны сопряжено с защитой конфиденциальности; статья 42 закрепляет гарантии справедливой процедуры, а статья 50(1)(b) предусматривает сохранение относящихся к предполагаемому нарушению доказательств [18]. Эти правила относятся к охраняемым Соглашением правам интеллектуальной собственности. Их нельзя без проверки режима массива объявлять специальной процедурой любого спора о данных.

В казахстанском процессе часть 2 статьи 19 ГПК позволяет закрытое рассмотрение для защиты предусмотренных законом тайн; части 4 и 6 сохраняют участие сторон и применение процессуальных правил. Право знакомиться с материалами дела предусмотрено частью 1 статьи 46 [6]. Следовательно, исключение публики не означает возможности положить в основу решения сведения, от исследования которых полностью устранена противоположная сторона. Закрытое заседание решает вопрос гласности, но само по себе не определяет объем раскрытия между участниками.

В деле C-268/21 *Norra Stockholm Bygg*, решение от 2 марта 2023 года, Суд ЕС рассматривал представление в гражданском споре реестра работников, первоначально создававшегося для налогового

контроля. Пункты 53-59 связывают доступ к необходимым доказательствам с оценкой интересов субъектов данных и минимизацией, включая возможность ограничить раскрываемые сведения [19]. Правовая ценность дела заключается в отсутствии безусловного приоритета любой из сторон: ни наличие персональных данных не блокирует доказательство, ни ссылка на судопроизводство не оправдывает раскрытие всего реестра.

Для коммерческой тайны статья 9(2) Директивы ЕС 2016/943 предусматривает ограничение доступа и публикацию неконфиденциальных версий судебных актов. При этом круг допущенных лиц должен включать как минимум одно физическое лицо от каждой стороны и их представителей; пункт 3 требует учитывать справедливое разбирательство и интересы участников [20]. Директива регулирует определенные споры о коммерческой тайне, а не все дела о персональных данных. Ее нельзя использовать для обоснования универсального режима «только для суда» или «только для адвокатов».

Предлагается устанавливать защитный режим применительно к конкретным полям и операциям: исключать нерелевантные записи, отделять идентификаторы третьих лиц, проводить исследование защищенного фрагмента без выдачи всей базы. При этом сокращенная копия должна сохранять контекст, позволяющий оспорить вывод другой стороны. Полное удаление идентификаторов непригодно, когда спор касается именно ошибочного сопоставления записей; тогда требуется контролируемое исследование идентификаторов, а не объявление их недоступными по определению.

Статья 232 ГПК требует указать действия, которые обязан совершить ответчик, и срок их совершения. Часть 2 статьи 233 предусматривает определение действий и их объема для каждого из нескольких ответчиков [6]. В споре о данных это делает недостаточным решение «устранить нарушение законодательства». Необходимо индивидуализировать запись или массив, недопустимую операцию и требуемый результат. Сам по себе запрет обработки не объясняет, нужно ли прекратить передачу, исправить источник, ограничить доступ или удалить незаконно полученную копию.

Для требования о восстановлении достоверности предлагается последовательно устанавливать первоначальную запись, получателей исправления и тот результат обработки, который подлежит пересмотру. Обязанности каждого адресата должны иметь самостоятельное основание; распространение последствий ошибки не создает автоматически обязанности любого участника отвечать за весь процесс. При определении исполнения полезно отделить исправление факта от повторной аналитической оценки на исправленных исходных данных. Суду необходимо определить требуемый правовой результат, не подменяя специалиста самостоятельным расчетом нового рейтинга.

Особую проблему образует конфликт удаления и сохранения доказательства. В праве ЕС подпункт «е» пункта 3 статьи 17 GDPR исключает удаление в той мере, в какой обработка необходима для предъявления, осуществления или защиты правовых требований [8]. Это исключение не переносится автоматически в Казахстан и не оправдывает бессрочную хозяйственную эксплуатацию спорного массива. Для отечественной модели предлагается связать необходимое сохранение с процессуальным решением, определяющим состав, цель и режим доступа, а не с односторонним заявлением оператора о возможном будущем споре.

В развитие статей 69-71 ГПК предлагается обсудить следующую норму: «При обеспечении цифровых доказательств суд определяет относящийся к делу состав сохраняемых сведений, период их формирования, способ фиксации, место и срок хранения, круг допущенных лиц и порядок прекращения хранения. Сведения сохраняются в объеме, необходимом для доказывания, с учетом права сторон на их исследование и защиты охраняемой законом тайны. Их использование для иных целей не допускается». Это авторская редакция для сравнительной таблицы поправок, а не описание уже введенного специального режима.

Процессуальное решение должно также разграничивать сохранение доказательственной копии и прекращение оспариваемой обработки в действующей системе. Иначе обязанность представить доказательства способна стать объяснением продолжения нарушения. Срок хранения необходимо

соотносить с потребностями разбирательства, возможного пересмотра и установленными правилами судебного архивирования. Ни немедленное уничтожение всех копий, ни их бесконтрольное бессрочное сохранение не обеспечивают надлежащего согласования этих интересов.

Практическим результатом предлагается считать адресную модель доказывания: для требования о доступе проверяются обращение, принадлежность данных и содержание ответа; для оспариваемого согласия - основание и предел разрешения; для исправления - первичный факт и путь распространения ошибки; для компенсации - предусмотренные законом последствия и их связь с нарушением. Модель дополняется перечнем источников и процедурой их получения, а не заменяет ее. Формулировать новые презумпции необходимо лишь после установления недостаточности действующих статей 73 и 76 ГПК, а не вместо их применения.

Судебная защита в сфере больших данных зависит от согласования материального требования и возможности доказать относящиеся к нему обстоятельства. Массовость обработки не превращает всех заявителей в лиц с одинаковым предметом доказывания. Сведения о публичном взыскании, материалы проверки и вступивший в силу судебный акт имеют различное значение, конфиденциальность не устраняет состязательность, а цифровая форма записи не придает ей заранее установленной достоверности.

Предлагаемая модель соединяет способ защиты, юридически значимый факт, держателя доказательства, процедуру получения и исполнимый результат. Ее развитие связано с целевым сохранением записей, контролируемым раскрытием и определенностью восстановительного предписания. Тем самым совершенствование защиты направляется не на повторное провозглашение права на доступ или истребование, а на устранение конкретного разрыва между существующим правом, доступным доказательством и фактически исполнимым судебным решением.

Финансирование. Исследование подготовлено в рамках проекта ИРН АР23489796 «Проблемы регламентации правового режима больших данных (Big Data): отечественный и

международный опыт», финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан.

Список использованных источников

1 Сулейменов, М. К. Понятие и способы защиты гражданских прав [Электронный ресурс] / М. К. Сулейменов // Параграф. - 2014. - 16 июня. - Электронная публикация авторского текста. URL: https://prg.kz/document/?doc_id=33100058 (дата обращения: 02.06.2026).

2 Гражданский кодекс Республики Казахстан (Общая часть): Кодекс Республики Казахстан от 27 декабря 1994 г. № 268-ХІІІ // Ведомости Верховного Совета Республики Казахстан. - 1994. - № 23–24 (приложение). - Официальная карточка акта: ИПС «Әділет». - Используемое положение: ст. 9. URL: https://old.adilet.zan.kz/rus/docs/K940001000_/info (дата обращения: 03.06.2026).

3 О персональных данных и их защите: Закон Республики Казахстан от 21 мая 2013 г. № 94-V // Ведомости Парламента Республики Казахстан. - 2013. - № 7. - Ст. 35. - Официальная карточка акта: ИПС «Әділет». - Используемые положения: ст. 24–25. - Связанный акт о внесении изменений указан в записи 4. URL: <https://old.adilet.zan.kz/rus/docs/Z1300000094/info> (дата обращения: 02.07.2026).

4 О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам цифровизации, защиты персональных данных, дорожного движения и регулирования передовых технологий на транспорте: Закон Республики Казахстан от 24 июня 2026 г. № 326-VІІІ ЗРК // Казахстанская правда. - 2026. - 25 июня. - № 117 (30746). - Электронное воспроизведение: Учет.kz. - URL: <https://zakon.uchet.kz/rus/docs/Z2600000326> (дата обращения: 03.07.2026).

5 Административный процедурно-процессуальный кодекс Республики Казахстан: Кодекс Республики Казахстан от 29 июня 2020 г. №350-VІ // Ведомости Парламента Республики Казахстан. - 2020. - № 13. - Ст. 66. - Официальная карточка акта: ИПС «Әділет». - URL: <https://old.adilet.zan.kz/rus/docs/K2000000350/info> (дата обращения: 04.06.2026).

6 Гражданский процессуальный кодекс Республики Казахстан: Кодекс Республики Казахстан от 31 октября 2015 г. № 377-V ЗРК // Ведомости Парламента Республики Казахстан. - 2015. - № 20-VІ. - Ст. 114. - Официальная карточка акта: ИПС «Әділет». - URL: <https://old.adilet.zan.kz/rus/docs/K1500000377/info> (дата обращения: 05.06.2026).

7 Александрова, В. Как ошибка банка и халатность полиции лишили жителя Уральска покоя на два года [Электронный ресурс] / В. Александрова // Фонд-бюро расследования коррупции. - 2025. - 16 октября. URL: <https://fbrk.kz/articles/kak-oshibka-banka-i-khalatnost-policii-lishili-zhitelya-uralska-pokoya-na-dva-goda> (дата обращения: 08.06.2026).

8 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. - 4 May. - P. 1–88. - URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (дата обращения: 09.06.2026).

9 Court of Justice of the European Union. Pankki S [Электронный ресурс]: judgment of the Court (First Chamber) of 22 June 2023, Case C-579/21. - ECLI:EU:C:2023:501. - Электронное воспроизведение судебного акта: IPcuria. - Используемый фрагмент: п. 60–66, 83. URL: <https://ipcuria.eu/case?reference=C-579%2F21> (дата обращения: 10.06.2026).

10 Häuselmann, A. The Right to Rectification and Inferred Personal Data [Электронный ресурс] / A. Häuselmann, B. Custers // European Journal of Law and Technology. - 2024. - Vol. 15, no. 3. - 30 December. - 24 p. - URL: <https://ejlt.org/index.php/ejlt/article/view/1004> (дата обращения: 11.06.2026).

11 Цифровой кодекс Республики Казахстан: Кодекс Республики Казахстан от 9 января 2026 г. № 255-VIII ЗРК // Казахстанская правда. - 2026. - 10 января. - № 5–6 (30634–30635). - Официальная карточка акта: ИПС «Әділет». - URL: <https://old.adilet.zan.kz/rus/docs/K2600000255/info> (дата обращения: 01.07.2026).

12 Court of Justice of the European Union. CK v Magistrat der Stadt Wien (Dun & Bradstreet Austria) [Электронный ресурс]: judgment of the Court (First Chamber) of 27 February 2025, Case C-203/22 // EUR-Lex. - 2025. - ECLI:EU:C:2025:117. - Используемый фрагмент: п. 58–62, 73–75. - URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0203> (дата обращения: 15.06.2026).

13 О нотариате: Закон Республики Казахстан от 14 июля 1997 г. № 155-І // Ведомости Парламента Республики Казахстан. - 1997. - № 13–14. - Ст. 206. - Официальная карточка акта: ИПС «Әділет». - URL: https://old.adilet.zan.kz/rus/docs/Z970000155_info (дата обращения: 16.06.2026).

14 Guttman, B. Digital Evidence Preservation: Considerations for Evidence Handlers [Электронный ресурс] / B. Guttman, D. R. White, T. Walraven. - Gaithersburg, MD: National Institute of Standards and Technology, 2022. - September. - IV, 15 p. - (NIST Interagency Report, NIST IR 8387). - DOI: 10.6028/NIST.IR.8387. - Используемый фрагмент: разд. 3.2, с. 7, 11. - URL: <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8387.pdf> (дата обращения: 17.06.2026).

15 Federal Rules of Civil Procedure. Rule 37(e): Failure to Preserve Electronically Stored Information [Электронный ресурс] // Legal Information Institute / Cornell Law School. - Редакция правила 37 с изменениями от 29 апреля 2015 г., вступившими в силу 1 декабря 2015 г. - Электронный текст с примечаниями Консультативного комитета. - URL: https://www.law.cornell.edu/rules/frcp/rule_37 (дата обращения: 18.06.2026).

16 Баймолдина, З. Х. О фактах, принимаемых судом без доказывания / З. Х. Баймолдина // Ежегодник публичного права 2022. Доказательства и доказывание в административном праве / гл. ред. Й. Пуделька. - Берлин: Инфотропик Медиа, 2022. - С. 64–72. - URL: https://www.ostinstitut.de/files/ru/materialy/Ежегодник_публичного_права_2022_Доказательства_и_доказывание_в_административном_праве.pdf (дата обращения: 19.06.2026).

17 Минцифры объявило результаты проверки в отношении ТОО «МФО Робокэш.кз» [Электронный ресурс] / Пресс-служба Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан // Gov.kz. - Официальное сообщение. - Номер публикации: 740137. - URL: <https://www.gov.kz/memleket/entities/maidd/press/news/details/740137?lang=ru> (дата обращения: 22.06.2026).

18 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) [Электронный ресурс]: 15 April 1994: Annex 1C to the Marrakesh Agreement Establishing the World Trade Organization // WTO legal texts / World Trade Organization. - 1994. - Part III: Enforcement of Intellectual Property Rights. - Используемые положения: ст. 42, 43, 50. - URL: https://www.wto.org/english/docs_e/legal_e/27-trips_05_e.htm (дата обращения: 23.06.2026).

19 Court of Justice of the European Union. Norra Stockholm Bygg AB v Per Nycander AB [Электронный ресурс]: judgment of the Court (Third Chamber) of 2 March 2023, Case C-268/21. - ECLI:EU:C:2023:145. - Электронное воспроизведение судебного акта: IPcuria. - Используемый фрагмент: п. 53–59. URL: <https://ipcuria.eu/case?reference=C-268%2F21> (дата обращения: 24.06.2026).

20 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure // Official Journal of the European Union. - 2016. - L 157. - 15 June. - P. 1–18. - Используемое положение: ст. 9. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0943> (дата обращения: 26.06.2026).

Алимкулов Е.Т.

Казахский национальный университет имени аль-Фараби,

Республика Казахстан, г. Алматы

E-mail: alerbol@mail.ru

ДЕПОНИРОВАНИЕ ПОКАЗАНИЙ – КАК ОДИН ИЗ ОСНОВНЫХ ПОЛНОМОЧИЙ СЛЕДСТВЕННОГО СУДЬИ

В новом Уголовно-процессуальном кодексе принятом 4 июля 2014 года предусмотрена должность следственного судьи, который будет осуществлять функции судебного контроля.

В статье 7 п. 40 проекта УПК процессуально-правовой статус следственного судьи определен как - судья районного или приравненного к нему суда, осуществляющий предусмотренные

настоящим кодексом полномочия в ходе досудебного производства [1].

Следственный судья будет рассматривать ходатайства о санкционировании десяти видов процессуальных действий. Из них пять видов санкционирования связаны с мерами пресечения (содержание под стражей, домашний и экстрадиционный аресты, продление сроков указанных мер пресечения и применение залога) [2]. Следственный судья также будет санкционировать наложение ареста на имущество, эксгумацию трупа и объявление международного розыска подозреваемого.

В новом УПК предусмотрена принципиально новая функция суда - депонирование показаний. В процессуальном праве С.Пашин предлагал предусмотреть процедуру депонирования у судьи или следственного судьи: «Представляется необходимым... наделить стороны правом беспрепятственно приобщать к материалам уголовного дела полученные ими документы, включая объяснения очевидцев и заключения специалистов; установить процедуру депонирования доказательств у мирового судьи либо у судебного следователя» [3]. Л.А. Воскобитова, в качестве способа узаконить факты, полученные адвокатом, отмечает судебное депонирование. По словам автора, в ходе предварительного следствия депонирование показаний целесообразно в тех случаях, когда адвокат, принимая во внимание реальные возможности неправомерных действий со стороны следователя в отношении свидетеля, либо угрозы со стороны других лиц, либо возраст свидетеля, не уверен что может вызвать свидетеля в суд и допросить его. Судебное депонирование показаний дает возможность адвокату получить процессуальное доказательство, и чтобы его узаконить, не требуется производить дополнительные следственные действия [4].

Внедрение института судебного депонирования показаний по инициативе адвоката, будет способствовать развитию элементов состязательности на досудебной стадии производства, укрепит самостоятельность адвоката в сфере получения доказательств, и уменьшит зависимость адвоката от следователя или прокурора. Депонирование показаний является самостоятельным способом процессуализации фактов, полученных по инициативе стороны

защиты. Суд не является стороной обвинения и в случае судебного депонирования показаний может обеспечить равные возможности для органа уголовного преследования и для адвоката.

В отличие от допроса в кабинете следователя, производимого без контроля, в случае допроса и депонирования показаний, производимых в зале судебных заседаний по инициативе адвоката, суд обеспечит полное представление данных со стороны свидетеля и полное протоколирование сведений, а также будет обеспечено право добровольной дачи показаний.

В случае судебного депонирования показаний, хотя допрос проводится следователем, однако право на справедливое судебное следствие предусматривает стандарт, что первым вопрос задает сторона, которая инициировала допрос. В случае судебного депонирования показаний по инициативе адвоката, существенно ограничивается усмотрение следователя на снятие вопроса адвоката или на оставление их без ответа. Если в случае депонирования показаний между следователем и адвокатом возникает спор относительно относимости или допустимости вопроса, то правомочность заданного адвокатом вопроса решает суд.

Одновременно отдельные авторы считают, что судебное депонирование доказательств не отменяет неравные возможности следователя и адвоката в сфере получения доказательств, поскольку прежде всего, по новому Уголовно-процессуальному кодексу Казахстана подобное право предусматривается для обеих сторон, во-вторых депонирование относится к ограниченному кругу свидетелей и потерпевших: «В новом УПК Казахстана данное неравенство надлежащим образом не сбалансировано, так как прямого запрета использовать такие показания в обвинительном приговоре суда не предусмотрено. Депонирование показаний при помощи допроса следственным судьей не меняет ситуации, так как, во-первых, касается обеих сторон, а во-вторых, касается лишь ограниченных категорий свидетелей и потерпевших» [5]. На данном этапе развития уголовно-процессуального права судебное депонирование показаний имеет ограниченное применение. Оно может применяться только в том случае, когда есть основания предполагать, что свидетель или потерпевший не могут

впоследствии явиться в суд, или не смогут воспользоваться своим правом на отказ от дачи показаний. На основании подведения итогов относительно практики судебного депонирования в дальнейшем возможно будет затронуть другие проявления судебного депонирования показаний. Например, в теории отмечается, что будет возможным по инициативе адвоката привлечь следственного судью к осмотру места происшествия, предметов и документов. Для обеспечения полномочий защитника авторитетом и силой судебной власти, может законом предусматриваться процедура получения адвокатом судебного приказа для предоставления предприятиями, организациями сведений: «Вместе с тем, сама идея депонирования доказательств посредством вовлечения в процесс следственного судьи, в последующем свободного от рассмотрения дела по существу, заслуживает дальнейшей поддержки и развития. Вполне возможно, вовлечь следственного судью в процесс осмотра мест, предметов и документов, по мнению защиты, относимых и допустимых в качестве доказательств. Здесь также необходимо предусмотреть обязательное удовлетворение соответствующего ходатайства адвоката, разумеется, при его надлежащей мотивированности и обоснованности. В целях обеспечения полномочий защитника силой и авторитетом судебной власти, допустимо закрепить в законе процедуру получения защитником судебного приказа о предоставлении предприятиями, учреждениями, организациями и гражданами сведений, имеющих значение для всестороннего и полного исследования обстоятельств дела. Такой механизм стал бы полноценной гарантией права стороны защиты на собирание доказательств» [6].

Список использованных источников

1 Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V (с изменениями и дополнениями по состоянию на 07.11.2014 г.) // http://online.zakon.kz/Document/?doc_id=31575852

2 Маджитов А. Депонирование доказательств защиты на стадии расследования // <http://skachate.ru/pravo/107376/index.html> (12.08.2014).

3 Пашин С. Болевые точки уголовного процесса (общий анализ) // <http://www.hrights.ru/text/b22/Chapter3%202.htm> (13.08.2014).

4 Воскобитова Л. А. Состязательность: две концепции участия адвоката в доказывании / Теория уголовного процесса: состязательность: монография. - М.: Юрлитинформ. - 2013. - 291 с.

5 Касько В. Реализация принципа состязательности в уголовном процессуальном законодательстве Украины и проекте УПК Казахстана // Материалы Центра исследования правовой политики. «Реформирование уголовного процесса республики Казахстан». - Алматы, 2014. - С. 75-79.

6 Канафин Д.К. Совершенствование правового статуса адвоката в свете разработки нового Уголовно-процессуального кодекса Республики Казахстан // Материалы Центра исследования правовой политики. «Реформирование уголовного процесса республики Казахстан». - Алматы, 2014. - С. 28-32.

Арын А.А.

*Әл-Фараби атындағы Қазақ ұлттық университеті
Қазақстан Республикасы, Алматы қ.
E-mail: aizhan_moon777@mail.ru*

КРИМИНАЛИСТІК ОДОРОЛОГИЯ ЖӘНЕ ОНЫҢ ҚЫЛМЫСТАРДЫ АШУ МЕН ТЕРГЕУДЕГІ МАҢЫЗЫ

Қазақстан Республикасы тәуелсіздік жылдары ішінде криминалистиканы жете дамытып келеді. Яғни, бүгінгі біздің зерттеп отырған тақырыбымыз криминалистік одорология және оның қылмыстарды ашу мен тергеудегі маңызы болып табылады.

Криминалистік одорология- иістер туралы ілімнің жүйесін және иіс шығаратын заттарды ғылыми тұрғыда зерттей отырып, қылмыстық сот ісін жүргізуде оларды- табу, талдау, алу бойымен дәлелденген тәсілдерді, техникалық құралдардың көмегімен оларды пайдалану болып табылады. Криминалистік одорология криминалистиканың жаңа бөлімі болып табыла отырып, ол соңғы он жылдықта пайда болған. Криминалистік одорология сөзі екі сөзден құрылған: (латынша odor - иіс және грек logos – оқу) дегенді білдіреді [1].

Криминалистік одорологияны иістерді алу, анализ жасау мен тіркеуге байланысты келесідей түрлерге бөлеміз: кинологиялық және құрал-жабдықтық (аспапты) ольфактроникалық (латынша-olfactus- иіс) болып бөлінеді. Кинологиялық одорологияда иісі бар

заттарды іздейтін арнайы жануарлар танылады. Құрал-жабдықтық (аспапты) ольфактроникалық одорологияда арнайы физика-химиялық арнайы құрал-жабдықтар, яғни адамнан бөлініп шыққан арнайы иістерді зерттеу болып табылады. Криминалистік одорология көп жылдар бойы ғалымдардың зерттеу объектісі болып табылды. Ежелден мәлім, жан-жануарлар арнайы құрал-жабдықтардан, арнайы иістерді зерттейтін құрал-саймандарға қарағанда иіс сезу қабілеттері өте мықты, өте сезімтал болып табылады. Осы жан-жануарларға қарап адамзат қазіргі таңда арнайы иісті зерттейтін құрал-жабдықтар (аспаптар) жасап шығарады. Яғни, иттің иіскеу қабілеті қандай мықты болса, сондай мінездемелік жақтарын алып, криминалистік аспаптар жасап шығарылуда. Мысал ретінде айтатын болсақ, жан-жануарларды қазіргі таңда, бағалы заттардың жабылған жерлерін іздеуде, газ құбырлары бұзылған кезде-бұзылған жерді табу кезінде атқаратын рөлдері өте маңызды және табу деңгейі 94-98%-ды құрайды. Қазіргі таңда, Қазақстан Республикасында криминалистік одорологияның басты мәселесі, ол – арнайы одорологиялық аспаптардың, техникалардың жетіспеушілігінде болып табылады. Яғни, құқық қорғау органдарының қызметкерлерінің, криминалист-мамандардың арнайы сараптама мен тексеріс жүргізген кезде қызметінің біршама ауырлығы. Мысалы, Америка Құрама Штаттарының әділет министрлігінің жанында құрылған, федералдық тергеу бюросының криминалист-мамандары, сарапшылары қазіргі таңда әлемнің ең мықты криминалист-мамандар қатарында, тіпті арнайы құрал жабдықтарын зерттеп, жасап шығаратын арнайы зертханалары бар. Отандық криминалистік одорологияның маңызды мәселелерінің бірі осы болып табылуда. Қазіргі кезде, техника саласында қызмет атқаратын маман-профессорлар құрамы аз. Сондықтан да, Отандық криминалистика саласында жұмыс атқаратын құқық қорғау органдарының қызметкерлерінің қызметі ауыртпашылықтарға ұшырауда. Криминалистік одорологияның тағы да бір маңызды мәселерінің бірі – ол, әлемдік деңгейдегі, халықаралық стандарттарға сәйкес жұмыс істейтін аспаптармен жұмыс атқаратын кадрлар санының жетіспеушілігі. Яғни, барлығымызға мәлім –

мұндай заман талабына сай техникамен жұмыс атқаратын кадрларды дайындау үшін арнайы оқу курстары керек болып табылады, осы аталып отырған техникалар шетел мемлекеттерінде жасап шығарылғандықтан шетел оқытушыларының дәріс беріп үйретуі қажет. Бұл жердегі шешім – ол, шетел мемлекеттерінен ғалым – профессорларды шақырып, біздің криминалист – мамандарға арнайы білім беруі арқылы көрініс табуы керек деген ойдамыз. Ұлыбритания королдігінде маман-криминалисттерді, құқық қорғау қызметкерлерін міндетті түрде заңда көзделген мерзімдерде арнайы криминалистік ғылыми-зерттеуші институттарда білім беріп, қазіргі заманда шығып жатқан ғылыми-техникалық құралдармен жұмыс істеуді үйретіп, тәжірибесін молықтырып отырады. Ең алғашында қылмыспен күрес жүргізу үшін иттерді қолдануды 1896 жылы австриялық криминалист Ганс Гросс ұсынған болатын, яғни Гильдесгеймде полициялық қызметті жүзеге асыратын арнайы үйретілген 12 ит болды. Иттің иіскеу қабілеттілігі адаммен салыстарғанда 800000 есе өткір болып табылады [2].

Одан кейін, иттерді қылмыстылықпен күресуде пайдалану Германия мемлекетінде пайда болды. Қазіргі таңда, одорология ғылымын зерттеп жатқан мемлекеттердің бірі – Израиль. Израиль мемлекетінде қазіргі таңда оқиға болған жерден табылған иістерді идентификациялауды нақты, барынша дәл салыстырмалы жүзеге асыратын арнайы техникалық құралдар жасалуда. Яғни, біздің бұл жердегі ұсынысымыз арнайы иістерді идентификациялайтын құрал-жабдықтарды жасайтын лабораториялар ашып, қызметтерін Ішкі Істер Министрлігімен және Әділет Министрлігімен тығыз байланыстар орнату. Одорологиялық сараптама келесідей жүзеге асырылады: адамның қолтығына стерильдік фланел салынып 30 минут ішінде адамның қолтығында болады және осы фланельді итке иіскеуге береді. Оқиға болған жерден табылған иісті арнайы контейнерге салып қасына бірнеше өзге иісті контейнерлерді қояды. Итті осы контейнерлерді иіскетуге кинолог-маман итті жақындатады, сәйкесінші ұқсас иісті тапқаннан кейін ит сол контейнердің қасына жатады. Бұл процедура 3-4 рет қайталанады және өзге тағы басқа 2-3 иттер қатыстырылады. Бұл процедура

куәгерлердің қатысуымен ғана жүзеге асырылады. Тергеуші, куәгерлер және тағы да басқа адамдар арнайы көрінбейтін айнаның артында тұрып бұл процедураны бақылап тұрады. Бұл жағдайда ешқандай тұлға сараптаманың қорытындысына әсер ете алмайды. Ең алғашында одорологиялық сараптамаға Қазақстан Республикасының сот органдары теріс көзқараспен қараған, бірақ та сотта белгілі бір іс шешіле алынбай жатқан кезде, судья ұры-рецидивистті өзі одорологиялық сараптаманы жүргізу үшін сараптама орталығына жіберетін, нәтижесінде – ит қылмыскердің иісін тауып, қылмысқа қатыстылығы толығымен анықталатын. Қазақстан Республикасында одорологиялық сараптама жүргізудің тәсілі 5 жыл ішінде қолданылып келеді. Қазақстан Республикасының құқық қорғау органдарының одорология саласындағы қызметкерлері қазіргі таңда арнайы криминалистік одорологияға байланысты тәжірибелері жиналып, оқулықтар мен оқу құралдарын жазып шығаруда және Республиканың басқа аймақтарында және көршілес мемлекеттердің одоролог қызметкерлері осы оқулықтармен өз тәжірибелерін арттыруда. Қазіргі таңда, Қазақстан Республикасында криминалистік одорологияны зерттеп отырған орталық ол – Алматы қаласы болып табылады, 75% криминалистік одорологиялық зерттеулер Алматы қаласында жүзеге асырылады. Тек Алматы қаласының өзінде 100-ге жуық қылмыстық іс одорологиялық сараптаманың қорытындысы негізінде ашылады. Криминалистік одорология аса ауыр қылмыстар мен жалдаулы адам өлтіру қылмыстарын ашуда тигізетін әсері зор. Яғни, егер кінәлі емес адам ұсталған жағдайда, оны түгелмен жауапкершіліктен босатуда және нағыз қылмыскерді тауып әділ жазасын беруінде болып табылады. Криминалистік одорологиялық сараптама жай көзбен қарағанда оңай, әрі қарапайым болып көрінеді, бірақ та бұл процесс күрделі, әрі қиын болып табылады, өйткені арнайы иттерді жаттықтырып тұрмаса арнайы алған тәжірибелерін жоғалтып алады. Тек арнайы үйретілген иттер ғана қылмыскердің иісін ондаған басқа иістерден ажыратып таба алады. Басқа ешбір құрал мұндай процесті жүзеге асыра алмайды. Адамның қылмыс жасаған кезде иіс іздері қалады. Оны жасыру

мүмкін емес болып табылады. Иіс іздері міндетті түрде тегіс бетті және өзге де объектілерде міндетті түрде қалады [3].

Отандық криминалистік одорологияның маңызды проблемаларының бірі, ол – арнайы иттерді дайындайтын мекемелердің аз болуында болып табылады. Арнайы үйретілген иттер шетел мемлекеттерінен алып келінеді, мысалы, Германиядан – неміс овчаркалары, Англиядан – лабрадор және тағы да басқа. Әрбір адамның иісі индивидуалды, өзіне ғана тән болып келеді. Адам терлеу барысында, шыққан терісінен өзіне ғана тән иісі шығып әр түрлі материалдарға жағылады, сол материалдарда қалған иіс іздері криминалистік одорологияның зерттеу объектісі болып табылады [4].

Адамның иісі туылған кезінде пайда болады және өмір бойы сол иісі өзгеріссіз қалады. Криминалистік одорология қазіргі таңда Қазақстан Республикасында шекара қызметтерінде кеңінен қолданылады. Заңсыз өткен қылмыскерлерді, шекараны кесіп қашу әрекетін істеген қылмыскерлерді идентификациялауда қолданылады. Бұл жерде қызметтік иттердің атқаратын қызметі өте күрделі, әрі қиын болып табылады. Мысалы, арнайы көлік құралдарында заңсыз шекараны кесіп қашып бара жатқан қылмыскерді арнайы техникалық құралдар көрмеуі әбден мүмкін, бірақ арнайы үйретілген иттерден мұндай заңсыз әрекеттерді жасыру мүмкін емес. Көршілес мемлекетіміз, Ресей Федерациясында осы айла тәсіл кеңінен қолданылады. Яғни, криминалистік одорология сараптамасын жүргізу үшін арнайы үйретілген иттерге жүгінеді. Сараптаманы жүзеге асыру процесі біздің мемлекетімізбен өте ұқсас болып табылады. Отандық криминалистік одорологияның маңызды проблемаларының бірі болып – иіс іздерінің ұзақ мерзімде сақталмауы танылады. Яғни, оқиға болған жерден табылған иіс іздерін арнайы шүберекке енгізіп, ауасы тартылған арнайы контейнерге енгізіп, сақтау арқылы көрініс табады, осы іздер климаттық және сақталу жағдайына байланысты бірнеше жылдар бойы сақталуы мүмкін. Табылған иіс іздері ешқандай теорияда жоқ иістерге жатқызылуы мүмкін, осы да криминалистік одорологияның қазіргі таңдағы маңызды проблемасы болып табылады. Иіс іздерін идентификациялауда

қиыншылықтарға әкеліп соғады. Қазіргі таңдағы тек Қазақстан Республикасы үшін ғана емес, бүкіл әлем үшін криминалистік одорологияда маңызды проблемалардың бірі болып, ол – арнайы иіс іздерін идентификациялайтын арнайы ғылыми техникалық құралдардың 100%-ды нақты қорытынды бермейтіндігінде болып табылады, осы криминалистік одорологияның басты қиыншылығы. Бұл жердегі шешу жолы– криминалистік одорология тақырыбына арнайы одоролог профессор, мамандардың съездерін өткізіп, тәжірибе алмасуы, арнайы құралдар ойлап табуда бас біріктірулері арқылы көрініс табуы керек деп ойлаймыз. Арнайы иттерді таңдауда криминалист одоролог мамандар арнайы үйрету курсынан өткен, емтихан тапсырған кезде оң қорытынды алған иттермен ғана жұмыс істеуі және иттің белгілі бір жасқа дейінгі мөлшерінде ғана иістерді ажырата білуінде болып табылады. Егер осы міндеттер орындалмаған жағдайда, криминалистік одорология сараптама қорытындысы дұрыс болмай, кінәсіз адам жауапкершілікке тартылып кетуі мүмкін, осы мәселеде де – Отандық криминалистік одорологияның проблемалық тұсы болып табылады. Криминалистік одорологияның тағы да бір маңызды проблемаларының бірі болып – арнайы иттерді үйрететін курстардың болмауы, яғни, үйрету мекемелерінің аздығында болып табылады. Көбінесе мұндай үйретілген иттер жоғарыда айтылғандай шетел мемлекеттерінен әкелінеді. Біздің бұл жердегі басты ұсынысымыз – құқық қорғау органдарының мекемелерінің оқыту орындарында арнайы криминалист одоролог мамандарды дайындау және арнайы криминалистік одорология сараптамасын жүзеге асыру үшін иттерді үйретудің арнайы курстарын ашу болып табылады. Біз арнайы иттерді үйретудің курстарын басқа мемлекеттерден тәжірибе ретінде енгізуіміз қажет деп ойлаймыз, біздің ұсынысымыз – Америка Құрама Штаттарының К-9 құқық қорғау мекемесінің арнайы криминалистік одорология сараптамасын жүзеге асыру үшін үйретілетін курстар дұрыс деп ойлаймыз. Өйткені, криминалистік одорология сараптамасының дұрыстығы – 96 %-ды құрайды. Отандық криминалистік одорологияның маңызды проблемаларының бірі болып – қылмыстық іс жүргізу заңнамасында криминалистік одорология сараптамасының көлемді түрде көрініс

табылмауы болып табылады. Криминалистік одорология сараптамасы қылмыстық процесте әрқашанда 100%-ды дәлелдеме ретінде пайдаланылмайды, яғни, шешуде айтарлықтай үлкен салмаққа ие емес, осы айтылып отырған мәселе де, криминалистік одорологияның өте маңызды проблемаларының бірі. Мысалы, Америка Құрама Штатының, Калифорния штатының нормативтік заңнамасына сәйкес, криминалистік одорология сараптамасы негізгі дәлелдеу қорытындысы болып табылады деп көрініс тапқан. Біздің ойымызша, криминалистік одорология сараптамасы қылмыстарды ашу мен тергеуде және соттың әділ шешім шығаруында маңызы өте зор және біздің нормативтік заңнамаларымызда да негізгі, әрі міндетті дәлелдеу қорытындысы болуы керек деп ойлаймыз.

Қазіргі таңда, Қазақстан Республикасы Президентінің жыл сайынғы Жолдауларында құқық қорғау қызметін жетілдіру бағыттары өте көп көрініс табады. Ата-бабаларымыз айтқандай, ел бірлігі – ел теңдігі, отандық криминалистиканы дамыту үшін біз өте көп ерінбей еңбек етуіміз қажет. Қазақстан Республикасы жас мемлекет, тәуелсіздік жылдарында отандық криминалистика өте жақсы дамыды, қазіргі таңда да өте жақсы дамып келуде. Егер талпынсақ, бұдан жоғары жетістіктерге жетеміз деп ойлаймыз. Қазақстан Республикасында криминалистік одорологияны дамытуға өте жақсы профессор-мамандар, заңгерлер өз үлестерін қосып, жоғары нәтижелер көрсетуде, криминалистік одорология саласын дамыту үшін барлық мүмкіндіктер жасалуда. Болашақта Қазақстан Республикасы криминалистік одорология саласынан бірінші орында болады деген сеніммен қараймыз.

Қазақстан Республикасында криминалистік одорология саласын дамыту үшін біздің ұсыныстарымыз келесідей болып табылады:

Біріншіден, құқық қорғау органдарының оқу мекемелерінде криминалистік одорология саласын оқып үйрететін арнайы мамандық ашу.

Екіншіден, құқық қорғау органдарында арнайы иттерді криминалистік одорология сараптамасын жүргізу үшін оқып үйрететін арнайы оқу курстарын ашу және осы оқу курстарына

шетел мемлекеттерінен арнайы криминалист-одоролог мамандарды шақыру.

Үшіншіден, әлемнің барлық мемлекеттерінен криминалист-одоролог мамандардың съезін жасап тәжірибе алмасуы және бас қосып арнайы криминалистік одорологиялық сараптама жүргізу үшін арнайы техникалық құралдарды ойлап шығару.

Төртіншіден, криминалистік-одорологиялық сараптаманың сотта маңызды болуы және қылмыстық іс жүргізу заңнамасында көлемді орынға ие болуы.

Бесіншіден, Отандық криминалистік одорологияны дамыту үшін шетел тәжірибесінің оң жақтарын басшылыққа алу. Мысалы: Америка Құрама Штаттары, Ұлыбритания королдігі және тағы да басқа мемлекеттер.

Әдебиеттер тізімі

- 1 Жәкішев Е. Ғ., Исаев А. А., Найманова Г. Х., Тапалова Р.Б., Темірболат Н. С. Криминалистика.- Алматы, Қазақ университеті, 2005.- 243 б.
- 2 Рейс Р.А. Полицейские собаки. Научная техника расследования преступлений. - СПб.: Сенатская типография, 1912.- 112 с.
- 3 Кириченано А.А., Басай В.Д. Криминалистика. Полный комплект учебно-методического обеспечения частей «Теорологии» и «Техника»: Учебно-методическое пособие. – Хмельницкий: Изд.-во АПВ Украины, 2001.- 132 с.
- 4 Салтевский М. В Криминалистическая одорология. - Киев, 1976. - 90 с.

Әбдіразақ Б.

*Магистрант Сеульского Национального Университета,
Республика Корея*

ЗАРУБЕЖНЫЕ МОДЕЛИ ПРАВОВОГО РЕЖИМА БОЛЬШИХ ДАННЫХ: МЕЖДУНАРОДНЫЕ ПОДХОДЫ К ОТВЕТСТВЕННОСТИ, ЗАЩИТЕ И ЗАКОНОДАТЕЛЬНОМУ РЕШЕНИЮ

Проблема правового режима больших данных начинается не с выбора между разрешением и запретом их оборота. Предварительно необходимо установить, что именно участвует в соответствующем отношении: отдельные сведения, организованная база, доступ к

непрерывно обновляемому ресурсу либо аналитический результат. Объединение этих элементов в технической системе не устраняет различий между правом гражданина на защиту относящейся к нему информации, интересом организации в сохранении конфиденциальности и договорным правом пользователя на получение данных. Поэтому выражение «владелец больших данных» не должно заранее предрешать принадлежность всех включенных в массив сведений одному субъекту.

Й. Дрексл рассматривает регулирование промышленных данных через соотношение их проприетаризации и доступа, помещая вопрос в контекст формирования конкурентных рынков [1]. Н. Пуртова и Г. ван Маанен показывают ограничения подходов, выводящих управление данными исключительно из их характеристик как экономического блага: стимулирование производства данных само по себе не обеспечивает достижения остальных общественно значимых целей [2]. Эти позиции позволяют поставить более точный юридический вопрос: не кому следует предоставить абсолютное господство над массивом, а какое правомочие необходимо для защиты определенного интереса и какими встречными ограничениями оно должно сопровождаться.

В настоящем исследовании сопоставляются не правопорядки «в целом», а решения одной функциональной проблемы - как обеспечить использование экономически ценных массивов без утраты правовой защиты затронутых лиц. Рассматриваются объект охраны, основание доступа, условия ответственности и содержание восстановительной меры. Европейское регулирование, законодательство Республики Корея и правоприменение США используются как разные способы решения этой проблемы, а не как исчерпывающие характеристики национальных систем.

Нормативный анализ проводится по состоянию на 26 сентября 2026 года. Судебные и административные дела отобраны для проверки конкретных юридических конструкций; такая выборка не позволяет делать статистические выводы об эффективности правопорядков. Казахские эпизоды исследуются в пределах официальных сообщений, без приписывания им содержания неопубликованных судебных актов. Законодательство 2026 года

используется для оценки дальнейшего регулирования, а не для ретроспективной квалификации событий 2024 года.

Международное регулирование не дает основания отождествлять охрану массива с исключительным правом на каждое содержащееся в нем сведение. Пункт 2 статьи 10 Соглашения ТРИПС связывает охрану подборок данных с интеллектуальным характером отбора или расположения материалов, одновременно отделяя такую охрану от самих данных. Иную конструкцию закрепляет пункт 2 статьи 39, а именно защищается законно контролируемая информация, которая является секретной, имеет коммерческую ценность вследствие секретности и охраняется разумными мерами ее держателя. Подпункты «а»-«с» устанавливают совокупность условий, а не альтернативные основания [3].

Особенно существенно примечание 10 к статье 39. Оно относит к действиям, противоречащим честной коммерческой практике, в том числе приобретение информации третьими лицами, которые знали либо вследствие грубой неосторожности не знали о неправомерности ее получения [3]. Значение этой нормы для больших данных заключается в юридической оценке последующего оборота: договор с поставщиком не исчерпывает вопроса о правомерности поведения приобретателя. Вместе с тем норма не устанавливает универсальную ответственность любого получателя за неизвестное ему нарушение на предшествующем этапе.

Из этого следует разграничение двух исследовательских задач. Для защиты конфиденциального массива необходимо доказать существование охраняемого интереса и нарушение условий обращения с информацией. Для оценки приобретателя дополнительно устанавливаются обстоятельства получения данных и его осведомленность. Смешение этих задач ведет либо к необоснованному освобождению последующего пользователя, либо к возложению на него ответственности исключительно за участие в обороте. Ни один из таких результатов не вытекает из статьи 39 Соглашения ТРИПС.

Другой уровень регулирования представлен рекомендациями ОЭСР о защите частной жизни. Пункт 14 закрепляет подотчетность

контролера данных. Подпункты «ii»-«vi» пункта 15(a) связывают программу управления приватностью с объемом и чувствительностью информации, оценкой рисков, внутренним надзором, реагированием и регулярным пересмотром. Пункт 15(b) предполагает готовность продемонстрировать программу компетентному органу, а пункт 15(c) - уведомление о существенных нарушениях безопасности и, при вероятности неблагоприятных последствий, затронутых лиц [4].

Рекомендации ОЭСР, в отличие от ТРИПС, имеют рекомендательную, а не международно-договорную природу; сами по себе они не образуют основания для взыскания убытков с казахстанского оператора. Их значение иное: они позволяют оценить, создает ли национальное регулирование условия для подтверждения надлежащего поведения. Подотчетность теряет практическое содержание, когда оператор предъявляет только внутреннюю политику, но не способен показать, как она исполнялась. Поэтому предметом заимствования должна становиться не новая декларация об ответственности, а связь между обязанностью, документированием ее исполнения и доступностью соответствующих доказательств.

Европейский подход доступа к данным без устранения охранительных режимов. Регламент ЕС 2023/2854 - Акт о данных - представляет интерес именно сочетанием доступа и ограничений, а не созданием общего права собственности на информацию. Подпункт «а» пункта 2 статьи 1 относит главу II к данным подключенных продуктов и связанных услуг. Соответствующие правила нельзя автоматически распространять на любые массивы Big Data. Пункт 5 статьи 1 сохраняет действие законодательства о персональных данных. Пункт 1 статьи 4 предусматривает предоставление пользователю доступных держателю данных и необходимых метаданных в пригодном для использования формате [5].

Пункты 6-9 статьи 4 образуют важное ограничение, что коммерческая тайна требует согласования защитных мер, но не служит безусловным основанием отказа. Приостановление предоставления данных и исключительный отказ при высокой

вероятности серьезного экономического ущерба сопровождаются требованиями обоснования и возможностью обжалования. Статья 43 исключает применение права *sui generis* на базы данных к данным, получаемым или генерируемым подключенным продуктом либо связанной услугой в пределах соответствующего регулирования [5].

Представляется, что здесь юридически значима не максимизация доступа, а превращение отказа в проверяемое решение. Пользователь должен иметь возможность оспорить не само существование коммерческой тайны, а достаточность приведенных оснований ограничения. Однако механическое распространение этой конструкции на казахстанский рынок любых данных означало бы смешение разных отношений, то есть использования приобретенного подключенного устройства и получения доступа к самостоятельно сформированному коммерческому ресурсу. Обязанность раскрытия нуждается в определенном круге адресатов и правообладателей.

При этом формальная доступность еще не означает пригодности полученных сведений. Д. Ким и М. В. Квок обращают внимание на неопределенность используемых в Акте о данных критериев доступности, предварительной обработки, простоты операции и непропорциональных усилий [6]. Их критика показывает, почему недостаточно перенести в национальный закон само право требовать данные: без определения необходимого состояния массива спор может переместиться от отказа в доступе к передаче технически непригодного результата.

Для Казахстана отсюда выводится необходимость различать обязанность предоставить существующий ресурс и обязанность создать новый аналитический продукт. Под видом доступа нельзя без специального основания требовать выполнения самостоятельной исследовательской работы. Но нельзя считать обязанность исполненной и посредством передачи набора файлов, лишенного необходимых метаданных. Проверяемым критерием должно быть соответствие предоставленного результата назначению конкретного права доступа, а не любая потенциальная полезность данных для получателя.

Не менее показательным судебное развитие статьи 82 GDPR [7]. В решении от 4 мая 2023 года по делу C-300/21, *UI v Österreichische Post AG*, рассматривалось формирование предполагаемых политических предпочтений лица на основе обработки информации. В пунктах 32-33 Суд ЕС выделил три совокупных условия компенсации: нарушение, вред и причинную связь. В пунктах 49-51 отвергнут дополнительный порог серьезности неимущественного вреда, но сохранена необходимость доказать его наличие [8]. Решение не означает, что за любое нарушение автоматически присуждается компенсация.

Это разграничение позволяет критически оценить предложение о безусловной презумпции вреда при любой утечке. Презумпция может облегчать доказывание конкретного обстоятельства, но не должна незаметно превращать компенсацию в дополнительную публичную санкцию. С другой стороны, отсутствие медицинского диагноза нельзя заранее приравнивать к отсутствию неимущественных последствий. Вопрос заключается в доказанности нарушения личного интереса и его последствий в обстоятельствах дела, а не в использовании одного формального документа как универсального условия защиты.

В деле C-340/21, *VB v Natsionalna agentsia za prihodite*, решение от 14 декабря 2023 года, Суд ЕС рассмотрел последствия несанкционированного доступа к данным болгарского налогового органа. Пункты 29-39 не допускают вывода о ненадлежащих мерах защиты только из факта утечки. Вместе с тем пункты 42-46 требуют оценки конкретных рисков и реально принятых мер, а не намерений контролера. Пункт 74 исключает автоматическое освобождение лишь потому, что вмешательство совершили третьи лица. По пунктам 84-86 опасение будущего неправомерного использования способно составлять неимущественный вред, если оно обоснованно обстоятельствами [9].

Практическая ценность этого решения состоит в отказе от двух одинаково упрощенных конструкций: «произошла утечка - оператор во всем виновен» и «действовал внешний нарушитель - оператор ни за что не отвечает». Между ними находится исследование организационного поведения, причинной связи и последствий. Для

национального правоприменения полезна именно такая структура оценки. Размеры европейских штрафов или публичная известность дела сами по себе не дают основания переносить его выводы в иной состав правонарушения.

Республика Корея: защита экономического интереса без универсального присвоения информации. Рамочный закон Республики Корея о развитии индустрии данных и использовании данных № 18475 заслуживает внимания не только категорией «data asset». Пункт 1 статьи 12 связывает ее с экономической ценностью и существенными человеческими или материальными вложениями. Пункт 2 запрещает определенные формы неправомерного получения, использования и раскрытия, а пункт 3 отсылает вопросы такой защиты к законодательству о недобросовестной конкуренции и коммерческой тайне. Одновременно пункт 2 статьи 7 сохраняет специальные режимы персональной информации, авторских прав и публичных данных [10].

Следовательно, юридический смысл конструкции нельзя свести к формуле «тот, кто понес расходы, становится собственником данных». Расходы объясняют наличие экономического интереса, но не устраняют требования правомерности его формирования и пределы противопоставления этого интереса другим лицам. Для Казахстана заимствование только определения актива, без соответствующих ограничений, создало бы риск усиления фактического держателя в отношениях, где правомерность его контроля еще должна быть установлена.

Статья 42 корейского закона также требует точного прочтения. По пункту 1 нарушитель может освободиться от обязанности возмещения, доказав отсутствие умысла или неосторожности. По пункту 2 суд вправе разумно определить размер компенсации, когда причинение вреда установлено, но доказать его величину затруднительно [10]. Здесь облегчаются разные элементы доказывания: вина и размер, причем трудность расчета не заменяет установления самого вреда.

Для сравнения, пункт 6 статьи 9 ГК РК уже предполагает вину нарушителя, если законом не предусмотрено иное. Пункт 2 статьи 917 Особенной части также допускает освобождение причинителя

вреда при доказанности отсутствия вины [11; 12]. Поэтому введение «корейской презумпции вины» как принципиально нового решения не отражало бы содержание действующего казахстанского права. Сопоставление выявляет более узкий вопрос: как определять компенсацию за доказанное ухудшение экономической пригодности массива, когда размер потерь нельзя установить с арифметической точностью.

С другой стороны, пункты 1-2 статьи 126 ГК РК уже связывают охрану коммерческой тайны с ценностью неизвестной третьим лицам информации, отсутствием свободного законного доступа и принятием мер конфиденциальности, предусматривая последствия незаконного получения и определенных случаев разглашения [11]. Недостаточно просто назвать массив «данными» вместо «информации», чтобы обосновать необходимость новой нормы. Самостоятельное предложение требуется лишь для установленной ситуации, не получающей достаточного решения в рамках действующих конструкций.

По нашему мнению, сравнительный результат должен выражаться в проверке трех обстоятельств: законности происхождения массива, характера присваиваемого результата чужих вложений и конкретного недобросовестного действия. Одна лишь коммерческая ценность не оправдывает запрета независимого получения общедоступных сведений. Но и отсутствие абсолютного права собственности не означает допустимости обхода технической защиты, нарушения доверия или использования заведомо незаконно полученной базы.

США: восстановительная мера в отношении производных результатов. Американское дело Everalbum позволяет поставить вопрос, который не исчерпывается штрафом или удалением исходных записей. В жалобе Федеральной торговой комиссии США описаны несоответствия между заявлениями сервиса об использовании распознавания лиц и удалении материалов после деактивации аккаунта и фактическим обращением с данными. Пункты 23-27 связывали эти действия с запретом обманных практик по разделу 5(а) Закона о Федеральной торговой комиссии [13]. Это

утверждения административного обвинения, а не самостоятельно установленная исследователем виновность компании.

Окончательное решение и предписание от 6 мая 2021 года по делу С-4743 принято в согласительной процедуре; компания не признала и не опровергла изложенные в жалобе обвинения. Подпункт С раздела III потребовал удалить в течение 90 дней затронутые производные результаты. Согласно определению А к ним относились модели и алгоритмы, созданные полностью или частично с использованием соответствующей биометрической информации пользователей [14]. Таким образом, предписание охватило не только исходные данные, но и результат их обработки.

Юридически значимый вопрос состоит в том, прекращается ли нарушение после удаления базы, если получатель сохраняет извлеченное из нее преимущество. Рассмотренное предписание показывает возможный восстановительный ответ, но не доказывает существования универсального правила об уничтожении любой модели, обученной на спорных данных. Индивидуальное административное урегулирование нельзя выдавать за общее судебное толкование, обязательное для всех технологий и правопорядков.

Для Казахстана это основание исследовать судьбу производного продукта отдельно от судьбы исходного массива. Предлагаемая мера должна учитывать доказанную связь продукта с неправомерной обработкой, сохраняющиеся последствия нарушения и возможность их устранения менее ограничительным способом. Исправление, исключение неправомерно использованной части, переобучение и уничтожение не являются взаимозаменяемыми действиями. Выбор между ними должен быть мотивирован, иначе защита одного интереса способна превратиться в необоснованное прекращение правомерной деятельности.

6. Применимость зарубежных решений к законодательству и практике Казахстана

Цифровой кодекс РК от 9 января 2026 года № 255-VIII уже содержит специальную конструкцию продукта цифровых данных. Пункт 1 статьи 30 связывает его с агрегированным и формализованным результатом обработки. Подпункты 1-3 пункта 4

той же статьи устанавливают для продукта, участвующего в предусмотренном Кодексом платформенном обороте, требования об исключении прямо или косвенно идентифицирующих персональных данных, качестве, безопасности и метаданных. Поэтому дальнейшее совершенствование не следует начинать с повторного предложения «признать продукт данных» [15].

Существеннее другое: допустимость характеристик готового продукта и правомерность получения исходного материала - не тождественные вопросы. Из того, что результат не позволяет идентифицировать человека, логически не следует правомерность первоначального сбора. Пункт 7 статьи 17 Кодекса дополнительно исключает признание открытыми сведений, ставших доступными вследствие утечки или ошибочного раскрытия. Пункт 2 статьи 105 сохраняет обязанность устранить нарушение независимо от уголовной или административной ответственности [15]. Эти положения позволяют обсуждать последующий оборот без презумпции, что техническая доступность равна юридической свободе использования.

В подпунктах 1-3 пункта 1 статьи 22 Закона РК «О персональных данных и их защите» уже предусмотрены предотвращение несанкционированного доступа, его своевременное обнаружение и минимизация неблагоприятных последствий. Подпункт 5 устанавливает регистрацию и учет действий, предусмотренных подпунктами 3-6 пункта 4 статьи 8 [16]. Следовательно, новое предложение о «введении журналирования» без анализа действующей обязанности было бы неточным. Исследования требуют достаточность состава фиксируемых сведений для восстановления последовательности передачи и представления доказательств в споре.

Практическое значение такого разграничения видно на примере «Робокэш.кз». Согласно официальному сообщению министерства, 5 марта 2024 года обнаружена утечка более двух миллионов персональных данных; указанная формулировка не устанавливает число уникальных потерпевших. По результатам проверки назначен штраф в 1000 МРП по части 4 статьи 79 КоАП; в сокращенном производстве уплачено 500 МРП - 1 846 000 тенге. Сообщается об

уведомлении граждан через eGov и возможности обращения в суд [17].

Показательна точность разъяснения способов защиты. Сообщение связывает возмещение материального и морального вреда со статьей 951 ГК. Однако статья 951 регулирует моральный вред; имущественные требования нуждаются в самостоятельном обосновании, в частности по пункту 4 статьи 9 и пункту 1 статьи 917 ГК, в зависимости от характера отношения [11; 12; 17]. Это не доказывает ошибочность решения по административному делу, текст которого не исследован. Но показывает, почему информационное сопровождение инцидента не должно подменять разграничение оснований гражданских требований.

Административный штраф в этом случае нельзя считать ни совокупной компенсацией гражданам, ни доказательством индивидуального размера их потерь. С европейской практикой сопоставим прежде всего вопрос распределения доказательств: какие обстоятельства устанавливаются проверкой для всего инцидента, а какие требуют оценки применительно к конкретному заявителю. Правомерно обсуждать возможность использования материалов проверки, но не автоматически придавать информационному сообщению преюдициальную силу.

В официальном сообщении КНБ о вступившем в силу приговоре суда Актау указаны неправомерный доступ к государственным информационным системам и получение персональных данных для возмездной передачи третьим лицам. Назначено три года лишения свободы по частям 3 и 4 статьи 147, части 2 статьи 205 и пункту 1 части 2 статьи 208 УК [18]. Этот эпизод подтверждает применение нескольких существующих составов, но без полного приговора не позволяет оценить все основания их совокупности.

Само наличие подобных дел не обосновывает нового универсального состава «неправомерное использование больших данных». Напротив, сначала требуется установить, какое конкретное действие остается вне существующих запретов: доступ, извлечение, передача, обход защиты либо причинение определенного вреда. Иначе технологический термин может лишь

наложиться на действующие составы, не устраняя выявленной проблемы. Сравнение с ТРИПС и корейским законом ориентирует на определенность запрещенного поведения, а не на наказуемость всякого использования экономически ценного массива.

Практический результат проведенного анализа видится в нескольких взаимосвязанных уточнениях. Требование к метаданным по подпункту 3 пункта 4 статьи 30 Цифрового кодекса целесообразно дополнить указанием на документируемое основание получения исходных данных и ограничения последующего использования. Объем подтверждения следует соотносить с риском и назначением продукта; при этом раскрытие доказательств не должно требовать публикации самих персональных данных или чужой коммерческой тайны.

Для гражданско-правовой защиты необходимо разграничить доказательства инцидента, индивидуального нарушения и размера возмещения. Материалы проверки могут служить источником доказательств, однако вопрос об их процессуальном значении должен решаться с учетом вида акта, порядка его принятия и возможности оспаривания. Заимствование корейского подхода к определению размера компенсации заслуживает обсуждения именно при доказанности вреда и объективной трудности расчета, а не как замена этих условий фиксированной выплатой за факт утечки.

Наконец, восстановительная мера должна охватывать сохраняющиеся последствия неправомерной обработки. Здесь заслуживает развития предусмотренное статьей 105 Кодекса разграничение наказания и устранения нарушения. Предписание об исправлении или удалении исходной информации следует сопоставлять с правовой судьбой переданных копий и производных результатов. Однако распространение меры на аналитический продукт требует самостоятельного обоснования причинной связи и соразмерности; одного упоминания Big Data либо искусственного интеллекта для этого недостаточно.

Рассмотренные зарубежные решения показывают не движение к единой собственности на большие данные, а дифференциацию правомочий и средств защиты. Международная охрана нераскрытой

информации связывает защиту с определенными условиями и характером поведения. Европейские решения соединяют доступ с конфиденциальностью и отделяют нарушение от условий компенсации. Корейское регулирование учитывает экономический интерес держателя, не отменяя специальных режимов. Дело Everalbum позволяет исследовать восстановление права за пределами удаления исходных записей.

В результате исследования мы пришли к выводу, что для Казахстана критерием применимости такого решения должна быть его функциональная совместимость с национальным правом, то есть совпадение охраняемого интереса, определенность адресата обязанности, доступность доказательств и исполнимость восстановительной меры. Отдельное иностранное правило не должно переноситься без его ограничений. Наиболее предметные направления дальнейшей работы связаны с подтверждением законного происхождения данных, согласованием публичного реагирования и частной защиты, а также устранением доказанных последствий неправомерной обработки на последующих этапах оборота.

Финансирование. Исследование подготовлено в рамках проекта ИРН АР23489796 «Проблемы регламентации правового режима больших данных (Big Data): отечественный и международный опыт», финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан.

Список использованных источников

1 Drex1, J. Designing Competitive Markets for Industrial Data – Between Propertisation and Access / J. Drex1 // JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law. - 2017. - Vol. 8, no. 4. - P. 257–292. - URN: urn:nbn:de:0009-29-46365. URL: <https://www.jipitec.eu/jipitec/article/view/209> (дата обращения: 01.07.2026).

2 Purtova, N. Data as an economic good, data as a commons, and data governance [Электронный ресурс] / N. Purtova, G. van Maanen // arXiv. - 2023. - 18 April. - Version 2. - 57 p. - arXiv:2212.10244v2. - DOI: 10.48550/arXiv.2212.10244. URL: <https://arxiv.org/abs/2212.10244v2> (дата обращения: 03.07.2026).

3 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) [Электронный ресурс]: 15 April 1994 : Annex 1C to the Marrakesh Agreement Establishing the World Trade Organization // WTO legal texts / World Trade Organization. - 1994. - Используемые положения: ст. 10, п. 2, ст. 39, п. 2 и

примечание 10. URL: https://www.wto.org/english/docs_e/legal_e/27-trips_04_e.htm, https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm (дата обращения: 06.07.2026).

4 OECD. Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [Электронный ресурс] : OECD/LEGAL/0188 : принята 23 сентября 1980 г., пересмотрена 11 июля 2013 г. // OECD Legal Instruments. - Используемые положения: п. 14–15 приложения. URL: <https://legalinstruments.oecd.org/public/doc/114/114.en.pdf> (дата обращения: 07.07.2026).

5 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) // Official Journal of the European Union. - 2023. - Series L. - 22 December. - 2023/2854. - Используемые положения: ст. 1, 4, 43. URL: <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng> (дата обращения: 09.07.2026).

6 Kim, D. Data Usability as a Parameter of Rights and Obligations under the EU Data Act / D. Kim, M. W. Kwok // JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law. - 2024. - Vol. 15, no. 2. - P. 139–155. URL: <https://www.jipitec.eu/jipitec/article/view/405> (дата обращения: 10.07.2026).

7 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. - 4 May. - P. 1–88. - Используемые положения: ст. 24, 32, 82. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (дата обращения: 13.07.2026).

8 Court of Justice of the European Union. UI v Österreichische Post AG [Электронный ресурс]: judgment of the Court (Third Chamber) of 4 May 2023, Case C-300/21 // EUR-Lex. - 2023. - ECLI:EU:C:2023:370. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62021CJ0300> (дата обращения: 14.07.2026).

9 Court of Justice of the European Union. VB v Natsionalna agentsia za prihodite [Электронный ресурс]: judgment of the Court (Third Chamber) of 14 December 2023, Case C-340/21 // EUR-Lex. - 2023. - ECLI:EU:C:2023:986. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0340> (дата обращения: 16.07.2026).

10 Republic of Korea. Framework Act on Promotion of Data Industry and Data Utilization [Электронный ресурс]: Act No. 18475 of 19 October 2021, amended by Act No. 21066 of 1 October 2025 // Statutes of the Republic of Korea / Korea Legislation Research Institute. - Английский консолидированный текст. - Используемые положения: ст. 7, 12, 42. URL: https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=72239&key=18&type=part (дата обращения: 17.07.2026).

11 Гражданский кодекс Республики Казахстан (Общая часть) : Кодекс Республики Казахстан от 27 декабря 1994 г. № 268-ХІІІ // Ведомости Верховного

Совета Республики Казахстан. - 1994. - № 23–24 (приложение). - Электронная версия: ИПС «Әділет». - Используемые положения: ст. 9, 126. URL: https://old.adilet.zan.kz/rus/docs/K940001000_ (дата обращения: 20.07.2026).

12 Гражданский кодекс Республики Казахстан (Особенная часть): Кодекс Республики Казахстан от 1 июля 1999 г. № 409 // Ведомости Парламента Республики Казахстан. - 1999. - № 16–17. - Ст. 642. - Электронная версия: ИПС «Әділет». - Используемые положения: ст. 917, 951. URL: https://old.adilet.zan.kz/rus/docs/K990000409_/info (дата обращения: 21.07.2026).

13 Federal Trade Commission. In the Matter of Everalbum, Inc., also d/b/a Ever and Paravision [Электронный ресурс]: Complaint: issued 6 May 2021. - Docket No. C-4743. - File No. 1923172. - 7 p. - Используемый фрагмент: п. 23–27. URL: https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_complaint_final.pdf (дата обращения: 22.07.2026).

14 Federal Trade Commission. In the Matter of Everalbum, Inc., also d/b/a Ever and Paravision [Электронный ресурс]: Decision and Order : issued 6 May 2021. - Docket No. C-4743. - File No. 1923172. - 8 p. - Используемые положения: Definition A, Section III(C). URL: https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_decision_final.pdf (дата обращения: 23.07.2026).

15 Цифровой кодекс Республики Казахстан: Кодекс Республики Казахстан от 9 января 2026 г. № 255-VIII ЗРК // Казахстанская правда. - 2026. - 10 января. - № 5–6 (30634–30635). - Электронная версия: ИПС «Әділет». - Используемые положения: ст. 17, 30, 105. URL: <https://old.adilet.zan.kz/rus/docs/K2600000255/info> (дата обращения: 24.07.2026).

16 О персональных данных и их защите: Закон Республики Казахстан от 21 мая 2013 г. № 94-V // Ведомости Парламента Республики Казахстан. - 2013. - № 7. - Ст. 35. - Электронная версия: ИПС «Әділет». - Используемое положение: ст. 22, п. 1. URL: <https://old.adilet.zan.kz/rus/docs/Z1300000094/info> (дата обращения: 27.07.2026).

17 Минцифры объявило результаты проверки в отношении ТОО «МФО Робокэш.кз» [Электронный ресурс] / Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан // Gov.kz. - [2024]. - Официальное сообщение. - Номер публикации: 740137. URL: <https://www.gov.kz/memleket/entities/maidd/press/news/details/740137?lang=ru> (дата обращения: 29.07.2026).

18 О пресечении правонарушений в сфере информатизации и связи [Электронный ресурс] / Комитет национальной безопасности Республики Казахстан // Gov.kz. - [2024]. - Официальное сообщение о вступившем в законную силу приговоре суда Актау. - Номер публикации: 710060. URL: <https://www.gov.kz/memleket/entities/knb/press/news/details/710060?lang=ru> (дата обращения: 31.07.2026).

Abdirazak B.
*Master's Student at Seoul National
University (Republic of Korea)*

THE LEGAL REGIME OF DE-IDENTIFIED DATA IN BIG DATA APPLICATIONS

This article examines when changing personal data changes the legal rules that apply to them. It distinguishes the lawfulness of obtaining the original data, the result of de-identification, and the basis for later use. Kazakhstan's Personal Data Law, the 2026 amendments, the Digital Code and the existing irreversibility rule are analysed together. The Breyer and EDPS v SRB proceedings provide comparative material on additional identifying information and the difference between a sender's duties and a recipient's position. The article develops an assessment tied to a particular dataset version and release setting. Two draft additions to Article 17 would require a documented assessment and review after a material change or credible new evidence. They neither create automatic liability nor turn contractual promises into proof of anonymity. The study is legal rather than experimental; it does not claim that a particular dataset is safe or that the proposals have already reduced harm.

A name is only one way to recognise a person. A dataset may contain no names and still reveal who visited a place, received a service, or made a particular statement. The legal question is therefore not simply whether identifying fields were removed. It is whether the remaining information can still be connected to someone, and what follows for the proposed use. Ohm's study of re-identification challenged the assumption that deleting obvious identifiers provides lasting protection [1]. The important lesson is not that every dataset identifies everyone. It is that a description of a technical operation is not yet evidence of its legal result.

A real study makes this distinction easier to understand. De Montjoye and colleagues examined mobility records concerning 1.5 million people. At the spatial and temporal resolution studied, four randomly selected location-and-time points were enough to distinguish 95 per cent of individual traces from the others [2]. This did not mean that the researchers discovered the names of 95 per cent of those people.

Uniqueness and identification are different findings. Yet uniqueness matters because outside information may connect a distinctive trace to a person. The result concerns that dataset and those conditions; it is not a universal percentage for big data.

For Kazakhstan, this problem has become more specific. The Personal Data Law now distinguishes de-identification, anonymisation and masking. The Digital Code also regulates anonymisation and the content of data products [3–6]. A useful study must explain how these rules work together. Merely proposing a new category called “anonymous data” would leave unanswered the more important questions: who must establish that a transformation worked, what must be checked, and what happens when the information available to a recipient changes?

This article addresses those questions through legal interpretation and two draft additions to Article 17 of the Personal Data Law. The statutory analysis uses the provisions relevant on 26 September 2026, reading the Law together with the June 2026 amending act rather than treating every online consolidation as complete. Comparative material includes the Court of Justice’s 2025 judgment in *EDPS v SRB* and its official account of Breyer. Scholarly research helps identify the limits of technical and legal claims. No dataset was tested for this article, and no statistical claim is made about Kazakhstan’s enforcement practice. English renderings of Kazakhstan’s provisions are the author’s explanatory translations, not official statutory wording.

Article 1(7) of the Personal Data Law defines de-identification through the impossibility of attributing personal data to their subject. The June amendments add Article 1(2-5), which describes anonymisation as an irreversible transformation of personal-data identifiers that makes such attribution impossible. Article 1(3-1), by contrast, defines masking through replacement of part of the real information with invalid and/or de-identified information [3; 4, Article 1(37)]. These are not interchangeable descriptions. Masking says how information is changed or presented. The other definitions also require an outcome concerning attribution.

The difference can be stated without technical language. Changing what a screen displays does not necessarily change what the underlying

system knows. Likewise, replacing a name with a code does not remove the connection when a usable code-to-name list remains. That list is often called a key. It is additional information that allows the connection to be restored. Whether a particular method satisfies the statutory definition must therefore be assessed from its actual operation. The name of the method, the supplier's assurance, or a tick in a compliance form is not a substitute for this assessment.

Kazakhstan's rules already address reversibility. Paragraph 20 of the Rules approved by Order No. 395 requires de-identification before distribution, using a lawful method compatible with the processing task. Paragraph 21 requires the procedure to exclude restoration of the original personal data [5]. A proposal merely to introduce irreversibility would repeat an existing requirement. The remaining interpretive question concerns how to demonstrate that requirement, especially where the original field cannot be restored directly but information from another source may still reveal the person. Irreversibility of one operation and impossibility of attribution must be examined together.

The June amendments also define a personal-data identifier broadly enough to include information that links separate datasets into an identifiable whole [4, Article 1(37), new Article 1(14-1)]. This matters for big data because combination is part of the legal issue, not an external concern that the legislation wholly overlooks. The scientific contribution should therefore explain how to assess combinations. It should not claim to discover that linking is legally relevant for the first time. Nor should it assume that checking a short list of names and identification numbers exhausts the statutory inquiry.

A related distinction appears in European scholarship. Schwartz and Solove argue that information can move along a continuum of identification risk rather than remaining permanently inside one category [7]. Finck and Pallas examine the difficulty of drawing the boundary between personal and non-personal data when technical change and legal concepts do not fit neatly together [8]. These arguments support attention to context. They do not establish that Kazakhstan has adopted the same risk threshold as European law. Using scholarship to interpret a domestic rule requires explaining that difference, not translating a foreign concept and treating it as national legislation.

Stalla-Bourdillon and Knight similarly question a static division under which a dataset is released once and then assumed to remain anonymous indefinitely [9]. Mourby and her co-authors distinguish key-coding in ordinary research language from pseudonymisation as a defined legal concept [10]. Under GDPR Article 4(5), pseudonymisation involves separation and protection of additional identifying information; Recital 26 still requires an assessment of identifiability [11]. Thus “coded,” “de-identified” and “anonymous” should not be used as automatic synonyms. In this article, “de-identified data” is an umbrella description of transformed information. A claim that Kazakhstan’s legal definition is satisfied requires a separate finding.

Hashing needs a similarly careful explanation. The new Article 1(18) describes it as transforming digital data into a fixed-length string for protection [4, Article 1(37)]. In ordinary terms, information is converted into a code of a set length. The statutory description does not say that every such code makes a person impossible to identify. The assessment must still ask what connections remain in the whole dataset and in the setting where it will be used. A transformation may help protect information without satisfying every condition for treating the result as legally de-identified. This is why the method and the claimed legal outcome must be recorded separately.

Masking and hashing also have their own regulatory setting. Article 23(2), as amended in June 2026, provides for these protection methods, and Order No. 535 of 3 September 2026 approves implementing rules [4; 12]. The accessible opening provisions confirm that scope; the full technical instructions were not available for this study. Accordingly, no claim is made that those instructions contain no assessment or documentation duties. The proposals below concern what Article 17 should state expressly at statutory level. They must be coordinated with implementing requirements rather than presented as substitutes for them.

De-identification is itself part of processing under Article 1(12). Therefore, the organisation carrying it out must have a lawful basis for handling the original personal data. Article 7 governs collection and processing, including purpose and proportionality of the information collected. Article 9 provides exceptions to consent, but those exceptions have conditions [3; 4]. The order of inquiry is important: first establish

authority to handle the input, then assess the output. An effective transformation may reduce later exposure. It does not retroactively authorise an earlier unlawful acquisition.

Research does not reverse this order. Article 9(6) addresses lawful scientific and other specified activity subject to requirements protecting rights and freedoms. Article 17(1) separately requires transferring owners, operators and third parties to de-identify personal data for the statistical, sociological, scientific and marketing research covered by that paragraph [3]. The first provision concerns a possible basis for processing without consent. The second concerns a protection condition attached to transfer. Calling a commercial project “research” does not merge the two questions. Conversely, the existence of a consent exception does not make the transfer safeguard unnecessary.

Tene and Polonetsky show why analytics creates pressure on familiar principles such as purpose limitation and individual control [13]. Their account helps explain the practical attraction of transformed datasets. However, the usefulness of a later purpose does not establish the lawfulness of every earlier step. This article treats de-identification as a safeguard within a legally justified activity, not as a general permission to obtain information first and explain its purpose afterwards. That distinction is particularly important when data are bought from an intermediary rather than collected directly from individuals.

Article 17 also contains different institutional arrangements. Paragraph 2 assigns specified governmental analytics de-identification to the digital-government operator, unless it has already been performed by the owner or operator. Paragraph 3 deals separately with the national artificial-intelligence platform [3]. These provisions should not be extended to every private analytics service. Their practical implication is narrower: when one participant relies on another participant’s completed transformation, the underlying result still needs to be understood. “Already de-identified” describes an asserted condition. It does not explain which version was assessed or whether its later use remains within the same conditions.

The Digital Code adds another threshold. Article 30(4)(1) requires a data product on the exchange-and-circulation platform not to contain personal data enabling direct or indirect identification. Article 30(4)(3)

concerns metadata describing its content, structure, purpose and conditions of use [6]. Metadata are information about the dataset, not proof that its content is safe. A product description may accurately say that names were removed while leaving unanswered whether other fields permit identification. Equally, these platform conditions should not be described as a blanket prohibition on every lawful transfer outside a platform.

Anonymity also does not make every remaining restriction disappear. Article 16(4) of the Digital Code preserves special regimes for protected information [6]. Civil Code Article 126 and Articles 1017–1019 govern confidential information where their conditions are met [14; 15]. A dataset without identifiable people may still contain commercially secret material. Permission to use it must therefore be examined independently. The same separation applies to the storage and cross-border requirements in Articles 12(2) and 16 of the Personal Data Law: a label cannot remove them while the relevant information remains personal [3].

Breyer concerned dynamic internet addresses recorded by German public websites. The Court’s official account explains that an address constitutes personal data for a website operator when it has legal means to identify the visitor using additional information held by the internet provider [16]. The judgment, delivered on 19 October 2016, interpreted the earlier Data Protection Directive, not the GDPR. The point used here is limited: missing names within one organisation’s file do not end the inquiry when a relevant route to identification exists. The official account is not used as a substitute for unexamined findings in the full case record.

The 2025 judgment in *EDPS v SRB* concerns comments collected by the Single Resolution Board and transmitted to Deloitte with codes. In paragraphs 73–78, the Court rejected an automatic classification for every recipient and required attention to the effectiveness of safeguards against identification. Yet paragraphs 99–115 place the collection-stage information duty in the controller’s circumstances at collection, not simply in the later recipient’s circumstances [17]. The case concerns Regulation 2018/1725 governing EU institutions [18]. Its findings do not establish that all coded data are anonymous or that the sender’s duties disappear when the recipient lacks a key.

The two issues should be separated in any comparison with Kazakhstan. One asks what a recipient can identify. The other asks what the sender was required to do before transfer. A recipient's restricted position cannot rewrite the sender's history. This is an inference from the comparison, not a domestic judicial precedent. It provides a reason to record the relevant actor, operation and date whenever a legal consequence is said to follow from de-identification. Otherwise, a conclusion about one participant may be used to excuse a different participant's conduct.

There is also an important limit to recipient-based reasoning. Checking only the recipient's statement that it has no key may ignore information already in its other systems, contractual access to additional sources, or the conditions of onward disclosure. Purtova's examination of the breadth of personal data warns that digital connections can put pressure on the boundary of the regulatory concept [19]. The appropriate response is neither to ignore plausible links nor to declare every remote imagined link decisive. The relevant legal standard and the evidence supporting its application must be identified explicitly.

In particular, the European language of means reasonably likely to be used, found in Recital 26 GDPR, cannot silently replace Kazakhstan's wording on impossibility and irreversibility [3–5; 11]. Describing the receiving environment is a way to investigate whether the domestic requirement is met. It is not an automatic exemption for a useful dataset with residual identifying links. If the required result cannot be established, lawful controlled processing may remain possible on another applicable basis. What is unavailable is the unsupported claim that the statutory de-identification condition has already been fulfilled.

The practical model proposed here treats a de-identification conclusion as relating to a defined release. A release consists of a particular dataset version, its recipients or access setting, its permitted uses and the information available for linking. This is not a new class of property. It is a way to state exactly what was examined. The model asks an organisation to move from "our data are anonymous" to a reasoned explanation of the actual information and conditions assessed. A conclusion without these limits is difficult for either a recipient or a court to check.

Rubinstein and Hartzog emphasise managing the process of release, including contractual restrictions and controlled access, rather than relying only on an anonymisation label [20]. These measures may reduce opportunities for identification, but a promise not to identify people does not by itself establish that identification is impossible. Contract and technical design perform different functions. The former sets permitted conduct and possible consequences. The latter changes information or access. The proposed assessment records both, while avoiding the claim that either one automatically supplies the full legal result.

A release assessment should identify the remaining fields and explain their possible connections. It should record whether a linking key exists, who can use it, and whether other available information could perform a similar function. It should distinguish a named recipient working within restricted access from public publication. It should also state the method applied, the evidence examined, the date, and important limits of the conclusion. These are proposed elements of an assessment record, not a finding that every listed item is already an express statutory obligation.

Stalla-Bourdillon's 2025 study draws attention to the range of relevant actors, including unintended recipients, and to the importance of evidence supporting anonymity claims [21]. This supports testing the release setting rather than accepting a description supplied only by the intended recipient. It does not require an impossible inventory of every future attacker. In the proposed model, the assessment explains which routes were considered, why they matter, and why others fall outside the stated conditions. A security specialist's conclusions remain open to legal evaluation; technical expertise does not determine the legal consequence on its own.

A changed setting requires a fresh question. Combining a released version with another dataset, adding more detailed fields, or changing restricted access to public access may make the former conclusion inapplicable. This does not prove that the earlier release was unlawful. It means that an assessment cannot answer a question it did not examine. The proposed review duty is therefore triggered by a material change or credible new evidence, not by a demand to repeat a full assessment after

every trivial edit. The organisation must explain materiality rather than invoke it as an undefined excuse.

Documentation should be proportionate. Reusable descriptions and references to existing assessments can reduce repetition where releases genuinely share the same relevant conditions. The record should not reproduce an entire personal dataset or expose secret technical details to everyone. Its purpose is to preserve reasons, not to create another vulnerable database. An internal record, a limited explanation for the recipient, and material provided confidentially to an authorised body may legitimately contain different levels of detail. The proposed model does not confer unrestricted public access to security documentation.

Article 22(2), as amended, links the period of protection measures to events including destruction, deletion, anonymisation and de-identification [3; 4]. This creates a reason to be precise about what was transformed. A protected output does not anonymise a separate source database that still identifies people. Nor does it remove identifying information retained in another relevant component. The article should therefore be applied to the actual data and measures, not to the commercial name given to the whole project. This reading also avoids treating the end of one protection stage as retrospective approval of all preceding conduct.

Article 41 of the Digital Code gives individuals rights concerning deletion, anonymisation and restriction, while preserving specified exceptions and the applicable procedural framework [6]. These remedies are not identical. Restriction controls use while retaining data; anonymisation changes the possibility of connecting them to a person. A response should explain which action was performed and on what scope of information. It should not promise deletion while merely hiding a name on a screen. At the same time, a legal obligation to retain information may require a different response from immediate destruction.

Maintaining evidence does not justify preserving an identification key forever. GDPR Article 11 provides a useful comparison: it does not require acquiring or keeping extra information solely to identify people for compliance purposes where processing no longer requires identification [11]. This is not a Kazakhstan rule imported by analogy. It illustrates a design constraint for the proposed record. Evidence of a

transformation should normally describe its method, version and conditions. Keeping the full original or a key needs its own legal justification. Record-keeping should not recreate the very identification route that the process was meant to remove.

Civil liability requires further analysis. Article 350 of the Civil Code addresses loss caused by breach of an obligation; Article 917 addresses harm caused by unlawful conduct and the applicable conditions of responsibility [14; 15]. A false contractual assurance about a dataset may therefore raise a different claim from harm suffered by the person whose information becomes identifiable. Neither follows automatically from the word “re-identified.” The claimant’s right, the defendant’s duty, the relevant act, causation and the legally required proof must be examined. Measures that stop further disclosure should likewise not be confused with an award of money.

The assessment record can help establish what was known and promised without becoming conclusive evidence. Article 72 of the Civil Procedure Code governs the parties’ proof obligations, while Articles 68 and 73 concern evaluation and production of evidence [22]. A court must still examine completeness, reliability and relevance. The absence of a record cannot simply be declared proof of a particular amount of loss. Conversely, producing a signed record cannot defeat contrary evidence that a usable identifying link was ignored. The proposed obligation improves the material available for evaluation; it does not decide the dispute in advance.

The analysis supports two drafting options focused on the transfers already covered by Article 17(1). Neither creates a general ownership right in anonymous information or relaxes the existing outcome standard. Their added value is to make the basis and continuing limits of reliance on de-identification explicit. The following English texts are research proposals. They are not existing law or official translations, and their incorporation would require coordination with the implementing rules, including the masking and hashing requirements noted above.

The first option is a new paragraph 4: “Before transferring data under paragraph 1 of this Article, the owner, operator or third party making the transfer shall document the assessment of whether the de-identification requirements are met. The assessment shall identify the dataset version,

the method applied, the transfer and access conditions, and the additional information considered when assessing attribution to a data subject. It shall state the grounds and limits of the conclusion and identify the person responsible for the assessment. A description of the method alone does not establish compliance.”

This option does not require a new independent certificate for every transfer. The responsible organisation may use existing technical reports and contractual documentation, provided that they answer the stated questions. It also does not create authority to send data that fail the substantive standard. Its purpose is evidential clarity: the organisation invoking de-identification must be able to explain the result it relies on. More detailed procedures can vary with the dataset and release setting without turning the legislation into a catalogue of quickly ageing technical methods.

The second option is a new paragraph 5: “For transfers under paragraph 1 of this Article, where transfer or access conditions materially change, or credible information indicates that the transferred data may be attributable to a data subject, the transferring person shall review the assessment without undue delay and before making further transfers in reliance on its previous conclusion. Pending that review, it shall suspend such further transfers where compliance cannot be established. Known recipients shall be informed of a change in the conclusion to the extent necessary for lawful protection measures. This paragraph does not authorise otherwise unlawful processing or retention of identifying information.”

The second text deliberately limits the immediate suspension to further transfers relying on the disputed conclusion. It does not order every recipient to destroy everything, cancel unrelated processing or accept liability without investigation. Existing law determines the appropriate protection, notification, restriction or deletion duties in the circumstances. A credible security report should trigger examination, not be treated as proof that its author committed an offence. The proposal also does not authorise intrusive testing of real individuals. Testing, like other processing, requires a lawful basis and limits appropriate to its purpose.

There are costs and limits. Assessments take time, recipients may possess information unknown to the sender, and publicly released copies may be impossible to recall. These difficulties support proportionate records and controlled disclosure where appropriate; they do not support an assurance of perfect recoverability. The proposals need practical evaluation against existing procedures, including the full implementing rules. Useful measures would include whether assessments identify their scope, whether changes are noticed, and whether protective actions are traceable. No reduction in breaches or compliance costs has been measured by this article.

The legal regime of de-identified data cannot be determined by a missing name or a completed technical step. Kazakhstan already regulates de-identification, anonymisation, masking, linking information and the conditions of data-product circulation. The first result of this study is to distinguish the lawfulness of the input, the demonstrated result of transformation, and the authority for the later use. None of these questions can safely substitute for the others.

The second result is a release-specific assessment model. It connects the dataset version with the relevant information, recipients, uses and conditions, while keeping the statutory standard separate from a technical estimate of risk. European material helps test these distinctions but does not establish Kazakhstan's judicial position. The third result consists of two drafting options for Article 17: documented assessment and review after a material change or credible new evidence. These address protection mechanisms and concrete legislative development under the project's 2026 research tasks. Their value lies in making a legal conclusion explainable and reviewable, not in adding another reassuring label to a file.

Funding. *This research was prepared with the financial support of the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan under project AP23489796, "Problems of Regulating the Legal Regime of Big Data: Domestic and International Experience."*

References

1. Ohm P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization // *UCLA Law Review*. 2010. Vol. 57. P. 1701–1777. Publisher’s article page.
2. de Montjoye Y.-A., Hidalgo C. A., Verleysen M., Blondel V. D. Unique in the Crowd: The privacy bounds of human mobility // *Scientific Reports*. 2013. Vol. 3. Article 1376. DOI: 10.1038/srep01376. MIT research repository.
3. Republic of Kazakhstan. Law of 21 May 2013 No. 94-V On Personal Data and Their Protection. Articles 1, 7, 9–10, 12, 16–17, 22–24. Read together with the applicable 2026 amendments, including Law No. 326-VIII; the cited online consolidation does not display all June amendments in the main text. Statutory text in Russian.
4. Republic of Kazakhstan. Law of 24 June 2026 No. 326-VIII on amendments concerning digitalisation, personal-data protection, road traffic and advanced transport technologies. Article 1(37), amending the Personal Data Law; Article 2, commencement provisions. Text of the amending law in Russian.
5. Republic of Kazakhstan. Order of the Minister of Digital Development, Innovations and Aerospace Industry of 21 October 2020 No. 395/HK, approving the Rules for the Collection and Processing of Personal Data. Registered on 23 October 2020, No. 21498. Paragraphs 20–21. Text of the Rules in Russian.
6. Republic of Kazakhstan. Digital Code of 9 January 2026 No. 255-VIII. Articles 16, 30 and 41. Provisions are analysed for the research date, not retrospectively applied to earlier cases. Text of the Code in Russian.
7. Schwartz P. M., Solove D. J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information // *New York University Law Review*. 2011. Vol. 86, no. 6. P. 1814–1894. Full article, university repository.
8. Finck M., Pallas F. They who must not be identified—distinguishing personal from non-personal data under the GDPR // *International Data Privacy Law*. 2020. Vol. 10, no. 1. P. 11–36. DOI: 10.1093/idpl/ipz026. Authors’ institutional publication record.
9. Stalla-Bourdillon S., Knight A. Anonymous Data v. Personal Data—A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data // *Wisconsin International Law Journal*. Vol. 34, no. 2. P. 284–322. Publication year 2017 in the author’s institutional record; 2016 author preprint consulted. Author preprint; Institutional publication record.
10. Mourby M., Mackey E., Elliot M., Gowans H., Wallace S. E., Bell J., Smith H., Aidinlis S., Kaye J. Are ‘pseudonymised’ data always personal data? Implications of the GDPR for administrative data research in the UK // *Computer Law & Security Review*. 2018. Vol. 34, no. 2. P. 222–233. DOI: 10.1016/j.clsr.2018.01.002. Authors’ institutional publication record.
11. European Parliament and Council. Regulation (EU) 2016/679 of 27 April 2016 (General Data Protection Regulation). Recital 26; Articles 4(1), 4(5) and 11. Official EU text.

12. Republic of Kazakhstan. Order of the Deputy Prime Minister—Minister of Artificial Intelligence and Digital Development of 3 September 2026 No. 535/HK, approving the Rules on Applying Masking and Hashing Methods. Only the available opening provisions and document particulars were examined; the full technical instructions were not accessible. Document record and available statutory excerpt.

13. Tene O., Polonetsky J. Big Data for All: Privacy and User Control in the Age of Analytics // *Northwestern Journal of Technology and Intellectual Property*. 2013. Vol. 11, no. 5. P. 239–273. Publisher’s article page.

14. Republic of Kazakhstan. Civil Code (General Part) of 27 December 1994. Articles 126 and 350. Text of the Code in Russian.

15. Republic of Kazakhstan. Civil Code (Special Part) of 1 July 1999 No. 409-I. Articles 917 and 1017–1019. Text of the Code in Russian.

16. Court of Justice of the European Union. An operator of a website may have a legitimate interest in storing certain personal data relating to visitors to that website in order to protect itself against cyberattacks. Press release No. 112/16, 19 October 2016, concerning Patrick Breyer v Bundesrepublik Deutschland, C-582/14. The article relies on this official account, not an independently reviewed full case record. Official Court press release.

17. Court of Justice of the European Union. Judgment of 4 September 2025, European Data Protection Supervisor v Single Resolution Board, C-413/23 P. ECLI:EU:C:2025:645. Paragraphs 73–78, 99–115 and operative part. Full judgment.

18. European Parliament and Council. Regulation (EU) 2018/1725 of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data. Articles 3(1), 3(6) and 15(1)(d). Official EU text.

19. Purtova N. The law of everything. Broad concept of personal data and future of EU data protection law // *Law, Innovation and Technology*. 2018. Vol. 10, no. 1. P. 40–81. DOI: 10.1080/17579961.2018.1452176. Author’s institutional publication record.

20. Rubinstein I. S., Hartzog W. Anonymization and Risk // *Washington Law Review*. 2016. Vol. 91, no. 2. P. 703–760. Publisher’s article page.

21. Stalla-Bourdillon S. Identifiability, as a Data Risk: Is a Uniform Approach to Anonymisation About to Emerge in the EU? // *European Journal of Risk Regulation*. 2025. Vol. 16, no. 4. P. 1456–1474. DOI: 10.1017/err.2025.16. First published online 30 June 2025. Full article.

22. Republic of Kazakhstan. Civil Procedure Code of 31 October 2015 No. 377-V. Articles 68, 72 and 73. Text of the Code in Russian.

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ МЕРЫ БОРЬБЫ С КОМПЬЮТЕРНЫМИ ПРЕСТУПЛЕНИЯМИ

Одной из наиболее актуальных проблем правовой охраны компьютерной информации является определение понятия "компьютерное преступление". Общепринятого определения в науке уголовного права еще не предложено. При этом, следует отметить, что его отсутствие является не только теоретической проблемой, оно также значительно усложняет деятельность правоохранительных органов по противодействию преступлениям в сфере использования компьютерной техники.

Компьютерные преступления, любое противоправное действие, при котором компьютер выступает либо как объект, против которого совершается преступление, либо как инструмент, используемый для совершения преступных действий. К компьютерным преступлениям относится широкий круг действий, которые можно разделить на четыре категории: кража компьютерного оборудования; компьютерное пиратство (незаконная деятельность в сфере программного обеспечения); несанкционированный доступ к компьютерной системе в целях повреждения или разрушения информации; использование компьютера для совершения противозаконных или мошеннических действий. Поскольку компьютерные системы получают все более широкое распространение, а деловые круги во все большей степени полагаются на компьютеры и часто хранят на них конфиденциальную информацию, преступники находят все больше путей использования компьютеров для совершения противоправных действий.

Кража компьютерного оборудования.

Наиболее очевидной формой компьютерных преступлений является кража компьютерного оборудования и компонентов из

мест их производства, продажи или эксплуатации. Воры похищают компьютеры, принтеры и другое оборудование, чтобы нажиться на их перепродаже. Украденные изделия обычно продаются на черном рынке. Компьютерная отрасль положила начало «серому» рынку, который, строго говоря, не считается нелегальным, но действует, не используя общепринятые каналы распространения и продаж. На сером рынке неофициальные дилеры продают товары, купленные в других странах по более низким ценам или у какого-нибудь официального дилера, закупившего, в расчете на значительную скидку от изготовителя, больше аппаратуры, чем он был в состоянии продать. Компьютеры, продаваемые на сером рынке, зачастую имеют поврежденные заводские номера и не обеспечиваются гарантией.

Компьютерная техника и микросхемы обладают высокой стоимостью. Один лишь микропроцессор, интегральная схема или группа микросхем, предназначенных для обработки информации, могут стоить 100 долл. и более. Микропроцессоры и другие компьютерные микросхемы не имеют заводских номеров, что затрудняет их отслеживание. Высокая ценность таких микросхем и трудность идентификации делают их мишенью преступных организаций, которые часто продают похищенные микросхемы на рынках в считанные часы после хищения. Чтобы ограничить воровство микропроцессоров, изготовители микросхем разрабатывают различные способы гравировки заводских номеров на микросхемах или внесения идентифицирующей информации в цепь микросхемы. Организованные преступные группы проявляют изобретательность и расширяют масштабы грабежа компаний, выпускающих микропроцессоры, схемы памяти и другие компоненты компьютеров. Ежегодно стоимость микросхем и других компонентов, похищенных в «Кремниевой долине» (шт. Калифорния; иногда называемой также «Силиконовой долиной») оценивается в 100 млн. долл. В 1996 органы поддержания правопорядка в США раскрыли несколько преступных группировок, действовавших в сферах высокотехнологичных отраслей, обнаружив и изъяв у них электронные компоненты на миллионы долларов.

Пиратское использование программного обеспечения.

Компьютерные программы защищены авторским правом, и, следовательно, их нельзя репродуцировать и использовать без разрешения правообладателя. Пиратские действия в области программного обеспечения – это несанкционированное копирование компьютерных программ для собственного пользования или перепродажи. Часто какая-либо компания или физическое лицо, которые приобрели, например, одну копию той или иной программы, полагают, что это дает им право копировать данную программу. В действительности такое копирование противозаконно до тех пор, пока оно не будет разрешено специальным соглашением (лицензией), оговаривающим условия ее использования.

Некоторые люди, стараясь не нарушать законы, все же покупают копию программного обеспечения, а не оригинальную программу у того, кто ее выпускает. Незаконное тиражирование копий программ и продажа фальшивых версий популярного программного обеспечения осуществляется в широких масштабах. Нарушение авторских прав и пиратство в области компьютерного программного обеспечения оказались также в центре международных экономических отношений. Фальшивые программные средства можно приобрести по очень низким ценам на блошиных рынках, в розничной торговле, на восточных базарах и в других слабо контролируемых местах торговли [1].

Хакерство.

Один из видов компьютерных преступлений называют «хакерством» (этот термин относится к несанкционированному входу в компьютерную систему). Чтобы получить доступ к «защищенной» компьютерной системе или сети, пользователь должен иметь пароль. Хакеры пользуются множеством разных способов для того, чтобы распознавать секретные пароли или обойти парольную защиту системы. Возможность вторжения в компьютеры по телефонным сетям и через сложным образом связанные между собой компьютерные системы, не оставляя после себя отпечатков пальцев или следов, существенно затрудняет идентификацию и задержание хакеров [2].

Оказавшись «внутри» компьютерной системы, хакер может изменить, удалить или скопировать данные, хранящиеся в сети. Хакер может собрать конфиденциальную личную и финансовую информацию о компаниях и отдельных лицах, а затем использовать ее с помощью вымогательства или путем банковского мошенничества. Он может перехватить информацию, передаваемую по линиям связи, скопировать данные, передаваемые по сети Интернет, зафиксировать номера кредитных карточек и личные пароли. Хакер может ввести в систему программные коды или изменить существующие, в результате чего компьютеры будут выполнять команды этого хакера. Так, например, хакер может разместить небольшую программу на одном из сетевых серверов, чтобы собрать пароли законных пользователей сети. Располагая паролями, хакер затем может снова проникнуть в сеть, но уже с меньшими трудностями. Со времени появления персонального компьютера хакеры многократно вторгались в компьютерные системы, чтобы манипулировать данными всеми мыслимыми способами – от исправления своих школьных оценок и счетов за телефонные разговоры до «вторжения со взломом» в кажущиеся надежно защищенными системы правительственных и финансовых организаций. Хотя такие действия противозаконны, не все хакеры действуют с преступными намерениями. Многие из них при этом пытаются решить ту или иную техническую задачу либо преодолеть систему защиты компьютера в целях самоутверждения. Поскольку термин «хакер» может иметь и положительное значение, дающее образ смышленного программиста, способного соединить в одно целое коды программ и заставить компьютеры выполнять сложные задания, то тех, кто вламывается в компьютерные системы с преступными намерениями, называют «взломщиками» (crackers). Термин «телефонные жулики» (phone phreaks) используется для характеристики людей, детально разбирающихся в телефонных системах и использующих свои знания и опыт для того, чтобы делать телефонные вызовы, которые не поддаются прослеживанию и за которые телефонная компания не в состоянии выставить счет.

Хакеры, кракеры и телефонные жулики – это обычно молодые люди, и Интернет служит для них виртуальным сообществом, где

они могут поделиться своими секретами и другой информацией, а также похвастаться своими «подвигами». Поскольку ни одно правительство не имеет юрисдикции над киберпространством и Интернет вообще трудно защитить обычными законами, глобальная сеть оказалась привлекательной сферой действий для хакеров. В то же время Интернет стал одним из новых средств борьбы с преступностью, так как полиция использует собираемую по сети информацию для отслеживания и задержания лиц, совершающих противоправные действия [3].

Программные вирусы.

Программный вирус – это компьютерная программа, рассчитанная на то, чтобы нарушить нормальное функционирование компьютера. Вирус можно рассматривать как досадную помеху, но повреждение, которое он способен причинить хранящимся данным, является преступлением. Хакеры, пишущие такие программы, подвергаются арестам, судебным преследованиям и наказаниям за совершенные ими правонарушения. Обычно вирусная программа встраивается в другую внешне вполне безобидную программу, например такую, как утилита для обработки текста, которую можно бесплатно получить из сети Интернет или из какой-либо другой компьютерной системы с электронной доской объявлений. Когда такая утилита исполняется на компьютере, он освобождает вирус, который выполняет те несправедливые дела, на которые его запрограммировали. Некоторые вирусы скорее пустячные или фривольные, нежели злобные. Они могут воспроизвести на экране эксцентричное сообщение и затем стереть его из памяти компьютера, чтобы нельзя было проследить их происхождение. Однако многие вирусы повреждают основные характеристики компьютера или данные. Известны вирусы, копирующие себя в память компьютера, что вызывает замедление работы компьютера, вплоть до его предельной перегрузки вирусом и невозможности выполнения своих задач. Вирус может также стереть важные компьютерные файлы или разрушить и даже уничтожить данные на жестком диске. Большинство вирусных программ написано способными программистами в качестве эффектных трюков, демонстрирующих высокий уровень их

технических знаний. Чтобы противодействовать таким вирусам, компании разрабатывают программы обнаружения вирусов, которые распознают и удаляют вирусы из зараженных компьютеров, а также защищают компьютеры от инфицирования.

Компьютерное мошенничество.

Компьютеры могут быть использованы и в качестве инструментов для совершения различных преступлений, начиная от распространения противозаконных материалов и кончая содействием бизнесу, основанному на мошенничестве [4].

Список использованных источников

1. Расследование преступлений в сфере компьютерного контрафакта // Гурьянова Г.К.
2. Специфика организации правоохранительной деятельности при расследовании преступлений в сфере компьютерного контрафакта // Гурьянова Г.К.
3. Интернет-ресурс: <http://www.krugosvet.ru/>
4. Оксфордская иллюстрированная энциклопедия. Под ред. Р. Хоггарта, 2002 г.

Жәнібеков А.К.

*Ә.Қуатбеков атындағы Халықтар достығы университеті.
Жастар саясаты және әлеуметтік даму жөніндегі проректор*

ҚОРҒАУШЫНЫҢ ҚЫЛМЫСТЫҚ ІС ЖҮРГІЗУДЕГІ ҚҰҚЫҚТЫҚ МӘРТЕБЕСІН АРТТЫРУ МӘСЕЛЕЛЕРІ

Азаматтық және саяси құқықтар туралы Халықаралық пактінің 14-бабының 3 тармағына сәйкес, әрбір адам өзіне тағылған кез келген қылмыстық айыпты қарастырған кезде өзін қорғауға жеткілікті түрде дайындалуға; өзі таңдаған адвокат-қорғаушымен қарым-қатынаста болуға; өзін өзі қорғауға не өзі таңдаған адвокаттың көмегіне жүгінуге; егер адвокаты жоқ болса, сондай құқығы бар екені туралы хабардар болуға; мүмкіндігі болмаған жағдайда тегін адвокатпен қамтамасыз етілуге құқылы.

Осы аталған құқықтарды білікті және мемлекеттік билік органдарынан тәуелсіз заңгерлердің көмегімен жүзеге асыру мүмкін емес. Қылмыстық сот төрелігінің эволюциясы нәтижесінде,

қылмыстық және азаматтық істер бойынша кәсіби білікті құқықтық қорғауды жүзеге асыру функциясы құқықтанушы-адвокаттардың қолдарына шоғырланды деуге болады.

Отандық адвокатура ресейлік адвокатурамен сабақтас болып табылатыны айқын. Адвокатураның толық дамуы тәуелсіз сот, тараптардың шынайы тепе-теңдігі мен бәсекелестігі болған кезде ғана мүмкін болады. Олар, өз кезегінде, биліктің тармақтарға бөліну, тепе-теңдік тежемелік жүйесі сияқты қағидаларға негізделген демократиялық және құқықтық мемлекетте ғана қалыптасып, дами алады. Диктаторлар мен тоталитарлық режимдер адвокатураны өздерінің шексіз билігін шектеуге бағытталған институт ретінде қарастырған. Бұл шынында да солай деуге болады. Тіпті адвокаттар күмәнді субъектілер ретінде қарастырылатын. Олар өз клиенттері – қорғанушылары үшін кез келген іс-әрекетке баруға дайын тұратын тұлғалар деп сипатталатын.

Кеңестік дәуірде тәуелсіз адвокатураның дамуына мүмкіндік болмады. Өйткені коммунистік режим адвокаттарды толыққанды субъектілер ретінде танымады. Кеңестік мемлекеттің адвокатураға қатысты қатынасы саяси жүйенің қаталдығына қарай құбылып отырды. Онда адвокатураны мүлдем жою, оны әлсіз институт ретінде құру сияқты талпыныстар болды.

Қазақстан өз тәуелсіздігіне ие болған сәттен бастап адвокаттардың құқықтық мәртебесі мен адвокаттық қауымдастықты ұйымдастыру бірте-бірте заңнамада нақтылана түсіп, өз даму жолын қалыптастырды. 1997 жылғы 5 желтоқсанда бүгінгі күнге дейін өз күшінде болып табылатын «Адвокаттық қызмет туралы» заң қабылданды. Бұл заң адвокатураға белгілі бір деңгейде өз тәуелсіздігін сақтауға, ал адвокаттарға өз қызметін қолайлы жағдайда жүзеге асыруға мүмкіндік береді. Адвокаттар алқасының құқықтық жағдайы, кәсіби сословие мүшелерінің өздерінің өкілеттіктері, адвокат мәртебесін иелену және одан айырылу тәртібі, құқықтық көмекке жүгінетін тұлғалармен қарым-қатынасқа түсудің негіздері, адвокаттық қызметтің кепілдері және тағы да басқа елеулі мәселелер ретке келтірілді.

Қылмыстық сот өндірісінде қорғаушылардың құқықтары кеңейтіліп, нақтыланған болатын. Соның ішінде дәлелдемелерді

жинақтау, процесске ерте ену, куәгерлік иммунитетке деген құқық, іс материалдары құжаттарының көшірмелерін алу, қылмыстық қудалау органдарының заңсыз іс-әрекеттеріне сот тәртібінде шағым келтіру, қылмыстық іске қатысты ақпаратқа ие тұлғалардан сұрау алу, сараптама өткізуге бастама көтеру және т.б. құқықтар нақтыланды. Жалпы айтқанда, осы саладағы өзгерістер жеткілікті түрде динамикалық және бір ізді болған жоқ, бірақ олар позитивті сипатта болды. Бәрі де салыстырмалы түрде айтылатын болғандықтан, бүгінгі таңда Қазақстандағы адвокатура Орталық Азияның басқа мемлекеттеріне қарағанда озық және дамыған болып табылады.

Бүгінгі таңда адвокат қолданыстағы заңнамаға сәйкес сотөндірісінің белсенді қатысушысы бола алады және тиісті істің тағдырына белгілі бір ықпал ете алады. Дей тұрғанмен, заңнама мен құқыққолдану тәжірибесіндегі жағымды үрдістің болғанына қарамастан, орын алған жағдай үлгілі болудан әлде қайда қашық деуге болады.

Адвокат көбіне инквизициялық қылмыстық сот өндірісінде демократиялық декорация іспеттес рөлде. Қорғаушылардың шағымдары мен ұсынымдары көбіне ескерусіз қалады, не формальды жауапқа ғана ие болады. Айыпталушылар мен олардың адвокаттардың бұзылған құқықтарына прокуратура да, сот та көз бояушылықпен қарайды. Адвокаттардың өздері кейде процессуалды оппоненттерінің заңсыз қудалауына түсіп жатады. Адвокатураның тәуелсіздігіне берілген кепілдік жиі бұзылады. Адвокаттардың офистерінде заңсыз тінту жүргізу, адвокаттық құпияға қатысы бар тиісті құжаттарды тартып алу фактілері жиі кездеседі. Адвокаттар өздеріне қатысты жедел-іздістіру іс-әрекеттері орын алатынына шағымданады. Бір сөзбен айтқанда, адвокаттың құқықтық және әлеуметтік мәртебесіне қатысты тиісті құрмет жоқ.

Қазақстанда соттармен шығарылатын үкімдердің басым көпшілігі айыптау сипатына ие. Осындай жағдайда адвокат қылмыстық іс жүргізуде «бейшара сұраушы» деген теңеу өз өзектілігін сақтауда. Осы орайда қалыптасқан тәртіпті жетілдіру айқын болып табылады. Адвокаттың қоғамдағы орны, соған сәйкес,

қылмыстық процестегі қорғаушы рөлі лайықты деңгейге көтерілуге тиіс. Бұл ұстаным жай ғана корпоративті мүддені қорғау болып табылмайды. Іс жүзінде, қылмыстық іс жүргізудің тұтас жүйесі қайта қаралуға тиіс деп ойлаймыз. Мәселеге осындай ұстаныммен қарайтын болсақ, тараптардың теңдігі мен бәсекелестігін, қылмыстық істерді қараудың объективтігі мен әділ қаралуын қамтамасыз ету қажет. Бұл өз кезегінде қылмыстық істер бойынша сот өндірісі кезінде адам құқықтарының сақталуын қамтамасыз ететін негізгі субъект болып табылатын қорғаушының құқықтық мәртебесін дамытуды, жетілдіруді меңзейді.

Объективті зерттеуші үшін адвокатураның жетілдірілуі шынайы тәуелсіз сот билігін орнатусыз мүмкін болмайтыны айқын [1, 65 б.]. Бұл мәселе, өз кезегінде, өтпелі кезеңдегі елдер үшін құқықтық аяға қарағанда саяси аяға жататын мәселе болып табылады. Қоғам, халық және мемлекет әлеуметтік эволюцияның белгілі бір деңгейіне жетпегенше, сот билігі мемлекеттік билік жүйесінде өзіне лайықты орынға ие бола алмайды. Оған дейін, адвокаттардың қызметіндегі елеулі кедергілер мен кемшіліктер олардың кәсіби қызметінде болатыны анық.

Дей тұрғанмен, жоғарыда атап өткен әлеуметтік эволюция құқықтық қамтамасыз ету тұрғысынан қолдауды қажет етеді. Сол себептен заңнаманы жетілдіру және қорғаушының құқықтық мәртебесін дамыту процесін жалғастыра беру керек. Реформаның қажеттілігі туралы сезім саяси элитада да бар. Оған дәлел ретінде қазіргі таңда Парламентте талқыланып жатқан жаңа қылмыстық іс жүргізу кодексінің жобасы дәлел бола алады.

Қолданыстағы қылмыстық іс жүргізу заңнамасына сәйкес, судья басты сот талқылауы сатысында тараптардың бастамасы бойынша сотқа келген тұлғалардан мамандар немесе куәгерлер ретінде жауап алу туралы өтінімді қанағаттандырудан бас тарта алмайды [2, 110 б.]. Осы норманы аналогия бойынша пайдалана отырып, тиісті өтінімдер берілген барлық жағдайларда дәлелдемелерді депонированиеге бойынша сот отырыстарын тағайындауға тиіс және осы сот отырыстарына келген тұлғалардан жауап алуға тиіс.

Қорғаушының өкілеттігін сот билігінің күшімен және беделімен қамтамасыз ету мақсатында, істің мән-жайын толық және жан-жақты зерттеу үшін маңызды болатын мәліметтерді кәсіпорындармен, мекемелермен, ұйымдармен және азаматтармен беру туралы сот бұйрығын қорғаушымен алу процедурасын заңда бекітуге болады деп ойлаймыз. Мұндай тетік қорғаушы тарабының дәлелдемелерді жинау құқығына кепілдік беретін тетік болар еді. Сондай-ақ, айыптаушы мен қорғаушы тараптарының құқықтық мүмкіндіктерін теңестіру мақсатында, жеке детективтік қызметті заңдастыруға және адвокаттың жеке детективтермен ынтымақтасуының құқықтық нысандарын реттеуге назар аударған жөн. Сот бақылауы - әділ қылмыстық процесс қағидаларын және тараптардың арасындағы балансты сақтауды қамтамасыз ететін бірден бір институт болып табылады. Өкінішке қарай, қолданыстағы заңнамада бұл институт тек бастаушы, толық емес сипатқа ие болып, процесске қатысушылардың қылмыстық қудалау органдарының іс-әрекетіне шағым келтіру мүмкіндігімен ғана шектелген.

Жаңа қылмыстық іс жүргізу заңнамасында сот бақылауын одан ары дамыту идеясы тергеу судьясы лауазымын құрумен байланыстырылған. Тергеуші судья ретінде қылмыстық қудалау органдарының іс-әрекеттері мен шешімдеріне келтірілген шағымдарды қарайтын және жекелеген тергеу әрекеттеріне санкция беретін аудандық соттың судьясы немесе оған теңестірілген судья бекітілді.

Біздің ойымызша, сот бақылауы функцияларын негізгі міндеттері қылмыстық істерді мәнісі бойынша қарастыру болып табылатын аудандық соттардың судьяларына жүктеу, судьялардың өздерінің толыққанды жұмыс істеуіне кедергі болады және сот төрелігін сапалы атқаруға жағымсыз әсер етеді. Өйткені, сот бақылауы мен қылмыстық істер бойынша сот төрелігін атқару – бір бірінен түпкілікті түрде ерекшеленетін функциялар болып табылады және сол себептен әртүрлі, бір біріне байланысты емес, бір бірінен автономды сот жүйелеріне жатататын судьялармен жүзеге асырылуға тиіс. Қорғаушы тарап үшін бұл мәселе елеулі болып табылады. Өйткені әділ және объективті, қылмыстық қудалау

органдарының ықпалынан еркін сот қана қылмыстық сот өндірісінің орбитасына тартылған тұлғалардың құқықтарын толыққанды жүзеге асыруды қамтамасыз ете алады. Қорғаушы сотқа жүгінгенде оның сөзіне құлақ асатынына, дәлелдемелері мәнісі бойынша әділ және адал қарастырылатынына сенімді болуға тиіс.

Қылмыстық процесске тергеу судьясы лауазымын енгізу тұжырымдамасы декоративті сипатқа ие екенін мойындау қажет. Өйткені ол іс жүзінде толыққанды сот бақылауын құру және қылмыстық процессте адам құқықтарын қорғауды білдірмейді.

Азаматтардың конституциялық құқықтарын шектейтін тергеу әрекеттерін жүргізуге санкция беруді тек сот қана жүзеге асыру керек. Сот бақылауы идеясының өзі құқыққорғау органдары ретінде шығатын атқарушы билік азаматтардың құқықтарына қысым жасағанда осы құқықтардың сақталуын тәуелсіз және әділ сот қоғауға тиіс дегенге саяды. Сол себептен, тінту, тұрғын үйінен еріксіз шығару, телефон арқылы сөздерін тыңдау, хабарламаларды алу және жеке өмірге қол сұғатын басқа да әрекеттер тек қана соттың санкциясымен жүзеге асуға тиіс.

ҚПК-те сотқа дейінгі кезеңде бас бостандығынан айыру гуманизация мен дамудың пәніне айналмағаны байқалады. Сотқа дейінгі алдын ала қамаудың жетпіс екі сағаттық мерзімі сақталған. Бұл сұрақ процессуалист ғалымдар мен заңгерлер арасында бұрыннан қызу талқыланып келе жатқан мәселелердің бірі болып табылады. Тіпті, Біріккен Ұлттар ұйымының адам құқықтары жөніндегі комиссиясының арнайы комиссары бұл мерзімді қырық сегіз сағатқа дейін қысқарту туралы Қазақстанға ұсыныс жасаған екен.

Азаматтық және саяси құқықтар жөніндегі Халықаралық пакт әрбір адамға өз таңдауы бойынша адвокатпен қорғана алу құқығының болуына кепілдік береді [3, 28 б.]. Бұл құқық әділ сот процесінің фундаменталды негіздерінің бірі болып табылады. Өйткені ол толыққанды қорғаудың басты шартын – айыпталушы мен оның адвокаты арасындағы сенімді қамтамасыз етеді, сонымен бірге осы сенімді және кәсіби қорғаушы мәртебесін асыра пайдалануға жол бермейді. Өкінішке қарай, бүгінгі таңда Қазақстанда адвокатты еркін таңда құқығы сол бір немесе өзге

адвокатта мемлекеттік құпияларға рұқсаты жоқ деген сылтаумен өрескел бұзу фактісі жиі кездеседі. Әсіресе аталған құқық ұлттық қауіпсіздік органдарының өндірісіндегі істер бойынша тергеу және сот тәжірибесінде кездеседі. Бұл орайда мемлекеттік құпияларға рұқсат алу тәртібі ашық қайнар көздерде жарияланбаған нұсқауларда реттелген. Рұқсат берудің өзі адвокатты арнайы тексерістен өткізуден кейін ғана мүмкін болады. Осылайша, алдын ала тергеу жүргізетін аталған органдар өздерінің процессуалдық оппоненттеріне рұқсат беру процесіне ықпал ете алады. Бұл, өз кезегінде, қылмыстық процесстегі тараптардың теңдігі мен бәсекелестігі тұрғысынан әділ емес. БҰҰ-ның адам құқықтары жөніндегі Комитеті өзінің бірқатар шешімдерінде адвокаттарды таңдау құқығын шектеуді заңсыз деп таныды.

Қылмыстылықтың алдын алу жөніндегі БҰҰ-ның сегізінші Конгресімен 1990 жылдың тамыз айында Нью-Йоркте қабылданған Негізгі ережелердің 19-тармағына сәйкес, сот немесе әкімшілік орган тәжірибеге рұқсаты бар адвокаттың құқықтарын танудан бас тартуға тиіс емес, егер бұл адвокат ұлттық құқыққа және тәжірибеге сәйкес дисквалификацияланбаған болса. ҚІЖК-нің жаңа жобасын талдай отырып, онда отандық заңнаманы тиісті саладағы халықаралық стандарттармен сәйкес келтіру идеялары жоқ екенін байқауға болады. Бұл жағдай тез арада түзетуді қажет етеді деп ойлаймыз.

Біздің ойымызша, қылмыстық қудалау органдарының қатаң бақылауымен рұқсат етудің дискриминациялық жария емес процедурасын адвокаттарға қатысты қолдануға болмайды. Қылмыстық процесті жүргізетін органдар адвокаттардан мемлекеттік құпияны қамтитын мәліметтерді жария етпеуі туралы жазбаша міндеттеме алуы жеткілікті болады. Бұл орайда ондай мәліметтердің көлемі мен тізімі нақты анықталуға тиіс және ол қылмыстық сот өндірісінің заңдылығы мен оған қатысушылардың құқықтарын сақтау туралы ақпаратты қамтымауға тиіс.

Адвокаттың құқықтық мәртебесінің негізін заңда көрсетілген өкілеттіктері ғана құрамайды, сонымен бірге сол өкілеттікті жүзеге асыруға мүмкіндік беретін заңдық тетіктер де құрайды. Сондай заңдық тетіктердің біріне, басқаларын айтпағанда, мемлекеттік

құқыққолдану органдарынан адвокаттың өзінің кәсіби міндеттерін атқару кезіндегі тәуелсіздігіне кепілдік беру жатады. «Адвокаттық қызмет туралы» заңның 17-бабында адвокаттық қызметтің кепілдіктері көзделген. Атап айтқанда, заңнамаға сәйкес жүзеге асырылатын адвокаттық қызметке араласуға не осы қызметке қандай да болмасын тәсілмен кедергі жасауға тыйым салынады. Адвокатты ол заң көмегін көрсетіп отырған адаммен теңдестіруге тыйым салынады. Адвокаттан өз кәсіби міндеттерін жүзеге асыруға байланысты оған мәлім болған мән-жайлар туралы куәгер ретінде жауап алуға тыйым салынады.

Адвокаттардан, олардың көмекшілері мен тағылымдамадан өтушілерінен, адвокаттар алқасы төралқасының, заң консультацияларының, адвокаттық кеңселердің басшылары мен қызметкерлерінен, заңмен белгіленген жағдайларды қоспағанда, белгілі бір адамға заң көмегін көрсетуге байланысты қандай да болмасын мәліметтер беруді талап етуге тыйым салынады. Адвокаттық іс жүргізу, онымен байланысты өзге де материалдар мен құжаттар, сондай-ақ адвокаттың мүлкі, оның ішінде ұялы байланыс құралдары, аудиоаппаратурасы, компьютерлік техникасы Қазақстан Республикасының заңдарында көзделгеннен басқа жағдайларда, тексеруге, қарауға, алуға, алып қоюға және тексеріске жатпайды. Адвокатқа өзі қорғайтын адаммен оңаша жолығудың құпиялылығын қамтамасыз ететін жағдайларда осылайша жолығуына рұқсат беруден бас тартуға, сондай-ақ олардың саны мен ұзақтығына шек қоюға тыйым салынады. Анықтау және сотқа дейінгі тергеу органдары, іс жүргізу заңында көзделген жағдайларда, адвокатпен келісілген мерзімде тергеу және өзге іс жүргізу әрекеттеріне оның қатысуы қажеттігі туралы адвокатқа хабарлауға міндетті. Мемлекеттік қызметшілер және мемлекеттік емес ұйымдардың басшылары адвокаттың нақты іс бойынша заң көмегін көрсетуіне байланысты өтінішіне он жұмыс күні ішінде жазбаша жауап беруге міндетті. Адвокаттардың қызметіне заңсыз араласуға жол берген немесе осындай қызметті жүзеге асыруға кедергі келтіретін адамдар заңға сәйкес жауапқа тартылады.

Өкінішке қарай, тәжірибе көрсеткендей, аталған тетіктер тиімді емес. Іс жүзінде адвокаттар өздері қорғайтын тұлғалар сияқты

қорғаусыз болып табылалы. Адвокаттардың офистері санкциясыз тінтуге тап болуы мүмкін, оларға қатысты арнайы жедел-ізвестіру шаралары қолданылу мүмкін.

Заңнамалық деңгейде адвокаттардың мәртебесін нығайтатын нормалар қабылдау қажет екені сөзсіз. Осыған орай адвокаттық және жедел-ізвестіру қызметі туралы заңнамаға адвокаттарды конфиденциалды негізде құқыққорғау органдарымен ынтымақтасуға тартуға тыйым салыну керек. Мұндай ынтымақтастық этикалық тұрғыдан да дұрыс емес және қылмыстық процестегі тараптардың теңдігі мен бәсекелестігі қағидасын бұзады. Адвокаттар алқасына алдыңғы заңдық тәжірибе барысында өздерінің беделіне нұқсан келтірген тұлғаларды қабылдаудан бас тарту құқығы берілсе деген ұсыныс бар. Әрине, адвокаттар алқасының ондай шешімдері тиісті түрде ресімделуге тиіс және қажет болған жағдайда сот тәртібінде шағымдалуға тиіс.

Адвокаттарға қатысты тәртіптік өндіріс адвокаттар қауымдастығы органдарының айрықша құзырында болған жөн. Өкінішке қарай, бүгінгі таңда бұл мәселе заңнамада екі мағыналы түрде реттелген. ҚПК ережелерін талдау, өкінішке қарай, бұл нормативтік құқықтық акті қылмыстық сот өндірісін толыққанды реформалауды көздемейді деген түйін жасауға болады. Ойымызды қорытындылай келе мынадай ұсыныстар жасауға болады.

1) Қылмыстық процесте толыққанды сот бақылауын енгізу керек. Ол үшін сот жүйесінің өз алдына дербес құрылымын құру қажет. Онда процестің сотқа дейінгі сатыларында адам құқықтарының сақталуын және заңдылықты қамтамасыз етуге жауапты судьялар ғана болуға тиіс. Ондай судьялардың құзырына адамның конституциялық құқықтарын шектеуді көздейтін барлық іс-шараларға санкция беру жатқызылу керек.

2) Қылмыстық процестік кодексте адвокаттардың дәлелдемелерді жинау өкілеттігін одан дамыту және нақтылау қажет. Соның ішінде, фактілік мәліметтерді депонирование, сараптамалар тағайындау мен жүзеге асыру, жеке детективтік қызметтің мүмкіндіктерін пайдалану процедуралары нақтылануға тиіс.

3) Ұстау мен қамауға алудың процессуалды тәртібін халықаралық стандарттарға сәйкес келтіру керек. Атап айтқанда, қамауда ұстау мерзімін 48 сағатқа дейін қысқартып, әрбір ұсталғанның жеке бас бостандығын шектеудің заңдылығы мен негізділігіне сот бағалауын беруді міндетті ету керек.

4) Азаматтардың конституциялық құқықтарын шектейтін тергеу әрекеттері мен жедел-ізвестіру іс-шараларын біртұтас процессуалды нысан аясында унификациялау керек және сол нысанды қылмыстық іс жүргізу заңнамасында ретету қажет.

5) Адвокаттардың өздерінің кәсіби қызметтерін жүзеге асыруына байланысты жеке басына құлсұқпаушылығына деген кепілдікті күшейту және жетілдіру керек. Атап айтқанда, олардың телефон байланыстарын заңсыз тыңдауға, жазуға тыйым салу, қызметтік және тұрғын жайларына кез келген нысанда заңсыз басып кіруге тыйым салу қажет.

6) Заңнамада адвокаттарды жасырын түрде құқыққорғау органдарымен ынтымақтасатын тұлғалар ретінде тартуға тыйым салу керек.

7) Адвокаттарды өздерінің кәсіби қызметін жүзеге асыруға байланысты жасаған заңды әрекеттері үшін қылмыстық, азаматтық-құқықтық және әкімшілік тәртіпте қудалауға тыйым салу керек, соның ішінде адвокаттардың бұқаралық ақпарат құралдары мен сот отырысы залдарында жария түрде айтақан сөздері үшін де қудалауға тыйым салу.

8) Адвокаттардың барлық категориялы, соның ішінде мемлекеттік құпияны қамтитын, істерге қатысуына рұқсат ету қажет. Бұл орайда олардан өздеріне белгілі болған мемлекеттік құпиялы мәліметті жария етпеу туралы арнайы міндеттеме алу жеткілікті деп ойлаймыз.

9) Адвокаттар алқасының президиумына лицензиясы бар, бірақ алдыңғы заңнамалық кәсіби тәжірибесі барысында өздерінің беделіне нұқсан келтірген тұлғаларды қабылдаудан бас тарту құқығын беру қажет. Бұл адвокаттар алқасына шынайы білікті және лайықты адвокаттарды тартуға стимул болып табылады.

Әдебиеттер тізімі

1 Қоғамов А.М. Защитник-адвокат в контексте проекта новой редакции Уголовно-процессуального кодекса Республики Казахстан // Право и Государство. №3 (60), 2013. – 63-68 с.

2 Тащилина С.М. Адвокат и суд присяжных в России. М.: Юридическая литература, 2001. – 150 с.

3 Торьянников, А.Г. Адвокат в уголовном процессе (Деятельность адвоката по оказанию юридической помощи обвиняемому в реализации прав на заявление ходатайств и принесение жалоб): Учебное пособие. М.: ВЮЗИ, 1987. – 235 с.

Казбекова А.

ОТВЕТСТВЕННОСТЬ ПРИ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: КИБЕРРИСКИ В РЕСПУБЛИКЕ КАЗАХСТАН. ПОЧЕМУ ЭТО ВАЖНО ПРЯМО СЕЙЧАС

Вопрос об ответственности за использование технологий уже перестал быть теоретическим и стал практической необходимостью для бизнеса и государства. Распространение алгоритмов, автоматизированных решений и систем искусственного интеллекта неизбежно сопровождается рисками: ошибки в работе систем, дискриминирующие решения, утечки данных, вводящие в заблуждение ответы цифровых сервисов. В таких ситуациях ключевой становится не столько сама техническая ошибка, сколько вопрос о том, кто должен нести за нее юридическую ответственность.

Размытость ролей между разработчиками, поставщиками технологий и компаниями, внедряющими решения, существенно усложняет определение субъекта ответственности. Традиционные правовые конструкции не всегда позволяют однозначно квалифицировать такие случаи, особенно когда решение принимается автономной системой без прямого вмешательства человека.

В условиях активной цифровизации данный вопрос приобретает особую актуальность для Республики Казахстан, где

формируется и постепенно вступает в силу нормативная база, регулирующая использование таких технологий. Настоящая статья посвящена анализу того, как действующее и планируемое законодательство Казахстана отвечает на вопрос распределения ответственности при использовании цифровых и ИИ-решений. В январе 2026 года вступил в силу **Закон РК «Об искусственном интеллекте»**, а в июле этого года вводится в действие **Цифровой кодекс**.

Еще один элемент этой новой реальности - Указ Президента от 9 июня 2026 года № 1311, которым утверждена Общенациональная стратегия масштабной цифровизации и тотального внедрения технологий искусственного интеллекта «Digital Qazaqstan» до 2029 года. Стратегия закрепляет переход к модели государства-платформы, тотальному внедрению ИИ и киберфокусу, а значит - к системному росту как возможностей, так и юридических и киберрисков.

ИИ - инструмент, а не субъект: главный принцип.

Прежде чем говорить о распределении ответственности - нужно обозначить базовый принцип, от которого все строится.

Искусственный интеллект не является субъектом права.

Это кажется очевидным - но на практике многие компании ведут себя так, будто именно ИИ отвечает за результаты своей работы. «Система так решила», «алгоритм так посчитал» - эти фразы часто звучат как попытка снять с себя ответственность. Но **Закон об ИИ прямо указывает: ИИ - инструмент**. Сложный, автономный, обучающийся - но инструмент. Ответственность за него несут люди и организации.

Закон устанавливает это недвусмысленно: **собственник, владелец и пользователь обязаны обеспечивать постоянный контроль** над системой ИИ на всех этапах ее жизненного цикла. Все субъекты, занимающиеся созданием и эксплуатацией систем ИИ, несут ответственность за деятельность этих систем и за их результаты.

Иными словами, **любое решение, принятое с использованием ИИ, юридически рассматривается как решение той организации, которая этот инструмент внедрила и применяет.**

Роль владельца: центр конструкции ответственности.

Закон об ИИ выстраивает модель распределенной ответственности. В ней есть разные роли: разработчик, интегратор, оператор данных, пользователь. Каждый отвечает за то, что в его зоне контроля.

Но в центре этой конструкции - **собственник и владелец системы ИИ**. Именно он принимает решение о внедрении, определяет цели использования, управляет жизненным циклом и несет ответственность за последствия.

Что требует Закон от владельца системы ИИ?

Во-первых: осуществлять управление рисками - непрерывно, на протяжении всего жизненного цикла системы. Выявлять риски, оценивать их, принимать меры, обновлять оценку не реже раза в год.

Во-вторых: обеспечивать безопасность и надежность системы, включая защиту от несанкционированного доступа и сбоев.

В-третьих: вести документацию, поддерживать пользователей, обеспечивать возможность ознакомиться с условиями использования до начала работы с системой.

Закон вводит **классификацию систем ИИ по степени риска**:

- минимальный риск - минимальное воздействие на пользователей при сбое;
- средний риск - снижение эффективности, материальный или моральный вред;
- высокий риск - возможность чрезвычайной ситуации, значительные последствия для экономики, безопасности, прав граждан.

При этом квалифицировать степень риска своей системы владелец обязан самостоятельно в соответствии с Правилами классификации объектов информатизации и классификатора объектов информатизации, утвержденных Приказом Министра по инвестициям и развитию РК. Это означает: уже сегодня каждый, кто внедряет систему ИИ, должен принять правовое решение о том, какую степень риска представляет его система - и нести ответственность за правильность этой оценки.

Ответственность: от административной до уголовной

Что именно грозит тем, кто не выполняет требования закона?

Административная ответственность: статья 641-1 КоАП РК

Эта статья охватывает два ключевых блока.

Первый: обязанность информировать пользователей о синтетическом характере контента, созданного или измененного ИИ, если он может ввести в заблуждение. Текст, изображение, видео, аудио - если это создал ИИ и выглядит «реальным», нужна маркировка.

Второй: обязанность управлять рисками систем ИИ высокой степени риска. Если этого нет - и в результате возник вред здоровью или благополучию людей, распространилась ложная или запрещенная информация, произошла дискриминация - это административное правонарушение.

Штрафы:

- физические лица - **15 МРП**^{*1},
- малый бизнес - **20 МРП**,
- средний - **30 МРП**,
- крупный бизнес - **100 МРП**.

При повторном нарушении штрафы увеличиваются; для отдельных категорий нарушителей они могут быть выше первоначального размера в несколько раз. И самое серьезное: при повторном нарушении закон допускает **приостановление или запрещение деятельности самой системы ИИ**.

Ответственность за кибербезопасность: статьи 639 и 641 КоАП

Также следует отметить ответственность по статье 639 КоАП РК. В случае воспрепятствования работе государственной технической службы или блокирования ее программных средств компания может быть привлечена к административной ответственности.

Санкция предусматривает предупреждение либо штраф в размере от 10 до 100 МРП в зависимости от категории нарушителя, при этом для субъектов крупного предпринимательства штраф составляет 100 МРП.

¹ МРП на 2026 год = 4 325 тенге

Параллельно действует ответственность за ненадлежащую защиту информационных систем. **Если компания не приняла меры по защите персональных данных или не уведомила Национальный координационный центр информационной безопасности об инциденте - это самостоятельное основание для привлечения к административной ответственности.**

Уголовная ответственность: УК РК

Уголовный кодекс содержит несколько релевантных составов: **ст. 205** - неправомерный доступ к информации; **ст. 206** - уничтожение или модификация информации; **ст. 207** - нарушение работы объекта информатизации; **ст. 208**- неправомерное завладение информацией. По критически важным объектам - до двух лет лишения свободы.

Эти составы применяются прежде всего к злоумышленникам. Но если организация, подвергшаяся атаке, **не обеспечила должного уровня защиты** - она может быть привлечена к административной или гражданско-правовой ответственности параллельно с уголовным преследованием виновных.

И здесь ст. 105 Цифрового кодекса закрепляет принципиально важное правило: **привлечение к административной или уголовной ответственности не освобождает от обязанности устранить допущенные нарушения.** Заплатить штраф - недостаточно.

Что это означает на практике: пять шагов

Первое. Инвентаризация систем ИИ. Определить, какие системы уже используются, провести их классификацию по степени риска. Это не только техническая, но и юридическая задача.

Второе. Договорная работа. Пересмотреть договоры с разработчиками и интеграторами. Прописать распределение ответственности четко: кто отвечает за технику, кто - за безопасность, кто несет риски при инциденте.

Третье. Внутренние политики. Разработать или актуализировать политику использования ИИ, обработки данных, кибербезопасности и реагирования на инциденты.

Четвертое. Обучение сотрудников. Люди, работающие с ИИ, должны понимать его ограничения, уметь выявлять аномалии,

знать, что делать в случае инцидента. Бездумное доверие алгоритму - источник правового риска.

Пятое. Мониторинг. Выстроить процессы регулярной переоценки рисков, тестирования на уязвимости, мониторинга инцидентов. Управление рисками - не разовая формальность, а непрерывный процесс.

Калиев Ж.А.

*Частнопрактикующий юрист по экономическим
и налоговым спорам, налоговый консультант*

ПРОБЕЛЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ БОЛЬШИХ ДАННЫХ (BIG DATA) В РЕСПУБЛИКЕ КАЗАХСТАН: ОТЕЧЕСТВЕННЫЙ И ЗАРУБЕЖНЫЙ ОПЫТ

В статье рассматриваются актуальные проблемы правового регулирования больших данных (Big Data) в Республике Казахстан в условиях цифровизации и развития технологий искусственного интеллекта. Анализируются существующие пробелы законодательства, связанные с определением правового статуса больших данных, их использованием, защитой персональных данных и обеспечением информационной безопасности. Особое внимание уделяется сравнительному анализу отечественного и зарубежного опыта регулирования Big Data. По результатам исследования сформулированы предложения по совершенствованию правового режима больших данных в Республике Казахстан.

Развитие цифровых технологий оказывает существенное влияние на современную систему общественных отношений. Технологии больших данных (Big Data) находят широкое применение в государственном управлении, финансовой сфере, здравоохранении, образовании, электронной коммерции и других секторах экономики. Их использование позволяет обрабатывать значительные массивы информации, выявлять закономерности

развития различных процессов, осуществлять прогнозирование и повышать качество принимаемых управленческих решений [1, с.6].

Активное развитие цифровой экономики обусловило появление качественно новых массивов информации, характеризующихся значительным объемом, высокой скоростью формирования и разнообразием источников происхождения. Обработка таких данных зачастую выходит за пределы возможностей традиционных информационных систем и требует использования специализированных технологических решений. В научной литературе отсутствует единый подход к определению понятия «большие данные» (Big Data). Одни авторы рассматривают Big Data как совокупность методов и технологий, предназначенных для анализа значительных объемов структурированных и неструктурированных данных с целью выявления скрытых закономерностей и прогнозирования различных процессов [2, с.9]. Другие исследователи связывают данное понятие прежде всего с информационными массивами, обработка которых невозможна с применением традиционных баз данных и требует использования специальных вычислительных инструментов и алгоритмов [3, с.3].

Для Республики Казахстан вопросы правового регулирования больших данных приобретают особую значимость в условиях последовательной реализации политики цифровой трансформации и внедрения технологий искусственного интеллекта. Развитие электронного правительства, государственных информационных систем, цифровых платформ и иных технологических сервисов сопровождается постоянным накоплением значительных объемов сведений о физических и юридических лицах, что обуславливает необходимость формирования эффективных правовых механизмов регулирования отношений, связанных со сбором, обработкой и использованием данных [4].

Несмотря на широкое распространение технологий больших данных в государственном и частном секторах, законодательство Республики Казахстан пока не сформировало самостоятельного правового механизма регулирования отношений, возникающих в связи с их использованием. Действующие нормативные правовые

акты, включая Закон Республики Казахстан «Об информатизации» и Закон Республики Казахстан

«О персональных данных и их защите», регулируют отдельные вопросы обращения информации и защиты персональных данных, однако не содержат определения понятия Big Data и не устанавливают специальных правил, учитывающих особенности сбора, хранения, обработки, передачи и использования больших массивов данных [4; 5].

Сложившаяся ситуация свидетельствует о наличии определенного нормативного пробела, который становится все более заметным по мере развития цифровых технологий. Отсутствие специального правового регулирования затрудняет определение правового режима больших данных, создает риски неоднозначного толкования прав и обязанностей участников соответствующих правоотношений, а также снижает эффективность механизмов защиты прав субъектов данных. Кроме того, правовая неопределенность может выступать фактором, сдерживающим дальнейшее развитие цифровых сервисов и полноценную реализацию потенциала цифровой экономики Республики Казахстан [6, с.137–139].

В соответствии с подпунктом 12 статьи 1 Закона Республики Казахстан «О персональных данных и их защите» обработка персональных данных охватывает широкий круг действий, включая их сбор, систематизацию, накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение [5]. Учитывая содержание данного определения, значительная часть операций, выполняемых при функционировании систем больших данных, подпадает под правовой режим обработки персональных данных.

Специфика технологий Big Data состоит в возможности работы не только с информацией о различных экономических, производственных либо социальных процессах, но и со сведениями, позволяющими прямо или косвенно идентифицировать физическое лицо. При этом современные методы анализа данных и алгоритмы машинного обучения способны устанавливать ранее неочевидные связи между различными информационными массивами. В

результате даже обезличенные данные в отдельных случаях могут использоваться для повторной идентификации лица посредством сопоставления информации из различных источников, что создает дополнительные риски для обеспечения конфиденциальности и защиты персональных данных [7, с.1705].

В этих условиях особую актуальность приобретает вопрос о достаточности действующих правовых механизмов Республики Казахстан для обеспечения защиты прав и законных интересов субъектов данных при использовании технологий Big Data. Для оценки эффективности существующего регулирования необходимо рассмотреть, насколько особенности обработки больших данных соотносятся с основополагающими принципами защиты персональных данных, закрепленными в национальном законодательстве и международных правовых актах.

Международная практика регулирования обработки персональных данных, в том числе положения Общего регламента Европейского Союза по защите данных (GDPR), основывается на ряде фундаментальных принципов, к которым относятся законность, добросовестность и прозрачность обработки, целевое ограничение использования данных, минимизация объема собираемой информации, обеспечение ее точности, ограничение сроков хранения, гарантирование конфиденциальности и целостности данных, а также подотчетность лиц, осуществляющих их обработку [8, с.35].

Сходные подходы лежат в основе правового регулирования персональных данных и в Республике Казахстан, что позволяет использовать указанные принципы в качестве критерия для оценки действующего законодательства в сфере больших данных.

Наибольший научный интерес в контексте правового регулирования больших данных представляют принципы законности обработки, ограничения целей использования информации и минимизации данных. Именно указанные принципы чаще всего вступают в противоречие с технологической природой Big Data, предполагающей накопление значительных объемов сведений, их многократное использование и последующий анализ для выявления ранее неизвестных закономерностей [9, с. 137–139].

Одним из ключевых вопросов правового регулирования больших данных является соотношение технологий Big Data с фундаментальными принципами обработки персональных данных.

Несмотря на то, что законодательство Республики Казахстан не содержит специальных норм, посвященных большим данным, деятельность по их сбору и анализу неизбежно затрагивает сферу действия законодательства о персональных данных. В связи с этим возникает необходимость оценки того, насколько действующие правовые механизмы способны обеспечить эффективную защиту прав субъектов данных в условиях стремительного развития цифровых технологий [10, с.54].

Вместе с тем технология больших данных во многом основывается на возможности последующего выявления новых закономерностей и взаимосвязей между ранее собранными данными. Практическая ценность Big Data заключается именно в способности находить неизвестные на момент сбора информации зависимости, которые невозможно определить заранее. По этой причине использование технологий больших данных нередко выходит за рамки первоначально заявленных целей обработки данных. Например, информация, первоначально собранная банком для оценки платежеспособности клиента, в дальнейшем может использоваться для построения поведенческих моделей, прогнозирования потребительских предпочтений или разработки новых финансовых продуктов.

Аналогичным образом данные, собираемые государственными информационными системами для предоставления государственных услуг, могут использоваться при разработке механизмов прогнозирования социальных процессов или оценки эффективности государственных программ.

Практическое значение рассматриваемой проблемы можно проиллюстрировать на примере деятельности банков и цифровых платформ. Первоначально сведения о финансовых операциях клиента собираются для исполнения договора банковского обслуживания и соблюдения требований финансового законодательства. Однако в дальнейшем эти же данные могут использоваться для построения моделей кредитного скоринга,

персонализированной рекламы, оценки потребительского поведения и прогнозирования платежеспособности. Аналогичная ситуация возникает при обработке данных мобильными операторами, маркетплейсами и государственными информационными системами, где первоначальная цель сбора информации со временем трансформируется в комплексную аналитическую деятельность.

Использование больших данных неизбежно ставит вопрос о допустимых границах повторного применения ранее собранной информации. С одной стороны, жесткая привязка обработки данных исключительно к первоначально заявленным целям способна существенно ограничить возможности использования технологий Big Data и снизить практическую ценность получаемых результатов. С другой стороны, чрезмерно широкое толкование целей обработки создает риск вмешательства в частную жизнь граждан и может привести к нарушению их права на контроль над собственной информацией и ее дальнейшим использованием [11, с.3].

Не менее значимой проблемой является реализация принципа минимизации данных. Международные стандарты в сфере защиты персональных данных исходят из необходимости сбора только тех сведений, которые действительно требуются для достижения конкретной и заранее определенной цели обработки.

Вместе с тем логика функционирования технологий больших данных во многом основана на ином подходе. Эффективность аналитических моделей напрямую зависит от объема и разнообразия используемой информации, поскольку именно расширение массива данных повышает вероятность выявления новых взаимосвязей и закономерностей. По своей природе технологии Big Data ориентированы на накопление максимально возможного объема информации для ее последующего анализа и использования в различных целях, которые не всегда могут быть определены на момент сбора данных. Вследствие этого возникает объективное противоречие между принципом минимизации данных и практикой функционирования систем больших данных, поскольку необходимость использования конкретных сведений нередко

становится очевидной лишь после проведения комплексной аналитической обработки информации [12, с. 2].

Дополнительные правовые вызовы обусловлены активным развитием технологий искусственного интеллекта и методов машинного обучения. Современные алгоритмы способны формировать новые знания о человеке на основе анализа данных, которые первоначально не относились к категории специальных либо чувствительных персональных данных. Так, обработка сведений о пользовательской активности в сети Интернет, потребительском поведении, геолокации и взаимодействии с цифровыми сервисами позволяет делать выводы о состоянии здоровья лица, его материальном положении, мировоззренческих взглядах, религиозных убеждениях и иных аспектах частной жизни. В подобных условиях происходит изменение информационной ценности отдельных данных. Сведения, которые по отдельности не позволяют идентифицировать физическое лицо либо установить его чувствительные характеристики, в результате комплексного анализа могут приобретать новое содержание и использоваться для формирования детализированного цифрового профиля личности. Вместе с тем действующее законодательство Республики Казахстан не содержит специальных правовых механизмов, регулирующих подобные случаи трансформации данных в процессе их аналитической обработки, что создает дополнительные риски нарушения прав субъектов персональных данных и требует дальнейшего совершенствования правового регулирования в данной сфере [13, с.648].

Существенное значение в контексте правового регулирования больших данных имеет принцип законности обработки персональных данных. Согласно законодательству Республики Казахстан обработка персональных данных допускается при наличии предусмотренного законом правового основания либо согласия субъекта персональных данных. Однако практическая реализация данного принципа в условиях функционирования технологий Big Data сопряжена с рядом объективных сложностей. Как правило, большие массивы данных формируются путем объединения информации из различных источников, включая

цифровые платформы, мобильные приложения, интернет-ресурсы, государственные информационные системы и иные базы данных. В подобных условиях получение отдельного информированного согласия субъекта на каждое последующее действие по обработке информации становится организационно затруднительным, а в ряде случаев практически невозможным [14, с.1426].

Дополнительную проблему создает использование сложных алгоритмов анализа данных, принципы функционирования которых зачастую остаются недостаточно понятными для большинства пользователей. В результате даже наличие формально выраженного согласия не всегда свидетельствует о том, что субъект персональных данных в полной мере осознает характер, цели и возможные последствия обработки информации о себе. В зарубежной юридической литературе данная ситуация получила наименование «кризис согласия» (consent crisis), отражающее постепенное снижение эффективности традиционного механизма согласия как основного способа обеспечения защиты прав личности в цифровой среде. В связи с этим отдельные исследователи обосновывают необходимость перехода к риск-ориентированной модели регулирования, предусматривающей предварительную оценку потенциальных рисков обработки данных и внедрение дополнительных гарантий защиты прав субъектов еще до начала использования соответствующих технологий [13, с.653].

Представляется, что в условиях стремительного развития технологий искусственного интеллекта и больших данных традиционная конструкция согласия субъекта персональных данных уже не всегда способна обеспечить надлежащий уровень защиты его прав и законных интересов. В большинстве случаев лицо не обладает реальной возможностью предвидеть все направления последующего использования информации, способы ее аналитической обработки и потенциальные последствия объединения различных информационных массивов. В связи с этим совершенствование правового регулирования должно быть ориентировано не только на получение формального согласия субъекта, но и на усиление ответственности операторов данных, внедрение риск-ориентированных механизмов надзора, проведение

оценки воздействия на права субъектов данных, а также развитие инструментов независимого контроля и аудита алгоритмических систем.

Одним из наиболее актуальных направлений применения технологий больших данных является использование результатов автоматизированной обработки информации при принятии различных решений. Современные системы искусственного интеллекта обладают способностью анализировать значительные объемы данных, выявлять скрытые взаимосвязи и закономерности, формировать прогнозы и рекомендации, а в отдельных случаях принимать решения без непосредственного участия человека. Подобные технологии уже нашли широкое применение в банковской и страховой деятельности, электронной коммерции, здравоохранении, государственном управлении и других сферах общественной жизни.

Вместе с тем развитие автоматизированных механизмов принятия решений сопровождается возникновением серьезных правовых рисков. Прежде всего речь идет о возможности принятия решений, затрагивающих права и законные интересы граждан, на основании алгоритмов, принцип работы которых остается недостаточно прозрачным для пользователей. В отличие от решений, принимаемых человеком, алгоритмические системы нередко функционируют на основе сложных математических моделей и технологий машинного обучения, логика которых не всегда может быть полностью раскрыта или объяснена даже специалистами, участвовавшими в их разработке [15, с.187].

Следует отметить, что действующее законодательство Республики Казахстан пока не предусматривает комплексного правового регулирования отношений, связанных с использованием технологий искусственного интеллекта и автоматизированным принятием решений на основе больших данных. Нормы законодательства о персональных данных регулируют отдельные вопросы обработки информации, однако не содержат специальных требований, касающихся прозрачности алгоритмов, объяснимости принимаемых решений и порядка обжалования результатов автоматизированной обработки данных. Отсутствие

соответствующих правовых механизмов способно привести к ситуации, при которой решения, оказывающие существенное влияние на права и законные интересы граждан, будут приниматься без достаточных гарантий их объективности, справедливости и последующего контроля со стороны человека.

Изучение зарубежной практики свидетельствует о том, что проблемы правового регулирования больших данных являются актуальными для большинства современных государств. При этом используемые модели регулирования существенно различаются в зависимости от особенностей национального законодательства, уровня развития цифровой экономики и приоритетов государственной политики в сфере защиты информации. Наиболее комплексный подход к регулированию вопросов обработки данных сформирован в Европейском Союзе. Ключевым нормативным актом в данной области выступает Общий регламент по защите данных (GDPR), который применяется с 2018 года и устанавливает единые правила обработки персональных данных на территории государств-членов Европейского Союза [8, с.88]. Несмотря, что GDPR не содержит самостоятельного определения понятия «большие данные», его положения распространяются на значительную часть процессов, связанных с использованием технологий Big Data в случаях, когда такая деятельность затрагивает обработку персональных данных.

Существенное значение в европейской модели регулирования имеет статья 22 GDPR, устанавливающая ограничения в отношении решений, принимаемых исключительно на основе автоматизированной обработки данных, если такие решения способны повлечь юридические последствия для лица либо иным образом существенно затронуть его права и законные интересы. Одновременно субъектам данных предоставляется право требовать участия человека в процессе принятия решения, представлять собственные доводы и оспаривать результаты автоматизированной обработки информации. Важным элементом правового механизма Европейского Союза также является принцип «privacy by design» («защита данных на этапе проектирования»), предусматривающий необходимость учета требований по защите персональных данных

еще на стадии создания информационных систем и цифровых платформ [16, с.195]. Реализация данного подхода позволяет минимизировать риски нарушения прав субъектов данных и обеспечить более высокий уровень защиты информации до начала практического использования соответствующих технологий.

Определенный научный и практический интерес представляет опыт Соединенных Штатов Америки в сфере регулирования обработки данных.

В отличие от европейской модели, основанной на едином комплексном нормативном регулировании, в США отсутствует универсальный федеральный закон, посвященный защите персональных данных. Регулирование осуществляется посредством совокупности отраслевых нормативных правовых актов, распространяющихся на отдельные сферы деятельности, включая здравоохранение, финансовый сектор, телекоммуникации и защиту прав потребителей.

Одним из преимуществ такого подхода считается его адаптивность к быстро меняющимся технологическим условиям и создание благоприятной среды для внедрения инноваций. Вместе с тем фрагментарный характер регулирования приводит к различиям в правоприменительной практике и затрудняет формирование единых стандартов защиты персональных данных на национальном уровне [17, с.1818].

Значительный интерес также представляет опыт Китайской Народной Республики, которая за последние годы сформировала самостоятельную модель регулирования цифровой сферы и обработки данных. Важным этапом развития китайского законодательства стало вступление в силу в 2021 году Закона о защите персональной информации (Personal Information Protection Law - PIPL), который установил комплексные требования к обработке персональных данных и использованию современных цифровых технологий [18, с.370]. Особенностью китайского подхода является сочетание активного государственного регулирования информационной сферы с поддержкой развития цифровой экономики и технологий искусственного интеллекта. Законодательство КНР предусматривает специальные механизмы

контроля трансграничной передачи данных, оценки рисков обработки информации и обеспечения безопасности критически важных информационных инфраструктур.

Проведенный анализ зарубежной практики позволяет сделать вывод о том, что большинство государств стремится к формированию специальных правовых механизмов регулирования больших данных, направленных на достижение баланса между интересами цифрового развития, экономической эффективностью использования данных и необходимостью обеспечения надлежащего уровня защиты прав субъектов информации. Учитывая масштабы цифровой трансформации в Республике Казахстан, отдельные элементы зарубежного опыта могут быть использованы при совершенствовании национального законодательства в области больших данных, искусственного интеллекта, информационной безопасности и защиты персональных данных.

Подводя итоги проведенного исследования, следует отметить, что развитие технологий больших данных существенно опережает формирование соответствующих правовых механизмов их регулирования. Несмотря на активную цифровизацию общественных отношений и широкое использование технологий Big Data в государственном управлении, экономике и социальной сфере, законодательство Республики Казахстан пока не содержит комплексного подхода к регулированию отношений, связанных со сбором, обработкой и использованием больших данных.

Проведенный анализ показал, что существующие нормы законодательства о персональных данных не в полной мере учитывают особенности современных технологий, включая возможность повторной идентификации субъектов данных, автоматизированное принятие решений и применение алгоритмов искусственного интеллекта.

Изучение зарубежного опыта позволяет сделать вывод о том, что эффективное регулирование больших данных должно основываться на сочетании механизмов защиты прав личности и создания благоприятных условий для цифровых инноваций. В этой связи дальнейшее совершенствование законодательства Республики

Казахстан представляется целесообразным осуществлять путем формирования самостоятельного правового режима Big Data, предусматривающего требования к прозрачности алгоритмов, оценке рисков обработки данных, защите обезличенной информации и обеспечению эффективных гарантий прав субъектов данных. Реализация указанных мер будет способствовать созданию сбалансированной правовой модели, отвечающей современным вызовам цифровой экономики и обеспечивающей устойчивое развитие Республики Казахстан в условиях цифровой трансформации.

Список использованной литературы

1. Kitchin R. The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences. - London: Sage Publications, 2014. - 240 p.
2. Mayer-Schönberger V., Cukier K. Big Data: A Revolution That Will Transform How We Live, Work and Think. - London: John Murray Publishers, 2013. - 242 p.
3. Ward J.S., Barker A. Undefined By Data: A Survey of Big Data Definitions. - St Andrews: University of St Andrews, 2013. - 11 p.
4. Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации» (с изменениями и дополнениями по состоянию на 2026 год).
5. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 2026 год).
6. Gandomi A., Haider M. Beyond the Hype: Big Data Concepts, Methods and Analytics // International Journal of Information Management. - 2015. - Vol. 35. - No. 2. - P. 137–144.
7. Ohm P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization // UCLA Law Review. - 2010. - Vol. 57. - No. 6. - P. 1701–1777.
8. Регламент (ЕС) 2016/679 Европейского парламента и Совета Европейского Союза от 27 апреля 2016 года «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных и об отмене Директивы 95/46/ЕС (Общий регламент по защите данных (GDPR))» // Official Journal of the European Union. - 2016. - L 119. - P. 1–88.
9. Goodman B., Flaxman S. European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation” // AI Magazine. - 2017. - Vol. 38. - No. 3. - P. 50–57.
10. Алиаскаров Р.Ж. Проблемы обеспечения информационной безопасности Республики Казахстан в современных условиях // [указать наименование журнала, сборника или конференции]. - [год]. - С. [страницы].

11. Нургалиева Е.Н. Цифровизация и развитие информационного законодательства Республики Казахстан // Право и государство. - 2022. - № 4.
12. Mantelero A. The Future of Consumer Data Protection in the E.U.: Re-thinking the “Notice and Consent” Paradigm in the New Era of Predictive Analytics // Computer Law & Security Review. - 2014. - Vol. 30. - No. 6. - P. 643–660.
13. Solove D.J. Privacy and Power: Computer Databases and Metaphors for Information Privacy // Stanford Law Review. - 2001. - Vol. 53. - No. 6. - P. 1393–1462.
14. Pasquale F. The Black Box Society: The Secret Algorithms That Control Money and Information. - Cambridge, MA: Harvard University Press, 2015. - 320 p.
15. Voigt P., von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. - Cham: Springer International Publishing, 2017. - 383 p.
16. Schwartz P.M., Solove D.J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information // New York University Law Review. - 2011. - Vol. 86. - No. 6. - P. 1814–1894.
17. Ding C. China's Personal Information Protection Law: Text, Context, and Implications for the Future of International Data Transfer // Chinese Journal of Comparative Law. - 2022. - Vol. 10. - No. 2. - P. 367–388.

Куандыкова Э.С.

КеАҚ "Нархоз Университет" Құқық және мемлекеттік басқару мектебінің PhD докторы, қауымдастырылған профессоры, Қазақстан Республикасы, Алматы қ.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҚЫЛМЫСТЫҚ ЗАҢНАМАСЫНДАҒЫ ТЕРМИНОЛОГИЯЛЫҚ ДӘЛДІК МӘСЕЛЕЛЕРІ: ЦИФРЛАНДЫРУ ЖАҒДАЙЫНДАҒЫ ҚҰҚЫҚ ҚОЛДАНУ ТӘЖІРИБЕСІ

Құқықтық мемлекет жағдайында заңнаманың сапасы құқықтық терминдердің дәлдігі мен бірізділігіне тікелей байланысты. Бұл талап қылмыстық құқықта ерекше маңызды, өйткені қылмыстық заң адамның құқықтары мен бостандықтарын шектейтін құқықтық жауаптылықты белгілейді.

Терминологиялық дәлдік құқықтық ұғымдардың мазмұнын нақты айқындауды және оларды заңнаманың барлық деңгейінде біркелкі қолдануды білдіреді. Құқықтық термин нақты құқықтық салдарға негіз болатын нормативтік құрал болғандықтан, оның

мағынасы құқықтық реттеу жүйесінде анық әрі тұрақты болуы тиіс [1].

Қылмыстық құқықтағы терминологиялық нақтылық заңдылық пен құқықтық айқындық қағидаттарын қамтамасыз етеді. Конституцияның 77-бабына сәйкес қылмыстық жауаптылық заңда белгіленген негіздер мен тәртіпке сай жүзеге асырылады. Сондықтан қылмыстық-құқықтық нормалардың анық әрі бірімәнді болуы маңызды [2].

Қылмыстық кодекстегі «қылмыстық құқық бұзушылық», «кінә», «қасақаналық», «абайсыздық», «елеулі зиян», «ақпараттық жүйе» сияқты негізгі ұғымдардың бірізді қолданылуы құқық қолдану практикасының тұрақтылығын қамтамасыз етеді [3]. Осыған байланысты терминологиялық дәлдік заң техникасының маңызды элементі ретінде құқықтық коллизияларды азайтып, заңнаманың тиімділігін арттырады [4].

Қылмыстық құқықта терминологиялық дәлдік ерекше маңызды, өйткені ұғымдық қателік қылмыстық жауаптылыққа және әрекетті саралауға тікелей әсер етуі мүмкін. Цифрландыру жаңа қоғамдық қатынастар мен құқық бұзушылықтардың пайда болуына байланысты қылмыстық-құқықтық терминологияны жетілдіруді талап етті. Қазақстан заңнамасында «ақпараттық жүйе», «цифрлық актив», «майнинг», «цифрлық платформа» сияқты жаңа ұғымдар бекітілді [5]. Олардың қылмыстық құқықта бірізді қолданылуы құқық қолдану практикасының тұрақтылығын қамтамасыз етудің маңызды шарты болып табылады.

Цифрландыру жағдайында «цифрлық актив» ұғымының қылмыстық-құқықтық мазмұнын нақтылау өзекті. 2023 жылғы 6 ақпандағы «Цифрлық активтер туралы» Заң цифрлық активтердің құқықтық режимін белгілегенімен, оларды ұрлау, заңсыз иелену немесе алаяқтық жолмен алу кезінде қолсұғушылық объектісін анықтау мәселесі толық шешілмеген [6]. Бұл цифрлық активтердің дәстүрлі мүліктен ерекшеленетін құқықтық табиғатына байланысты.

Қылмыстық құқықтағы жаңа бағыттардың бірі – жасанды интеллектіні қолдануға байланысты құқықтық қатынастар. Жасанды интеллекттің әртүрлі салаларда қолданылуы оның

шешімдері нәтижесінде келтірілген зиян үшін жауаптылық мәселесін өзекті етуде. Бұл мәселе халықаралық құқықтық доктринада да талқылануда [7].

Киберқылмыстылықтың дамуы «компьютерлік деректер», «цифрлық дәлелдемелер», «заңсыз қол жеткізу», «киберқауіпсіздік», «зиянды бағдарламалық қамтамасыз ету» сияқты терминдердің құқықтық мазмұнын нақтылауды талап етеді [8]. Сонымен қатар цифрландыру дәстүрлі «мүлік», «құжат», «ақпарат» және «дәлелдеме» ұғымдарының мазмұнына да әсер етуде. Сондықтан қылмыстық заңнаманың терминологиялық аппаратын жүйелі түрде жаңарту қажеттілігі туындайды.

Бұл мәселені шешуде шетелдік тәжірибені зерделеудің маңызы зор. Мәселен, Түркия Республикасының 2004 жылғы №5237 Қылмыстық кодексінің 243–245-баптарында ақпараттық жүйелерге қатысты қылмыстар арнайы реттелген. Кодексте «bilisim sistemi» (ақпараттық жүйе) және «veri» (деректер) сияқты цифрлық ортаға тән ұғымдар тікелей қолданылады. Мұндай тәсіл цифрлық қылмыстарды саралаудың құқықтық негізін нақтылауға және құқық қолдану бірізділігін қамтамасыз етуге бағытталған [9]. Түркия тәжірибесі Қазақстанның қылмыстық-құқықтық терминологиясын жетілдіруде салыстырмалы-құқықтық негіз ретінде пайдаланылуы мүмкін.

Терминологиялық дәлдік және құқықтық айқындық қағидаты. Құқықтық айқындық (legal certainty) – құқықтық мемлекеттің негізгі қағидаттарының бірі. Ол құқық нормаларының түсінікті, тұрақты және болжамды болуын, сондай-ақ оларды біркелкі қолдануды көздейді. Қылмыстық құқықта бұл талаптың маңызы жоғары, себебі қылмыстық жауаптылық тек заңда нақты белгіленген негіздер бойынша туындауы тиіс [1].

Терминологиялық дәлдік құқықтық айқындықтың маңызды шарты болып табылады. Заңда қолданылатын ұғымдардың мазмұны нақты әрі бізмәнді болмаған жағдайда, қылмыстық құқық бұзушылықтарды саралауда әртүрлі түсіндірулер мен құқық қолдану қателіктері туындауы мүмкін. Осыған байланысты қылмыстық заңдағы терминдер тұрақты және бірізді қолданылуы тиіс [2].

Қазақстан Республикасының Қылмыстық кодексінің 4-бабында қылмыстылық пен жазаланушылықтың тек қылмыстық заңмен айқындалатыны бекітілген. Бұл *nullum crimen sine lege* және *nulla poena sine lege* қағидаттарының көрінісі болып табылады. Олардың тиімді жүзеге асырылуы заң мәтінінің анықтығы мен терминдердің дәлдігіне байланысты [2].

Цифрландыру жаңа құқықтық ұғымдардың пайда болуына байланысты құқықтық айқындық мәселесін күрделендіруде. «Цифрлық актив», «жасанды интеллект», «блокчейн», «компьютерлік деректер» сияқты ұғымдардың мазмұнын нақтылау олардың қылмыстық-құқықтық мәртебесін және құқық бұзушылықтарды дұрыс саралауды қамтамасыз ету үшін қажет. Сондықтан терминдерді біріздендіру заң техникасының маңызды талабы болып табылады [3].

Бұл бағытта Түркия тәжірибесі назар аударуға тұрарлық. Түркияның Қылмыстық кодексінде ақпараттық жүйелерге қатысты қылмыстар арнайы реттеліп, тиісті терминдер қылмыстық-құқықтық нормаларда жүйелі түрде қолданылған. Түрік құқықтық доктринасында терминологиялық тұрақтылық құқықтық қауіпсіздіктің (*hukuki güvenlik*) маңызды элементі ретінде қарастырылады [10]. Қазақстан үшін бұл тәжірибе цифрлық саладағы қылмыстық-құқықтық терминдерді жүйелеу мен біріздендіруде пайдалы болуы мүмкін.

Осылайша, цифрландыру жағдайында терминологиялық дәлдік құқықтық айқындықты қамтамасыз етудің маңызды құралы болып табылады. Қылмыстық заңнамадағы цифрлық ұғымдарды нақты әрі бірізді бекіту құқық қолдану практикасының тұрақтылығын және қылмыстық жауаптылық шектерінің болжамдылығын қамтамасыз етеді.

Қылмыстық құқықта құқықтық белгісіздікке жол берілмеуі тиіс. Терминдердің нақты әрі бірізді қолданылуы құқықтық айқындықты, заңдылықты және құқық қолдану практикасының тұрақтылығын қамтамасыз етеді. Әсіресе цифрландыру жағдайында жаңа технологиялық ұғымдардың мазмұнын нақтылау қылмыстық жауаптылықтың шектерін дұрыс белгілеудің маңызды шарты болып табылады.

Цифрландыру жағдайында «ақпараттық жүйе» және «электрондық ақпараттық ресурс» қылмыстық-құқықтық қорғаудың маңызды объектілеріне айналды. «Ақпараттандыру туралы» Қазақстан Республикасының Заңында ақпараттық жүйе ақпараттық өзара іс-қимылды жүзеге асыратын бағдарламалық және аппараттық құралдар, ақпараттық технологиялар мен деректер базаларының жиынтығы ретінде анықталады [11].

Қылмыстық кодекстің 205–213-баптары ақпараттандыру және байланыс саласындағы құқық бұзушылықтарды қамтиды [3]. Алайда бұл ұғымдардың технологиялық дамуға сәйкес қолданылуы мәселесі өзекті болып отыр. Бұлттық сақтау жүйелері, мобильді қосымшалар, блокчейн және жасанды интеллект жүйелерінің құқықтық мәртебесін нақтылау қажеттілігі туындайды.

Электрондық ақпараттық ресурс электрондық нысанда тіркелген және ақпараттық жүйелерде сақталатын ақпаратты қамтиды [11]. Оның материалдық емес сипаты цифрлық ортадағы қылмыстық қолсұғушылық объектісін анықтауға жаңа талаптар қояды. Сондықтан ақпараттық жүйе мен электрондық ақпараттық ресурс ұғымдарын біріздендіру құқықтық айқындық пен қылмыстық құқық бұзушылықтарды дұрыс саралау үшін қажет.

Халықаралық тәжірибеде бұл мәселе 2001 жылғы Киберқылмыс туралы Будапешт конвенциясында да көрініс тапқан, онда компьютерлік жүйелер мен деректерді қорғауға ерекше мән берілген [12]. Түркияның Қылмыстық кодексінің 243–245-баптарында ақпараттық жүйелерге заңсыз қол жеткізу және электрондық деректерге қатысты әрекеттер үшін жауаптылық көзделген [9]. Түркиядағы технологиялық бейтарап тәсіл, яғни нақты техникалық құралдардан гөрі олардың функцияларына назар аудару, Қазақстан үшін де пайдалы болуы мүмкін.

Цифрлық экономиканың дамуы «цифрлық актив», «компьютерлік ақпарат» және «электрондық құжат» ұғымдарының қылмыстық-құқықтық маңызын арттырды. Қазақстан Республикасының «Цифрлық активтер туралы» 2023 жылғы 6 ақпандағы Заңында цифрлық активтің құқықтық негіздері белгіленген [13]. Алайда цифрлық активтерді заңсыз иемдену немесе алаяқтық жолмен алу кезінде олардың мүлік, мүліктік құқық

немесе ақпараттық ресурс ретіндегі құқықтық табиғатын анықтау мәселесі туындайды.

Бұл мәселе криптовалюта, токен және блокчейн негізіндегі активтерге қатысты ерекше өзекті. Олардың құқықтық мәртебесін нақтылау қылмыстық әрекетті дұрыс саралауға және жауаптылық шектерін белгілеуге мүмкіндік береді.

Осыған байланысты цифрлық активтер мен электрондық деректердің құқықтық табиғатын нақтылау, сондай-ақ оларды қылмыстық заңнамада бірізді қолдану қажеттілігі артып отыр. Бұл терминологиялық дәлдікті қамтамасыз етіп қана қоймай, цифрлық ортадағы қылмыстық құқық бұзушылықтарды дұрыс саралауға мүмкіндік береді.

Цифрлық құқықтағы маңызды ұғымдардың бірі – компьютерлік ақпарат. Қазақстан Республикасының Қылмыстық кодексындағы ақпараттық қауіпсіздікке қарсы құқық бұзушылықтардың басым бөлігі осы саладағы қатынастарды қорғауға бағытталған [3]. Алайда «компьютерлік ақпарат», «электрондық деректер», «ақпараттық ресурс» және «цифрлық деректер» ұғымдарының арақатынасы бірізді анықталмаған.

Компьютерлік ақпараттың материалдық емес сипаты оны дәстүрлі мүлік объектілерінен ерекшелендіреді. Электрондық құжат электрондық нысандағы, белгіленген тәртіппен куәландырылған ақпарат болып табылады және қағаз құжатпен тең заңдық күшке ие [14]. Осыған байланысты электрондық құжаттарды заңсыз өзгерту, жою немесе қолдан жасау қылмыстық-құқықтық қорғауды талап етеді.

«Электрондық құжат» пен «электрондық ақпараттық ресурс» ұғымдарын нақты ажырату құқық бұзушылық объектісін дұрыс анықтау үшін қажет. Халықаралық тәжірибеде цифрлық активтер мен компьютерлік ақпаратты қорғау мәселесі өзекті болып отыр [12]. Түркияда криптоактивтер экономикалық құндылығы бар цифрлық мүлік ретінде қарастырылып, сот тәжірибесінде олардың мүліктік сипаты мойындалуда [15]. Қазақстан үшін де бұл ұғымдарды біріздендіру құқық қолдану практикасының тұрақтылығын қамтамасыз етеді.

Цифрлық трансформация «жасанды интеллект», «автоматтандырылған жүйе» және «киберқауіпсіздік» ұғымдарын қылмыстық-құқықтық тұрғыдан нақтылауды талап етеді. Жасанды интеллект ақпаратты талдап, болжам жасап және белгілі бір деңгейде дербес шешім қабылдайтын бағдарламалық-аппараттық жүйелер ретінде түсіндіріледі [16]. Қазақстанның қылмыстық заңнамасында оның дербес анықтамасы жоқ. Қазіргі кезде ЖИ қылмыстық әрекеттің құралы ретінде қарастырылады, ал жауаптылық оны пайдаланған тұлғаға жүктеледі [17].

Автоматтандырылған жүйелер адамның тікелей немесе шектеулі қатысуымен белгілі бір функцияларды орындайды [11]. Олар қылмыстық қолсұғушылық объектісі немесе қылмыс құралы болуы мүмкін. «Ақпараттық жүйе», «автоматтандырылған жүйе» және «цифрлық платформа» ұғымдарының аралас қолданылуы терминологиялық қайшылықтарға әкелуі мүмкін.

Киберқауіпсіздік ақпараттық-коммуникациялық инфрақұрылымды қауіптерден қорғауға бағытталған құқықтық, ұйымдастырушылық және техникалық шаралар жүйесін білдіреді [18]. Ақпараттық жүйелерге заңсыз қол жеткізу, деректерді жою немесе өзгерту сияқты әрекеттер киберқауіпсіздікке қатер төндіреді. Халықаралық деңгейде киберқауіпсіздік қоғамдық және құқықтық қауіпсіздіктің маңызды элементі ретінде танылады [19]. Түркияда да ол ұлттық қауіпсіздіктің басым бағыттарының бірі ретінде қарастырылып, қылмыстық-құқықтық қорғау тетіктері дамуда [20].

Осылайша, цифрлық терминдерді біріздендіру қылмыстық заңнаманың құқықтық айқындығын арттырып, цифрлық ортадағы құқық бұзушылықтарды дұрыс саралауға мүмкіндік береді.

Қазақстан мен Түркия тәжірибесін салыстыру цифрлық қауіпсіздік саласындағы терминологияның қарқынды дамып отырғанын көрсетеді. «Киберқауіпсіздік», «ақпараттық қауіпсіздік», «ақпараттық қорғау» және «цифрлық қауіпсіздік» ұғымдарын нақты ажыратпау құқық қолдануда әртүрлі түсіндіруге әкелуі мүмкін. Сондықтан жаңа технологиялық терминдердің мазмұнын ғылыми және құқықтық тұрғыдан нақтылау, сондай-ақ технологиялық бейтараптық қағидатын сақтау маңызды.

Цифрлық құқық бұзушылықтарды саралауда терминдердің анықтылығы ерекше мәнге ие. «Ақпараттық жүйе», «электрондық ақпараттық ресурс», «компьютерлік ақпарат» және «деректер базасы» ұғымдарының мазмұндық шекаралары әрдайым нақты ажыратылмаған [11]. Бұл құқық бұзушылық объектісін анықтауда қиындық туғызуы мүмкін. Сонымен қатар цифрлық ортадағы зиян көбіне материалдық емес сипатта болатындықтан, «зиян», «залал», «қауіп», «қатер» және «теріс салдар» ұғымдарын нақтылау қажеттілігі туындайды.

Цифрлық активтерге қатысты құқық қолдануда да терминологиялық дәлдік маңызды. Криптовалюта, токен және өзге де цифрлық активтердің құқықтық табиғатын дұрыс анықтау олармен байланысты құқық бұзушылықтарды саралаудың қажетті шарты болып табылады [13].

Халықаралық тәжірибеде киберқылмысқа қарсы күресте терминологиялық бірізділікке ерекше мән беріледі [12]. Түркияда электрондық деректердің дәлелдемелік мәні мен цифрлық құқық бұзушылықтарды саралау мәселелері сот практикасында және ғылыми әдебиетте талқыланды [21]. Қазақстан мен Түркия тәжірибесі жаңа технологиялық қатынастарды реттеуде терминологиялық нақтылықтың әмбебап маңызын көрсетеді.

Осыған байланысты терминологиялық коллизияларды жою заңнаманы жетілдірумен қатар, сот практикасы, Жоғарғы Соттың нормативтік қаулылары және құқықтық түсіндіру арқылы да жүзеге асырылуы тиіс. Терминдердің ғылыми негізделген және бірізді қолданылуы қылмыстық құқық бұзушылықтарды дұрыс саралауға, құқықтық айқындықты және сот практикасының тұрақтылығын қамтамасыз етуге мүмкіндік береді.

Цифрлық қылмыстарды тергеу мен сот тәжірибесіндегі терминологиялық коллизиялар: Қазақстан және Түркия тәжірибесі келетін болсақ, цифрландыру жағдайында тергеу және сот органдарының тиімділігі қылмыстық заңнамадағы ұғымдардың анықтығы мен бірізділігіне тәуелді. Дәстүрлі қылмыстарға қатысты тұрақты сот практикасы қалыптасқанымен, цифрлық құқық бұзушылықтар саласында мұндай тәжірибе әлі толық орнықпаған. Сондықтан жаңа технологиялық құбылыстарды құқықтық бағалау

кезінде терминологиялық коллизиялар туындап, оларды біріздендіру қажеттілігі артып отыр.

Қазіргі құқық қолдану тәжірибесіндегі негізгі мәселелердің бірі – құқықтық терминдердің технологиялық дамудан кейін қалып қоюы. Қазақстан Республикасының Қылмыстық кодексінде ақпараттандыру және байланыс саласындағы құқық бұзушылықтарға жауаптылық көзделгенімен, көптеген нормалар жалпы сипатта берілген. Бұл технологиялық бейтараптықты қамтамасыз еткенімен, жаңа технологияларға қатысты әртүрлі түсіндірулерге әкелуі мүмкін [3]. Мысалы, бұлттық сақтау, виртуалды серверлер және трансшекаралық платформалар жағдайында «компьютерлік ақпаратқа заңсыз қол жеткізу» ұғымының мазмұнын анықтау қиындық туғызады.

Терминологиялық коллизиялар цифрлық активтерге қатысты да байқалады. Олардың мүліктік мәртебесін, құнын және келтірілген залалды анықтау құқық бұзушылықтарды саралауға тікелей әсер етеді [13]. Сол сияқты «электрондық құжат», «электрондық дәлелдеме», «цифрлық дерек» және «ақпараттық ресурс» ұғымдарының арақатынасын нақтылау дәлелдеу процесінің тиімділігі үшін қажет [14].

Халықаралық тәжірибеде терминологиялық бірізділік киберқылмысқа қарсы күрестің маңызды шарты ретінде қарастырылады [12]. Түркияда «*bilişim sistemi*» ұғымын түсіндіруде технологиялық бейтараптық, ал цифрлық құқық бұзушылықтарды саралауда жүйелік түсіндіру тәсілі қолданылады [9; 22]. Бұл тәжірибе Қазақстан үшін де маңызды, өйткені цифрлық терминдер бірнеше құқық саласында қатар қолданылып келеді.

Терминологиялық коллизиялар құқықтық бағалауға ғана емес, дәлелдеу процесі мен халықаралық құқықтық ынтымақтастыққа да әсер етеді. Трансшекаралық киберқылмыстар жағдайында терминдердің әртүрлі түсіндірілуі құқықтық көмек көрсету рәсімдерін қиындатуы мүмкін [12]. Сондықтан цифрлық терминдерді халықаралық стандарттармен үйлестіру және салааралық бірізділікті қамтамасыз ету қажет.

Осылайша, терминологиялық дәлдік цифрлық дәуірдегі құқықтық қауіпсіздіктің маңызды шарты болып табылады.

Терминдерді нақтылау құқық бұзушылықтарды дұрыс саралауға, сот практикасының біркелкілігі мен құқықтық айқындықты қамтамасыз етуге мүмкіндік береді.

Цифрландыру жағдайында қылмыстық заңнаманың терминологиялық аппаратын жетілдірудің негізгі бағыттарына тоқталып кетейік:

Цифрландыру қылмыстық заңнаманың терминологиялық аппаратын жүйелі түрде жаңартуды талап етеді. Құқықтық терминдер қылмыстық жауаптылықтың шектерін айқындайтындықтан, олардың мазмұны нақты әрі бірізді болуы тиіс. Терминологиялық тұрақсыздық құқықтық белгісіздікке және құқық қолдану практикасының әркелкілігіне әкелуі мүмкін [12].

Бірінші бағыт-цифрлық құқықтағы бірыңғай ұғымдық модельді қалыптастыру. «Ақпараттық жүйе», «электрондық ақпараттық ресурс», «цифрлық актив», «электрондық құжат», «цифрлық деректер» сияқты ұғымдардың анықтамалары мен өзара арақатынасын нақтылау қажет.

Екінші бағыт-қылмыстық құқықтың цифрлық тезаурусын әзірлеу. Онда цифрлық терминдердің заңнамалық анықтамалары, ғылыми түсіндірмелері және қазақ, орыс, ағылшын және түрік тілдеріндегі баламалары қамтылуы мүмкін. Түркия тәжірибесі мұндай терминологиялық жүйелеудің маңызын көрсетеді [23].

Үшінші бағыт - заң жобаларын екі тілде қатар әзірлеу және терминологиялық сараптаманы күшейту. Бұл қазақ және орыс тілдеріндегі құқықтық мәтіндердің мазмұндық сәйкестігін арттырып, терминологиялық алшақтықтарды азайтады.

Төртінші бағыт-заңнамалық терминологиялық мониторингті цифрландыру. Жасанды интеллект негізіндегі жүйелер қайталанатын дефиницияларды, терминологиялық сәйкессіздіктер мен коллизияларды анықтауға мүмкіндік береді.

Бесінші бағыт-цифрлық терминдерді халықаралық стандарттармен үйлестіру. Киберқылмыстардың трансшекаралық сипаты ұлттық заңнамалар арасындағы терминологиялық сәйкестікті талап етеді [12]. Бұл ретте Түркия тәжірибесін пайдалану Қазақстанның ұлттық ерекшеліктерін сақтай отырып, халықаралық тәсілдермен үйлесуге мүмкіндік береді.

Алтыншы бағыт-құқық қолданушылардың цифрлық-құқықтық құзыреттерін арттыру. Судьялар, прокурорлар, адвокаттар мен құқық қорғау органдарының қызметкерлері жаңа цифрлық ұғымдардың құқықтық мазмұнын меңгеруі қажет.

Жетінші бағыт - жасанды интеллектке қатысты қылмыстық-құқықтық терминологияны қалыптастыру. Автономды алгоритмдер мен интеллектуалдық жүйелердің дамуына байланысты олардың құқықтық мәртебесін және қылмыстық құқықтағы қолданылу шектерін ғылыми тұрғыдан нақтылау қажет.

Осылайша, Қазақстан мен Түркия тәжірибесі цифрлық дәуірде терминологиялық дәлдіктің құқықтық айқындық, заңдылық және құқық қолдану тұрақтылығы үшін шешуші маңызға ие екенін көрсетеді. Қылмыстық заңнаманың терминологиялық аппаратын жүйелеу цифрлық технологиялардың дамуы мен құқықтық реттеудің тұрақтылығы арасындағы тепе-теңдікті қамтамасыз етудің маңызды бағыты болып табылады.

Қорытындылай келе, цифрландыру қылмыстық құқықтың дәстүрлі ұғымдық аппаратын кеңейтіп, «цифрлық актив», «компьютерлік ақпарат», «электрондық құжат», «киберқауіпсіздік», «жасанды интеллект» және басқа да жаңа терминдерді құқықтық айналымға енгізді. Олардың мазмұнының бірізді болмауы құқық бұзушылықтарды саралауға, дәлелдеу процесіне және сот практикасының тұрақтылығына әсер етуі мүмкін.

Қазақстан мен Түркия тәжірибесін салыстыру цифрлық терминологияны жүйелеу, халықаралық стандарттармен үйлестіру және құқық қолдану практикасы арқылы ұғымдық тұрақтылықты қамтамасыз етудің маңызын көрсетеді. Осыған байланысты қылмыстық заңнамадағы цифрлық терминдердің ғылыми негізделген дефиницияларын әзірлеу, олардың салааралық сәйкестігін қамтамасыз ету және терминологиялық мониторингті енгізу қажет.

Зерттеу нәтижесінде цифрлық қылмыстық құқықтың терминологиялық аппаратын жетілдірудің негізгі бағыттары ретінде бірыңғай ұғымдық модель, цифрлық тезаурус, терминологиялық сараптама, жасанды интеллект негізіндегі мониторинг,

халықаралық үйлестіру және құқық қолданушылардың цифрлық құзыреттерін арттыру ұсынылады.

Қорытындылай келе, терминологиялық дәлдік қылмыстық заңнаманың техникалық сипаты ғана емес, **құқықтық айқындықты, заңдылықты және цифрлық кеңістіктегі құқықтық қауіпсіздікті қамтамасыз етудің маңызды шарты** болып табылады.

Әдебиеттер тізімі

1. Айымбетов М.А. Заң терминдерін жүйелеудің кейбір мәселелері // ҚР заңнама және құқықтық ақпарат институтының жаршысы. -2020. - №3 (61). – 191-194 бб.
2. Қазақстан Республикасының Конституциясы. 30 тамыз 1995 ж. // URL: <https://adilet.zan.kz/kaz/docs/K950001000>
3. Қазақстан Республикасының Қылмыстық кодексі. 3 шілде 2014 ж. №226-V ҚРЗ. // URL: <https://adilet.zan.kz/kaz/docs/K1400000226>
4. Құқықтық актілер туралы Қазақстан Республикасының Заңы. 6 сәуір 2016 ж. №480-V ҚРЗ.// URL: <https://adilet.zan.kz/kaz/docs/Z1600000480>
5. Ақпараттандыру туралы Қазақстан Республикасының Заңы. 24 қараша 2015 ж. №418-V ҚРЗ // URL: <https://adilet.zan.kz/kaz/docs/Z1500000418>
6. Цифрлық активтер туралы Қазақстан Республикасының Заңы. 6 ақпан 2023 ж. №193-VII ҚРЗ. URL: <https://adilet.zan.kz/kaz/docs/Z2300000193>
7. Council of Europe. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their Environment. Strasbourg, 2018. // URL: <https://www.coe.int/en/web/cepej>
8. United Nations Office on Drugs and Crime (UNODC). Comprehensive Study on Cybercrime. Vienna: UNODC // URL: <https://www.unodc.org>
9. Уголовный Кодекс Турции (закон №5237 от 26.09.2004. г. с изменениями) // <https://www.wipo.int/>
10. Türk Ceza Kanunu. Resmî Gazete, 12.10.2004 // URL: <https://www.mevzuat.gov.tr>
11. Қазақстан Республикасының «Ақпараттандыру туралы» Заңы. 24 қараша 2015 ж. №418-V // URL: <https://adilet.zan.kz/kaz/docs/Z1500000418>
12. Budapest Convention on Cybercrime // URL: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
13. Қазақстан Республикасының «Цифрлық активтер туралы» Заңы. 6 ақпан 2023 ж. № 193-VII // URL: <https://adilet.zan.kz/kaz/docs/Z2300000193>
14. Қазақстан Республикасының «Электрондық құжат және электрондық цифрлық қолтаңба туралы» Заңы. 7 қаңтар 2003 ж. №370-II // URL: <https://adilet.zan.kz/kaz/>
15. Central Bank of the Republic of Türkiye. Resmî Gazete, 16 April 2021 // URL: <https://www.resmigazete.gov.tr>

- 16.UNESCO. Paris, 2021 // URL: <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
- 17.European Parliament. Brussels, 2020 // URL: <https://www.europarl.europa.eu>
18. Қазақстан Республикасының «Қазақстанның киберқауіпсіздігі тұжырымдамасы («Киберқалқан»))» // URL: <https://adilet.zan.kz>
- 19.United Nations // URL: <https://www.un.org>
- 20.Digital Transformation Office of the Presidency of the Republic of Türkiye // URL: <https://cbddo.gov.tr>
- 21.Council of Judges and Prosecutors of Türkiye. Ankara, 2023 // <https://www.cjp.gov.tr/>
- 22.Ministry of Justice of the Republic of Türkiye. Ankara, 2022 // <https://justice.gov.tr/>
23. Ministry of Justice of Türkiye. Ankara, 2024. // <https://justice.gov.tr/>

Куандыкова Э.С.

КеАҚ "Нархоз Университет" Құқық және мемлекеттік басқару мектебінің PhD докторы, қауымдастырылған профессоры, Қазақстан Республикасы, Алматы қ.

ҚАЗАҚСТАННЫҢ ҚЫЛМЫСТЫҚ ҚҰҚЫҒЫНДАҒЫ ЛИНГВИСТИКАЛЫҚ КОЛЛИЗИЯЛАР: ТЕРМИНОЛОГИЯЛЫҚ АЛШАҚТЫҚТАРДЫҢ ІС-ӘРЕКЕТТЕРДІ САРАЛАУҒА ӘСЕРІ

Қылмыстық құқық бұзушылықты саралау - нақты өмірлік мән-жайларды қылмыстық заңда көзделген құрам белгілерімен сәйкестендірудің күрделі зияткерлік және құқықтық процесі. Бұл процесте қолданылатын әрбір термин тек тілдік таңба емес, қылмыстық жауаптылықтың негізі мен шегін айқындайтын нормативтік құрал ретінде әрекет етеді. Терминнің көлемі тарылса, заңмен қорғалатын қатынастың бір бөлігі құқықтық бағалаудан тыс қалуы мүмкін; оның көлемі негізсіз кеңейсе, қылмыстық репрессияның шекарасы ұлғаяды. Сондықтан қазақ және орыс тілдеріндегі ресми мәтіндердің ұғымдық сәйкестігі заңнамалық редакция сапасының ғана емес, адамның бостандығы мен құқықтарын қорғаудың тікелей кепілі болып табылады.

Қазақстандағы екітілді құқықтық кеңістіктің бастапқы конституциялық негізі **2026 жылғы 15 наурызда республикалық референдумда қабылданған Қазақстан Республикасының Конституциясының 9-бабында** бекітілген. Аталған баптың 1-тармағына сәйкес, Қазақстан Республикасының мемлекеттік тілі - қазақ тілі, ал 2-тармағында мемлекеттік ұйымдарда және жергілікті өзін-өзі басқару органдарында қазақ тілімен қатар орыс тілінің ресми қолданылатыны белгіленген [1]. Осы конституциялық норма бір тілдегі мәтінді негізгі, ал екіншісін қосалқы түсіндірме ретінде қабылдауға мүмкіндік бермейді: құқық қолданушы үшін екі нұсқа да құқықтық коммуникацияның ресми арнасы болып қалады. Қылмыстық заң саласында мұндай қатар қолданылу әр тілдегі құқықтық мәтіннің түсінікті, алдын ала болжамды және бірдей құқықтық салдар туғызуын талап етеді [1]

Нормативтік құқықтық актілерді әзірлеуге қойылатын жалпы талаптар қазақ және орыс тілдеріндегі мәтіндердің теңтүпнұсқалы болуын, ал заң жобасына ғылыми лингвистикалық сараптама жүргізген кезде терминологияның бірізділігі мен екі нұсқаның мағыналық сәйкестігін тексеруді көздейді. Осы талаптың қылмыстық заң үшін айрықша маңызы бар, себебі диспозициядағы бір етістіктің модальды реңкі, бір анықтауыштың шегі немесе бір ұғымның тектік-түрлік арақатынасы іс-әрекеттің қылмыстылығына, баптың бөлігіне және жаза мөлшеріне әсер етуі мүмкін. Демек, теңтүпнұсқалықты орфографиялық ұқсастық емес, екі мәтіннің нормативтік ықпалының бірдейлігі ретінде түсіну қажет [2].

Қолданыстағы Қылмыстық кодекс қылмыстық жауаптылықтың бірден-бір материалдық негізін белгілейді және қылмыстық құқық бұзушылық ұғымын қоғамға қауіпті іс-әрекет арқылы сипаттайды; мәтінде тектік «іс-әрекет» ұғымы оның түрлері болып табылатын «әрекет» пен «әрекетсіздікті» қамтиды. Кодекстің 188-бабында «ұрлық» бөтеннің мүлкін жасырын «жымқыру» ретінде айқындалады, ал қылмыстық кірістерге қатысты нормаларда «қылмыстық жолмен алынған» конструкциясы қолданылады. Бұл мысалдар терминдердің мағынасын жалпы тілден емес, кодекстің ішкі жүйесі мен заңдық анықтамаларынан шығару қажеттігін көрсетеді [3].

Тіл туралы заңнамадағы «мәтіннің теңтүпнұсқалы аудармасы» ұғымы түпнұсқаның мағынасы мен мазмұнын өзгеріссіз сақтайтын аударманы білдіреді. Алайда қылмыстық заңда аударманың сапасы тек бастапқы сөйлемнің жалпы мазмұнын сақтаумен өлшенбейді. Мұнда құқықтық ұғымның денотаты, оның өзге институттармен байланысы, адресатқа жүктейтін тыйымның көлемі, кінәні дәлелдеуге қоятын талабы және санкцияға әкелетін белгісі де өзгеріссіз берілуі тиіс. Сондықтан теңтүпнұсқалықты статикалық мәтіндік ұқсастықтан гөрі функционалдық құқықтық баламалылық ретінде қарастырған жөн [4].

Осы мақалада лингвистикалық коллизия деп қылмыстық заңның қазақ және орыс тілдеріндегі нұсқаларының, не бір тілдегі өзара байланысты нормалардың арасында құқықтық ұғымның мазмұнына, көлеміне немесе функциясына қатысты пайда болатын және норманы әртүрлі қолдануға объективті мүмкіндік беретін мағыналық қайшылық түсініледі. Әрбір редакциялық айырма коллизия болып саналмайды. Мысалы, синтаксистік құрылым өзгеше болғанымен нормативтік мазмұн толық сақталса, ол заңды локализацияның қалыпты тәсілі болуы мүмкін. Коллизияның шешуші белгісі - екі мәтінді адал түсіндіру нәтижесінде қылмыстық-құқықтық салдардың бірдей болмау қаупі.

Лингвистикалық коллизияларды бірнеше деңгейге бөлу орынды. Лексикалық деңгейде бір терминге көлемі басқа балама таңдалады немесе бір ұғым бірнеше сөзбен беріледі. Морфологиялық деңгейде жекеше мен көпше түр, аяқталған және аяқталмаған іс-қимыл, міндеттілік пен мүмкіндікті білдіретін нысандар алшақтайды. Синтаксистік деңгейде анықтауыштың қай сөзге қатысты екені, баламалы әрекеттердің шекарасы немесе шарт пен салдардың байланысы өзгеруі ықтимал. Прагматикалық деңгейде кәсіби заңгер мен қарапайым адресат терминді әртүрлі қабылдайды. Ал жүйелік коллизия бір баптағы атаудың Жалпы бөлімдегі анықтамамен немесе сабақтас қылмыстық-процестік ұғыммен сәйкес келмеуінен туындайды.

Саралау процесінде мұндай алшақтықтар қылмыстық құқық бұзушылық құрамының барлық элементіне әсер ете алады. Қол

сұғушылық объектісін білдіретін термин шамадан тыс кең түсіндірілсе, арнайы норма мен жалпы норманың арақатынасы бұзылады. Обьективтік жақтағы әрекет, тәсіл, құрал, орын немесе зардап атауы дәл болмаса, аяқталған құрам мен оқталуды, әрекет пен әрекетсіздікті, негізгі және сараланған құрамды ажырату қиындайды. Субьективтік жақтағы мақсат, себеп, «көрінеу» білу немесе абайсыздық дәрежесі дұрыс берілмесе, кінәнің мазмұны өзгеруі мүмкін. Субьектіні сипаттайтын лауазымдық не арнайы белгі алшақ аударылса, жауаптылыққа тартылатын адамдар шеңбері де бірдей болмайды.

«Іс-әрекет», «әрекет» және «әрекетсіздік» арақатынасы тектік және түрлік терминдерді ажыратудың маңызын көрсетеді. Орыс тіліндегі «деяние» ұғымы «действие» мен «бездействию» біріктіретін дербес тектік атау ретінде орныққан. Қазақ тілінде «іс-әрекет» көбіне осы жинақтаушы қызметті атқарады, бірақ күнделікті қолданыста ол белсенді қимылмен ассоциациялануы мүмкін. Егер құқық қолданушы тектік ұғымды тек белсенді мінез-құлықпен теңестірсе, заңмен жүктелген міндетті орындамау арқылы жасалатын құрамдарды бағалауда қате туындайды. Сондықтан кодекстің бүкіл мәтінінде тектік атауды бір нұсқада сақтап, оның әрекет пен әрекетсіздікті қамтитынын анықтамалық аппаратта айқын көрсету қажет.

Мүліктік қылмыстық құқық бұзушылықтардағы «жымқыру» мен «ұрлық» ұғымдарының арақатынасы да саралау үшін қағидатты. «Жымқыру» - бөтен мүлікті құқыққа қарсы иемденудің бірнеше нысанын біріктіретін тектік ұғым, ал «ұрлық» - жасырын тәсілмен жасалатын нақты нысан. Жалпы тілде «ұрлық» сөзі кейде бөтен мүлікті иемденудің барлық түріне ортақ атау ретінде қолданылады. Мұндай тұрмыстық мағына құқықтық мәтінге көшірілсе, алаяқтық, сеніп тапсырылған мүлікті иемдену, тонау және қарақшылық арасындағы шекара көмескіленеді. Құқық қолданушы терминді сөздік интуициямен емес, заңдағы тәсіл, ниет және мүліктің өту механизмі арқылы саралауға тиіс.

Субьективтік жақты сипаттайтын «көрінеу» термині ерекше назарды қажет етеді. Оның жалпы тілдегі «анық көрінетін», «айқын» мағынасы қылмыстық құқықтағы «адамның тиісті мән-

жайды анық әрі сенімді білуі» ұғымымен толық сәйкес емес. Орыс тіліндегі «заведомо» да арнайы заңдық мазмұнға ие. Егер «көрінеу» объективті жағдайдың айқындығы деп қабылданса, айыпталушының нақты білгенін дәлелдеудің орнына сыртқы жағдайдың түсініктілігі жеткілікті саналып кетуі ықтимал. Бұл кінәлі жауаптылық қағидатына қайшы. Сол себепті заңдық түсіндірмеде осы терминнің дәлелденуге тиіс интеллектуалдық сәтті білдіретіні бекітілуі керек.

«Зиян», «залал», «нұқсан» терминдерінің жарыспалы қолданылуы да құқықтық салдарға ие. Олардың кейбірі материалдық жоғалтуды, басқалары мүлдік емес қол сұғушылықтың салдарын немесе қорғалатын мүдденің жалпы нашарлауын білдіруі мүмкін. Орыс мәтініндегі «вред» пен «ущерб» те әр контексте бірдей емес. Егер сандық өлшеммен анықталатын мүлдік залал кең мағыналы зиянмен араластырылса, елеулі, ірі немесе аса ірі зардапты белгілеу кезінде дәлелдеу пәні өзгеруі мүмкін. Бірізділік үшін заң шығарушы әр терминнің қолданылатын саласын, өлшену тәсілін және бағалау критерийін анықтамалар жүйесінде байланыстыруы қажет.

Топтық қылмыстылыққа қатысты атауларда да күнделікті мағына мен заңдық мағынаны ажырату керек. «Адамдар тобы», «алдын ала сөз байласқан адамдар тобы», «қылмыстық топ», «ұйымдасқан топ» және өзге нысандар бір қатысушылар жиынтығын әртүрлі атау емес, құрылымдылық, тұрақтылық, алдын ала бірлесу және мақсат белгілері бойынша ажыратылатын құқықтық санаттар. Бір нұсқадағы жалпылаушы сөз екінші нұсқада арнайы терминмен ауыстырылса, саралаушы белгі негізсіз қолданылуы немесе, керісінше, назардан тыс қалуы мүмкін. Бұл жаза шегіне тікелей ықпал ететіндіктен, топ нысандарының атаулары кодекстің Жалпы және Ерекше бөлімдерінде бірдей терминологиялық матрица бойынша берілуге тиіс.

Лингвистикалық коллизияның саралауға ықпал ету механизмі бірнеше сатыдан тұрады. Алдымен термин дәлелдеу пәнін айқындайды: тергеуші қандай фактілерді іздеу керегін сол арқылы белгілейді. Кейін прокурор оны айыптау актісінде құқықтық формулаға айналдырады. Сот терминнің мағынасын дәлелденген

фактілерге қолданып, бап пен оның бөлігін тандайды. Апелляциялық және кассациялық сатылар осы пайымның дұрыстығын тексереді. Бастапқы термин қате түсіндірілсе, қателік барлық процессуалдық құжатқа таралады: дәлелдемелердің бір бөлігі жиналмайды, қорғану ұстанымы басқа белгіге бағытталады, ал сот шешіміндегі уәждеу жалған семантикалық алғышартқа сүйенеді.

Сот ісін жүргізу тілін қолдану жөніндегі жоғарғы соттық түсіндіру сот процесіне қатысушылардың тілдік құқықтарын қамтамасыз етуді құқықтық кепіл ретінде бағалайды. Бұл кепіл тек аудармашы ұсынумен немесе құжаттарды таңдалған тілде берумен шектелмейді. Айыптаудың мәні, саралау белгісі және сот қабылдаған түсіндіру сотталушыға нақты әрі бірмәнді жеткізілуі керек. Екі ресми мәтін арасында мағыналық айырма анықталған жағдайда, сот оны елемей бір нұсқаны механикалық пайдаланбай, қай ұғымның заң жүйесіне сәйкес екенін және таңдаудың адамның жағдайына қалай әсер ететінін шешімде негіздеуге тиіс [5].

Заң мәтіндеріндегі лингвистикалық қателерді зерттеу лексикалық, стилистикалық, грамматикалық және синтаксистік олқылықтардың құқықтық норманың мағынасын бұзуы, терминдердің негізсіз жарыспалылығы мен дұрыс емес баламалардың тентүпнұсқалықты әлсіретуі мүмкін екенін көрсетеді. Қылмыстық заңға қатысты мұндай қателердің салмағы жоғары: редакциялық кемшілік қылмыстық жауаптылықтың шекарасына айналады. Сондықтан лингвистикалық мониторинг қабылданған заңдарға ғана емес, әрбір өзгеріс пен толықтыру жобасына, соның ішінде салыстырмалы кестелер мен ілеспе актілерге де жүргізілуі қажет [6].

Қазақ тіліндегі заң мәтіндерінде терминдердің қолданылуын талдаған зерттеулер сөзбе-сөз аударма, терминологиялық бірізділіктің болмауы және ұғымдық сәйкестіктің толық сақталмауы әлі де жүйелік мәселе екенін атап көрсетеді. Бұл қорытынды қылмыстық заңды аудару моделін қайта қарауды талап етеді. Алдымен орысша жобаланып, кейін қазақшаға аударылған мәтінді соңғы кезеңде тексеру жеткіліксіз; құқықтық ұғым екі тілде жобаның бастапқы сатысынан қатар қалыптасуы тиіс. Сонда

аудармашы дайын мәтіннің сөздерін ғана емес, заң шығарушы көздеген құқықтық конструкцияны екі тілде бір мезгілде құрастырады [7].

Қылмыстық кірістерді тәркілеу саласындағы арнайы зерттеу «заңсыз жолмен» және «қылмыстық жолмен» алынған кірістер тәрізді сырттай ұқсас тіркестердің құқықтық көлемі бірдей еместігін көрсетеді. «Заңсыз» ұғымы әкімшілік, азаматтық немесе өзге құқық бұзушылықтарды да қамтуы мүмкін, ал «қылмыстық» белгі предикаттық қылмыстық құқық бұзушылықпен байланыс орнатады. Мұндай айырмашылық кірістің шығу тегін дәлелдеу, мүлікті тәркілеу және ақшаны жылыстатуды саралау кезінде шешуші болады. Терминдердің салааралық сәйкессіздігі материалдық және процестік нормаларды түрліше қолдануға алып келетіндіктен, бірыңғай «қылмыстық жолмен алынған кірістер» конструкциясын сақтау негізді [8].

Лингвистикалық коллизияны құқықтық нормалардың бәсекелестігінен және мазмұндық коллизиядан ажырату қажет. Нормалар бәсекелестігінде бір фактіге бірнеше өзара қайшы емес норма үміткер болады, ал арнайы, жалпы, бөлік және тұтас нормалардың арақатынасы бойынша біреуі таңдалады. Мазмұндық коллизияда екі норма қарама-қайшы міндет немесе құқықтық салдар белгілейді. Лингвистикалық коллизияда қайшылық көбіне бір нормативтік еріктің әртүрлі тілдік берілуінен немесе терминнің жүйе ішінде тұрақсыз қолданылуынан туындайды. Дегенмен ол нәтижесінде мазмұндық коллизияға айналуы мүмкін, өйткені әр тілдік нұсқа әртүрлі қылмыстық-құқықтық шешімге жетелейді.

Мұндай жағдайда құқық қолданушыға кезендік интерпретациялық алгоритм қажет. Бірінші кезеңде даулы сөздің нақты грамматикалық және синтаксистік шекарасы анықталады. Екінші кезеңде қазақ және орыс тілдеріндегі нұсқалар сөзбе-сөз емес, ұғымдық белгілер бойынша салыстырылады. Үшінші кезеңде Кодекстің анықтамалары, Жалпы бөлім қағидалары және сабақтас нормалар ескеріледі. Төртінші кезеңде өзгерістің заңнамалық тарихы, салыстырмалы кесте және түсіндірме материалдары тексеріледі. Бесінші кезеңде таңдалған мағына заңдылық, кінәлі жауаптылық және құқықтық айқындық талаптарымен

салыстырылады. Соңғы кезеңде қорытынды процессуалдық актіде ашық уәжделеді.

Алгоритмнің шекті ережесі - жойылмаған күмәнді адамның жағдайын нашарлататын кеңейтуші түсіндіруге айналдырмау. Қылмыстық заңның мәтініндегі мағыналық белгісіздік жаңа қылмыс құрамын жасауға, саралаушы белгіні ұқсастық бойынша қосуға немесе санкцияны ауырлатуға негіз болмауға тиіс. Бұл тәсіл соттың заң шығарушыны алмастыруын болдырмайды. Егер екі тілдегі нұсқаны жүйелік талдау арқылы бір мағынаға келтіру мүмкін болмаса, мәселе ресми заңнамалық түзетуге шығарылуы керек, ал нақты іс бойынша айыпталушының құқықтық жағдайын нашарлатпайтын шешім басым болуға тиіс.

Терминологиялық алшақтықтардың алдын алудың тиімді халықаралық ұйымдастырушылық тәсілдерінің бірі - қосарлас заң жобалау. Канаданың федералдық тәжірибесінде ағылшын және француз мәтіндері бірінің аудармасы ретінде емес, бір мезгілде әзірленетін екі түпнұсқа әрі тең беделді нұсқа ретінде құрылады. Бұл модельді тікелей көшіру міндетті емес, бірақ оның қағидасы Қазақстан үшін пайдалы: қылмыстық-құқықтық норманы әзірлеу тобына екі тілде еркін жұмыс істейтін заңгерлер, салалық мамандар және заң лингвистері бастапқы кезеңнен қатысуы қажет [9].

Бірінші институционалдық ұсыныс - қылмыстық құқықтың қазақша-орысша ұғымдық тезаурусын жасау. Ол жай аударма сөздігі болмауы тиіс. Әрбір терминге тұрақты идентификатор, екі тілдегі атау, нормативтік анықтама, тектік және түрлік байланыстар, қолданылатын баптар, рұқсат етілмейтін синонимдер, сабақтас процестік ұғымдар және мысалдық контекстер енгізілгені жөн. Мұндай тезаурус заң жобалау жүйесімен интеграцияланса, бір ұғымның жаңа редакцияда басқа баламамен кездейсоқ берілуі автоматты түрде белгіленеді. Ол соттар, прокуратура, адвокатура және жоғары оқу орындары үшін де ортақ ұғымдық база қалыптастырады.

Екінші ұсыныс - Қылмыстық кодекстің екі тілдегі параллель цифрлық корпусын және нұсқаларды бақылау жүйесін құру. Корпуста әр бап, бөлік, тармақ және термин өзара байланыстырылып, өзгерістер тарихы екі тілде бір уақытта

көрсетілуі керек. Автоматты талдау бір терминнің әртүрлі аударылуын, анықтауыштың түсіп қалуын, модальды етістіктің ауысуын, сандық шектер мен сілтемелердің сәйкессіздігін анықтай алады. Дегенмен алгоритм соңғы шешім қабылдамайды; ол сарапшыға тәуекел нүктесін көрсетеді. Құқықтық мағынаны бағалау міндетті түрде адамның кәсіби пайымымен аяқталуға тиіс.

Үшінші ұсыныс - заңдық-лингвистикалық сараптаманы формальды келісу рәсімінен тәуелсіз сапа сүзгісіне айналдыру. Сараптама қорытындысында кемінде терминологиялық бірізділік, тектік-түрлік қатынас, диспозиция элементтерінің толықтығы, модальдылық, субъект пен объект атаулары, зардап пен мөлшер санаттары, ішкі және салааралық сілтемелер тексерілуі керек. Қылмыстық жауаптылықты белгілейтін немесе күшейтетін түзетулер үшін екі тілдегі кері аударма және құқықтық салдар тесті қолданылғаны жөн: әр нұсқаны дербес оқыған екі сарапшы бірдей гипотетикалық істі бір баппен және бірдей белгілер бойынша саралай алуы тиіс.

Төртінші ұсыныс құқық қолдану практикасына бағытталады. Жоғарғы соттық түсіндірулерде терминологиялық қайшылықты анықтау мен еңсерудің өлшемдері, сот актісінде екі тілдік нұсқаны салыстыру тәртібі және жойылмайтын күмәннің құқықтық салдары бекітілуі қажет. Тергеушілер мен прокурорлар айыптау формуласында заңдағы терминді дәл пайдаланып, оның фактілік мазмұнын ашуы тиіс; аудармашыға құқықтық қорытынды жасау жүктелмеуге тиіс. Адвокаттарға екі нұсқаның айырмасын қорғау дәлелі ретінде көтеруге нақты процессуалдық мүмкіндік берілуі, ал сот лингвистикалық сараптаманың қорытындысын құқықтық түсіндіруді алмастырмайтын көмекші дәлел ретінде бағалауы керек.

Бесінші ұсыныс - анықталған коллизияларды жедел түзететін кері байланыс механизмін құру. Соттар, прокуратура, адвокаттар палаталары, ғылыми ұйымдар және азаматтар терминологиялық қайшылық туралы ұсынысты бірыңғай электрондық тізілімге енгізе алуы тиіс. Уәкілетті орган әр хабарламаны құқықтық және лингвистикалық тұрғыдан бағалап, оның мәртебесін, ұсынылған шешімін және заңнамалық түзету кезеңін ашық көрсетуі қажет. Мұндай тізілім бірдей мәселенің бірнеше рет қайталануын

азайтады, заң шығарушының жауаптылығын арттырады және қылмыстық заң мәтінінің сапасын тұрақты мониторингтеуге мүмкіндік береді.

Ұсынылған шаралардың практикалық нәтижесі тек мәтіннің көркемдігін арттыру емес. Бірізді терминология қылмыстық құқық бұзушылық құрамының белгілерін бірдей түсінуге, ұқсас істерді тең саралауға, айыптаудың шекарасын алдын ала болжауға және сот актілерінің уәжділігін күшейтуге мүмкіндік береді. Сонымен қатар ол мемлекеттік тілдегі кәсіби құқықтық дискурстың дербестігін қамтамасыз етеді: қазақша мәтін орысша нұсқаны түсіну үшін қолданылатын қосымша аударма емес, қылмыстық-құқықтық ойлау мен дәлелдеудің толыққанды құралына айналады. Бұл қылмыстық сот төрелігіне қоғамдық сенімнің тілдік негізін нығайтады.

Қорытындылай келе, Қазақстанның қылмыстық құқығындағы лингвистикалық коллизиялар редакциялық ұсақ кемшілік ретінде бағаланбауға тиіс. Терминологиялық алшақтық қылмыстық-құқықтық тыйымның көлемін, кінәнің мазмұнын, зардаптың сипатын, арнайы субъектінің шеңберін және саралаушы белгінің болуын өзгертуге қабілетті. Сондықтан оның түпкі салдары адамның іс-әрекетін басқа баппен немесе баптың неғұрлым ауыр бөлігімен саралау, дәлелдеу пәнін бұрмалау және қорғану құқығын әлсірету болуы мүмкін. Қылмыстық заңның тілдік дәлдігі осы мағынада заңдылық қағидатының материалдық құрамдас бөлігі болып табылады.

Мәселені шешу екі бағыттың бірлігін талап етеді. Біріншісі - профилактикалық бағыт: қосарлас әзірлеу, екітілді тезаурус, цифрлық корпус, міндетті сараптама және нұсқаларды автоматтандырылған салыстыру арқылы коллизияның заң мәтініне енуіне жол бермеу. Екіншісі - құқық қолданушылық бағыт: даулы терминді жүйелік талдау, екі ресми нұсқаны тең қарау, кеңейтуші түсіндіруге жол бермеу және таңдалған мағынаны сот актісінде толық уәждеу. Осы тетіктер кешенді енгізілгенде ғана қазақ және орыс тілдеріндегі қылмыстық заң мәтіндері формальды қатар өмір сүретін нұсқалардан біртұтас нормативтік еріктің шын мәніндегі теңтүпнұсқа көрінісіне айналады.

Қаржыландыру: Ғылыми мақала Қазақстан Республикасы Ғылым және жоғары білім министрлігі Ғылым комитеті қаржыландыратын, 2024-2027 жылдарға арналған ғылыми және (немесе) ғылыми-техникалық бағдарламалар бойынша бағдарламалық-нысаналы қаржыландыру аясында, ИРН BR24993217 «Қазақстан Республикасының қылмыстық құқық саласындағы заң мәтіндерінің лингвистикалық түпнұсқалығын қамтамасыз ету және заң терминологиясын үйлестіру» жобасын іске асыру шеңберінде дайындалды.

Әдебиеттер тізімі

1. Қазақстан Республикасының Конституциясы: 2026 жылғы 15 наурызда республикалық референдумда қабылданған [Электрондық ресурс]. - URL: https://adilet.zan.kz/kaz/docs/K950001000_ (қаралған күні: 28.08.2026).
2. Құқықтық актілер туралы: Қазақстан Республикасының 2016 жылғы 6 сәуірдегі № 480-V ҚРЗ Заңы [Электрондық ресурс]. – URL: <https://adilet.zan.kz/kaz/docs/Z1600000480> (қаралған күні: 21.06.2026).
3. Қазақстан Республикасының Қылмыстық кодексі: Қазақстан Республикасының 2014 жылғы 3 шілдедегі №226-V ҚРЗ Кодексі [Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/K1400000226> (қаралған күні: 21.06.2026).
4. Қазақстан Республикасындағы тіл туралы: Қазақстан Республикасының 1997 жылғы 11 шілдедегі №151-I Заңы [Электрондық ресурс]. - URL: https://adilet.zan.kz/kaz/docs/Z970000151_ (қаралған күні: 21.06.2026).
5. Сот ісін жүргізу тілі қағидатын қолданудың кейбір мәселелері туралы: Қазақстан Республикасы Жоғарғы Сотының 2016 жылғы 22 желтоқсандағы № 13 нормативтік қаулысы [Электрондық ресурс]. – URL: <https://adilet.zan.kz/kaz/docs/P160000013S> (қаралған күні: 21.06.2026).
6. Нұрбаева Н.А. Заң мәтіндеріндегі лингвистикалық қателер // Қазақстан Республикасының Заңнама және құқықтық ақпарат институтының Жаршысы. - 2024. - №2(77). - Б. 297-305. - DOI: 10.52026/2788-5291_2024_77_2_297. - URL: https://doi.org/10.52026/2788-5291_2024_77_2_297 (қаралған күні: 21.06.2026).
7. Капезов Д.Ш., Жуанышпаева С.Ж., Ауганбаева М.С., Аубакирова А.Е. Заң мәтіндерінде термин сөздердің қолданысы // М. Қозыбаев атындағы Солтүстік Қазақстан университетінің хабаршысы. - 2025. - № 4(68). - Б. 211-217. - DOI: 10.54596/2958-0048-2025-4-211-217. - URL: <https://doi.org/10.54596/2958-0048-2025-4-211-217> (қаралған күні: 21.06.2026).
8. Еркенов Б.Д., Букенесов А.С. Терминологические коллизии в уголовном и уголовно-процессуальном законодательстве Республики Казахстан при конфискации преступных доходов // Құқық қорғау органдары академиясының Жаршысы. - 2025. - № 4(38). - DOI: 10.52425/25187252_2025_38_170. - URL: https://doi.org/10.52425/25187252_2025_38_170 (қаралған күні: 21.06.2026).

9. Department of Justice Canada. Legislative Services Branch Evaluation: Evaluation Findings [Electronic resource]. - URL: <https://www.justice.gc.ca/eng/rp-pr/cp-pm/eval/rep-rap/13/lbs-dsl/p5.html> (accessed: 21.06.2026).

Кубанова Н.Б.

заң ғылымдарының магистрі,

Қазақстан Республикасы ИМ М. Есболатов атындағы

Алматы академиясы киберқауіпсіздік және ақпараттық технологиялар кафедрасының аға оқытушысы, полиция майоры

ЖАСАНДЫ ИНТЕЛЛЕКТТІ КИБЕРШАБУЫЛДАРҒА ҚАРСЫ ІС-ҚИМЫЛ ЖҮЙЕСІНДЕ ҚҰҚЫҚТЫҚ РЕТТЕУ

Қазіргі заманғы цифрлық трансформация жағдайында ақпараттық-коммуникациялық технологиялардың қарқынды дамуы мемлекеттердің экономикалық, әлеуметтік және құқықтық жүйелеріне тікелей әсер етуде. Әсіресе киберкеңістіктің кеңеюі мен цифрлық инфрақұрылымдардың күрделенуі кибершабуылдардың жаңа формаларының пайда болуына алып келді. Бұл өз кезегінде ұлттық қауіпсіздік жүйелеріне, мемлекеттік басқару органдарына және жеке секторға елеулі қауіп төндіреді. Кибершабуылдардың күрделенуі мен автоматтандырылуы жағдайында оларды анықтау және алдын алу үшін дәстүрлі әдістер жеткіліксіз болып отыр, сондықтан жасанды интеллект технологиялары киберқауіпсіздік саласында негізгі құралдардың біріне айналды [1].

Жасанды интеллект (ЖИ) жүйелері қазіргі таңда үлкен деректерді өңдеу, үлгілерді тану, аномалияларды анықтау және болжам жасау қабілетіне ие. Киберқауіпсіздік саласында бұл технологиялар желілік трафикті талдау, зиянды бағдарламаларды анықтау, фишингтік шабуылдарды алдын алу, пайдаланушылардың мінез-құлқын бақылау және инциденттерге автоматты жауап беру үшін кеңінен қолданылады. Мысалы, машиналық оқыту алгоритмдері қалыпты және күдікті әрекеттерді ажыратып, бұрын белгісіз болған шабуыл түрлерін де анықтай алады [2].

Қазіргі заманғы киберқауіпсіздік архитектурасы көпдеңгейлі қорғаныс моделіне негізделеді, оның ішінде желілік деңгей,

қолданбалы деңгей және деректер деңгейі бар. Жасанды интеллект осы барлық деңгейлерге интеграцияланып, қауіптерді ерте кезеңде анықтау мен реакция уақытын қысқартуға мүмкіндік береді. Дегенмен, мұндай интеграция жаңа жүйелік тәуекелдерді де қалыптастырады.

Ең маңызды тәуекелдердің бірі – «жалған позитив» және «жалған негатив» нәтижелерінің пайда болуы. Жасанды интеллект кей жағдайда заңды әрекеттерді қате түрде шабуыл ретінде бағалауы немесе керісінше нақты шабуылды байқамай қалуы мүмкін. Бұл мәселе киберқауіпсіздік саласында құқықтық шешім қабылдау сапасына тікелей әсер етеді.

Осыған байланысты тәуекелдерді басқарудың көпдеңгейлі құқықтық моделі қажет. Мұндай модельде техникалық бақылаумен қатар, құқықтық аудит, тәуелсіз бағалау және стандарттау тетіктері қатар жұмыс істеуі тиіс. Бұл тәсіл халықаралық тәжірибеде «AI governance framework» ретінде қарастырылады.

Сонымен қатар жасанды интеллект тек қорғаныс құралы ретінде ғана емес, киберқылмыстық әрекеттерді жүзеге асырудың жаңа тәсілі ретінде де қолданыла бастады. Қазіргі генеративті модельдер жалған мәтіндер, бейнежазбалар және дыбыстық материалдарды өте жоғары дәлдікпен жасай алады. Бұл технологиялар фишингтік шабуылдарды жетілдіруге, әлеуметтік инженерия әдістерін күшейтуге және deepfake арқылы жалған ақпарат таратуға мүмкіндік береді. Сонымен қатар жасанды интеллект автоматтандырылған түрде зиянды код генерациялап, ақпараттық жүйелердің осал тұстарын анықтай алады [3]. Бұл жағдай киберқылмыстардың сапалық тұрғыдан жаңа деңгейге өтуін білдіреді.

Жасанды интеллект жүйелері деректер негізінде үйренетіндіктен, оларда алгоритмдік дискриминация тәуекелі бар. Егер оқыту деректері тарихи немесе құрылымдық бұрмалауларды қамтыса, жүйе белгілі бір топтарға қатысты әділетсіз шешім қабылдауы мүмкін.

Киберқауіпсіздік саласында бұл мәселе ерекше маңызды, себебі жүйе белгілі бір IP-адресстерді, пайдаланушыларды немесе

аймақтарды негізсіз жоғары тәуекел санатына жатқызуы мүмкін. Мұндай жағдай құқықтық теңдік қағидатына қайшы келеді.

Халықаралық құқықтық доктринада алгоритмдік әділеттілік (algorithmic fairness) ұғымы осы тәуекелдерді азайту үшін енгізілген. Бұл қағидат деректерді теңгерімді пайдалану және шешім қабылдау логикасының ашық болуын талап етеді.

Халықаралық құқықтық тәжірибе жасанды интеллектіні реттеудің бірыңғай моделінің жоқ екенін көрсетеді, алайда бірқатар мемлекеттер бұл бағытта жүйелі қадамдар жасауда. Еуропалық Одақтың 2024 жылы қабылданған Artificial Intelligence Act (AI Act) актісі жасанды интеллектіні құқықтық реттеудің ең кешенді үлгісі болып табылады. Бұл акт тәуекелге негізделген тәсілді енгізіп, жасанды интеллект жүйелерін минималды, шектеулі, жоғары және жол берілмейтін тәуекел санаттарына бөледі [4, б.3]. Аталған құжаттың негізгі мақсаты – технологиялық инновацияларды дамыту мен адам құқықтарын қорғау арасындағы тепе-теңдікті қамтамасыз ету.

OECD ұйымының жасанды интеллект бойынша қағидаттары (OECD AI Principles) ашықтық, әділдік, қауіпсіздік және жауапкершілік қағидаттарын бекітеді [5]. Ал біріккен ұлттар ұйымының киберқылмыс жөніндегі зерттеулері цифрлық кеңістіктегі қылмыстардың трансұлттық сипатын атап өтеді және халықаралық ынтымақтастықтың маңыздылығын көрсетеді [6].

Жасанды интеллекттің маңызды функцияларының бірі – кибершабуылдарды алдын ала болжау. Predictive security жүйелері тарихи деректерге сүйене отырып, болашақтағы ықтимал шабуылдарды модельдейді.

Алайда мұндай жүйелердің құқықтық салдары күрделі. Егер жүйе белгілі бір пайдаланушыны «ықтимал қауіп» ретінде белгілеуі нәтижесінде оның аккаунты бұғатталса немесе құқықтары шектелсе, бұл адамның құқықтарына тікелей әсер етеді.

Сондықтан алдын алу модельдерін қолдану кезінде «ықтималдық шешімдердің құқықтық шектеулері» нақты регламенттелуі қажет. Бұл жерде пропорционалдық қағидаты және құқықтарды шектеудің заңдылығы басты рөл атқарады.

Қазақстан Республикасында цифрлық даму мен жасанды интеллект технологияларын енгізу белсенді түрде жүргізілуде. Дегенмен, ұлттық заңнамада жасанды интеллектіні кешенді реттеу жеткілікті деңгейде қалыптаспаған. Қолданыстағы құқықтық актілерде жасанды интеллект ұғымының нақты заңдық анықтамасы жоқ, алгоритмдік шешімдердің құқықтық салдары толық реттелмеген және киберқауіпсіздік саласында ЖИ қолдануға қатысты арнайы талаптар жеткіліксіз.

Бұл жағдай құқық қолдану тәжірибесінде бірқатар мәселелер туындатады. Біріншіден, жасанды интеллект негізінде қабылданған шешімдер үшін жауапкершілікті анықтау қиын. Екіншіден, деректерді өңдеу және пайдалану процесінде құқықтық белгісіздік бар. Үшіншіден, кибершабуылдарды алдын алу жүйелерінде қолданылатын алгоритмдердің ашықтығы жеткіліксіз деңгейде.

Киберқылмыстарды тергеуде цифрлық дәлелдемелердің рөлі ерекше. Жасанды интеллект бұл процесті автоматтандырып, үлкен деректер арасынан маңызды ақпаратты бөліп алуға мүмкіндік береді.

Алайда цифрлық дәлелдемелердің жасанды интеллект арқылы өңделуі олардың құқықтық күшіне қатысты жаңа сұрақтар туындатады. Мысалы, алгоритм арқылы алынған деректердің сотта дәлел ретінде қолданылуы үшін олардың түпнұсқалығы мен бұрмаланбағандығы дәлелденуі тиіс.

Бұл контекстте «chain of custody» қағидаты цифрлық форматқа бейімделуі қажет. Сонымен қатар алгоритмдердің жұмысын тіркеу және лог-файлдарды сақтау міндетті құқықтық талап ретінде енгізілуі мүмкін.

Осыған байланысты Қазақстан Республикасының цифрлық кодексін әзірлеу шеңберінде жасанды интеллектіні құқықтық реттеудің жүйелі моделін қалыптастыру қажет. Бұл модель келесі элементтерден тұруы тиіс: жасанды интеллект жүйелерін тәуекел деңгейі бойынша жіктеу; жоғары тәуекелді жүйелерге міндетті құқықтық және техникалық аудит енгізу; алгоритмдердің ашықтығы мен түсіндірмелілігін қамтамасыз ету; деректерді қорғау және қауіпсіздік талаптарын күшейту [7].

Жасанды интеллект қолданылған кибершабуылдар жағдайында құқықтық жауапкершілік мәселесі ерекше күрделі сипатқа ие. Қазіргі құқықтық доктринаға сәйкес жасанды интеллект құқық субъектісі болып табылмайды, сондықтан барлық жауапкершілік адамға немесе заңды тұлғаға жүктеледі. Мұндай жағдайларда жауапкершілік бірнеше субъект арасында бөлінеді: жүйені әзірлеуші, иеленуші, оператор және пайдаланушы. Әсіресе генеративті модельдерді пайдалану арқылы жасалған киберқылмыстарда кінә дәрежесін анықтау құқық қолдану тәжірибесінде маңызды ғылыми және практикалық мәселе болып отыр [8].

Киберқауіпсіздікті құқықтық реттеу бастапқыда реактивті сипатта болды, яғни тек оқиға орын алғаннан кейін әрекет етті. Қазіргі кезеңде мемлекеттер проактивті модельге көшуде, онда алдын алу және тәуекелді басқару негізгі рөл атқарады.

Қазақстан үшін бұл эволюция ерекше маңызды, себебі цифрлық инфрақұрылымның кеңеюі мемлекеттік қызметтердің толық цифрлануына алып келді. Осыған байланысты мемлекеттік реттеу тек нормативтік актілермен шектелмей, стратегиялық деңгейге көтерілуі тиіс. Цифрлық кодекс осы тұрғыда киберқауіпсіздік пен жасанды интеллектіні біріктіретін негізгі құқықтық платформаға айналуы мүмкін.

Құқық қорғау органдарының қызметінде жасанды интеллектіні қолдану киберқылмыстарды тергеу тиімділігін арттырады. ЖИ жүйелері үлкен деректер массивін талдау арқылы күдікті әрекеттерді анықтауға, цифрлық дәлелдемелерді өңдеуге және қылмыстық байланыстарды модельдеуге мүмкіндік береді. Сонымен қатар болжамдық аналитика әдістері арқылы ықтимал киберқауіптерді алдын ала анықтау мүмкіндігі бар.

Дегенмен мұндай жүйелерді қолдану барысында адам құқықтарын қорғау, дербес деректердің қауіпсіздігі және алгоритмдік шешімдердің ашықтығы міндетті түрде қамтамасыз етілуі тиіс [9].

Цифрлық егемендік мәселесі де жасанды интеллектіні реттеуде маңызды орын алады. Жасанды интеллект жүйелерінің көпшілігі шетелдік платформаларға және бұлттық инфрақұрылымдарға

тәуелді. Бұл жағдай мемлекеттердің ақпараттық тәуелсіздігіне қауіп төндіруі мүмкін. Сондықтан ұлттық жасанды интеллект экожүйесін дамыту, деректер орталықтарын құру және отандық технологияларды дамыту стратегиялық маңызды бағыт болып табылады [10].

Жасанды интеллектінің киберқауіпсіздік саласына енгізілуі тек техникалық жаңғыру емес, сонымен қатар құқықтық доктринаның трансформациясын талап ететін күрделі процесс болып табылады. Дәстүрлі құқық жүйелері көбіне адам әрекетіне негізделген жауапкершілік моделіне сүйенсе, жасанды интеллект автономды немесе жартылай автономды шешім қабылдай алатын жағдайда құқықтық себеп-салдар байланысын анықтау қиындай түседі. Бұл өз кезегінде «алгоритмдік белгісіздік» деп аталатын жаңа құқықтық феноменді қалыптастырады.

Алгоритмдік белгісіздік жағдайында жүйенің нақты қандай фактор негізінде шешім қабылдағанын анықтау мүмкін болмауы ықтимал. Әсіресе терең нейрондық желілер негізінде жұмыс істейтін модельдерде шешім қабылдау процесі «қара жәшік» (black box) сипатында болады. Мұндай жағдайда құқықтық бағалау үшін түсіндірмелілік (explainability) қағидаты ерекше маңызға ие болады. Еуропалық Одақтың AI Act актісінде де жоғары тәуекелді жүйелер үшін түсіндірмелілік және аудит талаптары осы себептен енгізілген.

Сонымен қатар киберқауіпсіздік саласында жасанды интеллектіні қолдану деректер сапасына тікелей тәуелді. Егер оқыту деректері бұрмаланған немесе толық емес болса, жүйе қате шешім қабылдауы мүмкін. Бұл құбылыс «алгоритмдік бұрмалау тәуекелі» ретінде сипатталады. Мұндай жағдайлар киберқауіпсіздік жүйелерінің сенімділігіне тікелей әсер етеді және құқықтық жауапкершілік мәселесін күрделендіреді.

Жасанды интеллект негізіндегі киберқауіпсіздік жүйелерінің тағы бір маңызды аспектісі – автоматтандырылған шешім қабылдау процесі. Кейбір жүйелер адам қатысуынсыз шабуылдарды блоктау немесе желілік қолжетімділікті шектеу сияқты әрекеттерді орындай алады. Бұл жағдайда адамның араласуынсыз қабылданған шешімдердің құқықтық салдары мәселесі туындайды. Мұндай тәжірибе жеке құқықтар мен бостандықтарға ықпал етуі мүмкін

болғандықтан, «адам бақылауы міндеттілігі» қағидатын енгізу ұсынылады.

Киберқылмыстардың жасанды интеллект арқылы күрделенуі халықаралық құқықтық ынтымақтастықтың маңызын арттырады. Себебі қазіргі кибершабуылдардың географиялық шекарасы жоқ және олар бірнеше юрисдикцияны қатар қамтуы мүмкін. Бұл жағдай трансұлттық тергеу механизмдерін жетілдіру қажеттігін көрсетеді. UNODC зерттеулерінде киберқылмыстарды тергеуде мемлекетаралық деректер алмасу және бірлескен тергеу топтарының рөлі ерекше атап өтіледі.

Қазақстан үшін бұл бағытта құқықтық инфрақұрылымды дамыту стратегиялық маңызға ие. Әсіресе киберинциденттерге жедел әрекет ету орталықтарын жасанды интеллект құралдарымен интеграциялау, ұлттық CERT жүйесін күшейту және халықаралық CERT желілерімен өзара әрекеттесуді дамыту қажет. Бұл тек техникалық емес, сонымен қатар құқықтық реттеуді талап етеді.

Жасанды интеллект технологияларының дамуы еңбек нарығына да әсер етеді, соның ішінде киберқауіпсіздік мамандарының рөлі өзгеруде. Болашақта құқық қорғау және ақпараттық қауіпсіздік саласындағы мамандар тек құқықтық біліммен шектелмей, деректер аналитикасы, машиналық оқыту және киберқауіпсіздік архитектурасы бойынша да құзыреттерге ие болуы тиіс. Бұл жаңа кәсіби стандарттарды қалыптастыру қажеттігін көрсетеді.

Осыған байланысты цифрлық құқық саласында «гибридті құзыреттер» моделін енгізу өзекті болып отыр. Бұл модель құқықтық, техникалық және аналитикалық білімнің интеграциясын көздейді. Мұндай тәсіл киберқауіпсіздік саласындағы құқық қолдану тиімділігін арттырады.

Жасанды интеллектіні құқықтық реттеу тек заң нормаларымен шектелмеуі тиіс, ол этикалық қағидаттармен тығыз байланысты болуы қажет. Әсіресе ашықтық, түсіндірмелілік, жауапкершілік және адам бақылауы қағидаттары негізгі орын алады.

Егер этикалық стандарттар құқықтық нормалармен үйлеспесе, онда технологиялық даму мен құқықтық жүйе арасында алшақтық

пайда болады. Бұл алшақтық киберқауіпсіздік саласында тәуекелдерді арттырады.

Сондықтан халықаралық тәжірибеде «ethics-by-design» және «law-by-design» тәсілдері енгізілуде, олар технологияны жобалау кезеңінен бастап құқықтық талаптарды ескеруді көздейді.

Жасанды интеллект технологияларының қарқынды дамуы киберқауіпсіздік саласында түбегейлі өзгерістерге алып келді. Бір жағынан, олар кибершабуылдарды ерте анықтау, алдын алу және тергеу тиімділігін арттыратын стратегиялық құралға айналды. Екінші жағынан, жасанды интеллекттің автономды және генеративті мүмкіндіктері киберқылмыстардың жаңа, күрделірек түрлерінің пайда болуына ықпал етуде.

Зерттеу нәтижелері көрсеткендей, қазіргі құқықтық реттеу жүйелері жасанды интеллекттің жылдам даму қарқынына толық бейімделмеген. Әсіресе алгоритмдік шешімдердің ашықтығы, жауапкершілікті бөлу, деректерді қорғау және кибершабуылдарды алдын алу салаларында құқықтық олқылықтар сақталуда. Бұл жағдай цифрлық кеңістіктегі құқықтық белгісіздікті күшейтеді.

Халықаралық тәжірибе, атап айтқанда Еуропалық Одақтың AI Акт актісі, ЭЫДҰ қағидаттары және БҰҰ-ның киберқылмысқа қатысты зерттеулері жасанды интеллектіні реттеуде тәуекелге негізделген, ашық және жауапкершілікке бағытталған тәсілдің тиімді екенін көрсетеді. Бұл модельдер технологиялық инновациялар мен адам құқықтарын қорғау арасындағы тепе-теңдікті қамтамасыз етуге бағытталған.

Қазақстан Республикасы үшін жасанды интеллектіні құқықтық реттеудің негізгі бағыты ретінде цифрлық кодекс шеңберінде бірыңғай, кешенді және жүйелі модель қалыптастыру қажеттілігі айқын көрінеді. Бұл модель алгоритмдік жүйелерді тәуекел деңгейі бойынша жіктеу, жоғары тәуекелді жүйелерге міндетті аудит енгізу, деректер қауіпсіздігін күшейту және құқықтық жауапкершілікті нақтылау элементтерін қамтуы тиіс.

Сонымен қатар құқық қорғау органдарының қызметінде жасанды интеллектіні қолдану тиімділігін арттырумен қатар, адам құқықтарын қорғау және заңдылық қағидаттарын сақтау басты талап ретінде қалуы тиіс. Осылайша, жасанды интеллект

киберқауіпсіздік жүйесінде тек техникалық құрал емес, сонымен бірге құқықтық реттеуді қажет ететін күрделі әлеуметтік-технологиялық құбылыс ретінде қарастырылады.

Жалпы алғанда, жасанды интеллект пен киберқауіпсіздік арасындағы өзара байланыс құқықтық ғылымның жаңа бағытын қалыптастырып отыр. Бұл бағыттың дамуы Қазақстан Республикасының цифрлық егемендігін нығайтуға, кибершабуылдарға қарсы іс-қимыл жүйесін жетілдіруге және цифрлық экономиканың тұрақты дамуын қамтамасыз етуге мүмкіндік береді.

Қорытындылай келе, жасанды интеллект киберқауіпсіздік саласында революциялық өзгерістер әкелгенімен, жаңа құқықтық тәуекелдерді де қалыптастырып отыр. Ол бір жағынан кибершабуылдарды анықтау мен алдын алудың тиімді құралы болса, екінші жағынан жаңа киберқылмыс түрлерінің пайда болуына себеп болуда. Осыған байланысты Қазақстан Республикасы үшін негізгі міндет – халықаралық тәжірибеге сүйене отырып, жасанды интеллектіні құқықтық реттеудің кешенді, тәуекелге негізделген және адам құқықтарын қорғауға бағытталған моделін қалыптастыру. Бұл ұлттық киберқауіпсіздікті нығайтуға және цифрлық экономиканың тұрақты дамуын қамтамасыз етуге мүмкіндік береді.

Әдебиеттер тізімі

1. OECD. AI Principles. Paris, 2019 // <https://oecd.ai>
2. ENISA. Artificial Intelligence Cybersecurity Report. 2024 // <https://www.enisa.europa.eu>
3. UNODC. Comprehensive Study on Cybercrime. Vienna, 2024 // <https://www.unodc.org>
4. Regulation (EU) 2024/1689 (AI Act). Official Journal of the EU // <https://eur-lex.europa.eu>
5. OECD. AI Risk and Governance Framework, 2024 // <https://oecd.org>
6. Конвенция о компьютерных преступлениях (Конвенция Совета Европы о киберпреступности, Convention on Cybercrime CETS № 185) (Будапешт, 23 ноября 2001 года) // https://online.zakon.kz/Document/?doc_id=30170556&pos=4;-108#pos=4;-108
7. Қазақстан Республикасының «Ақпараттандыру туралы» Заңы: 2015 жылғы 24 қарашада қабылданған, Қазақстан Республикасының №418-V Заңы.
8. Қазақстан Республикасының «Дербес деректер және оларды қорғау туралы»

Заңы: 2013 жылғы 21 мамырда қабылданған, №94-V.
9. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 Об утверждении Концепции кибербезопасности («Киберщит Казахстана»).

10. World Economic Forum. Global Cybersecurity Outlook 2025 // <https://weforum.org>

A. Kussainova
Doctor of Philosophy (PhD)

HARMONIZATION OF LEGAL TERMINOLOGY AND LINGUISTIC AUTHENTICITY IN THE CRIMINAL LAW OF KAZAKHSTAN

Financing. The scientific article was prepared within the framework of program-targeted funding for scientific and (or) scientific and technical programs for 2024-2027, aimed at implementing the project IRN BR 24993217 “Harmonization of legal terminology and linguistic authenticity of the texts of laws in the field of criminal law of the Republic of Kazakhstan”, financed by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan.

Modern criminal legislation of the Republic of Kazakhstan is developing in the context of active interaction with international organisations and the legal systems of other states [1]. Kazakhstan is a party to numerous international agreements aimed at combating crime, including the United Nations Convention against Corruption and the United Nations Convention against Transnational Organized Crime [2]. This interaction requires not only the alignment of national legislation with international standards, but also precise terminological consistency.

The harmonisation of legal terminology in the sphere of criminal law is a complex, multi-level process aimed at achieving conceptual equivalence between different legal systems. Its main objective is to ensure the uniform and consistent interpretation and application of criminal law provisions, irrespective of the legal context in which they are used – whether in domestic criminal practice, international agreements, or cross-border cooperation between law enforcement agencies.

The process of terminological harmonisation requires compliance with a number of key criteria:

1) legal precision - each term must have a strict and unambiguous meaning within a defined legal category, without allowing for free or arbitrary interpretation;

2) lexical-semantic equivalence - when translating international instruments or comparing legal provisions of different states, terms must convey the same intended conceptual meaning;

3) cultural and legal adaptability - terms must be embedded in the national legal system in such a way that their legal function is preserved, while the linguistic, historical and legal specificities of the country are considered.

Kazakhstan has ratified key international legal instruments governing the fight against crime. Article 218 of the Criminal Code of the Republic of Kazakhstan defines Legalization (laundering) of money and (or) other property, received by criminal way, [3] which generally corresponds to the provisions of Article 6 “Criminalization of the Laundering of Proceeds of Crime” of the United Nations Convention against Transnational Organized Crime. Nevertheless, the concept of “property received by criminal way” is not defined in detail in the legislation of the Republic of Kazakhstan, which may complicate its application.

A similar problem is observed in Article 366 of the Criminal Code of the Republic of Kazakhstan, “Acceptance of a bribe”. Within the framework of international anti-corruption legislation, in particular the United Nations Convention against Corruption, the concept of “public official” covers a broad range of individuals and entities defined on the basis of functional and legal criteria:

1) persons endowed with authority within the system of state power - legislative, executive, administrative or judicial - regardless of the nature of the conferral of authority (appointment or election), the form of employment (temporary or permanent), the level of the position held, and irrespective of whether they receive remuneration for their activities;

2) other entities performing public functions on behalf of the State, including employees of state-owned enterprises, institutions and public-sector organizations;

3) the status of a public official may be established directly in the national legislation of the relevant State. Any other person defined as a “public official” under domestic law.

In accordance with subparagraph 26 of paragraph 1 of Article 3 of the Criminal Code of the Republic of Kazakhstan a public official is defined as a person who permanently, temporarily, or by special authority exercises the functions of representative of authority or performing organizational/management or administrative-and-household functions in the state bodies, local government bodies, as well as in Armed Forces of the Republic of Kazakhstan, other military forces and military formations of the Republic of Kazakhstan. The concept of “public official” under the Convention is interpreted more broadly than the corresponding category under the national legislation of the Republic of Kazakhstan.

Such divergences affect the scope of criminal liability and Kazakhstan’s compliance with its international obligations. Thus, the United Nations Convention against Transnational Organized Crime uses the concept of an “organized criminal group”, which is characterized by a degree of permanence, a hierarchical structure, and a common purpose. By contrast, Article 262 of the Criminal Code of the Republic of Kazakhstan, “Creation and management of organized group, criminal organization, as well as participation in them”, provides a narrower set of criteria and does not expressly recognize its transnational nature.

The Republic of Kazakhstan has a unique bilingual legal system, where the Kazakh language holds the status of the state language, while the Russian language is officially used alongside Kazakh in the activities of state bodies (Article 9 of the Constitution of the Republic of Kazakhstan) [4]. This means that all laws, including the Criminal Code of the Republic of Kazakhstan, are published simultaneously in two languages, and both versions have equal legal force and are legally binding (paragraph 30 of Article 1 of The Law of the Republic of Kazakhstan "On legal acts") [2].

On the one hand, such a model ensures accessibility of legal provisions for speakers of both languages; on the other hand, it requires full semantic equivalence between the two versions. In practice, however, discrepancies are often observed in legal terminology and syntactic

structure, which can create uncertainty in the interpretation of legal provisions and lead to differences in their application.

In accordance with Article 93 of the Constitution of the Republic of Kazakhstan, “The President of the Republic creates conditions for the comprehensive functioning of the Kazakh language as the state language and for the development of the Russian language as the language of interethnic communication”. The Constitution of the Republic of Kazakhstan does not establish the primacy of one language over the other in legal application, which creates the need for legal and linguistic equivalence between both language versions of legislation.

With regard to the relevant legislation, the Law of the Republic of Kazakhstan “On Languages in the Republic of Kazakhstan” [2]. should be considered first. According to Article 21 of this Law: “Official texts of regulatory legal acts are drafted in the state language and translated into Russian. In the event of discrepancies in meaning between the texts in the state language and in Russian, the text in the state language shall prevail.” However, in practice, regulatory legal acts are often drafted in Russian and subsequently translated into Kazakh, which undermines the intended logic of linguistic priority.

In accordance with subparagraph 3 of paragraph 3 of Article 24 of the Law of the Republic of Kazakhstan on Legal Acts, “the texts of regulatory legal acts in Kazakh and Russian must be authentic in both languages.” As some scholars note, failure to comply with this requirement leads to ambiguity in the interpretation of legal provisions, divergent understandings, and, consequently, problems in law enforcement. This is especially critical in criminal law, where even the slightest ambiguity in a legal provision may affect the implementation of the principles of legality, justice, and human rights.

Linguistic authenticity is understood as the equivalence of legal provisions expressed in different languages, in which the same legal meaning is preserved without distortion, expansion, or narrowing of the scope of legal regulation. This principle is enshrined in a number of international instruments, including the Vienna Convention on the Law of Treaties (1969), which confirms the equal authenticity of texts in different languages, and the UN Guidelines on Legislative Drafting

(UNODC, 2020), which emphasise the importance of linguistic precision in preventing legal errors.

In Kazakhstan, in such a bilingual legal system, linguistic authenticity ensures:

- legal certainty;
- protection of individuals' right to understand the law in their native language;
- effective implementation of international obligations, including the bilingual drafting of ratified conventions and treaties.

One of the key problems in the legislative process in Kazakhstan lies in ensuring substantive equivalence of legal provisions in Kazakh and Russian.

In legal theory, a distinction is made between the linguistic and legal components of textual authenticity. Linguistic authenticity refers to the accuracy of translation and the use of equivalent linguistic means, whereas legal authenticity requires the equivalence of normative content and legal effects in both versions of the document. For criminal law, this is particularly important: the precise choice of terminology and formulations in two languages ensures a uniform understanding of the elements of an offence, the features of the unlawful act, sanctions, and so forth.

In criminal law, the linguistic authenticity of legal provisions is directly linked to guarantees of legality. A provision formulated differently in each language gives rise to a conflict of meanings - its content becomes unclear, which may allow for divergent interpretations or selective application.

The linguistic authenticity of criminal law texts ensures a unified legal regulatory space in conditions of linguistic plurality and serves as a guarantee that the punishability of acts and the applicable sanctions are understood uniformly by all participants in legal relations, regardless of language.

In practical terms, this means that when laws are drafted and adopted, the two versions of the text are subject to mandatory verification. Thus, in accordance with paragraph 26 of the Rules of Procedure of the Mazhilis of the Parliament of the Republic of Kazakhstan, a draft law in paper and electronic form is submitted to the Mazhilis in Kazakh and

Russian, with the necessary annexes (materials to the draft law), accompanied by a conclusion on the preliminary verification of the authenticity of the texts to each other. Similarly, the Rules of Procedure of the Government place responsibility on state bodies for the quality of draft preparation in the state language and for compliance with the requirements of textual authenticity in both languages.

The Kazakh legislator has established a fundamental principle: scientific expertise (including legal, linguistic, anti-corruption, economic, and other types of expertise) may be carried out in respect of draft regulatory legal acts, depending on the legal relations governed by those acts (paragraph 1 of Article 30 of the Law of the Republic of Kazakhstan on Legal Acts).

Scientific linguistic expertise is carried out in respect of draft legislative acts as regards the authenticity of their texts in Kazakh and Russian. Such expertise is conducted by the Centre for Linguistics, which is a structural subdivision of the «Institute of Legislation and Legal Information of the Republic of Kazakhstan» [3].

Lack of consistency between the Kazakh and Russian versions of legal provisions creates significant difficulties for law enforcement. In some cases, this merely leads to the need to compare the two texts and consult experts; in others, it results in judicial errors, the quashing of judgments, and delays in proceedings due to the need for official clarification.

In some cases, bilingual versions of draft laws are prepared by translators and linguists who do not possess specialized legal knowledge. A lack of understanding of the legal nature of terms, the specifics of their application in legislation, and the interrelationship between legal provisions often leads to a loss of terminological precision and even to changes in the substantive content of legal provisions. As a result, discrepancies may arise in law enforcement, creating risks to the uniform interpretation and application of legal provisions.

With regard to legislative initiatives prepared by state bodies and to be submitted to Parliament, the conduct of the above-mentioned expertise is a mandatory requirement ensuring the accuracy and equivalence of bilingual texts (Article 31 of the Law of the Republic of Kazakhstan on Legal Acts).

The introduction of mandatory linguistic and legal expertise at all stages of law-making has made it possible to minimize conceptual distortions and ensure genuine authenticity of texts in both languages.

An analysis of the current Criminal Code of the Republic of Kazakhstan reveals numerous instances of incomplete equivalence between the Kazakh and Russian versions of the text. Thus, in the criminal law doctrine of the Republic of Kazakhstan, the concept of “Guilt (culpability)” (Article 19 of the Criminal Code of the Republic of Kazakhstan) encompasses both the intellectual element - a person’s awareness of the factual nature and social harmfulness of their act - and the volitional element, reflecting the subject’s mental attitude towards the consequences of the socially dangerous act (intent or negligence). In Russian, this term has a clearly established legal meaning confined within the framework of criminal law. In the Kazakh version, however, the word “кіна” is used, which in everyday and moral-ethical usage may mean “fault”, “sin”, or “condemnable misconduct”, without a clear distinction between the forms of culpability. Such a semantic divergence means that the Kazakh term does not always fully convey the normatively established structure of the subjective side of the offence, in particular the distinction between intent and negligence, which may create risks of ambiguous interpretation in law enforcement and in the translation of criminal law provisions.

Further, the term “legalisation (money laundering)” in Russian and “ақшаны заңдастыру (жылыстату)” in Kazakh does not fully reflect the substance of financial schemes (Article 218 of the Criminal Code of the Republic of Kazakhstan, “Legalization (laundering) of money and (or) other property, received by criminal way”).

The term “bribe” is translated as “пара” or “сыйлық” (Article 366 of the Criminal Code of the Republic of Kazakhstan, “Acceptance of a bribe”), the latter of which may be interpreted as a gift, thereby undermining legal certainty.

Thus, literal translation often leads to semantic and legal distortions. Semantics plays a crucial role, especially in the translation of legal terms, since even a slight deviation in meaning may lead to misinterpretation of a legal provision.

The experience of selected foreign jurisdictions with bilingual or multilingual law-making is of particular interest. In Canada, under this model, every law is drafted and harmonised simultaneously in English and French. To ensure legal authenticity, both versions of the text undergo independent legal-linguistic review. Under Canada's Official Languages Act (1969), both texts have equal legal force, and neither is accorded priority. The responsible bodies are English- and French-speaking groups of legislative drafters who prepare draft legislation in parallel, coordinating terminology, style, and legal meaning [3].

The concept of the “equal authenticity rule” has emerged, according to which neither language version has priority, and equal weight must be given to both versions in interpretation. In judicial practice, this is implemented through the shared meaning rule: where the two texts diverge, courts seek an interpretation that reflects the meaning common to both versions [3]. In this way, the uniformity of legal provisions is ensured irrespective of linguistic expression.

In Switzerland, where German, French, and Italian are the official languages, legislative acts are drafted and published simultaneously in three languages [4]. The translation process is carried out with the involvement of specialists in legal linguistics. In the event of divergence between versions, all official languages may be used to ascertain the authentic meaning of the provision [5].

The experience of Canada and Switzerland provides important guidance for Kazakhstan. First, it demonstrates the importance of genuine adherence to the principle of equal authenticity of languages and the development of a culture of parallel law-making. It is also important to strengthen linguistic expertise, involve specialists in both languages at all stages of drafting, and train judges in working with bilingual texts. Such an approach enhances legal certainty in legal application and reduces the risk of errors arising from discrepancies between language versions [7].

The analysis conducted shows that, under conditions of official bilingualism in the Republic of Kazakhstan, the linguistic authenticity of regulatory legal acts – especially in the sphere of criminal law – is not merely a linguistic category, but also a legal one of decisive importance for ensuring the principles of legality, justice, and uniform law enforcement. Terminological divergences between the Kazakh and

Russian versions of the Criminal Code may distort the legal meaning of norms, complicate the qualification of acts and give rise to legal uncertainty [8].

The article demonstrates that achieving lexical-semantic equivalence of legal texts is impossible without a systemic approach, encompassing both institutional measures and regulatory frameworks. Important directions in this area include the introduction of mandatory legal-linguistic expertise at all stages of law-making, the development of glossaries with a unified conceptual apparatus, and the use of digital tools for authenticity control [9].

In order to eliminate the identified problems and improve the quality of legal regulation, it appears advisable to:

1. Develop and approve a Unified Dictionary of Legal Terms in Kazakh and Russian, for mandatory use in the preparation of draft laws, translation, and official publication of legal acts;

2. Establish a permanent interdisciplinary expert commission (comprising lawyers, linguists, and IT specialists) to coordinate the processes of terminological harmonisation and authentic translation.

Thus, the improvement of bilingual terminology policy is not only a matter of linguistic culture, but also a necessary condition for strengthening the rule of law and citizens' trust in the legal system.

References

1. United Nations Convention against Corruption. New York, 31 October 2003// https://treaties.un.org/pages/viewdetails.aspx?src=treaty&mtdsg_no=xviii-14&chapter=18

2. United Nations Convention against Transnational Organized Crime. New York, 15 November 2000// https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en

3. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 08.03.2026 г.)// https://prg.kz/document/?doc_id=31575252

4. Конституция Республики Казахстан (принята на республиканском референдуме 15 марта 2026 года)// URL: https://continent-online.com/Document/?doc_id=35502996

5. Закон Республики Казахстан от 6 апреля 2016 года № 480-V «О правовых актах» (с изменениями и дополнениями по состоянию на 01.01.2026 г.)// https://prg.kz/document/?doc_id=37312788)

6. Legislative Services Branch Evaluation//<https://www.justice.gc.ca/eng/csj-sjc/legis-redact/index.html>
7. Lambert N. Bill 96 erodes legislative language equality // *Policy Options*. 2025. //policyoptions.irpp.org/policyoptions.irpp.org.
8. Federal Constitution of the Swiss Confederation of 18 April 1999 (Status as of 3 March 2024)// <https://www.fedlex.admin.ch/eli/cc/1999/404/en>
9. Colin D Robertson Multilingual Legislation in the European Union. EU and National Legislative-Language Styles and Terminology// *Research in Language*, 2011, vol. 9.1. – P.51-67

Кусаинова А.К.
доктор философии (PhD),
профессор ШПИГУ Университет Нархоз

ЮРИДИКО-ЛИНГВИСТИЧЕСКИЕ ПРОБЛЕМЫ ФОРМИРОВАНИЯ И ГАРМОНИЗАЦИИ УГОЛОВНО-ПРАВОВОЙ ТЕРМИНОЛОГИИ РЕСПУБЛИКИ КАЗАХСТАН

Язык права представляет собой не только средство внешнего выражения нормативных предписаний, но и один из важнейших инструментов формирования, закрепления и передачи содержания правовых понятий. Юридический термин выполняет в законодательстве особую функцию: посредством него определенное социальное явление приобретает специальное нормативное значение, включается в систему юридических категорий и становится элементом механизма правового регулирования. Поэтому качество законодательства зависит не только от содержания устанавливаемых государством правил поведения, но и от точности понятийно-терминологического аппарата, используемого для их выражения.

Особенно высокие требования к терминологической определенности предъявляются в уголовном праве. Здесь значение отдельного термина непосредственно связано с определением преступности и наказуемости деяния, признаков состава уголовного правонарушения, форм вины, оснований уголовной ответственности, видов наказаний, обстоятельств освобождения от

ответственности и иных категорий, способных затрагивать права и свободы человека. Терминологическая неопределенность, использование одного понятия в различных значениях либо неадекватная передача его содержания в другом языке способны выйти за пределы лингвистической погрешности и приобрести собственно юридическое значение.

Для Республики Казахстан проблема формирования уголовно-правовой терминологии имеет особую специфику. Она развивается под воздействием одновременно нескольких процессов: укрепления функциональной роли государственного языка, сохранения устойчивой русскоязычной юридической традиции, интенсивного обновления законодательства, развития национальной юридической науки, включения международно-правовых понятий в отечественный правопорядок и появления новых сфер уголовно-правового регулирования. Именно сочетание указанных факторов определяет необходимость рассмотрения терминологии не как совокупности отдельных переводческих решений, а как самостоятельной системы юридических понятий.

Дополнительное значение проблема приобретает в связи с конституционным регулированием языковой сферы. В соответствии с новой Конституцией Республики Казахстан, принятой на республиканском референдуме 15 марта 2026 года, государственным языком Республики Казахстан является казахский язык. Статья 9 Конституции предусматривает, что в государственных организациях и органах местного самоуправления наряду с казахским официально употребляется русский язык [1].

Данная конституционная модель обуславливает функционирование юридической терминологии в условиях постоянного взаимодействия двух языков в сфере законодательства и государственной деятельности.

Законодательство Республики Казахстан непосредственно закрепляет требования к качеству языка нормативных правовых актов. Закон Республики Казахстан от 6 апреля 2016 года «О правовых актах» предусматривает, что текст нормативного правового акта должен излагаться с соблюдением норм литературного языка, юридической терминологии и юридической

техники, быть предельно кратким и содержать четкий смысл, не допускающий различного толкования. Закон также прямо устанавливает требование аутентичности текстов нормативных правовых актов на казахском и русском языках [2].

Особое значение имеет закрепленное в данном Законе правило о легальных дефинициях. Если возникает необходимость уточнить значение используемого понятия, нормативный правовой акт может содержать специальную норму, разъясняющую соответствующий термин. При этом термины и определения должны соответствовать понятиям, применяемым в вышестоящем нормативном правовом акте, регулирующем однородные общественные отношения.

Эти положения позволяют сделать важный вывод: терминологическая системность в Казахстане уже является не только научным или лингвистическим пожеланием, но и требованием юридической техники. Законодатель фактически исходит из необходимости вертикальной согласованности понятийного аппарата - термин, закрепленный актом более высокой юридической силы, должен сохранять свое содержание в актах нижестоящего уровня.

Однако наличие нормативных требований само по себе не устраняет терминологических проблем. Основные сложности проявляются при разработке новых понятий, выборе их языкового выражения, соотнесении казахской и русской терминологии, а также последующем использовании терминов в законодательстве, правоприменительной деятельности и юридической доктрине. Одной из центральных задач современного этапа является дальнейшее развитие казахского языка как полноценного языка уголовного законодательства, юридической науки и профессиональной правоприменительной деятельности.

При этом представляется неправильным ставить вопрос как проблеме «отсутствия» казахской юридической терминологии. Современное уголовное законодательство располагает сформированным массивом базовых понятий: қылмыс, жаза, кінә, қылмыстық жауаптылық, қылмыстық құқық бұзушылық, қылмыстық теріс қылық и др. Основная проблема заключается не в наличии или отсутствии отдельных слов, а в обеспечении

системности их значений, устойчивости употребления и понятийной взаимосвязи.

Юридический язык отличается от общеупотребительного тем, что каждый термин существует в определенной системе. Понятие «преступление» связано с общим понятием уголовного правонарушения, категория вины - с умыслом и неосторожностью, наказание - с установленной системой его видов, соучастие - с определенными формами совместного участия в уголовном правонарушении. Поэтому совершенствование отдельного термина без учета его системных связей может породить новые противоречия.

Следовательно, развитие казахской уголовно-правовой терминологии должно строиться не по модели накопления новых переводных эквивалентов, а по принципу формирования целостной понятийно-терминологической системы.

Это положение имеет особое значение в условиях постоянного обновления законодательства. Право все чаще сталкивается с явлениями, для обозначения которых отсутствует длительная национальная терминологическая традиция. Цифровизация, новые способы совершения уголовных правонарушений, транснациональная организованная преступность, финансирование терроризма, киберпреступность и иные явления приводят к расширению понятийного аппарата. Исходный материал обоснованно связывает современное развитие казахской юридической лексики с одновременным использованием национальных эквивалентов, интернациональной лексики, заимствований и неологизмов.

Для права первичным критерием должна оставаться юридическая функциональность термина. Термин должен точно выражать понятие, обладать устойчивым значением, быть понятным профессиональному сообществу, соответствовать системе уже закрепленных категорий и не создавать дополнительных возможностей для неоднозначного толкования. Данный критерий представляется более значимым, чем этимологическая природа соответствующего слова.

Серьезная юридико-лингвистическая проблема возникает при терминологизации слов естественного языка. Большинство юридических терминов не создается полностью искусственно:

право использует общеупотребительную лексику, придавая ей специальное нормативное содержание.

В праве термин приобретает содержание благодаря совокупности нормативных признаков. Поэтому при выборе казахского эквивалента необходимо устанавливать не только обычное словарное значение соответствующей единицы, но и отвечать на вопрос, способен ли данный термин устойчиво обозначать конкретную юридическую категорию во всех предусмотренных законодательством контекстах.

Отсюда следует необходимость разграничения трех видов значения: общеязыкового, доктринального и легального. Общеязыковое отражает использование слова в естественном языке; доктринальное складывается в юридической науке; легальное непосредственно закрепляется законодательством. При возникновении расхождений именно нормативное содержание определяет применение уголовно-правового термина, однако его языковая форма при этом должна быть достаточно удачной, чтобы не провоцировать устойчивое ошибочное восприятие.

Легальная дефиниция может способствовать решению данной проблемы, однако она не должна использоваться для компенсации заведомо неудачного наименования. Оптимальным является такое соотношение, при котором термин семантически соответствует обозначаемой категории, а законодательная дефиниция уточняет ее специальные юридические признаки.

Следует отметить, что одной из наиболее сложных проблем казахстанской юридической лингвистики является обеспечение смысловой согласованности казахского и русского текстов нормативных правовых актов.

В научной литературе обращается внимание на случаи неодинакового выражения юридических конструкций, терминологической непоследовательности и различий, способных влиять на восприятие содержания нормы [3]. Терминологическое расхождение может возникнуть еще до начала собственно переводческой деятельности. Причиной способны стать неопределенность исходного понятия, чрезмерно сложная конструкция нормы, несогласованность используемой терминологии с другими нормативными

актами либо отсутствие устойчивого способа выражения соответствующего института средствами одного из языков.

Поэтому юридический перевод принципиально отличается от обычного перевода текста. Его объектом в конечном счете является не совокупность предложений и слов, а нормативное содержание правового предписания. Это обстоятельство требует переосмыслить традиционную модель: «исходный текст - перевод текста» к конструкции «правовое понятие - два адекватных способа его нормативного выражения».

Различие между этими моделями носит не только теоретический характер. При буквальном переводе законодательная конструкция одного языка может механически воспроизводиться средствами другого, несмотря на различия синтаксиса, семантики и традиций юридического письма. В результате формально близкие тексты способны оказаться различными по ясности либо даже по смысловым оттенкам.

При понятийно ориентированном подходе отправной точкой является юридическая норма. Специалисты определяют, какой именно правовой результат должен быть закреплён, а затем формулируют его средствами каждого языка с соблюдением требований соответствующей языковой системы.

Отсюда следует необходимость более активного использования параллельного правового редактирования. Казахоязычные и русскоязычные специалисты должны участвовать в формировании наиболее значимых нормативных конструкций не исключительно на стадии окончательного перевода, а еще при разработке правового содержания проекта. Мы полагаем, что такой механизм способен одновременно повысить качество государственного языка законодательства и уменьшить риск смысловых расхождений.

Уголовно-правовая терминология представляет собой иерархически организованную систему. Поэтому проверка качества отдельного перевода без анализа его связи с другими категориями является недостаточной.

Показателен понятийный ряд, закреплённый статьей 10 УК РК [4]. Уголовные правонарушения подразделяются на преступления и уголовные проступки. Таким образом, понятие «уголовное

правонарушение» является родовым, а «преступление» и «уголовный проступок» - видовыми категориями.

В казахской терминологии данная система выражается соответствующим соотношением: қылмыстық құқық бұзушылық - родовое понятие; қылмыс - преступление; қылмыстық теріс қылық - уголовный проступок.

Аналогичную структуру имеют и многие другие уголовно-правовые институты. Категория вины раскрывается через формы психического отношения лица к деянию; институт соучастия включает самостоятельные формы и виды участников. Из этого следует важный практический вывод: существующего формата обычного двуязычного юридического словаря недостаточно для обеспечения терминологической гармонизации.

Существующая проблема показывает необходимость более тесного взаимодействия юридической науки и лингвистики. Юрист и лингвист исследуют нормативный текст с различных позиций. Юрист устанавливает содержание понятия, его место в правовой системе и нормативные последствия. Лингвист оценивает семантическую структуру, соответствие языковым нормам, однозначность и естественность выражения. Специалист в области юридического перевода должен одновременно учитывать оба уровня. Именно поэтому терминологическая экспертиза не может эффективно осуществляться специалистом только одной профессиональной области.

Юрико-лингвистическая экспертиза должна осуществляться не только после завершения работы над законопроектом, но и на стадии формирования его понятийного аппарата.

Если лингвист получает полностью подготовленный текст исключительно для исправления стилистики или перевода, возможности устранения концептуального терминологического дефекта уже существенно ограничены.

Эффективная модель предполагает участие отраслевых юристов, специалистов по юридической технике, лингвистов и переводчиков при: формировании перечня основных понятий будущего акта; определении их содержания; выборе терминов на государственном языке; согласовании казахских и русских

формулировок; проверке соответствия понятий терминологии вышестоящих и смежных актов; итоговом юридико-лингвистическом редактировании.

При этом стратегическое значение имеет развитие подготовки специалистов с междисциплинарной компетенцией в области права и лингвистики. Юрист, не учитывающий семантические особенности языка, способен сформулировать юридически понятную, но лингвистически неудачную конструкцию. В свою очередь, переводчик, не понимающий уголовно-правовой доктрины, может подобрать формально правильный эквивалент, изменяющий нормативное содержание понятия.

Поэтому юридическая лингвистика должна рассматриваться не как вспомогательное филологическое направление, а как один из механизмов обеспечения качества и определенности законодательства.

Одним из перспективных направлений решения выявленных проблем является цифровизация работы с юридической терминологией. Современное законодательство представляет собой большой и постоянно изменяющийся массив текстов. Ручное сопоставление всех вариантов использования конкретного понятия требует значительных ресурсов и не всегда позволяет обнаружить скрытые терминологические расхождения.

Национальная цифровая система юридической терминологии могла бы содержать для каждой терминологической единицы: казахское и русское обозначение; легальную дефиницию либо доктринальное определение при отсутствии законодательной; нормативный источник; дату появления термина в законодательстве; историю изменения его формулировки; родовые и видовые понятия; смежные и потенциально смешиваемые категории; международные эквиваленты; допустимые варианты перевода; указание на случаи расхождения терминологии в различных нормативных актах. Такая система позволила бы перейти от статичного словаря к динамической цифровой карте юридических понятий.

При разработке законопроекта специалист мог бы автоматически получать информацию о том, используется ли предлагаемый термин в действующем законодательстве, какое

значение уже закреплено за ним и существует ли другой вариант обозначения того же понятия.

Особый потенциал здесь имеют технологии обработки естественного языка и искусственного интеллекта. Они способны осуществлять автоматизированное сопоставление больших массивов нормативных текстов, выявлять терминологические коллизии, устанавливать неодинаковые варианты перевода и обнаруживать изменение семантического контекста.

Проведенный анализ позволяет сделать вывод о том, что проблемы формирования и гармонизации уголовно-правовой терминологии Республики Казахстан имеют комплексный юриди́ко-лингвистический характер. Их нельзя сводить исключительно к вопросам перевода нормативных правовых актов с одного языка на другой, поскольку терминологические сложности возникают уже на стадии формирования самого правового понятия, определения его содержания, места в системе уголовного права и выбора соответствующего языкового обозначения. Именно поэтому качество уголовного законодательства напрямую зависит от внутренней согласованности его понятийно-терминологического аппарата.

Особенность казахстанской модели заключается в необходимости обеспечения устойчивого функционирования уголовно-правовой терминологии в условиях взаимодействия казахского и русского языков в сфере законодательства и правоприменения. При этом ключевая задача состоит не в формальном совпадении языковых конструкций, а в достижении их смысловой и функциональной эквивалентности. Юри́дический перевод должен быть ориентирован прежде всего на воспроизведение нормативного содержания правового предписания, а не на буквальное воспроизведение лексической и синтаксической структуры исходного текста. В этой связи перспективным представляется переход от модели последовательного перевода к понятийно ориентированному параллельному правовому редактированию, при котором единое правовое содержание получает адекватное выражение средствами каждого языка.

Не менее важным условием является институционализация взаимодействия юристов, лингвистов и специалистов в области юридического перевода. Юрико-лингвистическая экспертиза должна осуществляться не только на завершающей стадии подготовки законопроекта, но и в процессе формирования его понятийного аппарата. Это позволит выявлять и устранять терминологические дефекты до того, как они получают нормативное закрепление. В долгосрочной перспективе особое значение имеет подготовка специалистов с междисциплинарной компетенцией в области права и лингвистики.

Отдельное направление совершенствования связано с цифровизацией терминологической работы. Создание национальной цифровой системы юридической терминологии, включающей казахские и русские обозначения, легальные и доктринальные дефиниции, их системные связи и международные эквиваленты, позволило бы перейти от статичного словаря к динамической цифровой карте правовых понятий. Такая система могла бы использоваться как инструмент мониторинга законодательства, выявления терминологических расхождений и предварительной экспертной проверки проектов нормативных правовых актов. Технологии искусственного интеллекта и обработки естественного языка способны существенно расширить возможности такого анализа, однако окончательная оценка юридической эквивалентности должна оставаться за специалистом.

Таким образом, гармонизацию уголовно-правовой терминологии Республики Казахстан целесообразно рассматривать как **системный процесс формирования, нормативного закрепления, межъязыкового согласования и последующей стабилизации юридических понятий в законодательстве, правоприменении, науке и образовании.** Ее конечной целью должно быть не формальное единообразие терминов, а создание внутренне согласованного и устойчивого уголовно-правового понятийного аппарата, обеспечивающего точность законодательного регулирования, развитие государственного юридического языка и единообразие правоприменительной практики.

Финансирование: Статья подготовлена в рамках грантового финансирования по научным и (или) научно-техническим программам на 2024-2026 годы, направленная на реализацию проекта BR 24993217 «Гармонизация юридической терминологии и лингвистическая аутентичность текстов законов в области уголовного права Республики Казахстан», финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан

Список использованных источников

1. Конституция Республики Казахстан, принятая на республиканском референдуме 15 марта 2026 года, вступившая в силу с 1 июля 2026 года// <https://adilet.zan.kz/rus/docs/K2600000000>
2. Закон Республики Казахстан от 6 апреля 2016 года № 480-V ЗРК «О правовых актах»// https://prg.kz/document/?doc_id=37312788
3. Тукабаева Ж.А. Проблемы юридической лингвистики государственного языка при переводе на русский язык в Республике Казахстан // *Russian Insights: Literature, Culture and Linguistics*. 2024. - №1. - С. 37–41.
4. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V// https://prg.kz/document/?doc_id=31575252&pos=22;159

Yeerkenbieke Zhuledezi

Master's student 1 year

Faculty of Law AL-Farabi Kazakh National University

CRIMINOLOGICAL CHARACTERISTICS OF THE CAUSES AND CONDITIONS OF JUVENILE DELINQUENCY (BASED ON THE EXPERIENCE OF THE REPUBLIC OF KAZAKHSTAN AND THE PEOPLE'S REPUBLIC OF CHINA)

Juvenile delinquency remains one of the most persistent challenges confronting legal systems worldwide, and both the Republic of Kazakhstan and the People's Republic of China have witnessed significant shifts in the nature and scale of youth offending in recent years. While the two countries share certain historical legacies in their approaches to juvenile justice, their respective trajectories of social transformation, economic development, and legal reform have produced

distinctive patterns in the causes and conditions of juvenile delinquency. This paper undertakes a comparative criminological analysis of the principal determinants of juvenile offending in Kazakhstan and China, examining the interplay between family, school, community, and digital-environment factors within each national context.

In both Kazakhstan and China, family-related factors consistently emerge as the most significant criminogenic conditions associated with juvenile offending. Kazakhstani criminological research identifies dysfunctional families as a primary source of criminogenic influence, alongside difficulties in social adaptation within the learning community and divergent perceptions of social justice among adolescents. Empirical data from Kazakhstani law enforcement agencies indicate that the absence of proper parental oversight constitutes the most characteristic cause of juvenile crime, with a substantial proportion of juvenile offenders—approximately 55 percent—being neither employed nor enrolled in educational institutions at the time of their offence.

Chinese studies similarly emphasize the centrality of family factors. A quantitative analysis of China's 2019 Recidivism Survey conducted by the Ministry of Justice revealed a significant correlation between negative parenting practices, poor parent-child relationships, and elevated rates of juvenile delinquency. Insufficient parental supervision was found to directly impair adolescents' self-regulation capacity, thereby increasing their propensity for delinquent behaviour. Chinese scholars further note that family love deficits and improper parenting methods exert profound influence on minors' value orientations and behavioural patterns, with rural left-behind children and single-parent family backgrounds disproportionately represented among juvenile offenders.

School disengagement represents a second convergent risk domain. In Kazakhstan, researchers have documented that difficulties in social adaptation within educational institutions contribute to the transformation of the criminological portrait of juvenile offenders, with peer group influence and hierarchical dynamics within delinquent subcultures playing significant roles. Chinese research similarly identifies school-related risk factors, including hidden dropout—particularly at the middle-school level—and inadequate school supervision, as critical precursors to delinquent pathways.

Both countries establish the general age of criminal responsibility at sixteen, with provisions for liability from fourteen for specified serious offences. Kazakhstan's Criminal Code of 2014 introduced a supplementary measure of probation control as a compulsory educational measure applied to juvenile offenders, extending the range of alternatives to custodial punishment. Educational measures under Kazakhstani law include warning, transfer under supervision, obligation to make amends, restriction of leisure activities and establishment of special behavioural requirements, and placement in educational organizations with a special regime of detention for terms ranging from six months to two years.

China's Law on the Prevention of Juvenile Delinquency, revised in 2020, establishes a three-tier classification of juvenile misconduct: 不良行为 (misconduct), 严重不良行为 (serious misconduct), and criminal behaviour, with corresponding levels of preventive intervention. This framework reflects a shift from a predominantly punitive orientation toward a "prevention–intervention–correction" continuum. Empirical research on the implementation of this graded intervention mechanism has identified persistent challenges, including ambiguous classification standards, inadequate supporting measures, and suboptimal intervention outcomes in practice.

A comparative assessment of prevention systems in Kazakhstan and China reveals that despite the existence of basic normative frameworks, Kazakhstan's system for preventing juvenile delinquency remains fragmented, with restorative practices implemented on a limited scale and inter-agency coordination characterized as unstable. In China, while the legal framework is comparatively comprehensive, the early intervention system has been found to operate suboptimally due to insufficient professionalization of law enforcement, scarcity of supporting resources, and problematic procedural coordination. Both countries thus confront a common challenge: the gap between normative aspiration and practical implementation.

The rapid proliferation of information and communication technologies has introduced new dimensions to juvenile delinquency in both jurisdictions. Kazakhstani researchers observe that with the development of ICT and remote communication, the influence of peer groups and traditional hierarchies within juvenile delinquency may be

weakening, while new sources of influence—including web-communication and social networks—are forming novel features of the adolescent psychological portrait. The emergence of juvenile cybercrime has created definitional and methodological challenges, with the concept of the “juvenile cybercriminal” remaining inadequately defined in Kazakhstani legal scholarship.

Chinese criminological analysis similarly identifies the rapid expansion of digital networks as a significant inducement to juvenile offending. Minors’ inadequate discernment and filtering capacities, combined with parents’ failure to supervise electronic device usage, expose adolescents to violent, pornographic, and fraudulent information that may be internalized uncritically. The phenomenon of “information cocoons” has been observed to erode empathy and responsibility among some minors, while commercially operated entertainment venues with regulatory loopholes continue to exert negative influences on juvenile behaviour.

The comparative analysis reveals both convergence and divergence in the criminogenic conditions of juvenile delinquency in Kazakhstan and China. The family domain emerges as the most consistent cross-national determinant, with parental absence, inadequate supervision, and negative parenting practices exerting comparable criminogenic effects in both societies. Institutional conditions differ in emphasis: Kazakhstan’s framework places greater reliance on judicial educational measures within the criminal justice system, whereas China has developed a more elaborate administrative prevention architecture centred on graded intervention. Both systems, however, struggle with implementation deficits that attenuate their preventive potential. The digital environment constitutes an increasingly significant shared risk domain, demanding coordinated regulatory responses that neither country has yet fully developed. Effective prevention in both contexts requires strengthening family support services, improving inter-agency coordination, and developing targeted interventions for technology-facilitated juvenile offending.

References

1. Zhamiyeva, R., Zhumabayeva, Z., Botagarin, R., Arenova, L., & Sabitov, S. (2024). Transformation of factors and mechanisms of involvement of juveniles in

criminal activity: Kazakhstan experience against the backdrop of foreign practice. DANUBE, 15(3), 266–286.

2. Sun, W., Wang, M., Zheng, F., & Wang, Y. (2024). From nurture to deviance: A study on parenting style and juvenile delinquency. *Deviant Behavior*, 45(5), 639–655.

3. Criminal Code of the Republic of Kazakhstan. (2014). Article 84: Compulsory measures of educational influence.

4. Law of the People's Republic of China on the Prevention of Juvenile Delinquency. (2020 Revision).

5. Ministry of Internal Affairs of the Republic of Kazakhstan. (2023). Statistical data on juvenile delinquency.

6. Supreme People's Procuratorate of China. (2025). White Paper on Juvenile Procuratorial Work (2024).

7. 未成年人犯罪低龄化现象浅析及治理建议. (2024). 正义网.

8. 未成年人罪错行为分级干预机制的实证研究. (2025). 中国知网.

9. OSCE. (2025). Kazakhstan strengthens inter-agency co-operation on youth crime.

10. 中国未成年人违法犯罪态势分析与防治对策. (2024). 社会科学文献出版社.

Yeerkenbieke Zhuledezi

Master's student 1 year Faculty of Law

AL-Farabi Kazakh National University

Scientific advisor: S.B. Duzbayeva

E-mail:erkinbek_zhuldyz1@live.kaznu.kz

CRIMINOLOGICAL CHARACTERISTICS OF THE CAUSES AND CONDITIONS OF JUVENILE DELINQUENCY (BASED ON THE EXPERIENCE OF THE REPUBLIC OF KAZAKHSTAN AND THE PEOPLE'S REPUBLIC OF CHINA)

Juvenile delinquency remains one of the most persistent challenges confronting legal systems worldwide, and both the Republic of Kazakhstan and the People's Republic of China have witnessed significant shifts in the nature and scale of youth offending in recent years. While the two countries share certain historical legacies in their approaches to juvenile justice, their respective trajectories of social transformation, economic development, and legal reform have produced distinctive patterns in the causes and conditions of juvenile delinquency. This paper undertakes a comparative criminological analysis of the

principal determinants of juvenile offending in Kazakhstan and China, examining the interplay between family, school, community, and digital-environment factors within each national context.

In both Kazakhstan and China, family-related factors consistently emerge as the most significant criminogenic conditions associated with juvenile offending. Kazakhstani criminological research identifies dysfunctional families as a primary source of criminogenic influence, alongside difficulties in social adaptation within the learning community and divergent perceptions of social justice among adolescents. Empirical data from Kazakhstani law enforcement agencies indicate that the absence of proper parental oversight constitutes the most characteristic cause of juvenile crime, with a substantial proportion of juvenile offenders—approximately 55 percent—being neither employed nor enrolled in educational institutions at the time of their offence.

Chinese studies similarly emphasize the centrality of family factors. A quantitative analysis of China's 2019 Recidivism Survey conducted by the Ministry of Justice revealed a significant correlation between negative parenting practices, poor parent-child relationships, and elevated rates of juvenile delinquency. Insufficient parental supervision was found to directly impair adolescents' self-regulation capacity, thereby increasing their propensity for delinquent behaviour. Chinese scholars further note that family love deficits and improper parenting methods exert profound influence on minors' value orientations and behavioural patterns, with rural left-behind children and single-parent family backgrounds disproportionately represented among juvenile offenders.

School disengagement represents a second convergent risk domain. In Kazakhstan, researchers have documented that difficulties in social adaptation within educational institutions contribute to the transformation of the criminological portrait of juvenile offenders, with peer group influence and hierarchical dynamics within delinquent subcultures playing significant roles. Chinese research similarly identifies school-related risk factors, including hidden dropout—particularly at the middle-school level—and inadequate school supervision, as critical precursors to delinquent pathways.

Both countries establish the general age of criminal responsibility at sixteen, with provisions for liability from fourteen for specified serious

offences. Kazakhstan's Criminal Code of 2014 introduced a supplementary measure of probation control as a compulsory educational measure applied to juvenile offenders, extending the range of alternatives to custodial punishment. Educational measures under Kazakhstani law include warning, transfer under supervision, obligation to make amends, restriction of leisure activities and establishment of special behavioural requirements, and placement in educational organizations with a special regime of detention for terms ranging from six months to two years.

China's Law on the Prevention of Juvenile Delinquency, revised in 2020, establishes a three-tier classification of juvenile misconduct: 不良行为 (misconduct), 严重不良行为 (serious misconduct), and criminal behaviour, with corresponding levels of preventive intervention. This framework reflects a shift from a predominantly punitive orientation toward a "prevention–intervention–correction" continuum. Empirical research on the implementation of this graded intervention mechanism has identified persistent challenges, including ambiguous classification standards, inadequate supporting measures, and suboptimal intervention outcomes in practice.

A comparative assessment of prevention systems in Kazakhstan and China reveals that despite the existence of basic normative frameworks, Kazakhstan's system for preventing juvenile delinquency remains fragmented, with restorative practices implemented on a limited scale and inter-agency coordination characterized as unstable. In China, while the legal framework is comparatively comprehensive, the early intervention system has been found to operate suboptimally due to insufficient professionalization of law enforcement, scarcity of supporting resources, and problematic procedural coordination. Both countries thus confront a common challenge: the gap between normative aspiration and practical implementation.

The rapid proliferation of information and communication technologies has introduced new dimensions to juvenile delinquency in both jurisdictions. Kazakhstani researchers observe that with the development of ICT and remote communication, the influence of peer groups and traditional hierarchies within juvenile delinquency may be weakening, while new sources of influence—including web-communication and social networks—are forming novel features of the

adolescent psychological portrait. The emergence of juvenile cybercrime has created definitional and methodological challenges, with the concept of the “juvenile cybercriminal” remaining inadequately defined in Kazakhstani legal scholarship.

Chinese criminological analysis similarly identifies the rapid expansion of digital networks as a significant inducement to juvenile offending. Minors’ inadequate discernment and filtering capacities, combined with parents’ failure to supervise electronic device usage, expose adolescents to violent, pornographic, and fraudulent information that may be internalized uncritically. The phenomenon of “information cocoons” has been observed to erode empathy and responsibility among some minors, while commercially operated entertainment venues with regulatory loopholes continue to exert negative influences on juvenile behaviour.

The comparative analysis reveals both convergence and divergence in the criminogenic conditions of juvenile delinquency in Kazakhstan and China. The family domain emerges as the most consistent cross-national determinant, with parental absence, inadequate supervision, and negative parenting practices exerting comparable criminogenic effects in both societies. Institutional conditions differ in emphasis: Kazakhstan’s framework places greater reliance on judicial educational measures within the criminal justice system, whereas China has developed a more elaborate administrative prevention architecture centred on graded intervention. Both systems, however, struggle with implementation deficits that attenuate their preventive potential. The digital environment constitutes an increasingly significant shared risk domain, demanding coordinated regulatory responses that neither country has yet fully developed. Effective prevention in both contexts requires strengthening family support services, improving inter-agency coordination, and developing targeted interventions for technology-facilitated juvenile offending.

References

1. Zhamiyeva, R., Zhumabayeva, Z., Botagarin, R., Arenova, L., & Sabitov, S. (2024). Transformation of factors and mechanisms of involvement of juveniles in criminal activity: Kazakhstan experience against the backdrop of foreign practice. *DANUBE*, 15(3), 266–286.

2. Sun, W., Wang, M., Zheng, F., & Wang, Y. (2024). From nurture to deviance: A study on parenting style and juvenile delinquency. *Deviant Behavior*, 45(5), 639–655.
3. Criminal Code of the Republic of Kazakhstan. (2014). Article 84: Compulsory measures of educational influence.
4. Law of the People's Republic of China on the Prevention of Juvenile Delinquency. (2020 Revision).
5. Ministry of Internal Affairs of the Republic of Kazakhstan. (2023). Statistical data on juvenile delinquency.
6. Supreme People's Procuratorate of China. (2025). White Paper on Juvenile Procuratorial Work (2024).
7. 未成年人犯罪低龄化现象浅析及治理建议. (2024). 正义网.
8. 未成年人罪错行为分级干预机制的实证研究. (2025). 中国知网.
9. OSCE. (2025). Kazakhstan strengthens inter-agency co-operation on youth crime.
10. 中国未成年人违法犯罪态势分析与防治对策. (2024). 社会科学文献出版社.

Маликова Ш.Б.

*«Нархоз Университеті» КеАҚ Құқық және мемлекеттік басқару мектебінің профессоры, заң ғылымдарының кандидаты
Қазақстан Республикасы, Алматы қ.
E-mail: msholpan7876@gmail.com
ORCID: <https://orcid.org/0000-0002-8762-7062>*

РАЗГРАНИЧЕНИЕ УГОЛОВНОЙ, АДМИНИСТРАТИВНОЙ И ГРАЖДАНСКО-ПРАВОВОЙ ОТВЕТСТВЕННОСТИ ЗА НЕПРАВОМЕРНОЕ ИСПОЛЬЗОВАНИЕ БОЛЬШИХ ДАННЫХ

Почему цифровое нарушение нельзя квалифицировать по одному его результату? Утечка массива может одновременно затронуть частную жизнь гражданина, коммерческую ценность клиентской базы и безопасность информационной системы. Однако множественность затронутых интересов не означает автоматического возникновения трех видов ответственности. Прежде необходимо установить, какая обязанность нарушена, кому она адресована и какие последствия закон связывает именно с этим нарушением. Отнесение сведений к большим данным характеризует

масштаб и организацию обработки, но не заменяет состава правонарушения.

В исследовании условий гражданско-правовой ответственности А.Г.Диденко обращается к самостоятельному значению противоправности и соотношению договора с законодательством [1]. Эта постановка существенна для цифрового оборота: неправомерность поведения нельзя устанавливать только по наличию неблагоприятного технического события. Нарушение согласованного назначения массива, срока предоставления доступа или обязанности сохранить конфиденциальность требует анализа конкретного правоотношения. Вместе с тем договорная свобода не позволяет сторонам устранить императивные ограничения обработки данных третьих лиц.

Пункт 1 статьи 9 Гражданского кодекса Республики Казахстан предусматривает как взыскание убытков и компенсацию морального вреда, так и пресечение действий, восстановление прежнего положения и исполнение обязанности в натуре [2]. Из этого следует различие между ответственностью и защитой: требование прекратить неправомерную обработку не должно оцениваться так, как будто заявитель непременно просит денежную компенсацию. Для последней необходимо установить предусмотренные законом условия; для пресечения угрозы нарушения назначение меры иное.

Статья 105 Цифрового кодекса РК не образует самостоятельного состава «неправомерного использования больших данных». Ее пункт 1 отсылает к ответственности, установленной законами, а пункт 2 сохраняет обязанность устранить нарушение независимо от уголовной или административной ответственности [3]. Поэтому исследовательская задача состоит не в конструировании универсальной санкции для Big Data, а в согласовании уже действующих оснований ответственности и восстановительных средств.

Международный пакт о гражданских и политических правах связывает защиту от незаконного вмешательства в частную жизнь со статьей 17 и эффективными средствами защиты по пункту 3 статьи 2. Одновременно пункт 1 статьи 15 закрепляет законность

уголовного преследования и запрет более тяжкого наказания, чем предусмотренное применимым законом [4]. Эти требования нельзя противопоставлять: обеспечение защиты данных не оправдывает расширения уголовного запрета по аналогии, а соблюдение границ уголовной ответственности не означает отказа в иных надлежащих средствах защиты.

Исследование основано на формально-юридическом сопоставлении диспозиций и санкций, функциональном сравнении зарубежных решений и анализе документированных эпизодов. Нормативный материал рассматривается по состоянию на 27 сентября 2026 года. Для исторических дел сохраняется различие между редакцией, относящейся ко времени деяния, и действующим регулированием. Официальные сообщения о казахстанских делах используются в пределах опубликованных сведений; они не подменяют отсутствующие полные судебные акты. Выборка служит проверке юридических разграничений, а не оценке статистической эффективности всей системы.

Существенный вред и границы уголовно наказуемого обращения с данными. По статье 4 УК РК основанием уголовной ответственности является деяние, содержащее все признаки предусмотренного Кодексом состава применение уголовного закона по аналогии не допускается. Части 1-2 статьи 19 требуют виновного отношения к вменяемому деянию и последствиям и запрещают объективное вменение. Часть 4 этой статьи специально ограничивает признание неосторожного деяния уголовным правонарушением случаями, предусмотренными Особенной частью [5]. Поэтому отсутствие технической защиты и виновное уголовно наказуемое нарушение соответствующей обязанности не являются тождественными выводами.

Часть 1 статьи 147 УК адресована лицу, обязанному принимать меры защиты персональных данных, и требует причинения существенного вреда. Иная конструкция содержится в части 2, где незаконное собирание сведений о частной жизни, составляющих личную или семейную тайну, без согласия лица отделено союзом «либо» от причинения существенного вреда вследствие незаконных сбора или обработки иных персональных данных. Аналогичное

различие предусмотрено частью 4 для распространения сведений [5]. Нельзя одинаково требовать существенный вред для всех альтернативных деяний или, напротив, считать его доказанность ненужной во всех случаях нарушения статьи 147 УК.

Это разграничение существенно для квалификации смешанного массива. Присутствие в базе отдельных сведений о частной жизни еще не превращает каждую ее запись в личную или семейную тайну. Но и большой объем обычных идентификационных сведений не устраняет уголовно-правового значения их обработки, когда доказаны необходимые законом последствия. Предмет оценки - содержание затронутой информации и конкретный способ обращения с ней, а не коммерческое название базы или программного продукта.

Подпункт 14) статьи 3 УК включает в понятие существенного вреда, с предусмотренной там оговоркой, нарушения охраняемых прав и интересов, значительный ущерб, трудную жизненную ситуацию потерпевшего, нарушение нормальной работы организаций и иные указанные последствия [5]. Оценочность понятия не освобождает от мотивировки. Формула «вред существенный, поскольку нарушено право на данные» способна сделать следствие неотличимым от самого действия. Необходимо объяснить, какое конкретное изменение в положении потерпевшего установлено, как оно связано с деянием и почему соответствует применяемому признаку.

Практическую границу показывает сообщение Генеральной прокуратуры «Перевел деньги потерпевшей и был осужден». Лицо использовало банковские реквизиты для исполнения судебных актов; после осуждения в первой и апелляционной инстанциях кассационный суд прекратил дело за отсутствием состава. В сообщении подчеркнуты недоказанность существенного вреда и различие между банковскими реквизитами как персональными данными и личной или семейной тайной [6]. Номер дела, дата судебного акта и примененная часть уголовной статьи в публикации не приведены, поэтому дополнять эти реквизиты предположениями нельзя.

Вывод из этого эпизода ограничен, а именно уголовно-правовая оценка не может строиться только на получении сведений о другом человеке. Из прекращения дела также не следует ни автоматическая правомерность любой операции с такими реквизитами, ни автоматическое право на гражданскую компенсацию. Для каждого возможного требования подлежат самостоятельной проверке его основания с учетом обязательного значения установленных судебным актом обстоятельств. В особенности недопустимо переносить требование уголовно значимого существенного вреда на любое требование о прекращении обработки или исправлении данных.

Также представляет научно-практический интерес вопрос охраны информационной системы и коммерческой тайны – речь идет о совокупности или конкуренция норм.

Большие данные не всегда являются персональными. Для защищаемой законом информации самостоятельное значение имеют статья 205 УК о неправомерном доступе и статья 208 о неправомерном завладении. В частях 1 этих статей предусмотрены умышленность соответствующего действия и причинение существенного вреда; специальные положения о критически важных объектах требуют отдельного прочтения [5]. Таким образом, одного доказательства копирования недостаточно, чтобы без дальнейшего анализа установить любой из названных составов. Необходимо также определить правовой режим информации и предел законного доступа.

Для коммерчески конфиденциального массива применима другая последовательность. Сначала проверяются условия охраны по пункту 1 статьи 126 ГК - ценность вследствие неизвестности третьим лицам, отсутствие свободного законного доступа и меры конфиденциальности [2]. Затем исследуются признаки статьи 223 УК. Ее часть 1 предусматривает незаконное собирание охраняемых сведений с целью разглашения или использования. Часть 2 относится к разглашению или использованию лицом, которому информация доверена либо известна по службе или работе, и дополнительно предусматривает корыстную или иную личную

заинтересованность и крупный ущерб [5]. Условие одной части нельзя переносить на другую без основания.

Коммерческая ценность массива и размер уголовно значимого ущерба - разные обстоятельства. Первое относится к режиму охраны, второе - к последствиям определенного деяния. Цена разработки базы сама по себе не доказывает размер потерь от ее раскрытия. Затраты на информационную систему нельзя механически считать ущербом от каждого неправомерного доступа. Вместе с тем отсутствие признаков именно статьи 223 не разрешает обход защиты системы и не исключает оценки самостоятельного нарушения договора либо иных охраняемых интересов.

Часть 3 статьи 13 УК исключает совокупность общей и специальной норм применительно к одному деянию. Части 1–2 допускают совокупность с учетом предусмотренных ими правил охвата признаков одной нормой [5]. Поэтому перечень операций «доступ - копирование - передача» не следует автоматически превращать в равное ему число преступлений. Требуется сопоставить, какие элементы уже охвачены квалифицированным составом и какое самостоятельное деяние или признак остается за его пределами. Различие охраняемых интересов существенно, но не освобождает от такого сопоставления.

Официальное сообщение КНБ о вступившем в силу приговоре суда Актау фиксирует осуждение к трем годам лишения свободы по частям 3 и 4 статьи 147, части 2 статьи 205 и пункту 1 части 2 статьи 208 УК за неправомерный доступ к государственным системам и получение данных для возмездной передачи [7]. Публикация подтверждает применение нескольких норм, но без полного приговора не позволяет заключить, какие именно эпизоды и признаки послужили основанием их совокупности.

Особенно важно не исправлять историческую квалификацию по современной нумерации. Статья 208 изменена Законом от 16 июля 2025 года № 210-VIII. Нынешнее содержание части 2 нельзя приписывать более раннему делу. Статьи 5-6 УК предусматривают действие уголовного закона во времени и обратную силу закона, улучшающего положение лица [5]. Поэтому научное использование старого приговора требует сохранения приведенных в источнике

реквизитов и отдельного сопоставления редакций, а не утверждения, что названный в сообщении пункт существует в неизменном виде сегодня.

Что касается административных составов и пределов повторного вменения, то часть 2 статьи 25 КоАП закрепляет субсидиарность административной ответственности по отношению к уголовной, а части 1–4 статьи 79 содержат соответствующие разграничительные оговорки. При этом статья 79 различает незаконные сбор и обработку, использование служебного положения, несоблюдение защитных мер и такое несоблюдение, повлекшее утрату либо незаконные сбор или обработку данных [8]. Выбор части должен основываться на установленном деянии и последствиях, а не на желательном размере штрафа или удобстве административной процедуры.

Сопоставление выявляет конкретное пересечение, а именно часть 3 статьи 79 предусматривает несоблюдение мер защиты персональных данных, тогда как подпункт 1) части 1 статьи 641 - неосуществление или ненадлежащее осуществление защитных мер собственником или владельцем соответствующих цифровых систем, собственником или оператором базы либо третьим лицом [8]. При совпадении лица, обязанности и фактического бездействия возникает вопрос о разграничении норм. Их размещение в разных главах не объясняет само по себе допустимость двух взысканий за одно и то же нарушение.

Подпункт 2) части 1 статьи 641 о единых требованиях цифровизации и кибербезопасности имеет более широкий предмет. Нарушение этих требований может относиться к иной обязанности, не исчерпываемой защитой персональных данных. Однако общая ссылка на кибербезопасность не доказывает самостоятельности второго правонарушения. Для дополнительной квалификации необходимо указать конкретный нормативный пункт и действие либо бездействие, не охваченное первой квалификацией. До такого обоснования говорить об установленной совокупности преждевременно.

При проверке ТОО «МФО Робокэш.кз», согласно сообщению министерства, нарушение квалифицировано по части 4 статьи 79

КоАП. Назначен штраф 1000 МРП, в сокращенном производстве уплачено 500 МРП - 1 846 000 тенге. В сообщении указано обнаружение 5 марта 2024 года утечки более двух миллионов персональных данных и последующее уведомление граждан [9]. Эти сведения не устанавливают количество уникальных потерпевших и не являются данными о присужденной им компенсации. Историческую сумму нельзя представлять как действующий размер санкции: статья 79 впоследствии изменялась [8].

Значение этого эпизода состоит в разграничении последствий одного события. Административное дело касается нарушения публичной обязанности. Требования граждан касаются их собственных прав и последствий нарушения. Размер уплаченного организацией штрафа не делится между субъектами данных и не определяет автоматически верхнюю границу их требований. Но и число обращений после утечки не доказывает тождественность либо одинаковую тяжесть вреда у всех заявителей.

Отдельно необходимо установить субъект ответственности. Часть 1 статьи 15 УК относится к вменяемому физическому лицу установленного возраста [5]. Для административной ответственности организации действуют собственные условия, в частности, часть 2 статьи 33 КоАП связывает деяние с его совершением, санкционированием или одобрением указанными в норме управленческими субъектами, а часть 4 освобождает работника от административной ответственности за данное правонарушение после привлечения индивидуального предпринимателя или юридического лица [8]. Поэтому нельзя безоговорочно предлагать одновременно штрафовать компанию и ее работника за один состав.

Пункт 7 статьи 14 Международного пакта запрещает повторное осуждение или наказание за преступление после окончательного осуждения либо оправдания в предусмотренных им условиях [4]. Эта гарантия требует проверки тождества лица и деяния. Вопрос о сочетании уголовного дела работника и самостоятельного административного нарушения организации нельзя решать одним лозунгом о тройной ответственности. Для каждого лица необходимо установить его собственное деяние, применимую норму и

специальные ограничения, включая часть 4 статьи 33 КоАП; гражданское требование дополнительно оценивается по своему назначению.

Сравнительный материал показывает, почему экономическая значимость оператора не заменяет условий ответственности. Статья 83 GDPR предусматривает административные штрафы, а подпункт «b» пункта 2 требует учитывать умышленный или неосторожный характер нарушения [10]. В решении от 5 декабря 2023 года по делу C-807/21 *Deutsche Wohnen* Суд ЕС в пунктах 60 и 66–68 разграничил два вопроса: штраф юридическому лицу не зависит от предварительного установления нарушения конкретного идентифицированного физического лица, но требует умысла или неосторожности контролера [11].

Это не модель автоматического наказания организации за любой инцидент. Для Казахстана значимо различие между установлением организационного поведения и поиском единственного сотрудника, которому можно приписать все решения. Одновременно нельзя непосредственно заменить статью 33 КоАП иностранным правилом. Европейское толкование служит материалом для оценки конструкции вины и атрибуции, а не дополнительным основанием казахстанского взыскания. Рассмотрение оборота группы компаний при расчете предела штрафа также не следует смешивать с установлением состава у конкретного адресата санкции.

Гражданско-правовое возмещение имеет собственную нормативную основу. Пункт 4 статьи 9 ГК определяет убытки через реальный ущерб и упущенную выгоду, пункт 6 содержит презумпцию вины в случаях, когда от нее зависят последствия нарушения. Статья 350 относится к возмещению убытков при нарушении обязательства [2], а статья 917 Особенной части закрепляет общие основания деликтного возмещения и освобождение при доказанности отсутствия вины, если законом не предусмотрено иное [12]. Ни одна из этих конструкций не требует в качестве универсальной предпосылки предварительного обвинительного приговора.

Особенно заметно различие при договорной обработке. По пункту 2 статьи 359 ГК предприниматель отвечает за ненадлежащее исполнение, если не докажет невозможность исполнения вследствие непреодолимой силы, с учетом допускаемых законом и договором отступлений [2]. Поэтому вывод об отсутствии доказанного умышленного умысла работника не разрешает вопрос о договорной ответственности организации. Ссылка на внешнюю кибератаку также требует оценки конкретных обстоятельств: участие третьего лица не тождественно чрезвычайности и непредотвратимости события и не объясняет автоматически невозможность надлежащего исполнения.

При этом перечень гражданских требований зависит от носителя интереса. Пункт 1 статьи 9 ГК прямо исключает право юридического лица на возмещение морального вреда [2]. Для гражданина пункт 1 статьи 951 связывает моральный вред с личными неимущественными благами и правами, а пункт 4 той же статьи ограничивает его возмещение при нарушении только имущественных прав; статья 952 определяет критерии размера [12]. Потерю клиентской базы организацией, расходы гражданина на защитные меры и его нравственные переживания нельзя обозначать одним недифференцированным «цифровым ущербом».

Д. Солов и Д. Ситрон обосновывают юридическую значимость риска и тревоги после утечек и критикуют слишком узкое признание информационного вреда [13]. Т. Зарски, обсуждая их подход, одновременно обращает внимание на неопределенность, которую расширение судебного усмотрения может создавать для сферы безопасности данных [14]. Обе позиции позволяют отказаться от крайностей: требовать от человека ожидания фактического мошенничества либо считать любой абстрактный риск достаточным для одинаковой компенсации. Американская дискуссия о доступе к суду не должна, однако, переноситься в казахстанское материальное право как готовый критерий существенного вреда.

Представляется обоснованным различать угрозу, требующую прекращения неправомерного состояния, необходимые расходы по предотвращению последствий и доказанный неимущественный вред. Возможность защиты от угрозы следует из статьи 9 ГК;

взыскание расходов и компенсация требуют своей юридической оценки [2; 12]. Отсутствие состоявшегося хищения денег не опровергает автоматически все остальные последствия утечки. Но потенциальная возможность любого последующего злоупотребления не устанавливает сама по себе размер убытков каждого субъекта массива.

Решение Суда ЕС от 11 апреля 2024 года по делу C-741/21 GP v juris GmbH позволяет точнее разделить компенсацию от штрафа. В пунктах 56–60 Суд признал различие целей статей 82 и 83 GDPR: критерии административного штрафа не применяются для расчета компенсации, выполняющей восстановительную, а не карательную функцию. В пунктах 34–43 сохранена необходимость установить вред и причинную связь, хотя универсальный порог серьезности неимущественного вреда отвергнут [15]. Предметом дела было продолжение обработки вопреки возражению; это материал о критериях защиты, а не доказательство существования самостоятельного режима ответственности за Big Data.

Для казахстанского анализа значима следующая граница: общественная опасность нарушения и индивидуальная тяжесть последствий могут учитывать пересекающиеся факты, но отвечают на разные вопросы. Число затронутых лиц характеризует масштаб инцидента; оно не умножает вред отдельного истца арифметически. Наличие нескольких нарушенных обязанностей также не означает, что один и тот же имущественный ущерб следует возместить несколько раз. Соблюдение этого разграничения не ослабляет защиту, а позволяет юридически обосновать именно тот результат, на который направлено требование.

Сочетание публичного взыскания и возмещения уже предусмотрено статьей 59 КоАП. Ее часть 1 допускает разрешение судьей вопроса об имущественном вреде при отсутствии спора о размере; часть 2 регулирует ситуацию рассмотрения административного дела иным органом, а часть 3 относит требования о деловой репутации и моральном вреде к гражданскому судопроизводству [8]. Поэтому предложение впервые «разрешить компенсацию после административного штрафа» не обладало бы

нормативной новизной. Развития требуют точность разграничения требований и устранение конкурирующих квалификаций.

Для квалификации предлагается последовательно устанавливать пять элементов: охраняемый интерес и режим сведений; конкретную нарушенную обязанность; деяние и его субъекта; требуемые данной нормой вину, последствия и причинную связь; допустимое сочетание санкции с другими мерами. Эти элементы образуют проверочную модель, а не новый универсальный состав. Она позволяет объяснить, почему технически сходные эпизоды получают разные правовые оценки, и одновременно требует мотивировать каждое такое различие.

Первое законодательное предложение касается пересечения статей 79 и 641 КоАП. Представляется целесообразным дополнить примечание к статье 641 специальным правилом: «При совпадении деяния и нарушенной обязанности несоблюдение мер по защите персональных данных, предусмотренное частями третьей и четвертой статьи 79 настоящего Кодекса, квалифицируется по указанной статье. Дополнительная квалификация по настоящей статье допускается при наличии самостоятельного нарушения, не охватываемого статьей 79 настоящего Кодекса». Это авторская редакция для обсуждения, сохраняющая необходимость проверки общих оснований и исключения уголовно наказуемого деяния.

Предложенное правило не означает декриминализации и не отменяет ответственности за иные нарушения кибербезопасности. Его назначение - ограничить выбор между пересекающимися административными диспозициями, когда орган ссылается на одно фактическое бездействие. При подготовке окончательного проекта необходимо согласовать субъектный состав обеих статей и проверить последствия для всех подпунктов части 1 статьи 641. Само обнаруженное пересечение не позволяет без анализа утверждать незаконность ранее вынесенных постановлений.

Второе направление относится к судебному толкованию существенного вреда. В разъяснениях о применении статьи 147 УК необходимо отделить ее альтернативные конструкции и требовать установления конкретных последствий там, где они включены в состав. Объем массива, число записей и возможность последующего

использования должны оцениваться в связи с содержанием затронутого права и фактическими последствиями, а не вместо них. Такое разъяснение не вправе создавать отсутствующий в законе квалифицирующий признак или, наоборот, устранять предусмотренный законом элемент.

Третье направление - последовательное отражение различия между публичной ответственностью и гражданской защитой. Для применения статьи 105 Цифрового кодекса во взаимосвязи со статьями 59 КоАП и гражданским законодательством существенно разъяснить: отсутствие уголовно значимого существенного вреда само по себе не разрешает все гражданские требования; состоявшееся публичное взыскание не определяет размер убытков или моральной компенсации; меры прекращения и исправления нарушения не тождественны денежной ответственности. Это предложение о согласованном толковании действующих положений, а не объявление их отсутствующими.

Научно-практический результат заключается также в разграничении установленных обстоятельств и пределов источника. Сообщение о штрафе подтверждает названный результат публичного производства, но не размер индивидуального вреда. Сообщение о прекращении уголовного дела подтверждает указанный процессуальный исход, но не заменяет решения гражданского спора. Исторический приговор позволяет исследовать квалификацию своего периода; он не доказывает применимость той же нумерации после изменения закона. Соблюдение этих границ необходимо для воспроизводимого анализа практики и обоснования поправок.

Разграничение уголовной, административной и гражданско-правовой ответственности за неправомерное использование больших данных должно строиться не по масштабу технологического ресурса, а по охраняемому интересу, содержанию обязанности и условиям конкретной нормы. Существенный вред не является универсальной предпосылкой любой защиты данных. Административная ответственность не служит свободной альтернативой уголовной, а привлечение организации не означает

допустимости повторного административного вменения того же правонарушения работнику.

Гражданско-правовое требование сохраняет собственное основание и назначение. Оно не выводится автоматически из публичного взыскания и не исключается только отсутствием признака, необходимого для уголовной квалификации. Предлагаемое уточнение соотношения статей 79 и 641 КоАП, поэлементная проверка состава и разграничение штрафа, компенсации и восстановительной меры позволяют перейти от общего тезиса об усилении ответственности к определенным, проверяемым правовым решениям.

Финансирование. Исследование подготовлено в рамках проекта ИРН AP23489796 «Проблемы регламентации правового режима больших данных (Big Data): отечественный и международный опыт», финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан.

Список использованных источников

1 Диденко, А. Г. Вызовы времени: условия гражданско-правовой ответственности [Электронный ресурс] / А. Г. Диденко // Гражданское законодательство. Статьи. Комментарии. Практика / под ред. А. Г. Диденко. - Алматы : [б. и.], 2017. - Вып. 50. - Электронное воспроизведение сборника на Zakon.kz от 4 мая 2017 г. URL: <https://www.zakon.kz/stati/4857805-grazhdanskoe-zakonodatelstvo.-stati..html> (дата обращения: 01.07.2026).

2 Гражданский кодекс Республики Казахстан (Общая часть) : Кодекс Республики Казахстан от 27 декабря 1994 г. № 268-ХІІІ // Ведомости Верховного Совета Республики Казахстан. - 1994. - № 23–24 (приложение). - Электронный текст: Учет.kz. - Используемые положения: ст. 9, 126, 350, 359. URL: https://zakon.uchet.kz/rus/docs/K940001000_ (дата обращения: 03.07.2026).

3 Цифровой кодекс Республики Казахстан : Кодекс Республики Казахстан от 9 января 2026 г. № 255-VІІІ ЗРК // Казахстанская правда. - 2026. - 10 января. - №5–6 (30634–30635). - Электронный текст: Учет.kz. - Используемое положение: ст.105. URL: <https://zakon.uchet.kz/rus/docs/K2600000255> (дата обращения: 27.07.2026).

4 Международный пакт о гражданских и политических правах : от 16 декабря 1966 г. : ратифицирован Законом Республики Казахстан от 28 ноября 2005 г. № 91-ІІІ // Бюллетень международных договоров Республики Казахстан. - 2006. - № 4. - Ст. 30. - Электронный текст: Учет.kz. - Используемые положения: ст. 2, 14, 15, 17. URL: https://zakon.uchet.kz/rus/docs/Z050000091_ (дата обращения: 06.07.2026).

5 Уголовный кодекс Республики Казахстан : Кодекс Республики Казахстан от 3 июля 2014 г. № 226-V ЗРК // Ведомости Парламента Республики Казахстан. - 2014. - № 13-II. - Ст. 83. - Электронный текст: Учет.kz. - Используемые положения: ст. 3–6, 13, 15, 19, 147, 205, 208, 223. URL: <https://zakon.uchet.kz/rus/docs/K1400000226> (дата обращения: 08.07.2026).

6 Перевел деньги потерпевшей и был осужден [Электронный ресурс] / Пресс-служба Генеральной прокуратуры Республики Казахстан // Gov.kz. - [Б. г.]. - Официальное сообщение. - Номер публикации: 1247871. URL: <https://www.gov.kz/memleket/entities/prokuror/press/news/details/1247871?lang=ru> (дата обращения: 10.07.2026).

7 О пресечении правонарушений в сфере информатизации и связи [Электронный ресурс] / Пресс-служба Комитета национальной безопасности Республики Казахстан // Gov.kz. - [2024]. - Официальное сообщение о вступившем в законную силу приговоре суда Актау. - Номер публикации: 710060. URL: <https://www.gov.kz/memleket/entities/knb/press/news/details/710060?lang=ru> (дата обращения: 13.07.2026).

8 Об административных правонарушениях : Кодекс Республики Казахстан от 5 июля 2014 г. № 235-V ЗРК // Ведомости Парламента Республики Казахстан. - 2014. - № 18-II. - Ст. 92. - Официальная карточка акта: ИПС «Әділет». - Используемые положения: ст. 25, 33, 59, 79, 641. URL: <https://old.adilet.zan.kz/rus/docs/K1400000235/info> (дата обращения: 15.07.2026).

9 Минцифры объявило результаты проверки в отношении ТОО «МФО Робокэш.кз» [Электронный ресурс] / Пресс-служба Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан // Gov.kz. - [2024]. - Официальное сообщение. - Номер публикации: 740137. URL: <https://www.gov.kz/memleket/entities/maidd/press/news/details/740137?lang=ru> (дата обращения: 17.07.2026).

10 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. - 4 May. - P. 1–88. - Используемые положения: ст. 82–83. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (дата обращения: 20.07.2026).

11 Court of Justice of the European Union. Deutsche Wohnen SE v Staatsanwaltschaft Berlin [Электронный ресурс] : judgment of the Court (Grand Chamber) of 5 December 2023, Case C-807/21. - ECLI:EU:C:2023:950. - Электронное воспроизведение судебного акта: IPscuria. - Используемый фрагмент: п. 53–60, 66–68. URL: <https://ipscuria.eu/case?reference=C-807%2F21> (дата обращения: 22.07.2026).

12 Гражданский кодекс Республики Казахстан (Особенная часть) : Кодекс Республики Казахстан от 1 июля 1999 г. № 409 // Ведомости Парламента Республики Казахстан. - 1999. - № 16–17. - Ст. 642. - Электронный текст: Учет.kz. - Используемые положения: ст. 917, 951–952. URL: https://zakon.uchet.kz/rus/docs/K990000409_ (дата обращения: 23.07.2026).

13 Solove, D. J. Risk and Anxiety: A Theory of Data-Breach Harms / D. J. Solove, D. K. Citron // Texas Law Review. - 2018. - Vol. 96. - P. 737–786. URL: https://scholarship.law.bu.edu/faculty_scholarship/616/, <https://texaslawreview.org/wp-content/uploads/2018/03/Solove.pdf> (дата обращения: 24.07.2026).

14 Zarsky, T. Data Breach Harms-Bringing in the Courts, or Leaving Them Out? [Электронный ресурс] / T. Zarsky // JOTWELL: The Journal of Things We Like (Lots). - 2019. - 19 February. - Раздел Technology Law. URL: <https://cyber.jotwell.com/data-breach-harms-bringing-in-the-courts-or-leaving-them-out/> (дата обращения: 29.07.2026).

15 Court of Justice of the European Union. GP v juris GmbH [Электронный ресурс] : judgment of the Court (Third Chamber) of 11 April 2024, Case C-741/21. - ECLI:EU:C:2024:288. - Электронное воспроизведение судебного акта: IPcuria. - Используемый фрагмент: п. 34–43, 56–60. URL: <https://ipcuria.eu/case?reference=C-741%2F21> (дата обращения: 31.07.2026).

Маликова Ш.Б.

«Нархоз Университеті» КеАҚ Құқық және мемлекеттік басқару мектебінің профессоры, заң ғылымдарының кандидаты

Қазақстан Республикасы, Алматы қ.

E-mail: msholpan7876@gmail.com

Scopus Author ID: 56028214800. ORCID:

<https://orcid.org/0000-0002-8762-7062>

ҚАЗАҚСТАННЫҢ ҚЫЛМЫСТЫҚ ҚҰҚЫҒЫНДАҒЫ ЛИНГВИСТИКАЛЫҚ КОЛЛИЗИЯЛАР: ТЕРМИНОЛОГИЯЛЫҚ АЛШАҚТЫҚТАРДЫҢ ІС-ӘРЕКЕТТЕРДІ САРАЛАУҒА ӘСЕРІ

Қылмыстық құқық бұзушылықты саралау - нақты өмірлік мән-жайларды қылмыстық заңда көзделген құрам белгілерімен сәйкестендірудің күрделі зияткерлік және құқықтық процесі. Бұл процесте қолданылатын әрбір термин тек тілдік таңба емес, қылмыстық жауаптылықтың негізі мен шегін айқындайтын нормативтік құрал ретінде әрекет етеді. Терминнің көлемі тарылса, заңмен қорғалатын қатынастың бір бөлігі құқықтық бағалаудан тыс қалуы мүмкін; оның көлемі негізсіз кеңейсе, қылмыстық репрессияның шекарасы ұлғаяды. Сондықтан қазақ және орыс

тілдеріндегі ресми мәтіндердің ұғымдық сәйкестігі заңнамалық редакция сапасының ғана емес, адамның бостандығы мен құқықтарын қорғаудың тікелей кепілі болып табылады.

Қазақстандағы екітілді құқықтық кеңістіктің бастапқы конституциялық негізі мемлекеттік тілдің мәртебесін және мемлекеттік ұйымдар мен жергілікті өзін-өзі басқару органдарында орыс тілінің ресми түрде қазақ тілімен тең қолданылуын бекітеді. Бұл норма бір тілдегі мәтінді негізгі, ал екіншісін қосалқы түсіндірме ретінде қабылдауға мүмкіндік бермейді: құқық қолданушы үшін екі нұсқа да құқықтық коммуникацияның ресми арнасы болып қалады. Қылмыстық заң саласында мұндай тең қолданылу әр нұсқаның түсінікті, алдын ала болжамды және бірдей құқықтық салдар туғызуын талап етеді [1].

Нормативтік құқықтық актілерді әзірлеуге қойылатын жалпы талаптар қазақ және орыс тілдеріндегі мәтіндердің теңтүпнұсқалы болуын, ал заң жобасына ғылыми лингвистикалық сараптама жүргізген кезде терминологияның бірізділігі мен екі нұсқаның мағыналық сәйкестігін тексеруді көздейді. Осы талаптың қылмыстық заң үшін айрықша маңызы бар, себебі диспозициядағы бір етістіктің модальды реңкі, бір анықтауыштың шегі немесе бір ұғымның тектік-түрлік арақатынасы іс-әрекеттің қылмыстылығына, баптың бөлігіне және жаза мөлшеріне әсер етуі мүмкін. Демек, теңтүпнұсқалықты орфографиялық ұқсастық емес, екі мәтіннің нормативтік ықпалының бірдейлігі ретінде түсіну қажет [2].

Қолданыстағы Қылмыстық кодексе қылмыстық жауаптылықтың бірден-бір материалдық негізін белгілейді және қылмыстық құқық бұзушылық ұғымын қоғамға қауіпті іс-әрекет арқылы сипаттайды; мәтінде тектік «іс-әрекет» ұғымы оның түрлері болып табылатын «әрекет» пен «әрекетсіздікті» қамтиды. Кодекстің 188-бабында «ұрлық» бөтеннің мүлкін жасырын «жымқыру» ретінде айқындалады, ал қылмыстық кірістерге қатысты нормаларда «қылмыстық жолмен алынған» конструкциясы қолданылады. Бұл мысалдар терминдердің мағынасын жалпы тілден емес, кодекстің ішкі жүйесі мен заңдық анықтамаларынан шығару қажеттігін көрсетеді [3].

Тіл туралы заңнамадағы «мәтіннің теңтүпнұсқалы аудармасы» ұғымы түпнұсқаның мағынасы мен мазмұнын өзгеріссіз сақтайтын аударманы білдіреді. Алайда қылмыстық заңда аударманың сапасы тек бастапқы сөйлемнің жалпы мазмұнын сақтаумен өлшенбейді. Мұнда құқықтық ұғымның денотаты, оның өзге институттармен байланысы, адресатқа жүктейтін тыйымның көлемі, кінәні дәлелдеуге қоятын талабы және санкцияға әкелетін белгісі де өзгеріссіз берілуі тиіс. Сондықтан теңтүпнұсқалықты статикалық мәтіндік ұқсастықтан гөрі функционалдық құқықтық баламалылық ретінде қарастырған жөн [4].

Лингвистикалық коллизия деп қылмыстық заңның қазақ және орыс тілдеріндегі нұсқаларының, не бір тілдегі өзара байланысты нормалардың арасында құқықтық ұғымның мазмұнына, көлеміне немесе функциясына қатысты пайда болатын және норманы әртүрлі қолдануға объективті мүмкіндік беретін мағыналық қайшылық түсініледі. Әрбір редакциялық айырма коллизия болып саналмайды. Мысалы, синтаксистік құрылым өзгеше болғанымен нормативтік мазмұн толық сақталса, ол заңды локализацияның қалыпты тәсілі болуы мүмкін. Коллизияның шешуші белгісі - екі мәтінді адал түсіндіру нәтижесінде қылмыстық-құқықтық салдардың бірдей болмау қаупі.

Лингвистикалық коллизияларды бірнеше деңгейге бөлу орынды. Лексикалық деңгейде бір терминге көлемі басқа балама таңдалады немесе бір ұғым бірнеше сөзбен беріледі. Морфологиялық деңгейде жекеше мен көпше түр, аяқталған және аяқталмаған іс-қимыл, міндеттілік пен мүмкіндікті білдіретін нысандар алшақтайды. Синтаксистік деңгейде анықтауыштың қай сөзге қатысты екені, баламалы әрекеттердің шекарасы немесе шарт пен салдардың байланысы өзгеруі ықтимал. Прагматикалық деңгейде кәсіби заңгер мен қарапайым адресат терминді әртүрлі қабылдайды. Ал жүйелік коллизия бір баптағы атаудың Жалпы бөлімдегі анықтамамен немесе сабақтас қылмыстық-процестік ұғыммен сәйкес келмеуінен туындайды.

Саралау процесінде мұндай алшақтықтар қылмыстық құқық бұзушылық құрамының барлық элементіне әсер ете алады. Қол сұғушылық объектісін білдіретін термин шамадан тыс кең

түсіндірілсе, арнайы норма мен жалпы норманың арақатынасы бұзылады. Объективтік жақтағы әрекет, тәсіл, құрал, орын немесе зардап атауы дәл болмаса, аяқталған құрам мен оқталуды, әрекет пен әрекетсіздікті, негізгі және сараланған құрамды ажырату қиындайды. Субъективтік жақтағы мақсат, себеп, «көрінеу» білу немесе абайсыздық дәрежесі дұрыс берілмесе, кінәнің мазмұны өзгеруі мүмкін. Субъектіні сипаттайтын лауазымдық не арнайы белгі алшақ аударылса, жауаптылыққа тартылатын адамдар шеңбері де бірдей болмайды.

«Іс-әрекет», «әрекет» және «әрекетсіздік» арақатынасы тектік және түрлік терминдерді ажыратудың маңызын көрсетеді. Орыс тіліндегі «деяние» ұғымы «действие» мен «бездействию» біріктіретін дербес тектік атау ретінде орныққан. Қазақ тілінде «іс-әрекет» көбіне осы жинақтаушы қызметті атқарады, бірақ күнделікті қолданыста ол белсенді қимылмен ассоциациялануы мүмкін. Егер құқық қолданушы тектік ұғымды тек белсенді мінез-құлықпен теңестірсе, заңмен жүктелген міндетті орындамау арқылы жасалатын құрамдарды бағалауда қате туындайды. Сондықтан кодекстің бүкіл мәтінінде тектік атауды бір нұсқада сақтап, оның әрекет пен әрекетсіздікті қамтитынын анықтамалық аппаратта айқын көрсету қажет.

Мүліктік қылмыстық құқық бұзушылықтардағы «жымқыру» мен «ұрлық» ұғымдарының арақатынасы да саралау үшін маңызды. «Жымқыру» - бөтен мүлікті құқыққа қарсы иемденудің бірнеше нысанын біріктіретін тектік ұғым, ал «ұрлық» - жасырын тәсілмен жасалатын нақты нысан. Жалпы тілде «ұрлық» сөзі кейде бөтен мүлікті иемденудің барлық түріне ортақ атау ретінде қолданылады. Мұндай тұрмыстық мағына құқықтық мәтінге көшірілсе, алаяқтық, сеніп тапсырылған мүлікті иемдену, тонау және қарақшылық арасындағы шекара көмескіленеді. Құқық қолданушы терминді сөздік интуициямен емес, заңдағы тәсіл, ниет және мүліктің өту механизмі арқылы саралауға тиіс.

Субъективтік жақты сипаттайтын «көрінеу» термині ерекше назар аударуды қажет етеді. Оның жалпы тілдегі «анық көрінетін», «айқын» мағынасы қылмыстық құқықтағы «адамның тиісті мән-жайды анық әрі сенімді білуі» ұғымымен толық сәйкес емес. Орыс

тіліндегі «заведомо» да арнайы заңдық мазмұнға ие. Егер «көрінеу» объективті жағдайдың айқындығы деп қабылданса, айыпталушының нақты білгенін дәлелдеудің орнына сыртқы жағдайдың түсініктілігі жеткілікті саналып кетуі ықтимал. Бұл кінәлі жауаптылық қағидатына қайшы. Сол себепті заңдық түсіндірмеде осы терминнің дәлелденуге тиіс интеллектуалдық сәтті білдіретіні бекітілуі керек.

«Зиян», «залал», «нұқсан» терминдерінің жарыспалы қолданылуы да құқықтық салдарға ие. Олардың кейбірі материалдық жоғалтуды, басқалары мүліктік емес қол сұғушылықтың салдарын немесе қорғалатын мүдденің жалпы нашарлауын білдіруі мүмкін. Орыс мәтініндегі «вред» пен «ущерб» те әр контексте бірдей емес. Егер сандық өлшеммен анықталатын мүліктік залал кең мағыналы зиянмен араластырылса, елеулі, ірі немесе аса ірі зардапты белгілеу кезінде дәлелдеу пәні өзгеруі мүмкін. Бірізділік үшін заң шығарушы әр терминнің қолданылатын саласын, өлшену тәсілін және бағалау критерийін анықтамалар жүйесінде байланыстыруы қажет.

Топтық қылмыстылыққа қатысты атауларда да күнделікті мағына мен заңдық мағынаны ажырату керек. «Адамдар тобы», «алдын ала сөз байласқан адамдар тобы», «қылмыстық топ», «ұйымдасқан топ» және өзге нысандар бір қатысушылар жиынтығын әртүрлі атау емес, құрылымдылық, тұрақтылық, алдын ала бірлесу және мақсат белгілері бойынша ажыратылатын құқықтық санаттар. Бір нұсқадағы жалпылаушы сөз екінші нұсқада арнайы терминмен ауыстырылса, саралаушы белгі негізсіз қолданылуы немесе, керісінше, назардан тыс қалуы мүмкін. Бұл жаза шегіне тікелей ықпал ететіндіктен, топ нысандарының атаулары кодекстің Жалпы және Ерекше бөлімдерінде бірдей терминологиялық матрица бойынша берілуге тиіс.

Лингвистикалық коллизияның саралауға ықпал ету механизмі бірнеше сатыдан тұрады. Алдымен термин дәлелдеу пәнін айқындайды: тергеуші қандай фактілерді іздеу керегін сол арқылы белгілейді. Кейін прокурор оны айыптау актісінде құқықтық формулаға айналдырады. Сот терминнің мағынасын дәлелденген фактілерге қолданып, бап пен оның бөлігін таңдайды.

Апелляциялық және кассациялық сатылар осы пайымның дұрыстығын тексереді. Бастапқы термин қате түсіндірілсе, қателік барлық процессуалдық құжатқа таралады: дәлелдемелердің бір бөлігі жиналмайды, қорғану ұстанымы басқа белгіге бағытталады, ал сот шешіміндегі уәждеу жалған семантикалық алғышартқа сүйенеді.

Сот ісін жүргізу тілін қолдану жөніндегі жоғарғы соттық түсіндіру сот процесіне қатысушылардың тілдік құқықтарын қамтамасыз етуді құқықтық кепіл ретінде бағалайды. Бұл кепіл тек аудармашы ұсынумен немесе құжаттарды таңдалған тілде берумен шектелмейді. Айыптаудың мәні, саралау белгісі және сот қабылдаған түсіндіру сотталушыға нақты әрі бірімәнді жеткізілуі керек. Екі ресми мәтін арасында мағыналық айырма анықталған жағдайда, сот оны елемей бір нұсқаны механикалық пайдаланбай, қай ұғымның заң жүйесіне сәйкес екенін және таңдаудың адамның жағдайына қалай әсер ететінін шешімде негіздеуге тиіс [5].

Заң мәтіндеріндегі лингвистикалық қателерді зерттеу лексикалық, стилистикалық, грамматикалық және синтаксистік олқылықтардың құқықтық норманың мағынасын бұзуы, терминдердің негізсіз жарыспалылығы мен дұрыс емес баламалардың теңтүпнұсқалықты әлсіретуі мүмкін екенін көрсетеді. Қылмыстық заңға қатысты мұндай қателердің салмағы жоғары: редакциялық кемшілік қылмыстық жауаптылықтың шекарасына айналады. Сондықтан лингвистикалық мониторинг қабылданған заңдарға ғана емес, әрбір өзгеріс пен толықтыру жобасына, соның ішінде салыстырмалы кестелер мен ілеспе актілерге де жүргізілуі қажет [6].

Қазақ тіліндегі заң мәтіндерінде терминдердің қолданылуын талдаған зерттеулер сөзбе-сөз аударма, терминологиялық бірізділіктің болмауы және ұғымдық сәйкестіктің толық сақталмауы әлі де жүйелік мәселе екенін атап көрсетеді. Бұл қорытынды қылмыстық заңды аудару моделін қайта қарауды талап етеді. Алдымен орысша жобаланып, кейін қазақшаға аударылған мәтінді соңғы кезеңде тексеру жеткіліксіз; құқықтық ұғым екі тілде жобаның бастапқы сатысынан қатар қалыптасуы тиіс. Сонда аудармашы дайын мәтіннің сөздерін ғана емес, заң шығарушы

көздеген құқықтық конструкцияны екі тілде бір мезгілде құрастырады [7].

Қылмыстық кірістерді тәркілеу саласындағы арнайы зерттеу «заңсыз жолмен» және «қылмыстық жолмен» алынған кірістер тәрізді сырттай ұқсас тіркестердің құқықтық көлемі бірдей еместігін көрсетеді. «Заңсыз» ұғымы әкімшілік, азаматтық немесе өзге құқық бұзушылықтарды да қамтуы мүмкін, ал «қылмыстық» белгі предикаттық қылмыстық құқық бұзушылықпен байланыс орнатады. Мұндай айырмашылық кірістің шығу тегін дәлелдеу, мүлікті тәркілеу және ақшаны жылыстатуды саралау кезінде шешуші болады. Терминдердің салааралық сәйкессіздігі материалдық және процестік нормаларды түрліше қолдануға алып келетіндіктен, бірыңғай «қылмыстық жолмен алынған кірістер» конструкциясын сақтау негізді [8].

Лингвистикалық коллизияны құқықтық нормалардың бәсекелестігінен және мазмұндық коллизиядан ажырату қажет. Нормалар бәсекелестігінде бір фактіге бірнеше өзара қайшы емес норма үміткер болады, ал арнайы, жалпы, бөлік және тұтас нормалардың арақатынасы бойынша біреуі таңдалады. Мазмұндық коллизияда екі норма қарама-қайшы міндет немесе құқықтық салдар белгілейді. Лингвистикалық коллизияда қайшылық көбіне бір нормативтік еріктің әртүрлі тілдік берілуінен немесе терминнің жүйе ішінде тұрақсыз қолданылуынан туындайды. Дегенмен ол нәтижесінде мазмұндық коллизияға айналуы мүмкін, өйткені әр тілдік нұсқа әртүрлі қылмыстық-құқықтық шешімге жетелейді.

Мұндай жағдайда құқық қолданушыға кезеңдік интерпретациялық алгоритм қажет. Бірінші кезеңде даулы сөздің нақты грамматикалық және синтаксистік шекарасы анықталады. Екінші кезеңде қазақ және орыс тілдеріндегі нұсқалар сөзбе-сөз емес, ұғымдық белгілер бойынша салыстырылады. Үшінші кезеңде Кодекстің анықтамалары, Жалпы бөлім қағидалары және сабақтас нормалар ескеріледі. Төртінші кезеңде өзгерістің заңнамалық тарихы, салыстырмалы кесте және түсіндірме материалдары тексеріледі. Бесінші кезеңде таңдалған мағына заңдылық, кінәлі жауаптылық және құқықтық айқындық талаптарымен

салыстырылады. Соңғы кезеңде қорытынды процессуалдық актіде ашық уәжделеді.

Алгоритмнің шекті ережесі - жойылмаған күмәнді адамның жағдайын нашарлататын кеңейтуші түсіндіруге айналдырмау. Қылмыстық заңның мәтініндегі мағыналық белгісіздік жаңа қылмыс құрамын жасауға, саралаушы белгіні ұқсастық бойынша қосуға немесе санкцияны ауырлатуға негіз болмауға тиіс. Бұл тәсіл соттың заң шығарушыны алмастыруын болдырмайды. Егер екі тілдегі нұсқаны жүйелік талдау арқылы бір мағынаға келтіру мүмкін болмаса, мәселе ресми заңнамалық түзетуге шығарылуы керек, ал нақты іс бойынша айыпталушының құқықтық жағдайын нашарлатпайтын шешім басым болуға тиіс.

Терминологиялық алшақтықтардың алдын алудың тиімді халықаралық ұйымдастырушылық тәсілдерінің бірі - қосарлас заң жобалау. Канаданың федералдық тәжірибесінде ағылшын және француз мәтіндері бірінің аудармасы ретінде емес, бір мезгілде әзірленетін екі түпнұсқа әрі тең беделді нұсқа ретінде құрылады. Бұл модельді тікелей көшіру міндетті емес, бірақ оның қағидасы Қазақстан үшін пайдалы: қылмыстық-құқықтық норманы әзірлеу тобына екі тілде еркін жұмыс істейтін заңгерлер, салалық мамандар және заң лингвистері бастапқы кезеңнен қатысуы қажет [9].

Бірінші институционалдық ұсыныс - қылмыстық құқықтың қазақша-орысша ұғымдық тезаурусын жасау. Ол жай аударма сөздігі болмауы тиіс. Әрбір терминге тұрақты идентификатор, екі тілдегі атау, нормативтік анықтама, тектік және түрлік байланыстар, қолданылатын баптар, рұқсат етілмейтін синонимдер, сабақтас процестік ұғымдар және мысалдық контекстер енгізілгені жөн. Мұндай тезаурус заң жобалау жүйесімен интеграцияланса, бір ұғымның жаңа редакцияда басқа баламамен кездейсоқ берілуі автоматты түрде белгіленеді. Ол соттар, прокуратура, адвокатура және жоғары оқу орындары үшін де ортақ ұғымдық база қалыптастырады.

Екінші ұсыныс - Қылмыстық кодекстің екі тілдегі параллель цифрлық корпусын және нұсқаларды бақылау жүйесін құру. Корпуста әр бап, бөлік, тармақ және термин өзара байланыстырылып, өзгерістер тарихы екі тілде бір уақытта

көрсетілуі керек. Автоматты талдау бір терминнің әртүрлі аударылуын, анықтауыштың түсіп қалуын, модальды етістіктің ауысуын, сандық шектер мен сілтемелердің сәйкессіздігін анықтай алады. Дегенмен алгоритм соңғы шешім қабылдамайды; ол сарапшыға тәуекел нүктесін көрсетеді. Құқықтық мағынаны бағалау міндетті түрде адамның кәсіби пайымымен аяқталуға тиіс.

Үшінші ұсыныс - заңдық-лингвистикалық сараптаманы формальды келісу рәсімінен тәуелсіз сапа сүзгісіне айналдыру. Сараптама қорытындысында кемінде терминологиялық бірізділік, тектік-түрлік қатынас, диспозиция элементтерінің толықтығы, модальдылық, субъект пен объект атаулары, зардап пен мөлшер санаттары, ішкі және салааралық сілтемелер тексерілуі керек. Қылмыстық жауаптылықты белгілейтін немесе күшейтетін түзетулер үшін екі тілдегі кері аударма және құқықтық салдар тесті қолданылғаны жөн: әр нұсқаны дербес оқыған екі сарапшы бірдей гипотетикалық істі бір баппен және бірдей белгілер бойынша саралай алуы тиіс.

Төртінші ұсыныс құқық қолдану практикасына бағытталады. Жоғарғы соттық түсіндірулерде терминологиялық қайшылықты анықтау мен еңсерудің өлшемдері, сот актісінде екі тілдік нұсқаны салыстыру тәртібі және жойылмайтын күмәннің құқықтық салдары бекітілуі қажет. Тергеушілер мен прокурорлар айыптау формуласында заңдағы терминді дәл пайдаланып, оның фактілік мазмұнын ашуы тиіс; аудармашыға құқықтық қорытынды жасау жүктелмеуге тиіс. Адвокаттарға екі нұсқаның айырмасын қорғау дәлелі ретінде көтеруге нақты процессуалдық мүмкіндік берілуі, ал сот лингвистикалық сараптаманың қорытындысын құқықтық түсіндіруді алмастырмайтын көмекші дәлел ретінде бағалауы керек.

Бесінші ұсыныс - анықталған коллизияларды жедел түзететін кері байланыс механизмін құру. Соттар, прокуратура, адвокаттар палаталары, ғылыми ұйымдар және азаматтар терминологиялық қайшылық туралы ұсынысты бірыңғай электрондық тізілімге енгізе алуы тиіс. Уәкілетті орган әр хабарламаны құқықтық және лингвистикалық тұрғыдан бағалап, оның мәртебесін, ұсынылған шешімін және заңнамалық түзету кезеңін ашық көрсетуі қажет. Мұндай тізілім бірдей мәселенің бірнеше рет қайталануын

азайтады, заң шығарушының жауаптылығын арттырады және қылмыстық заң мәтінінің сапасын тұрақты мониторингтеуге мүмкіндік береді.

Ұсынылған шаралардың практикалық нәтижесі тек мәтіннің көркемдігін арттыру емес. Бірізді терминология қылмыстық құқық бұзушылық құрамының белгілерін бірдей түсінуге, ұқсас істерді тең саралауға, айыптаудың шекарасын алдын ала болжауға және сот актілерінің уәжділігін күшейтуге мүмкіндік береді. Сонымен қатар ол мемлекеттік тілдегі кәсіби құқықтық дискурстың дербестігін қамтамасыз етеді: қазақша мәтін орысша нұсқаны түсіну үшін қолданылатын қосымша аударма емес, қылмыстық-құқықтық ойлау мен дәлелдеудің толыққанды құралына айналады. Бұл қылмыстық сот төрелігіне қоғамдық сенімнің тілдік негізін нығайтады.

Қорытындылай келе, Қазақстанның қылмыстық құқығындағы лингвистикалық коллизиялар редакциялық ұсақ кемшілік ретінде бағаланбауға тиіс. Терминологиялық алшақтық қылмыстық-құқықтық тыйымның көлемін, кінәнің мазмұнын, зардаптың сипатын, арнайы субъектінің шеңберін және саралаушы белгінің болуын өзгертуге қабілетті. Сондықтан оның түпкі салдары адамның іс-әрекетін басқа баппен немесе баптың неғұрлым ауыр бөлігімен саралау, дәлелдеу пәнін бұрмалау және қорғану құқығын әлсірету болуы мүмкін. Қылмыстық заңның тілдік дәлдігі осы мағынада заңдылық қағидатының материалдық құрамдас бөлігі болып табылады.

Мәселені шешу екі бағыттың бірлігін талап етеді. Біріншісі - профилактикалық бағыт: қосарлас әзірлеу, екітілді тезаурус, цифрлық корпус, міндетті сараптама және нұсқаларды автоматтандырылған салыстыру арқылы коллизияның заң мәтініне енуіне жол бермеу. Екіншісі - құқық қолданушылық бағыт: даулы терминді жүйелік талдау, екі ресми нұсқаны тең қарау, кеңейтуші түсіндіруге жол бермеу және таңдалған мағынаны сот актісінде толық уәждеу. Осы тетіктер кешенді енгізілгенде ғана қазақ және орыс тілдеріндегі қылмыстық заң мәтіндері формальды қатар өмір сүретін нұсқалардан біртұтас нормативтік еріктің шын мәніндегі теңтүпнұсқа көрінісіне айналады.

Ғылыми мақала Қазақстан Республикасы Ғылым және жоғары білім министрлігі Ғылым комитеті қаржыландыратын, 2024-2027 жылдарға арналған ғылыми және (немесе) ғылыми-техникалық бағдарламалар бойынша бағдарламалық-нысаналы қаржыландыру аясында, ИРН BR24993217 «Қазақстан Республикасының қылмыстық құқық саласындағы заң мәтіндерінің лингвистикалық түпнұсқалығын қамтамасыз ету және заң терминологиясын үйлестіру» жобасын іске асыру шеңберінде дайындалды.

Әдебиеттер тізімі

1. Қазақстан Республикасының Конституциясы: 1995 жылғы 30 тамызда республикалық референдумда қабылданған [Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/K950001000> (қаралған күні: 21.06.2026).

2. Құқықтық актілер туралы: Қазақстан Республикасының 2016 жылғы 6 сәуірдегі № 480-V ҚРЗ Заңы [Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/Z1600000480> (қаралған күні: 21.06.2026).

3. Қазақстан Республикасының Қылмыстық кодексі: Қазақстан Республикасының 2014 жылғы 3 шілдедегі № 226-V ҚРЗ Кодексі [Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/K1400000226> (қаралған күні: 21.06.2026).

4. Қазақстан Республикасындағы тіл туралы: Қазақстан Республикасының 1997 жылғы 11 шілдедегі № 151-І Заңы [Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/Z970000151> (қаралған күні: 21.06.2026).

5. Сот ісін жүргізу тілі қағидатын қолданудың кейбір мәселелері туралы: Қазақстан Республикасы Жоғарғы Сотының 2016 жылғы 22 желтоқсандағы № 13 нормативтік қаулысы [Электрондық ресурс]. - URL: <https://adilet.zan.kz/kaz/docs/P160000013S> (қаралған күні: 21.06.2026).

6. Нұрбаева Н.А. Заң мәтіндеріндегі лингвистикалық қателер // Қазақстан Республикасының Заңнама және құқықтық ақпарат институтының Жаршысы. - 2024. - № 2(77). - Б. 297-305. - DOI: 10.52026/2788-5291_2024_77_2_297. - URL: https://doi.org/10.52026/2788-5291_2024_77_2_297 (қаралған күні: 21.06.2026).

7. Капезов Д.Ш., Жуанышпаева С.Ж., Ауганбаева М.С., Аубакирова А.Е. Заң мәтіндерінде термин сөздердің қолданысы // М. Қозыбаев атындағы Солтүстік Қазақстан университетінің хабаршысы. - 2025. - № 4(68). - Б. 211-217. - DOI: 10.54596/2958-0048-2025-4-211-217. - URL: <https://doi.org/10.54596/2958-0048-2025-4-211-217> (қаралған күні: 21.06.2026).

8. Еркенов Б.Д., Букенесов А.С. Терминологические коллизии в уголовном и уголовно-процессуальном законодательстве Республики Казахстан при конфискации преступных доходов // Құқық қорғау органдары академиясының Жаршысы. - 2025. - № 4(38). - DOI: 10.52425/25187252_2025_38_170. - URL: https://doi.org/10.52425/25187252_2025_38_170 (қаралған күні: 21.06.2026).

9. Department of Justice Canada. Legislative Services Branch Evaluation: Evaluation Findings [Electronic resource]. - URL: <https://www.justice.gc.ca/eng/rp-pr/cp-pm/eval/rep-rap/13/lbs-dsl/p5.html> (accessed: 21.06.2026).

Магауия А.
старший преподаватель SDU University
Сейтжан А.А.
ассистент профессор НАО «Университет Нархоз»

РАСПРЕДЕЛЕНИЕ ПРАВ, ОБЯЗАННОСТЕЙ И ОТВЕТСТВЕННОСТИ МЕЖДУ УЧАСТНИКАМИ ОБРАБОТКИ БОЛЬШИХ ДАННЫХ

Отношения по обработке больших данных нельзя объяснить только противопоставлением владельца информации и ее пользователя. Для юридической квалификации необходимо установить, кто определил назначение обработки, кто выбрал состав сведений, кто обеспечивает исполнение и кому доступно прекращение конкретной операции. Право на технический объект, возможность распоряжаться массивом и обязанность отвечать на требование гражданина принадлежат не обязательно одному лицу. Поэтому исходным вопросом исследования является не составление перечня названий участников, а установление адресата каждой юридически значимой обязанности.

Пункт 1 статьи 27 Цифрового кодекса РК определяет центр обработки данных как объект, обеспечивающий размещение и функционирование других цифровых объектов; цифровая платформа также определена как объект в пункте 1 статьи 29 [1]. Следовательно, выражение «ответственность ЦОДа» требует уточнения: речь должна идти о физическом или юридическом лице, эксплуатирующем инфраструктуру либо предоставляющем соответствующие услуги. Само сооружение, оборудование или программная среда не превращается в самостоятельного должника.

Предлагается различать три уровня квалификации. Первый - организационная правосубъектность: какая организация или гражданин участвует в отношении и на каком основании действует.

Второй - функциональная роль: какие решения и операции относятся к этому участнику. Третий - категория применимых регуляторных требований: какие дополнительные обязанности связаны с масштабом, характером данных и назначением системы. Смещение уровней приводит к тому, что организационную форму ошибочно принимают за основание освобождения от обязанностей, а техническую возможность доступа - за доказательство ответственности за любое последующее использование массива.

Р. Махье, Й. ван Хобокен и Х. Асгари обращают внимание на неоднозначность установления контролера в сетевых сервисах и трудности координации обязанностей при совместном контроле. Существенны отмеченные ими неполнота представления о потоках данных и неравенство возможностей участников [2]. Эта постановка проблемы объясняет ограниченность договорной формулы, согласно которой каждый отвечает только «за свою систему»: граница системы еще не показывает, кто распорядился передать сведения, кто разрешил их дальнейшее использование и кто обязан восстановить нарушенное право.

Д. Казабуро применительно к цифровой рекламе сочетает анализ отдельных операций с проверкой организации обработки в целом [3]. Такой подход важен и за пределами рекламного рынка. Излишнее укрупнение делает всех участников неразличимыми; чрезмерное дробление позволяет не увидеть согласованное решение, исполняемое несколькими лицами. Для настоящего исследования поэтому избрана единица анализа «операция и связанная с ней обязанность», дополненная проверкой общей цели и организационных связей. Это метод юридической диагностики, а не утверждение о существовании универсального состава ответственности за участие в инфраструктуре Big Data.

Нормативная часть исследования учитывает законодательство по состоянию на 26 сентября 2026 года. Дела используются для проверки критериев разграничения обязанностей, а не для статистической оценки всей практики. При анализе казахстанских эпизодов предел выводов определяется содержанием официального сообщения; существование неопубликованных договоров, участие неназванных подрядчиков и их виновность не предполагаются.

Подпункт 10 статьи 1 Закона РК «О персональных данных и их защите» связывает понятие оператора с осуществлением сбора, обработки и защиты данных [4; 5]. Данное понятие нельзя без дополнительного обоснования переводить как европейский *processor*: казахстанская дефиниция сама по себе не ограничивает оператора исполнением чужого поручения. Для установления роли необходимо сопоставлять закон, договор и фактические решения, а не заменять одно нормативное понятие внешне похожим иностранным термином.

Пунктом 37 статьи 1 Закона от 24 июня 2026 года № 326-VIII введена статья 25-1: классификация учитывает уникальных субъектов персональных данных в одном или нескольких цифровых объектах независимо от организационно-правовой формы. Новая статья 10-1 предусматривает уведомительный порядок с исключением для малых и средних обработчиков [5]. Поэтому реестр и дифференциацию требований по масштабу нельзя предлагать как полностью отсутствующие институты. Предметом исследования становятся определенность критериев и их применение к фактически распределенной деятельности.

Наиболее очевидная трудность обнаруживается на границах категорий. В пункте 3 статьи 25-1 малые обработчики определены через предел «не более десяти тысяч», средние - от десяти тысяч до пятисот тысяч, крупные - пятьсот тысяч и более [5]. При буквальном прочтении значение 10 000 попадает в две категории; формулировка верхней границы средней категории также требует согласования с началом крупной. Это юридико-техническая неопределенность, а не основание утверждать, что весь механизм классификации неприменим.

Способ устранения должен быть сформулирован законодателем однозначно: нижняя граница каждой следующей категории и верхняя граница предшествующей не должны включать одно значение одновременно. При сохранении выбранных числовых ориентиров возможна конструкция «менее 10 000», «от 10 000 до менее 500 000», «500 000 и более». Это предлагаемое уточнение, а не воспроизведение действующей редакции. Выбор включения

пограничного значения в более высокую категорию должен быть прямо обозначен, поскольку с ним связывается объем обязанностей.

Для распределенной обработки не менее важно, что масштаб участника и масштаб отдельного договора - разные характеристики. В проектируемой модели оценки следует выяснять, какой объем относится к конкретному лицу, какие операции оно осуществляет и какие сведения учитываются повторно. Однако объединять показатели самостоятельных организаций только потому, что они пользуются одной площадкой, также нельзя без правового основания. Классификация не должна подменять установление участника: сначала определяется обязанное лицо, затем проверяется применимая к нему категория.

Подпункт 1 пункта 3 статьи 24 Цифрового кодекса предусматривает установление собственником или владельцем ресурса условий доступа и использования. При несовпадении собственника системы и ресурсов пункт 3 статьи 28 отсылает к соглашению между ними [1]. Это позволяет разграничить полномочие управлять инфраструктурой и договорное основание обращения с размещенным массивом: одно не заменяет другое.

Право поставщика предоставить массив следует отделять от права получателя использовать его для определенной цели. Для оператора уже предусмотрены утверждение необходимого и достаточного перечня сведений, защитные меры и представление доказательств согласия - подпункты 1), 2), 5) пункта 2 статьи 25 [4]. Эти обязанности не исполняются одним заверением контрагента о том, что «все разрешения получены». Проверять требуется соответствие подтверждения конкретной операции, а не наличие в договоре общей гарантии.

По нашему мнению, полезно разграничивать договорные обязанности поставщика и собственные обязанности приобретателя. Первый должен предоставлять предусмотренные договором сведения о составе, происхождении и ограничениях использования массива; второй - соотносить разрешенные пределы с собственной целью обработки. Гарантия поставщика может иметь значение для требований между контрагентами, но не превращает неподтвержденное основание обработки в подтвержденное. Вместе

с тем недостаточность документов еще не позволяет автоматически признать получателя причинителем любого возникшего впоследствии вреда: для этого необходим отдельный анализ оснований ответственности.

В пунктах 7 и 8 статьи 4 GDPR различаются лицо, определяющее цели и средства обработки, и лицо, обрабатывающее данные от его имени. Подпункты «а»–«д» пункта 3 статьи 28 требуют договорного закрепления инструкций, конфиденциальности, безопасности и условий привлечения другого исполнителя; пункт 10 связывает самостоятельное определение исполнителем целей и средств с приобретением роли контролера применительно к соответствующей обработке [6]. Эта конструкция относится к персональным данным и не может механически охватить любые неперсональные промышленные массивы.

Рекомендации Европейского совета по защите данных 07/2020 уточняют в пунктах 39–40 различие существенных и технических средств обработки. Выбор аппаратного обеспечения или конкретных мер безопасности может оставаться исполнителю, тогда как состав данных, категории субъектов, получатели и длительность обработки относятся к существенным параметрам. Пример стандартизированного облачного хранения показывает, что односторонне подготовленный договор еще не делает поставщика контролером, если он действует только в интересах заказчика и по его инструкциям [7].

Из этого не следует, что всякое нарушение инструкции означает появление самостоятельной цели. Необходимо различать ненадлежащее исполнение поручения и присвоение исполнителем возможности использовать сведения для своего назначения. В первом случае вопрос касается качества и пределов исполнения; во втором - самостоятельного основания обработки. Аналитический подрядчик не должен рассматриваться как свободный распорядитель массива только потому, что именно он обладает профессиональными знаниями. Но и заказчик не может объявить любого исполнителя единственным ответственным за цель, которую определил сам.

Решение Суда ЕС от 29 июля 2019 года по делу C-40/17 Fashion ID позволяет проверить эти различия на реальном споре. Суд толковал статью 2(d) Директивы 95/46, а не применял GDPR ретроспективно. В пунктах 74–85 статус совместного контролера связали с операциями сбора и передачи сведений посетителей через встроенную кнопку Facebook. Такой статус не распространялся автоматически на последующие операции, цели и средства которых владелец сайта не определял. Пункт 69 допускал совместный контроль без доступа каждого участника к самим данным, а пункт 70 исключал отождествление совместного участия с равной ответственностью [8].

Юридически значим здесь способ установления границы: не физическое нахождение файла и не только получение выгоды, а участие в решении, обусловившем конкретную обработку. Для казахстанского исследования это сравнительный аргумент, но не непосредственно действующее основание иска. Из него также нельзя выводить солидарную ответственность всех организаций, использующих внешние сервисы. Требуется выяснить, кто сформировал спорную операцию и какие последствия закон связывает именно с этой ролью.

Применительно к агрегатору предмет проверки целесообразно сосредоточить на объединении источников и определении нового назначения результата. Для аналитического исполнителя - на самостоятельности выбора цели и соблюдении согласованных параметров. Для получателя готового результата - на пределах его использования и возможности влияния на исходную обработку. Предлагаемое разграничение не закрепляет за организацией неизменную роль: одна и та же компания может исполнять поручение в одном отношении и определять самостоятельную обработку в другом. Поэтому описывать следует не организацию вообще, а ее участие в проверяемом процессе.

Пункт 4 статьи 29 Цифрового кодекса уже связывает требования к платформе с ее функциями, воздействием и характером контроля. Подпункт 3 пункта 5 статьи 31 предусматривает защиту платформ обмена продуктами данных от неправомерного доступа и утечек; подпункт 3 пункта 9

ограничивает передачу продуктов третьим лицам без согласия собственника, кроме предусмотренных законом случаев [1]. Следовательно, формула «мы только площадка» сама по себе не отвечает на вопрос об исполнении собственных обязанностей.

Одновременно возможность установить пользовательские условия не означает права произвольно расширить дозволенное поставщику использование чужих сведений. В предлагаемой модели договор платформы должен различать доступ к техническому интерфейсу, получение конкретного продукта и разрешение на дальнейшее использование. Эти действия нельзя объединять одним неопределенным согласием с условиями сервиса. Иначе из договора становится невозможно установить, на каком этапе участник вышел за пределы своего права и кто способен прекратить нарушение.

Для инфраструктуры необходима другая точность. Пункты 2–4 статьи 27 Кодекса различают возможность технического аудита, требования к устойчивому и безопасному функционированию и специальные обязательные требования к центрам, размещающим определенные категории данных и объектов [1]. Поэтому недопустимо представлять любую международную сертификацию как универсальное обязательное условие деятельности каждого ЦОДа. Проверке подлежат применимые требования и конкретная услуга, а не только наличие сертификата известной системы.

Размещение оборудования, управляемое хранение, администрирование системы и аналитическая обработка должны рассматриваться как разные виды исполнения. В договорной модели предлагается отдельно закреплять, кто управляет учетными записями и ключами, кто создает резервные копии, кто восстанавливает данные и кто вправе изменять сроки хранения. Перечисление этих вопросов не означает, что любому поставщику инфраструктуры следует поручить все перечисленные функции. Напротив, задача состоит в устранении неопределенности между фактически принятыми обязанностями.

Практическую проверку дает решение CNIL SAN-2022-009 от 15 апреля 2022 года о поставщике программных решений для медицинских лабораторий. В опубликованном тексте наименование

компании теперь обезличено. CNIL признала ее обработчиком, действовавшим для лабораторий, и установила нарушения статей 28(3), 29 и 32 GDPR. Наличие обязанности заказчиков заключить надлежащий договор не устранило собственной обязанности подрядчика. При миграции были извлечены сведения сверх согласованных параметров; ограниченность использованного программного инструмента не признана оправданием. Отмечены и недостатки защиты сервера [9].

Значение этого дела для квалификации инфраструктурной деятельности заключается не в размере санкции, а в самостоятельности обязанности исполнителя. Специализация на технической услуге не означает правового безразличия к ее содержанию. Однако неправильно делать и обратный вывод: из ответственности конкретного поставщика за установленные действия не следует, что всякий разработчик программы отвечает за любую обработку, выполняемую с ее помощью. Существенны фактическое участие, пределы поручения и адресованные исполнителю требования.

Для договорной практики отсюда вытекает необходимость различать согласование задания и подтверждение его исполнения. Акт оказанных услуг не должен автоматически считаться доказательством правомерности всех совершенных операций. В качестве самостоятельного исследовательского результата предлагается документировать границы исполнения: разрешенный набор сведений, операции, получателей, срок сохранения временных копий и порядок подтверждения удаления. Такая фиксация предназначена не для формального расширения документооборота, а для возможности сопоставить порученное и выполненное после возникновения спора.

5. Казахстанская практика и пределы передачи ответственности контрагенту

Официальное сообщение о проверках после публикаций февраля 2024 года указывает на привлечение «Казахтелекома» и Air Astana к ответственности по пункту 2 части 1 статьи 641 КоАП и отсутствие выявленных нарушений у ЕНПФ [10]. Оно позволяет анализировать индивидуализацию результатов проверки, но не

устанавливает распределение обязанностей между всеми возможными подрядчиками. Поэтому на его основе нельзя ни приписывать нарушение неназванному хостинг-провайдеру, ни объявлять заказчиков единственными ответственными за весь информационный инцидент.

Сообщение МВД от 9 июня 2025 года описывает расследование получения сведений из государственных баз и передачи через Telegram, в том числе отдельным коллекторским компаниям; указаны уголовные дела по статьям 205, 147 и 211 УК [11]. Это сообщение о расследовании, не о вступившем в силу приговоре. Для настоящей темы оно ставит вопрос о самостоятельной оценке получателя: необходимо исследовать содержание запроса, обстоятельства приобретения и дальнейшее использование, а не считать его положение производным только от действий первоначального источника.

Приведенные материалы не дают основания утверждать наличие устойчивой казахстанской судебной позиции по распределенной обработке. Их научное использование иное: они позволяют определить, каких фактов недостает для квалификации участника. В каждом эпизоде следует восстанавливать не только путь данных, но и путь решений. Передача массива доказывает участие в информационном обмене; она еще не отвечает на вопрос о правомерности цели, пределах поручения и причинной связи с конкретным последствием.

Гражданско-правовая оценка также требует разделения отношений. Пункт 1 статьи 363 ГК РК предусматривает ответственность должника перед кредитором за действия привлеченных третьих лиц, включая лиц, которым поручено исполнение, с предусмотренными законом исключениями. Пункты 2 и 4 устанавливают условия освобождения и возможность иных условий ответственности; статья 362 относит исполнение обязательства работниками к действиям должника [12]. Поэтому привлечение подрядчика нельзя автоматически считать заменой должника. Но и текст статьи 363 не позволяет игнорировать предусмотренные ею пределы и договорное регулирование.

Предлагается различать внешний и внутренний уровни распределения последствий. Внешний отвечает на вопрос, кто обязан перед заявителем по закону или договору. Внутренний - какие требования после исполнения могут возникнуть между участниками. Соглашение о возмещении потерь между заказчиком и исполнителем не должно подменять установление основания требования гражданина, не участвующего в таком соглашении. Аналогично внутреннее распределение технических работ не доказывает само по себе отсутствие нарушения у участника, которому законом адресована собственная обязанность.

Статья 932 Особенной части ГК связывает солидарную ответственность с совместным причинением вреда, а пункт 2 статьи 933 регулирует обратное распределение выплаченного возмещения между причинителями с учетом степени вины [13]. Следовательно, участие нескольких лиц в обработке и совместное причинение вреда - разные юридические обстоятельства. Первое описывает организацию процесса; второе требует установления предусмотренных гражданским законодательством оснований. Нельзя выводить солидарность исключительно из общего сервера, договора интеграции или последовательного доступа к одной базе.

Ту же границу необходимо сохранять при прекращении нарушения. Способность технически заблокировать операцию еще не означает обязанности единолично компенсировать все потери. Вместе с тем отсутствие такой компенсационной обязанности не оправдывает неисполнение собственного требования о блокировании, исправлении или предоставлении сведений. В предлагаемой модели меры прекращения и восстановления должны адресоваться участникам по содержанию их обязанностей, тогда как денежные последствия устанавливаются по соответствующему основанию ответственности.

Международный ориентир дает принцип подотчетности в пункте 14 рекомендаций ОЭСР о защите приватности. Пункт 15(a)(i) распространяет программу управления приватностью на все контролируемые персональные данные; подпункт «iv» требует механизмов внутреннего надзора, а пункт 15(b) - возможности продемонстрировать программу компетентному органу [14]. Это

рекомендательный документ, а не непосредственно применимое основание взыскания. Его значение для рассматриваемой проблемы - в необходимости проверить сохранение управляемости после передачи исполнения.

Для казахстанского права предлагается развивать не еще одно общее определение «оператора больших данных», а документируемое разграничение исполнения. Сведения следует организовать по связи «операция - правовое основание - лицо, определившее ее параметры, - исполнитель - доказательство исполнения». Не каждый элемент должен публиковаться: режим раскрытия необходимо согласовать с защитой чужих персональных данных и коммерческой тайны. Но существенные сведения должны быть доступны лицу, рассматривающему требование, и компетентному органу в установленном порядке.

В развитие пункта 4 статьи 29 Цифрового кодекса предметом законодательного обсуждения может стать следующее дополнение: «При привлечении иных лиц к обработке данных собственник или владелец цифровой платформы обеспечивает документирование распределения выполняемых операций, полномочий по определению их целей и существенных параметров, а также обязанностей по рассмотрению обращений и устранению нарушений. Такое распределение не изменяет установленные законом обязанности участников перед субъектами данных и иными управомоченными лицами». Это авторское предложение; оно не воспроизводит действующую норму и не устанавливает автоматической солидарной ответственности.

В отношении договоров инфраструктурного обслуживания предлагается согласовывать непрерывную последовательность действий при инциденте: фиксацию обнаруженного события, сохранение доказательств, уведомление управомоченного участника, исполнение мер ограничения и подтверждение результата. Договорный срок сообщения между исполнителями должен позволять адресату своевременно выполнить собственную публично-правовую обязанность. Простая оговорка «уведомление производится по внутренним правилам поставщика» не обеспечивает проверяемого распределения, если сами правила

неизвестны заказчику или допускают их одностороннее изменение без согласования.

Отдельного уточнения заслуживает передача исполнения следующему подрядчику. В проектируемой договорной модели заказчику должна быть доступна информация о существенном изменении состава исполнителей, влияющем на место обработки, доступ к данным или способы защиты. При этом право возражать против изменения следует связывать с определенными основаниями, а не с произвольным вмешательством в организацию услуги. Важно также предусмотреть передачу требований о сохранении доказательств и прекращении нарушения по всей относящейся к спорной операции цепочке.

Наконец, устранение выявленной неопределенности статьи 25-1 необходимо отделять от расширения обязанностей по существу. Исправление пересекающихся диапазонов является вопросом однозначности классификации; введение нового состава обязанностей требует самостоятельного обоснования. Смешивать эти предложения нельзя: иначе техническая корректировка границ может быть представлена как согласие с новым объемом регулирования. Для сравнительной таблицы поправок следует отдельно фиксировать действующее положение, выявленную неопределенность, предлагаемое решение и его предполагаемые правовые последствия.

Правовое положение участника обработки больших данных следует устанавливать применительно к конкретному отношению. Организационная форма определяет, какое лицо участвует в обороте; функциональная роль - какие решения и операции ему относятся; регуляторная категория - какие дополнительные требования применимы. Ни один из этих уровней не заменяет остальные. В частности, право на инфраструктуру не создает общего права на размещенную информацию, а исполнение чужого поручения не устраняет собственных обязанностей исполнителя.

Предложенная модель распределения основана на сопоставлении операции, ее правового основания, полномочий по принятию решений и доказательств исполнения. Ее прикладное назначение - определить адресата требования без необоснованного

переноса всех рисков на технического подрядчика либо на первоначального заказчика. При этом распределение работ, обязанность прекратить нарушение и обязанность возместить вред должны оцениваться отдельно. Такой подход позволяет формулировать конкретные договорные и законодательные решения, не подменяя юридическую квалификацию технологическими наименованиями участников.

Финансирование. Исследование подготовлено в рамках проекта ИРН AP23489796 «Проблемы регламентации правового режима больших данных (Big Data): отечественный и международный опыт», финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан.

Список использованных источников

1 Цифровой кодекс Республики Казахстан : Кодекс Республики Казахстан от 9 января 2026 г. № 255-VIII ЗРК // Казахстанская правда. - 2026. - 10 января. - № 5–6 (30634–30635). - Электронное воспроизведение: Учет.kz. - Используемые положения: ст. 24, 27–29, 31. URL: <https://zakon.uchet.kz/rus/docs/K2600000255> (дата обращения: 01.07.2026).

2 Mahieu, R. Responsibility for Data Protection in a Networked World: On the Question of the Controller, “Effective and Complete Protection” and its Application to Data Access Rights in Europe / R. Mahieu, J. van Hoboken, H. Asghari // JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law. - 2019. - Vol. 10, no. 1. - P. 84–104. - URN: urn:nbn:de:0009-29-48796. URL: <https://www.jipitec.eu/jipitec/article/view/247> (дата обращения: 02.06.2026).

3 Casaburo, D. Digital Advertising and the GDPR: Identifying the (Joint) Controllers in the Real-Time Bidding Ecosystem / D. Casaburo // JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law. - 2024. - Vol. 15, no. 3. - P. 212–228. URL: <https://www.jipitec.eu/jipitec/article/view/410> (дата обращения: 04.06.2026).

4 О персональных данных и их защите : Закон Республики Казахстан от 21 мая 2013 г. № 94-V // Ведомости Парламента Республики Казахстан. - 2013. - № 7. - Ст. 35. - Официальная карточка акта: ИПС «Әділет». - Используемые положения: ст. 1, 25. - Связанный акт о внесении изменений: Закон Республики Казахстан от 24 июня 2026 г. № 326-VIII, указанный в записи 5. URL: <https://old.adilet.zan.kz/rus/docs/Z1300000094/info> (дата обращения: 02.07.2026).

5 О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам цифровизации, защиты персональных данных, дорожного движения и регулирования передовых технологий на транспорте : Закон Республики Казахстан от 24 июня 2026 г. № 326-VIII ЗРК //

Казахстанская правда. - 2026. - 25 июня. - № 117 (30746). - Официальная карточка акта: ИПС «Әділет». - Используемые положения: п. 37 ст. 1, ст. 2. URL: <https://old.adilet.zan.kz/rus/docs/Z2600000326/info> (дата обращения: 03.07.2026).

6 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. - 4 May. - P. 1–88. - Используемые положения: ст. 4, 28, 29, 32. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата обращения: 08.06.2026).

7 European Data Protection Board. Guidelines 07/2020 on the concepts of controller and processor in the GDPR [Электронный ресурс]. - Version 2.1. - Adopted on 7 July 2021, minor corrections on 20 September 2022. - 51 p. - Используемые положения: п. 39–40, 117, 150. URL: https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf (дата обращения: 10.06.2026).

8 Court of Justice of the European Union. Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV [Электронный ресурс] : judgment of the Court (Second Chamber) of 29 July 2019, Case C-40/17 // EUR-Lex. - 2019. - ECLI:EU:C:2019:629. - Используемый фрагмент: п. 69–85. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A62017CJ0040> (дата обращения: 12.06.2026).

9 Commission nationale de l'informatique et des libertés. Délibération de la formation restreinte n° SAN-2022-009 du 15 avril 2022 concernant la société x [Электронный ресурс] // Légifrance. - 2022. - 21 avril. - Дата принятия: 15 апреля 2022 г., дата публикации: 21 апреля 2022 г. - Наименование компании в опубликованном тексте обезличено. URL: <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000045614368> (дата обращения: 15.06.2026).

10 Цифрлық даму министрлігі ақпан айындағы жеке деректердің тарап кетуіне қатысты аудит нәтижелері туралы айтты [Электронный ресурс] / Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан // Gov.kz. - [2024]. - Официальное сообщение о результатах проверок «Казахтелекома», Air Astana и ЕНПФ. - Номер публикации: 738683. URL: <https://www.gov.kz/memleket/entities/maidd/press/news/details/738683> (дата обращения: 17.06.2026).

11 Тұрлыбек, Ш. Ликвидирована группа, занимавшаяся продажей данных казахстанцев [Электронный ресурс] / Ш. Тұрлыбек // Polisia.kz : информационный медиа-портал. - 2025. - 9 июня. URL: <https://polisia.kz/ru/likvidirovana-gruppa-zanimavshayasya-prodazhej-dannyh-kazahstantsev/> (дата обращения: 19.06.2026).

12 Гражданский кодекс Республики Казахстан (Общая часть) : Кодекс Республики Казахстан от 27 декабря 1994 г. № 268-ХІІІ // Ведомости Верховного Совета Республики Казахстан. - 1994. - № 23–24 (приложение). - Электронное воспроизведение: Учет.kz. - Используемые положения: ст. 362–363. URL: https://zakon.uchet.kz/rus/docs/K940001000_ (дата обращения: 22.06.2026).

13 Гражданский кодекс Республики Казахстан (Особенная часть) : Кодекс Республики Казахстан от 1 июля 1999 г. № 409 // Ведомости Парламента Республики Казахстан. - 1999. - № 16–17. - Ст. 642. - Электронное воспроизведение: Учет.kz. - Используемые положения: ст. 932–933. URL: https://zakon.uchet.kz/rus/docs/K990000409_ (дата обращения: 24.06.2026).

14 OECD. Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [Электронный ресурс] : OECD/LEGAL/0188 : принята 23 сентября 1980 г., пересмотрена 11 июля 2013 г. // OECD Legal Instruments. - Используемые положения: п. 14–15 приложения. URL: <https://legalinstruments.oecd.org/public/doc/114/114.en.pdf> (дата обращения: 26.06.2026).

Мукашева А.А.

Доктор юридических наук, профессор Школы права и государственного управления НАО «Университет Нархоз»

РАЗГРАНИЧЕНИЕ КОМПЕТЕНЦИИ ГОСУДАРСТВЕННЫХ ОРГАНОВ ПРИ ЗАЩИТЕ ПРАВ В СФЕРЕ БОЛЬШИХ ДАННЫХ

Установить факт утечки данных и восстановить нарушенное право - разные задачи. Первая может требовать технической экспертизы, а вторая - прекращения обработки, исправления информации, пересмотра решения или возмещения вреда. Между ними находятся юридическая квалификация события и выбор процедуры. Поэтому исследование государственного контроля не следует сводить к перечислению ведомств. Необходимо определить, какое решение вправе принять каждый участник и какие правовые последствия оно способно вызвать.

Р.А. Подопригора раскрывает административную юстицию через судебный контроль законности деятельности публичной администрации [1]. Это доктринальное разграничение позволяет отделить разрешение спора с органом власти от исполнения самим органом контрольной функции. Его значение сохраняется независимо от технологической формы отношений: обращение через цифровой сервис не превращает административное рассмотрение жалобы в правосудие, а государственное

происхождение базы данных не устраняет возможности оспаривать действия ее держателя.

В исследовании А. Ньюмана институциональные различия режимов защиты информации связываются с устройством надзорных органов и их взаимодействием [2]. Дж. Блэк, анализируя полицентрическое регулирование, предлагает предварять институциональные решения исследованием фактических связей подотчетности и коммуникации [3]. Для рассматриваемой темы отсюда следует методологическое ограничение: ни централизация всех полномочий, ни увеличение числа контролирующих органов сами по себе не доказывают улучшения защиты. Проверять следует определенность ответственности за конкретное публичное решение.

Р.Болдуин и Дж.Блэк связывают результативное регулирование с согласованием инструментов, институционального контекста и оценки последствий их применения [4]. М. Маценайте различает использование риска при построении требований и при организации правоприменения [5]. Однако риск не может самостоятельно создавать компетенцию. Масштаб массива объясняет необходимость определенной интенсивности реагирования, но не позволяет органу выйти за предмет предоставленного полномочия либо заменить установленную процедуру технической целесообразностью.

Цифровой кодекс РК закрепляет контрольные функции уполномоченного органа в подпункте 2 пункта 2 статьи 14, подпункт 3 статьи 15 ограничивает контроль других органов пределами их компетенции [6]. Эти общие положения требуют конкретизации специальным законодательством. Выражение «нарушение в сфере Big Data» обозначает предмет исследования, но еще не отвечает на вопрос о правовом основании проверки, ее адресате и допустимой мере реагирования.

Границы исследования не совпадают с границами законодательства о персональных данных. Для коммерчески ценного массива существенны также условия охраны тайны по статье 126 и способы гражданской защиты по статье 9 ГК РК [7]. Поэтому цифровая форма договорного спора о неперсональных данных сама по себе не обосновывает вмешательство регулятора

персональных данных. Предмет его полномочия должен быть установлен отдельно; иначе комплексность режима ошибочно превращается в неограниченность ведомственной компетенции.

Цель настоящей работы - определить правила согласования центральной, территориальной, отраслевой и судебной компетенции. Применяются формально-юридический анализ, функциональное сравнение и разбор конкретных правоприменительных эпизодов. Законодательство рассматривается по состоянию на 27 сентября 2026 года. Новые нормы используются для оценки действующей модели, а не для ретроспективной квалификации событий 2024 года. Официальное сообщение о проверке не приравнивается к полному административному делу; зарубежные решения исследуются в пределах опубликованных судебных выводов. На этой основе формулируются качественные, а не статистические оценки.

Следует обратить внимание на вопросы центрального и территориального контроля, пересечение полномочий и выявление коллизий. Подпункты 1-1), 3) и 5) пункта 1 статьи 27-1 Закона РК «О персональных данных и их защите» предусматривают контроль, рассмотрение обращений и требования по устранению определенных нарушений. Вместе с тем подпункты 1)-4) пункта 2 статьи 27 наделяют местные исполнительные органы областей, городов республиканского значения и столицы полномочиями рассматривать обращения, контролировать частное предпринимательство на соответствующей территории и принимать защитные меры [8]. Следовательно, модель, в которой все обращения адресуются исключительно центральному ведомству, неполно отражает закон.

Официальная страница ведомства указывает действующее наименование «Комитет по информационной безопасности Министерства искусственного интеллекта и цифрового развития Республики Казахстан» [9]. Но наименование административной структуры и объем установленной законом компетенции не тождественны. При оценке конкретного акта надлежит проверять полномочие органа и подписавшего его должностного лица, а не

ограничиваться указанием министерства, с которым связан соответствующий цифровой сервис.

Сопоставление статей 27 и 27-1 обнаруживает вопрос о разграничении одновременно предусмотренных полномочий. Территория нахождения организации, место технического размещения массива и место жительства заявителя могут служить разными привязками; выбор одной из них нуждается в правовом обосновании. Однако из самого совпадения формулировок о контроле еще не следует, что два органа вправе принимать несовместимые решения либо что одна из норм не действует. Требуется различать пересечение сферы интереса, параллельную проверку разных обязанностей и действительное противоречие властных предписаний.

Изменения 2026 года уточняют и содержание восстановительных мер. Подпункты 18) и 19) пункта 37 статьи 1 Закона № 326-VIII дополняют соответствующие полномочия требованием удаления данных и предусматривают реестр нарушений безопасности [10]. Поэтому предложение заново «учредить учет утечек» не решало бы выявленную проблему. Развивать следует связь учетной записи с компетентным органом, процессуальным решением и результатом исполнения, не считая сам факт регистрации доказательством виновности.

Особого внимания заслуживает государственный орган, который одновременно организует обработку и участвует в публичном управлении. Контроль государственных органов специально регулирует статья 27-3: предусмотрены периодические и внеплановые проверки, а сведения Государственной технической службы названы одним из информационных источников. Подпункты 3) и 6) пункта 3 допускают, в частности, требование прокурора и поручение органа уголовного преследования как основания внеплановой проверки [8]. Это примеры взаимодействия, но не передачи проверяющему органу всех функций инициатора.

Предлагается оценивать такую проверку по двум самостоятельным критериям: компетентности органа и беспристрастности исполнителя. Подпункты 3) и 4) части 1 статьи 67 АПК уже предусматривают отвод при зависимости,

заинтересованности и иных обстоятельствах, вызывающих сомнение в объективности [11]. Значит, вопрос не исчерпывается учреждением новой контрольной структуры. Необходимо показать, как действующие гарантии применяются при проверке обработки, организационно связанной с публичной администрацией. Наличие такой связи само по себе еще не доказывает неправомерности каждого принятого решения.

Действующая редакция Закона от 24 ноября 2015 года № 418-V носит название «О кибербезопасности». Подпункты 1) и 4) пункта 1 статьи 9 предусматривают сбор и анализ информации Национальным координационным центром и уведомление органа защиты персональных данных в течение трех часов после обнаружения нарушения их безопасности. Подпункты 2) и 6) пункта 1 статьи 10 закрепляют информационное взаимодействие отраслевого центра и аналогичное уведомление [12]. Поэтому механизм передачи технического сигнала правовому регулятору уже существует.

Из этого следует необходимость различать содержание передаваемых сведений. Техническое сообщение должно позволять установить источник, время и характер обнаруженного события, но не подменяет юридической оценки согласия, допустимости цели обработки или размера индивидуального вреда. Отсутствие подтвержденной атаки также не означает правомерности использования данных: спор может касаться обработки, технически выполненной без нарушения защиты. Следовательно, завершение технического реагирования не должно автоматически закрывать рассмотрение самостоятельного требования субъекта.

Полномочия органов национальной безопасности нельзя сводить только к расследованию преступлений. Пункт 11 статьи 1 Закона № 326-VIII дополнил Закон «Об органах национальной безопасности Республики Казахстан»: подпункт 4-2) пункта 1 статьи 2 и подпункты 8-2), 8-3) статьи 12 предусматривают контроль кибербезопасности критически важных цифровых объектов и выдачу предписаний [10]. Это специальный предмет контроля, а не универсальное полномочие разрешать любой спор об информации.

Существенны квалификация объекта и конкретное требование безопасности.

Официальное сообщение о ТОО «МФО Робокэш.кз» показывает участие нескольких субъектов в одном эпизоде: обнаружение утечки Государственной технической службой, совместную проверку министерства и Агентства по регулированию и развитию финансового рынка, административное реагирование и уведомление граждан. Указаны более двух миллионов персональных данных, штраф по части 4 статьи 79 КоАП и возможность судебного обращения [13]. Источник не раскрывает полный состав проверочных документов, поэтому распределение всех действий между органами не может быть восстановлено предположительно.

Тем не менее этот материал позволяет поставить конкретный вопрос: чем отраслевое участие отличается от повторения общей проверки защиты данных? Подпункты 1), 2) и 4) статьи 13-6 Закона о регулировании финансового рынка предусматривают регулирование оценки защищенности, рисков и служб реагирования финансовых организаций. Пункты 1-2 статьи 15 одновременно закрепляют самостоятельность уполномоченного органа и координацию в пределах компетенции [14]. Таким образом, координация не означает отказ финансового регулятора от собственных критериев проверки.

Для правовой оценки дела важно установить, какое нарушение выявлено каждым органом, каким актом оно зафиксировано и кто проверяет исполнение восстановительного требования. Сообщение о совместной проверке не должно восприниматься как доказательство существования единого универсального производства. Назначение штрафа не подтверждает автоматически восстановление безопасности, прекращение дальнейшего распространения либо компенсацию каждому гражданину. Это самостоятельные результаты, для которых требуются свои основания и подтверждения.

Предлагаемый критерий согласования состоит в общности доказательственной основы при раздельной юридической квалификации. Повторное истребование одного документа

нуждается в объяснении, но получение документа другим ведомством не освобождает орган от проверки его относимости и достоверности. Особенно важно сохранять сведения об источнике и условиях получения, чтобы межведомственный обмен не превращал непроверенную техническую гипотезу в окончательный вывод о нарушении.

На обозначенные вопросы обращают внимание и европейские специалисты. Ф. Коста-Кабрал и О. Лински обосновывают возможность учитывать защиту данных при оценке неценовой конкуренции, одновременно подчеркивая различие целей и методов соответствующих отраслей [15]. Для Казахстана эта постановка полезна не как готовое правило подведомственности, а как способ различить совместное исследование фактов и применение разных юридических оснований. Одна операция с массивом способна затронуть несколько охраняемых интересов; это еще не делает их взаимозаменяемыми.

В решении от 4 июля 2023 года по делу C-252/21 Meta Platforms v Bundeskartellamt Суд ЕС допустил оценку соблюдения GDPR антимонопольным органом, когда она необходима для установления злоупотребления доминирующим положением. Пункт 1 резолютивной части связывает такую оценку со статьями 51 и последующими GDPR и пунктом 3 статьи 4 Договора о Европейском союзе: нельзя отступать от релевантного решения надзорного органа, а при указанных Судом сомнениях требуется консультация [16]. Это разрешение на ограниченную сопутствующую оценку, а не передача антимонопольному органу общей компетенции по данным.

А.-М. Хриску выделяет как возможности применения стандартов защиты данных в конкурентном анализе, так и трудности рассмотрения информационных прав исключительно через его призму [17]. О. Брук и М. Эбен, исследуя то же дело, указывают на недостаточную определенность соотношения права конкуренции ЕС и национальных правил по статье 3 Регламента 1/2003 [18]. Эти позиции не опровергают резолютивный вывод Суда, но предостерегают от представления одного решения как завершенной модели всех межведомственных отношений.

Применительно к казахстанскому регулированию предлагается различать оценку факта для собственной процедуры и вынесение обязательного предписания в сфере другого органа. Для первой может быть необходимо исследовать смежную норму; для второго требуется самостоятельное полномочие. Межведомственное соглашение способно определить сроки консультации и формат передачи материалов, но не должно становиться источником новой юрисдикции. Именно это ограничение позволяет использовать сравнительный результат без механического переноса европейской конструкции.

Другую границу раскрывает решение от 12 января 2023 года по делу C-132/21. Суд ЕС признал возможность параллельного и независимого использования средств по статьям 77(1), 78(1) и 79(1) GDPR, возложив на государства согласование процедур ради последовательности применения права и эффективной судебной защиты [19]. Следовательно, обращение к регулятору и требование непосредственно к обработчику нельзя неизменно представлять как последовательные ступени одной обязательной лестницы. Однако это толкование европейского права не отменяет казахстанских процессуальных предпосылок обращения в суд.

Части 1-3 статьи 65 АППК уже предусматривают перенаправление обращения либо отдельных требований в течение трех рабочих дней с уведомлением заявителя и возбуждением надлежащей процедуры. Поэтому предлагать «впервые разрешить передачу части жалобы» нет оснований [11]. Практический вопрос - правильно выделить требования: наличие вопроса, относящегося к другому ведомству, не должно служить объяснением отказа от рассмотрения собственной части. Передача материалов должна сопровождаться определенностью, а не исчезновением ответственности за ответ.

Необходимо также разграничивать обжалование публичного решения и частноправовой спор. Части 1-5 статьи 91 АППК регулируют административное обжалование и, по общему правилу, его предшествование судебному обращению; пункты 1 и 4 статьи 9 ГК РК предусматривают способы защиты гражданских прав и возмещение убытков [11; 7]. Эти положения относятся к различным

требованиям. Ссылка в ответе ведомства на возможность иска о возмещении вреда не разрешает вопрос о законности самого отказа в проверке либо восстановительной мере.

Юридическое значение имеет и различие между требованием наказать нарушителя и требованием восстановить право. Заявитель может добиваться устранения неверных сведений независимо от своей оценки необходимого штрафа. В свою очередь, административный орган не должен подтверждать размер гражданских потерь только фактом выявления нарушения. В модели согласованной защиты каждому результату соответствует определенная процедура: установленный факт, предписание, решение о публичной ответственности или судебное разрешение индивидуального требования.

Подпункты «а», «с», «е» и «f» пункта 19 рекомендаций ОЭСР о защите приватности соединяют межведомственную согласованность, ресурсную обеспеченность и объективность надзорных органов, доступность осуществления прав и надлежащие средства реагирования. Пункт 20 посвящен трансграничному сотрудничеству [20]. Это рекомендательные ориентиры, а не непосредственно действующее основание требований в Казахстане. Их значение для настоящей работы - возможность оценивать организацию контроля по достижению защитного результата, а не по одному числу проверок.

Дж. Робертс, П. Батчер, Э. Шерлок и С. Нейсон исследуют представление путей административной защиты на материале жилищных и образовательных споров [21]. Для споров о данных полезен сам метод: описание доступных процедур через желаемый результат и условия перехода, а не через список названий ведомств. Это предложение о применении исследовательского подхода, не утверждение об установленной авторами практике Казахстана.

Представляется необходимым дополнять уведомление заявителю кратким объяснением: какая часть требования рассмотрена, какие факты признаны установленными, кому переданы остальные вопросы и какое решение может быть обжаловано. При этом разъяснение не должно обещать определенный исход будущего гражданского дела. Его назначение -

обеспечить понятность распределения компетенции и возможность проверить исполнение каждой обязанности.

Научный результат исследования предлагается выразить через шесть последовательных вопросов: 1) какое право или требование нарушено; 2) какой объект и субъект подлежат проверке; 3) какой орган уполномочен действовать; 4) какое обстоятельство запускает процедуру; 5) какое решение допустимо; 6) кто проверяет его исполнение и рассматривает жалобу. Применение такой схемы позволяет выявлять конкретный разрыв, не объявляя недостатком само наличие нескольких ведомств.

Сопоставление статей 27 и 27-1 Закона о персональных данных показывает, что сами эти статьи не устанавливают развернутого правила приоритета центрального либо территориального рассмотрения. Поэтому предлагается конкретизировать территориальную привязку, согласование действий и разрешение разногласий о подведомственности с учетом действующих процедурных актов. Критерий должен учитывать, где осуществляется проверяемая деятельность и какое лицо отвечает за нее, а не только местонахождение оборудования. Межрегиональный характер обработки следует прямо учитывать в правилах координации; он не должен произвольно определяться удобством ведомства или подателя жалобы.

В развитие главы 5 этого Закона предлагается обсудить следующую норму: «При рассмотрении нарушений, относящихся к компетенции нескольких государственных органов, каждый орган определяет предмет осуществляемой им процедуры и принимает решения в пределах предоставленных законом полномочий. Органы обмениваются необходимыми материалами с соблюдением режима охраняемой законом информации и уведомляют заявителя о рассмотрении и передаче относящихся к ним требований. Координация не изменяет установленных законом сроков, оснований и порядка обжалования решений». Это авторское предложение, а не изложение действующей нормы.

Для информационного сопровождения предлагается использовать общий идентификатор инцидента, связанный с отдельными производствами. Он должен облегчать сопоставление

технических сведений, актов проверки и предписаний, не объединяя их в новое внесистемное «дело». В записи надлежит разграничивать подтвержденные обстоятельства, проверяемые предположения и правовую оценку конкретного органа. Доступ предоставляется по полномочию и необходимости, а не всем участникам автоматически. Такой подход развивает уже предусмотренный учет нарушений, вместо учреждения дублирующего реестра.

Оценку взаимодействия предлагается проводить по прослеживаемости результата. Для предписания существенны определенность адресата и проверка исполнения; для перенаправления - получение материалов компетентным органом; для уведомления - возможность понять содержание и доступный способ защиты. Само совпадение статистических показателей нескольких ведомств не доказывает дублирования, если они учитывают разные процедуры. Но сведения об одной проверке нельзя без пояснения выдавать за несколько самостоятельных восстановительных результатов.

Проверка предложенной модели на опубликованном эпизоде «Робокэш.кз» выявляет именно предел доступного знания: взаимодействие органов подтверждено, однако полнота восстановления прав из сообщения не устанавливается. Европейские дела позволяют дополнительно сформулировать ограничения координации: не присваивать чужую компетенцию, учитывать релевантные решения и не закрывать самостоятельный способ защиты только вследствие существования другого. Для эмпирической проверки исполнения предлагаемых правил необходимы полные дела и данные о выполнении предписаний; проведенный анализ не подменяет их отсутствующие сведения.

Разграничение компетенции в сфере больших данных требует отделить техническое знание об инциденте от полномочия принять юридически обязательное решение. Центральный, территориальный, отраслевой и судебный уровни должны сопоставляться по предмету, процедуре и результату. Пересечение интересов нескольких органов допустимо; неопределенность возникает тогда, когда невозможно установить адресата

обязанности, основание решения или порядок устранения противоречий.

Предложенная модель направлена на сохранение самостоятельности полномочий при согласованном исследовании фактов и контроле исполнения. Для совершенствования регулирования приоритетны определенность территориальной подведомственности, документирование передачи требований и проверка восстановительных результатов. Общая организационная координация не должна превращаться ни в новое основание ограничения прав, ни в объяснение бездействия компетентного органа.

Финансирование. Исследование подготовлено в рамках проекта ИРН AP23489796 «Проблемы регламентации правового режима больших данных (Big Data): отечественный и международный опыт», финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан.

Список использованных источников

1. Подопригора, Р. А. Административная юстиция в Казахстане: история, состояние, перспективы [Электронный ресурс] / Р. А. Подопригора // Параграф. - 2014. - 26 декабря. URL: https://prg.kz/Document/?doc_id=32016804 (дата обращения: 03.10.2026).
2. Newman, A. L. Protectors of Privacy: Regulating Personal Data in the Global Economy / A. L. Newman. - Ithaca : Cornell University Press, 2008. - 240 p. - ISBN 978-1-5017-2921-8 (электронное издание). URL: <https://www.jstor.org/stable/10.7591/j.ctv2n7f1b> (дата обращения: 03.10.2026).
3. Black, J. Constructing and contesting legitimacy and accountability in polycentric regulatory regimes / J. Black // Regulation & Governance. - 2008. - Vol. 2, no. 2. - P.137–164. - DOI: 10.1111/j.1748-5991.2008.00034.x. URL: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1748-5991.2008.00034.x> (дата обращения: 03.10.2026).
4. Baldwin, R. Really Responsive Regulation / R. Baldwin, J. Black // The Modern Law Review. - 2008. - Vol. 71, no. 1. - P. 59–94. - DOI: 10.1111/j.1468-2230.2008.00681.x. URL: <https://onlinelibrary.wiley.com/doi/10.1111/j.1468-2230.2008.00681.x> (дата обращения: 03.10.2026).
5. Macenaite, M. The “Riskification” of European Data Protection Law through a two-fold Shift / M. Macenaite // European Journal of Risk Regulation. - 2017. - Vol. 8, no. 3. - P. 506–540. - DOI: 10.1017/err.2017.40. URL: <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/riskification-of-european->

data-protection-law-through-a-twofold-shift/A91B3E7A0A1EF4E6889FD54F94 1D83D3 (дата обращения: 03.10.2026).

6. Цифровой кодекс Республики Казахстан : Кодекс Республики Казахстан от 9 января 2026 г. № 255-VIII ЗРК // Казахстанская правда. - 2026. - 10 января. - № 5–6 (30634–30635). - Электронная версия: ИПС «Әділет». - Используемые положения: ст. 14–15. URL: <https://old.adilet.zan.kz/rus/docs/K2600000255/info> (дата обращения: 03.10.2026).

7. Гражданский кодекс Республики Казахстан (Общая часть) : Кодекс Республики Казахстан от 27 декабря 1994 г. № 268-XIII // Ведомости Верховного Совета Республики Казахстан. - 1994. - № 23–24 (приложение). - Электронная версия: ИПС «Әділет». - Используемые положения: ст. 9, 126. URL: https://old.adilet.zan.kz/rus/docs/K940001000_/info (дата обращения: 03.10.2026).

8. О персональных данных и их защите : Закон Республики Казахстан от 21 мая 2013 г. № 94-V // Ведомости Парламента Республики Казахстан. - 2013. - № 7. - Ст. 35. - Электронная версия: ИПС «Әділет». - Используемые положения: ст. 27–27-3, с учетом изменений, предусмотренных Законом Республики Казахстан от 24 июня 2026 г. № 326-VIII. URL: <https://old.adilet.zan.kz/rus/docs/Z1300000094/info> (дата обращения: 03.10.2026).

9. Комитет по информационной безопасности Министерства искусственного интеллекта и цифрового развития Республики Казахстан. Общая информация [Электронный ресурс] // Gov.kz. - [Б. г.]. - Официальная страница органа со ссылкой на положение. URL: <https://www.gov.kz/memleket/entities/infsecurity/about?lang=ru> (дата обращения: 03.10.2026).

10. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам цифровизации, защиты персональных данных, дорожного движения и регулирования передовых технологий на транспорте : Закон Республики Казахстан от 24 июня 2026 г. № 326-VIII ЗРК // Казахстанская правда. - 2026. - 25 июня. - № 117 (30746). - Электронная версия: ИПС «Әділет». - Используемые положения: п. 11, 37 ст. 1, ст. 2. URL: <https://old.adilet.zan.kz/rus/docs/Z2600000326/info> (дата обращения: 03.10.2026).

11. Административный процедурно-процессуальный кодекс Республики Казахстан : Кодекс Республики Казахстан от 29 июня 2020 г. № 350-VI ЗРК // Ведомости Парламента Республики Казахстан. - 2020. - № 13. - Ст. 66. - Электронная версия: ИПС «Әділет». - Используемые положения: ст. 65, 67, 91. URL: <https://old.adilet.zan.kz/rus/docs/K2000000350/info> (дата обращения: 03.10.2026).

12. О кибербезопасности : Закон Республики Казахстан от 24 ноября 2015 г. № 418-V ЗРК (первоначальное наименование - «Об информатизации») // Ведомости Парламента Республики Казахстан. - 2015. - № 22-V. - Ст. 155. - Электронное воспроизведение: Учет.kz. - Используемые положения: ст. 9–10, с учетом изменений 2026 г. URL: <https://zakon.uchet.kz/rus/docs/Z1500000418> (дата обращения: 03.10.2026).

13. Минцифры объявило результаты проверки в отношении ТОО «МФО Робокэш.кз» [Электронный ресурс] / Министерство цифрового развития,

инноваций и аэрокосмической промышленности Республики Казахстан // Gov.kz. - [2024]. - Официальное сообщение. - Номер публикации: 740137. URL: <https://www.gov.kz/memleket/entities/maidd/press/news/details/740137?lang=ru> (дата обращения: 03.10.2026).

14. О государственном регулировании, контроле и надзоре финансового рынка и финансовых организаций : Закон Республики Казахстан от 4 июля 2003 г. № 474 // Ведомости Парламента Республики Казахстан. - 2003. - № 15. - Ст. 132. - Электронное воспроизведение: Учет.kz. - Используемые положения: ст. 13-6, 15. URL: https://zakon.uchet.kz/rus/docs/Z030000474_ (дата обращения: 03.10.2026).

15. Costa-Cabral, F. Family ties: the intersection between data protection and competition in EU law / F. Costa-Cabral, O. Lynskey // Common Market Law Review. - 2017. - Vol. 54, no. 1. - P. 11–50. - DOI: 10.54648/cola2017002. URL: <https://kluwerlawonline.com/journalarticle/Common%2BMarket%2BLaw%2BReview/54.1/COLA2017002> (дата обращения: 03.10.2026).

16. Court of Justice of the European Union. Meta Platforms Inc. and Others v Bundeskartellamt [Электронный ресурс] : judgment of the Court (Grand Chamber) of 4 July 2023, Case C-252/21. - ECLI:EU:C:2023:537. - Электронное воспроизведение резолютивной части: European Union Agency for Fundamental Rights. - Используемое положение: п. 1 резолютивной части. URL: <https://fra.europa.eu/en/caselaw-reference/cjeu-case-c-25221-judgement> (дата обращения: 03.10.2026).

17. Hriscu, A.-M. C-252/21 Meta v Bundeskartellamt: The lawfulness of Big Tech's processing of personal data and the relationship between data protection and competition law / A.-M. Hriscu // European Data Protection Law Review. - 2023. - Vol. 9, no.3. - P.371–377. - DOI: 10.21552/edpl/2023/3/15. URL: <https://research.tilburguniversity.edu/en/publications/c-25221-meta-v-bundeskartellamt-the-lawfulness-of-big-techs-proce/> (дата обращения: 03.10.2026).

18. Brook, O. Another Missed Opportunity? Case C-252/21 Meta Platforms v Bundeskartellamt and the Relationship between EU Competition Law and National Laws / O. Brook, M. Eben // Journal of European Competition Law & Practice. - 2024. - Vol.15, no.1. - P.25–29. - DOI: 10.1093/jeclap/lpad047. URL: <https://academic.oup.com/jeclap/article/15/1/25/7319218> (дата обращения: 03.10.2026).

19. Court of Justice of the European Union. BE v Nemzeti Adatvédelmi és Információszabadság Hatóság [Электронный ресурс] : judgment of the Court (First Chamber) of 12 January 2023, Case C-132/21. - ECLI:EU:C:2023:2. - Электронное воспроизведение резолютивной части: European Union Agency for Fundamental Rights. URL: <https://fra.europa.eu/en/caselaw-reference/cjeu-case-c-13221-judgement> (дата обращения: 03.10.2026).

20. OECD. Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [Электронный ресурс] : OECD/LEGAL/0188 : принята 23 сентября 1980 г., пересмотрена 11 июля 2013 г. // OECD Legal Instruments. - Используемые положения: п. 19–20 приложения. URL: <https://legalinstruments.oecd.org/public/doc/114/114.en.pdf> (дата обращения: 03.10.2026).

21.Explanatory Journeys: Visualising to Understand and Explain Administrative Justice Paths of Redress [Электронный ресурс] / J. C. Roberts, P. Butcher, A. Sherlock, S. Nason // arXiv. - 2021. - 29 July. - Version 1. - 11 p. - arXiv:2107.14013v1. - DOI: 10.48550/arXiv.2107.14013. URL: <https://arxiv.org/abs/2107.14013> (дата обращения: 03.10.2026).

Нұрмағанбет Е.Т.

Әл-Фараби атындағы Қазақ ұлттық университеті

Қазақстан Республикасы, Алматы қ.

E-mail: ermek004@mail.ru

ДӘЛЕЛДЕМЕЛЕРДІ ЖИНАУ БОЙЫНША АДВОКАТ- ҚОРҒАУШЫ ҚЫЗМЕТІНІҢ ДЕРБЕСТІГІН ЖҮЗЕГЕ АСЫРУ ҚҰҚЫҒЫНЫҢ МӘСЕЛЕСІ

Дәлелдемелерді жинау бойынша қорғаушы-адвокат қызметінің дербестігін жүзеге асыру құқығын беру қажеттілігі туралы мәселе 70-ші жылдары да талқыға салынған. М.С. Благоволинамен және Әдебиет газеттерінің беттерінде 1969 жылы жазылған көптеген сот очерктердің авторларымен қорғаушының алдын-ала тергеу жүргізгенде мүмкіндіктері анағұрлым тарылып кететіндігі көрсетілген. Онда, қорғаушы-адвокат істің тындалуына дейін куәгерлермен кездесіп, олармен әңгімелесуге және іске қатысты мән-жайларды білуге құқығы жоқ екендігі көрсетілген. Әңгімелесу фактісінің өзі-ақ адвокатқа қатысты тәртіптік өндіріске қарсы іс қозғау үшін негіз болғандығын білдіреді. Көрсетілген авторлардың пікірі бойынша, осының өзі қорғау мүмкіндіктерін елеулі түрде шектеткен. Осылар арқылы қорғаушы-адвокаттарға тергеу жүргізу мүмкіндігі берілген [1, 44 б.].

Қорғаушыға дәлелдемелерді жинау дербестігін жүзеге асыру құқығын беру туралы ұсыныс, ғалымдар арасында пікірталас туғызып, жақтаушылар мен қарсыластардың пайда болуына әкеп соқтырды. Бұл мәселе үш он жалдықта талқылануда болды, ал қазір қылмыстық іс жүргізу реформасының жағдайына байланысты ерекше маңызға ие болды.

Осы мәселенің теориялық талдау негізінде, сондай-ақ тәжірибені талдауда дәлелдемелерді жинау бойынша қорғаушы-адвокат қызметінің дербестігін жүзеге асыру құқығын беру қажеттілігін дәлелдеуге тырысып көреміз.

Жалпы сот өндірісі екі жақтың бәсекелестігі мен құқық теңділігі негізінде жүзеге асады. Қылмыстық іс жүргізу теориясында «қылмыстық сот өндірісі» және «қылмыстық іс жүргізу» деген түсініктер тепе-тең ұстанымы ретінде бекітілді. Бірақ, өзге ұстаным ретінде «қылмыстық өндіріс» түсінігі қазір беріле береді. Мәселен, В.З. Лукашевичтің пікірі бойынша, заң шығарушы конституцияның белгіленген бабында алдын-ала сот өндірісінің сатысы туралы емес, соттың істі қарау сатысы туралы әңгіме қозғайды [2, 41 б.]. Осы көзқарастың толық болмаушылығын көрсету үшін ең алдымен алдын-ала жедел тергеу жүргізу барысында сот отырысындағы шындыққа жетудің жүзеге асуын дәлелдеп көрейік.

А.О. Машовец, қылмыстық іс жүргізуге байланысты алдын-ала тергеу бүтіндей өзіне тән ерекше қасиетімен біршама дербес және жеке жүйе бөлігі ретінде алға шығып тұрады, деп жазады. Ол жүйенің тұтас тәртібіне сай негізгі тәртіппен құрылуы қажет. Алдын-ала тергеудің түпкілікті кемшілігі - оның негізгі бастауларының соттың істі қарау қағидаларымен сәйкес келмеуінде [3, 7 б.].

Алдында айтылғандай, алдын-ала тергеудің негізгі міндеті – сотқа мәлімет жинау. Заңи әдебиеттерінде алдын ала-тергеу жүргізу барысында істің барлық маңызды мән-жайларды анықтап, бүкіл қажетті дәлелдемелердің дереккөздерін табу керек, деп ескертіледі [4, 56 б.]. Яғни, мәліметтердің толық болуына байланысты сотта зерттелетін барлық мән-жайлар ең алдымен алдын-ала тергеу арқылы анықталуы қажет.

Олардың айырмашылығы - тек олардың шешілу күшінен ғана тұрады. Заң шығарушы тергеушіге айыптау және ақтау дәлелдемелерін жинау міндетін жүктеді. Сөйтіп, тергеуші ылғи да тіпті қарсы міндеттерді орындауға тиісті. Карл Маркс та былай деп жазған екен: тергеуші мен судьяның және айыпталушы мен

қорғаушының бір тұлғада болуы барлық психология заңдарына қарама-қайшылық келтіреді [5, 26 б.].

Тергеушінің айыптау жағынақызығушылық танытуы да әбден ықтимал. Қылмыстық істі қозғап, ол арқылы айыптауды құрастырып, айыпталушыға қатысты бұлтартпау шарасын қолдана отырып, тергеуші өзінің осындай шешімдерімен еркін емес байланыста болып қалады. Істің мән-жайларын онан арғы объективті зерттеу үшін оған кедергі келтіреді.

Тергеуші дәлелдемелер жинағанда объективті бола алмайды және өз жұмыс сапасының бағалар жүйесінің күшіне сәйкес, қылмыстық істің қысқартылуы, жұмыста сөзсіз жарамсыз етіп бағаланады және тергеушіні кінәға тартады [6, 97 б.]. Сотпен қосымша тергеу үшін жіберілген бұрыс тергелген істерді қайтарудан сақтандыру мақсатында тергеушілер тәжірибе жүзінде «артық айыптауды» жиі ұсынады.

Соттармен айыптаудың кейбір тармақтары мен эпизодтарының жойылуы, қылмыстық іс-әрекеттің саралауын аса ауыр емес қылмысты көздейтін қылмыстық кодекстің бабына сәйкес өзгертілуі тәжірибеде жиі кездеседі.

Тергеушімен айыптау және ақтау дәлелдемелерін бірдей алалықсыздықпен жинауға мүмкіндігінің болмау негізгі себептерінің бірі - тергеуші қызметінің ерекшелігінде негізделеді. Тергеуші әрдайым қылмыстық элементпен /қылмыскермен/ қатынаста болады. Л.М. Васильев өтірікті, зұлымдықты, екіжүзділікті жиі жеңу, тергеушілерге тиісті стереотиптердің қалыптасуына әкелетіндігін ескереді [7, 11 б.].

Көбінесе тергеушілер айыптаушыларды қылмыскер ретінде танып, олардың өз пайдасына айтылған дәлелдемелеріне біржақтылықпен қарайды. Қырағылық - сезіктілікке (барлығына және әр қайсысына сезіктенеді) айналып, ал сыншылдық - келіп түскен хабардың бағасы бойынша ешкімге толық сенімнің болмауына айналады. Әдебиетте тергеушілердің біржақтылығына мысалдар келтіріледі. Бірақ кейбір тергеушілер, егер айыпталушы алаңдай беретін болса, демек ол өз жағдайының қиындығын ұғына отырып, ар-ұжданы таза еместігін көрсетеді, деп есептейді. Егер де ол өзін емін-еркін және тежеусіз ұстаса – бұл қылмыскердің

әдепсіздігі ретінде есептеледі. Егер айыпталушы кез келген мән-жайды ұмытып қалса, онда бұл, олардың көзқарасы бойынша, оның өтірік айтуын білдіреді. Егер де ол барлық сұрақтарға қуана-қуана жауап беретін болса, онда ол алдын-ала құрылған жоспар бойынша әрекет жасап, өтірік түсіндірме беріп отырғандығын білдіреді [8, 40 б.].

Ғалымдар тергеу органдарында жұмыстың ұзақтылығы мен кәсіби өзгерістің деңгейі арасында тікелей тәуелділіктің болу туралы гипотезасын ұсынды. Сонымен, осы гипотезаға сәйкес, бағаланып жатқан қызметтің өзгерісі 5-10 жылдық жұмыс уақыт бөлігінде дамып келеді. Кәсіби өзгерістің бастапқы деңгейі тергеушінің бесінші жұмыс жылынан басталып, тергеушінің бірін-сарандаған өзгерісін жорамалдайды. Кәсіби өзгерістің орташа деңгейі тергеу жұмысында 10 жылдан кейін басталады [9, 38 б.].

Сөйтіп, объектілі себептердің күшіне байланысты тергеуші ҚР ҚІЖК 20 бабында көзделген міндетін орындай алмайды. Алдын ала тергеудің айыптау жалтаруы жиналған мәліметтің толық еместігі мен сыңар жақтылығына әкеледі. Шындықтың сыртқы көрінісі бар бұл мәлімет сотқа келіп түседі. Көбінесе айыпталушының пайдасына айтылғандар тергелмей қалады.

Тергеушінің алдында сыңар жақты зерттелген істің құжаттары бар болса, ол алғашқы бағалау мен дәлелдемелерді жинауда қатыспаса, оларды алу жолынан еш хабары жоқ болса, онда тәртіптің дұрыс орындалуына аса назар аударуға міндетті сот, алдын-ала тергеу тексерісін жүргізетіндігі туралы әдебиетте ескеріледі. Осыған байланысты айыптау жалтаруы тергеу кезеңінен бастап еріксіз соттың істі қарауына беріледі. Атқаруға тиісті ашық сот емес, құпия алдын-ала тергеу – азаматтың кінәсін көрсететін дәлелдемелері жиналып, зерттеліп, бағаланатын негізгі сатысына айналады, ал егер соңғы шешімге келмесе, онда маңызды дәрежеде оның кінәлілігі туралы мәселе алдын-ала шешіледі [10, 147 б.].

Сотта шынайы жарысты қамтамасыз ету үшін сотқа жақтар «қарулы» болып келулері тиіс, әрқайсысы қайта сот өндірісінің кезеңдерінде жиналған толық дәлелдемелер тізімімен келулері қажет (прокурор-айыптау, қорғаушы-ақтау). Сондай-ақ, ҚР ҚІЖК сәйкес айыпталушыға қатысты дәлелдемелерді жинау бойынша

прокурордың маңызды құралдары өте көп, басқа жақтың – қорғаушының дәлелдемелерді жинау бойынша мүмкіндіктері шектеулі. Бұл, сотқа келгенде екі жақтың тең болмаушылығына әкеледі. Осыған байланысты ешқандай жарыс туралы сөз қозғалмайды. Сот отырысында қорғаушының рөлі көбінесе тергеуші жұмысының кемшілігін анықтауға саяды. Соттың қорғаушыға деген сенімі пайда болу үшін, қорғаушыда ақтау дәлелдемелердің жеткілікті жиынтығы болуы керек.

Бұл жағдай тәжірибені зерттеу барысында да өз дәлелін тапты. Олай болса, басқа жақпен – айыпталушымен сотта нағыз жарысу үшін, алдын-ала тергеуде қорғаушылардың құқықтары жеткілікті ме деген сұраққа, сұралған Алматы қалалық адвокаттар алқасының 79,7% адвокаттары және Алматы облыстық адвокаттар алқасының 80,4% адвокаттары - олардың құқықтары жеткіліксіз деп жауап берді, тек сұралған 7,10% алматылық адвокаттары және 44% облыстық адвокаттар - қорғаушылардың құқықтары жеткілікті деп есептейді. Соған қарамастан сұралған 6,2% қалалық адвокаттар мен 4,40% облыстық адвокаттар - тек ресми түрде ғана құқықтары жеткілікті бола алады деп есептейді.

Сұралған адвокаттардың басым көпшілігі қылмыстық іс жүргізу кезінде қорғаушыға дәлелдеме ақпаратты алу үшін қосымша іс жүргізу мүмкіндіктерін беруді жөн көреді. Олардың ішінен 89,9% облыстық адвокаттар мен 94% қалалық адвокаттар - қорғаушыға дәлелдемелерді жинау үшін дербес құқығын беру керек деп есептейді. Сонымен, соттың істі қараудың жарысына, алдын-ала тергеуде қорғаушының дәлелдемелер жинау үшін тек жеткілікті құралдарын беру жолымен ғана қол жеткізуге болады.

Қорғаушыға дәлелдемелерді жинауға дербес құқығын беру туралы ұсыныс ғалымдар арасында кең қолдауын тауызд [11]. Сондықтан осы мәселе бойынша тергеушілердің де пікірін анықтау қажет болды. Тиісінше Алматы облысының ІІБ-ң 61 тергеушілер саралап сұралды. Олардың ішінен 75 %-ы қорғаушыға дәлелдемелерді жинауға дербес құқығын беру қажет деп есептейді, ал сұралған тергеушілердің 25 %-ы бұған жол бермеу керек деп есептейді.

Сонымен, сұралған тергеушілердің көбісі бұл шараның қажетті екеніне сенеді.

Қорғаушыға мұндай құқықты беруге қарсы шыққан іс жүргізуші-ғалымдар мен тәжірибелік қызметкерлер басқа да дәлелдерді келтіреді. Онда тергеушінің айыптау міндетінің күшеюіне әкеледі деген пікір бар. Яғни, тергеуші – әдеттегідей айыптау дәлелдемелерді, ал адвокат – ақтау дәлелдемелерді жинайтын болады. Сонымен қатар тергеуші үшін жауап беретін тиісті аппарат, маңызды қызмет қатары тұр, ол адвокатқа қарағанда, қажетті материалдық құралдармен жабдықталған және дәлелдемелерді жинауға анағұрлым мүмкіндіктері бар. Сыртқы көзге бұл жарысу сияқты көрінеді, ал мәні жағынан бұл күдіксіз айыптау жалтаруына әкеледі. Сонымен қатар, қорғау, материалдық тұрғыдан қарағанда, көпшілікке қол жетерліктей емес, өйткені тергеу әрекеттердің өндірісіне байланысты адвокаттың шығыны қорғалушыға ауыр таға секілді жүктеледі [12, 19 б.].

Келесі дәлел ретінде осы жағдай бойынша мемлекеттік органдармен қорғаушы адвокаттың бәсекеге түсуге мүмкіндігі жоқ, өйткені қорғаушы-адвокатта өктем өкілеттілігі жоқ және мәжбүрлеумен және т.б. байланысты оның қандай болмасын іс-әрекеттерді орындауға құқығы жоқ [13, 47 б.].

Қорғаушыға дәлелдемелерді жинауға дербес құқығын беруге қарсы тағы бір маңызды дәлел бар – кейбір ғалымдардың және тәжірибелік қызметкерлердің (адвокаттардың) пікірі бойынша, ол адвокат-қорғаушының қызметінің нәтижелеріне объективті және анық кепіл беру мүмкін емес. Келтірілген дәлелдерді толық қарастырайық.

Қорғаушыға дәлелдемелерді жинауға дербес құқықты беру әбден айыптау жалтаруға әкелмеу үшін, ол қажетті жағдайда тергеушінің, алдын-ала анықтау органының, соттың билігін пайдалануға нақты мүмкіндігі болу керек. Қылмыстық іс бойынша өндірісті жүзеге асыратын органдар қорғаушы-адвокатқа дәлелдемелерді жинауға жәрдем көрсету керек. Ол үшін, алдында көрсетілгендей, қорғаушымен өтінген қолдаухаттың нақты құрылымын жасау қажет.

Тергеуші мен адвокат-қорғаушыда ақпаратты алу құқықтары бірдей емес туралы пікірге негіз бар. Алдында көрсетілгендей, дәлелдемелерді жинамай тұрып, көбінесе жедел-ізвестіру жүргізіледі, өйткені ақпарат әрдайым оңай жерден табыла бермейді. Заңға сәйкес тергеуші тергеліп жатқан істер бойынша ізвестіру шараларының өндірісі туралы (уақиға көргендерді анықтау туралы, тұлғаларды және әлемнің материалдық заттарын іздеу туралы, тұлғалар арасында өзара қатынасты анықтау туралы және т.б.) тапсырыстарды алдын-ала анықтау органдарына береді. Қорғаушылар әдетте жедел-ізвестіру жұмысында жедел-ізвестіру қызметіне байланысты тиісті өкілеттілік тәжірибелері жоқ болады. Сонымен, қорғаушылардың өздері оларды қызықтаратын мән-жайларды кез-келген уақытта нақты анықтай алмайды.

Бұл жағдайдан шығу үшін бір амал ұсынылады. Қылмыстық істер бойынша қорғаушыларға дәлелдемелерді жинауға жеке детективтердің маңызды жәрдем көрсетуге мүмкіндіктері бар (адвокат-қорғаушы мен жеке детективтердің өзара әрекетінің қажеттілігі туралы мәселе ерекше өзектілікке ие). Бірақ мұндай өзара әрекеттің экономикалық, құқықтық және өзге де мәселелер қатары бар.

Қорғаушыға дәлелдемелерді жинауға дербес құқығын беруге қарсы шыққандардың келесі дәлелі - қорғаушылар қызметіндегі қорытындыларының дұрыстығы мен объективтілігін қамтамасыз ету мүмкін емес деген пікірді ұсынады [14, 19 б.].

Ең алдымен, бұл адвокат-қорғаушыға сенімсіздіктің және қорғаушылар құқықтарының ұлғаюы, қиянат етушіліктің көбеюіне әкелетін қауіптің пайда болуымен байланысты.

Осы мәселелер бойынша адвокаттардың пікірлеріне талдау жасалды. Сұралған Алматы облыстық адвокаттар алқасының 12,5% адвокаттары және Алматы қалалық адвокаттар алқасының 6,2% адвокаттары қорғаушылардың дәлелдемелерді жинауға дербес құқықтарының ұлғаюы қорғаушылар тарапынан қиянат етушілік оқиғалар санының көбеюіне әкеледі деп есептейді. Сонымен қатар сұралған облыстық адвокаттарының 21,1% және қалалық адвокаттарының 5,2% осы жағдаймен байланысты қиянат етушіліктердің болуы мәлім деп есептейді. Сұралған облыстық

адвокаттарының 37,3% мен мәскеу адвокаттарының 51,7% қорғаушылардың дәлелдемелерді жинауға дербес құқықтарының ұлғаюы қорғаушылар тарапынан қиянат етушілік оқиғалар санының көбеюіне әкелмейді деп есептейді. Өз кезегінде облыстық адвокаттарының 30,3% мен қалалық адвокаттарының 33,5% қорғаушылардың дәлелдемелерді жинауға дербес құқықтарының ұлғаюы қорғаушылар тарапынан қиянат етушілік оқиғалар санының көбеюіне әкелуі мүмкін деп есептейді. Қалған адвокаттарға қойылаған сұраққа жауап беру қиынға түсірді.

Сонымен, сұралған адвокаттардың көбісі қорғаушылар тарапынан қандай болмасын қиянат етушіліктер болмау керек деп есептейді. Оның барлығы нақты тұлғаның әдептілігіне байланысты.

Бірнеше он жылдықта қалыптасқан адвокаттардың әдепсіздік презумпциясына сену қазір дұрыс емес деп саналады. Мұндай қиянат етушіліктер тергеушілерде, прокурорларда және судьяларда да орын алады.

ҚР Қылмыстық Кодексінің 348 бабында дәлелдемелерді бұрмалаған үшін жауапкершілікке тарту туралы көрсетілген. Қорғаушы осы қылмыстың субъектілерінің шеңберіне қосылады. Бұл бап адвокат-қорғаушы тарапынан келтірілген қиянатқа қарсы кепіл ретінде жүреді. Бұдан басқа, адвокат-қорғаушы тарапынан қиянат етушілік анықталса, оларға адвокаттар алқасынан шығып кетуіне дейін тәртіптік сипаты бар шара қолданылады [15].

Екіншіден, А.Д. Бойковтың пікірі бойынша, егер тергеушінің қызметі көп жағдайда қорытындысының объективті болуына кепіл беретін белгілі бір іс жүргізу нысаны арқылы жүргізілсе, онда адвокаттық қатар жедел-ізвестіру ешбір іс жүргізу кепілдерін біле бермейді [16, 6 б.].

Заттар мен құжаттарды алуға бағытталған қорғаушының қызметі іс жүргізу нысанында жүргізілу керек деп есептеледі, өйткені оның қызметі жұмыс барысының шеңберінде жүзеге асады және жұмыс барысының көзделген мақсаттарына бағынады. Қорғаушының жүргізуге міндетті шаралар тізімі дәлелдемелерді жинауға арналған бапта енгізілу қажет.

Әдебиеттер тізімі

- 1 Благоволина М.С. Почта редактора/ Литературная газета, 1969 г. - № 44; Винберг А. Первая командировка// Литературная газета - № 41- 1969 г.
- 2 Лукашевич В.З. Конституция РФ 1993 года и дальнейшее совершенствование уголовно-процессуального законодательства// Уголовно-правовые проблемы борьбы с преступностью. - Калининград, 1995 г. – с 41.
- 3 Машовец А.О. Принцип состязательности и его реализация в предварительном следствии: Автореф. дис. на соиск. уч.ст.к.ю.н.- Екатеринбург, 1994 г.- с 7.
- 4 Стремовский В.А. Предварительное расследование в советском уголовном процессе. -М.: Госюриздат, 1958г.– с.11.; Воробьев Г.А.
- 5 Соотношение предварительного и судебного следствия: Автореф. дис. на соиск. уч. ст. к.ю.н.-М, 1967г.; Колбая Г.Н.Соотношение предварительного следствия и судебного разбирательства: М: Юрид.лит., 1975 г. с56.
- 6 К. Маркс, Ф. Энгельс. Сочинения (В 30 - т.). Изд. 2 - е. Т. 1. - М.: Госполитиздат, 1958 г. – с 26.
- 7 Резник Г.М. Внутреннее убеждение при оценке доказательств. - М.: Юрид. лит., 1977 г. - с 97.
- 8 Васильев Л.М. Организация следственной работы //Вопросы подготовки следователей и преодоление их профессиональной деформации - Краснодар, 1983 г. – с 11.
- 9 Стремовский В.А. Предварительное расследование в советском уголовном процессе.М.: Госюриздат, 1958 г – с 40.
- 10 Васильев Л.М. Указ.соч. – с 38.
- 11 Лившиц В.Л. Обвинительный уклон (Истоки и пути преодоления)// Закон и ведомственные нормативные акты в СССР. - Труды.-46 - М, 1989 г.-с 143.
- 12 Либус И. А. Защита в уголовном процессе // Перестройка и адвокатура. Научные и практические проблемы уголовного судопроизводства. - Ижевск, 1989 г. – с119.; ЛибусИ. А. Об эффективности деятельности защитника в стадии предварительного следствия.Ташкент, 1971г. – с 46.; Хорхина Т.В.
- 13 Проблемы деятельности адвокатуры (Обзор текстов на материалы круглого стола)// Советское государство и право. – 1986г.- №9;. Машовец А.О. Указ. соч. – с7., Капустин А.А.
- 14 Реформа советского предварительного расследования - сущность, предпосылки, основные направления: Автореф. дис. На соиск. уч. ст. к.ю.н. - Санкт - Петербург, 1992г.- с16.; Ведерников А.Н.
- 15 Актуальные вопросы участия защитника на стадии предварительного расследования (в свете осуществления судебной реформы) - Дис. на соиск. уч. ст. к. ю. н. - М.- 1990 г. – с.148;
- 16 Анашкин Г. З. Адвокат. Права и проблемы // Литературная газета, - 1969г. № 41;Бойков А. Карнеева Л. Об участии защитника на предварительном следствии //Советская юстиция, - 1970 г. – с.19.

17 Царев В.М. Эффективность участия защитника в доказывании на предварительном расследовании следствии - Красноярск.: Изд. Красноярск, ун-та, 1990 г. – с.47.

18 А.Бойков, Л.Карнеева. Об участии защитника на предварительном следствии.// Советская юстиция. -1970 г. - № 19.

19 ҚР Қылмыстық Кодексі 1997 жыл 16 шілде №167..

20 Бойков АД. Что же мешает защите?//Литературная газета. 1970г.-

Нурмуханов Ж.Б.

*Казахского национального университета имени аль-Фараби,
Республика Казахстан, г. Алматы*

НЕКОТОРЫЕ ВОПРОСЫ САМОУБИЙСТВА

Жизнь человека является существенным благом, и к ее сохранению человек не может относиться безразлично. Самоубийство - тот шаг, на который человек решается в особых экстремальных условиях, ставит себе целью умереть и совершает действия, прямо направленные на достижение этой цели. Для признания лишения себя жизни самоубийством в каждом конкретном случае необходимо установить факт совершения данным лицом действий, специально направленных на лишение себя жизни. К самоубийствам нельзя относить случаи причинения себе смерти лицом по своей неосторожности.

Это прежде всего, относится к случаям, когда лицо по обстоятельствам должно было и могло предвидеть наступление своей смерти. Также не являются самоубийствами случаи, когда лицо предвидит возможное наступление своей смерти, но надеется остаться в живых, например, случаи бравирования смелостью. Случаи, когда лицо предвидит возможные результаты своих действий, но безразлично относится к ним. к самоубийству не приемлемы (конструкция косвенного умысла). В любом случае, если лицо, совершая какие-либо саморазрушающие действия, подразумевает остаться в живых, самоубийства нет.

Объект самоубийства как существенное благо и интерес составляет жизнь человека.

Интересным обстоятельством является совпадение в одном человеке элементов и потерпевшего (в широком понимании слова), и субъекта самоубийства. То есть субъект самоубийства посредством деяния, направленного на лишение себя жизни, достигает поставленной цели -собственной смерти и тем самым становится потерпевшим.

Объективная сторона самоубийства - деяние (действия, бездействие совершаемое субъектом самоубийства и преследующее цель достижения последним собственной смерти. Большинство случаев самоубийства представлены объективной стороной в форме действий, то есть волевых, активных поведенческих актов человека. В качестве примера можно привести тривиальный случай повешенья.

Меньшее количество самоубийств совершается путем бездействия, а именно волевого, пассивного поведения человека, заключающегося в невыполнении действий, которое лицо могло и должно было совершить для сохранения и поддержания собственной жизни. Например, замерзание, смерть вследствие голодания и так далее.

Обязательным является наличие причинной связи между деянием и наступившим последствием - смертью лица. Время, место, способ, орудия и средства совершения самоубийства имеют важное значение и выступают основными объективными признаками, ибо иногда только на их анализе можно сделать вывод о том, что в действительности имело место - самоубийство или нет.

Анализ самоубийства как деяния с уголовно-правовых позиций позволил выделить следующие субъективные признаки:

Субъективную сторону представляет прямой умысел. Мы полностью исключаем косвенный умысел, а также неосторожность в форме легкомыслия или небрежности.

При совершении самоубийства лицо предвидит возможность или неизбежность наступления своей смерти и желает ее наступления. Поэтому нужно сразу исключить косвенный умысел, когда лицо только предвидит возможность наступления смерти в ходе своих действий, никак не неизбежность таковой. Прямым умыслом предполагается предвидение неизбежности и

возможности наступления смерти, а косвенным - только возможность наступления смерти. Вероятность предвидения при прямом умысле выше, чем при косвенном. Предвидение наступления смерти выражается в мысленных оставлениях лица, которые могут наступить в результате его деяния. Предвидение возможных последствий и развития причинных связей их возникновения и наступления обычно осуществляется на интуитивном, бытовом уровне. Тем не менее, при совершении самоубийства лицу не требуется полного осознания всех деталей механизма причинной связи.

Характерный для самоубийства прямой умысел предполагает наличие желания лица в наступлении смерти посредством совершаемого им деяния, тогда как при косвенном умысле лицо прямо не желает наступления своей смерти, хотя осознанно и допускает ее или безразлично относится к ее наступлению. Обстоятельство прямого нежелания, безразличного отношения к смерти сразу исключают данную форму умысла при самоубийстве.

При самоубийстве следует установить волевые моменты деяния лица, также обязательны мотив и цель. Воля без мотива и цели не реализуема. Только на основании установления реальных мотивов и целей деяния лица можно констатировать самоубийство. Наступление собственной смерти лица посредством его деяния обязательно должно выступать конечной целью такого деяния. Наступление вредных последствий, то есть смерти, при самоубийстве выступает целью в действиях лица. Это очень важный момент при разграничении самоубийств с несчастными случаями, повлекшими смерть. Очень сложным моментом является выявление истинных целей деяния лица, установление соотношения между целью «смерть» и другими целями, лежащими в основе деяния самоубийцы. К примеру, является ли самоубийством самопожертвование собой ради спасения жизней других в бою? Анализ целевых установок лица, которые, прежде всего, определены не достижением собственной смерти, а спасением через наступление собственной смерти жизней других лиц, позволяет отграничить подобное деяние от самоубийства в юридическом видении проблемы.

Волевой момент составляет прямое желание лица в наступлении своей смерти. Для признания деяния самоубийством необходимо установить факт совершения самоубийцей действий, специально направленных на лишение себя жизни.

Мотивами самоубийств выступают побудительные причины, толкнувшие лицо на совершение суицида. Следует отметить, что мотивы самоубийств очень разнообразны, но в каждом конкретном случае важно установить мотивы, побудившие лицо к самоубийству. Если у лица не было причин для самоубийства, то могут иметь место несчастный случай, убийство и так далее, но только не самоубийство в своем юридическом понимании. Подробная классификация мотивов и поводов к самоубийствам мужчин, осужденных к лишению свободы, будет проведена во второй главе настоящего исследования.

А.Г. Амбрумова, С.В. Бородин, А.С. Михлин приводят следующие мотивы самоубийств: семейные конфликты, развод, болезнь, смерть близких, одиночество, неудачная любовь, оскорбление со стороны окружающих, половая несостоятельность, психические заболевания, соматические заболевания, уродство, опасение уголовной ответственности, боязнь наказания или позора, конфликты на работе, неуспехи в учебе, материально-бытовые трудности и прочие [1].

Представляется, что умысел должен быть определенным или конкретизированным. При этом содержание прямого умысла, то есть предвидение и неизбежность собственной смерти, а также желание ее наступления должны быть конкретно определены. Однако самоубийца тоже четко и не должен осознавать все механизмы причинной связи между возникновением и наступлением вредных последствий, то есть собственной смерти.

Субъектом самоубийства, может выступать физическое вменяемое лицо и действовавшее при лишении себя жизни сознательно.

В действительности, возраст уголовной ответственности лиц, устанавливаемый статьей 15 УК РК, может иметь расхождения с возрастом субъекта самоубийства, определяемого психологическими методиками. Критерием в последних выступает

интеллектуальная возможность лица осознавать фактический характер совершаемого деяния и его последствий. Осознание лицом собственной смерти в возрастном диапазоне наступает у лица значительно раньше, нежели осознание общественной опасности даже квалифицированных составов убийства, что вполне понятно.

Вменяемость подразумевает такое психическое состояние лица, которое заключается в его способности по состоянию здоровья, уровню социально-психического развития и социализации, а также по возрасту осознавать фактический характер своего деяния или руководить им в момент совершения самоубийства. Сюда же относится ряд лиц, имеющих психические аномалии, которые в определенной степени оказывают свое влияние на осознанное поведение человека, а также лица с элементами умственной отсталости, степень которой позволяет лицу осознавать характер совершаемых действий и адекватно руководить

На наш взгляд нужно исключить из числа самоубийств в юридическом понимании все случаи самоубийств душевнобольных лиц, находящихся в состоянии невменяемости. С юридических позиций факт причинения себе смерти лицом, находящимся в состоянии невменяемости, не может быть расценен как самоубийство. Это несчастный случай, случайное стечение обстоятельств, но никак не самоубийство в правовом понимании, так как лицо не может осознавать фактический характер своих действий или не может ставить перед собой цели - собственную смерть направленно, по собственной воле, следовать ее достижению.

В любом случае прерогатива решения вопроса о степени психической нормальности лица, о медицинской составляющей понятия невменяемости принадлежит врачам.

Список использованных источников

1 Амбрумова А.Г., Бородин С.В., Михлин А.С. Предупреждение самоубийств. - М., 1980. - 164 с.

СООТНОШЕНИЕ ЗАЩИТЫ КОММЕРЧЕСКОЙ ТАЙНЫ И ПЕРСОНАЛЬНЫХ ДАННЫХ В СПОРАХ ОБ ИСПОЛЬЗОВАНИИ КЛИЕНТСКИХ БАЗ

Клиентская база становится предметом спора не только при ее копировании конкурентом. Конфликт возникает и тогда, когда клиент просит показать сведения о нем, а организация ссылается на коммерческую тайну, либо когда компания разрешает партнеру использовать базу, не выяснив, допускается ли передача данных граждан. Во всех этих случаях речь идет об одном информационном ресурсе, но о разных правах. Поэтому вопрос «кому принадлежит база?» недостаточен. Важно установить, кто предъявляет требование, что именно он хочет получить или прекратить и на каком основании.

Здесь полезно принятое в гражданском праве разграничение способов защиты. В частности, правовой результат определяется характером защищаемого права, а не одним названием процедуры [1]. Применительно к клиентским данным это означает, что запрет конкуренту использовать закрытую информацию и обязанность ответить клиенту о его собственных сведениях могут действовать одновременно. Один результат не отменяет другой. Для теории это пример сосуществования имущественного интереса и личного неимущественного права, а для практики - основание не соединять все требования в неопределенную просьбу «защитить базу».

В данном случае цель нашего исследования - объяснить, как согласовать эти права при доступе к базе, ее передаче и прекращении использования. Сопоставляются конкретные нормы и опубликованные дела, отдельно оцениваются доктринальные позиции и авторские предложения. Исторические эпизоды рассматриваются в пределах примененного тогда регулирования. Не каждая клиентская база является большими данными (Big Data). Для настоящей темы важны прежде всего объединение источников,

создание производных характеристик человека и передача результатов нескольким получателям, при которых границы прав особенно легко потерять из виду.

Начать следует с того, какой интерес защищает компания. Пункт 1 статьи 126 ГК РК требует коммерческой ценности вследствие неизвестности сведений другим лицам, отсутствия свободного законного доступа и мер конфиденциальности. Пункт 1 статьи 1017 Особенной части обращен к правомерному обладателю информации [2; 3]. Следовательно, наличие расходов на сбор клиентов не дает самостоятельного права распоряжаться любыми сведениями о них. Также нельзя признать секретным весь ресурс лишь потому, что отдельная его часть отвечает условиям охраны.

Для гражданина вопрос иной. Пункты 1-2 статьи 11 Закона «О персональных данных и их защите» устанавливают конфиденциальность сведений ограниченного доступа независимо от того, доказала ли организация собственную коммерческую тайну. Пункт 1 статьи 24 закрепляет самостоятельные права субъекта [4]. Это важно при отказе в иске компании, поскольку отсутствие у нее достаточных оснований для защиты тайны не превращает личные сведения клиентов в свободно распространяемый материал. Равным образом признание коммерческой тайны не устраняет требований граждан.

Оба интереса не всегда противоречат друг другу. Дж. Мальджери отмечает общую заинтересованность компании и человека в сохранении конфиденциальности, целостности и правильности информации, одновременно показывая возможное расхождение при доступе и прекращении обработки [5]. Работа подготовлена в период обсуждения европейских реформ и используется как доктринальная постановка, а не описание всех действующих норм. Ее полезность в том, что спор нельзя заранее представить как неизбежный выбор одной стороны. Сначала надо установить, где требования совместимы и в чем именно возникает конфликт.

В ранних наших исследованиях вопрос о пределах тайны ставился через соотношение коммерчески закрытой информации и права потребителя на информацию о товаре, работе или услуге [6].

Применительно к клиентским базам задача отличается. Здесь лицо запрашивает не сведения о товаре вообще, а информацию о себе. Однако сам способ рассуждения сохраняет значение. Прежде чем ограничить доступ, необходимо назвать защищаемую тайну и определить содержание встречного права. Общей ссылки на интерес бизнеса недостаточно, но и право на информацию не означает раскрытия всего информационного хозяйства компании.

Ф. Бантерле в исследовании клиентских списков и данных профилирования отдельно ставит вопросы допустимости коммерческой обработки и возможной охраны результата средствами интеллектуальной собственности [7]. Для рассматриваемого спора это два самостоятельных основания. Лицо может подтвердить свое право на закрытую структуру базы, но не показать основание для передачи клиентских записей новому получателю. И наоборот, наличие правомерно полученных сведений о клиентах еще не доказывает право запретить другому участнику независимо собрать те же открытые факты.

Международную основу разграничения дает пункт 2 статьи 39 Соглашения ТРИПС. Он обеспечивает защиту законно контролируемой нераскрытой информации от получения, раскрытия и использования вопреки честной коммерческой практике. Подпункты «а»-«с» связывают охрану с секретностью, обусловленной ею ценностью и разумными защитными мерами [8]. Это основание защиты от другого участника оборота, а не разрешение собирать любые сведения о гражданах. Следовательно, право препятствовать неправомерному использованию массива нужно отличать от собственного права предпринимателя совершать определенные операции с его содержанием.

Практическое решение состоит не в разделении базы на доли собственности между компанией и гражданами. Предлагается описывать права через разрешенные действия. Организация обосновывает, какую непубличную информацию она вправе защищать от чужого использования. Клиент указывает относящиеся к нему сведения и то действие, законность которого проверяется. Получатель массива подтверждает основание своего доступа и последующей обработки. Так устраняется ложный вывод, будто

один участник должен получить все права, чтобы остальные могли защитить хотя бы часть своих интересов.

Следующая проблема возникает при изменении назначения клиентских данных. Х. Ниссенбаум связывает защиту приватности с контекстом получения и распространения информации [9]. Для правового анализа это помогает поставить понятный вопрос - соответствует ли новая передача тому отношению, в котором сведения были получены? Само ожидание клиента не заменяет закон. Но и согласие сообщить данные для определенной услуги не следует без проверки превращать в разрешение на любое последующее коммерческое применение.

В Казахстане исходную проверку задают пункт 1 статьи 7 и статья 9 Закона о персональных данных. Согласие либо предусмотренное законом основание его отсутствия. Пункты 8-9 статьи 7 ограничивают цель и объем обработки, пункт 6 отдельно регулирует передачу третьим лицам [4]. Название договора между компаниями не восполняет эту проверку. Продажа доступа, лицензия, партнерская программа и соглашение о конфиденциальности могут определять отношения контрагентов, но сами по себе не показывают допустимость каждого действия с данными клиентов.

Хорошо видно это различие в европейском споре KNLTB. Регламент 2016/679 допускает обработку на основании законного интереса при совокупности условий статьи 6(1)(f) [10]. В деле C-621/22 Суд ЕС 4 октября 2024 года рассматривал передачу теннисной федерацией сведений о членах двум спонсорам за вознаграждение. Пункты 37-57 допускают коммерческий интерес как возможный законный интерес, но требуют необходимости обработки и оценки прав субъектов. Суд указал также на возможность предварительно выяснить желание участников получать предложения. Это предварительное толкование, а не окончательное разрешение национального спора о штрафе [11].

Из дела не следует ни запрет любых коммерческих целей, ни разрешение продавать клиентские контакты только потому, что они ценны. Для Казахстана европейское основание нельзя применять вместо статей 7 и 9 национального Закона. Сравнительный вывод

сводится к тому, что экономический интерес необходимо отделять от юридического основания конкретной операции. Сам Суд в этом деле не признавал сведения коммерческой тайной. Поэтому решение используется для проверки пределов коммерческого использования, а не как доказательство секретности определенной базы.

Не менее частый конфликт связан с ответом самому клиенту. Организация опасается показать внутреннюю систему оценок, условия работы с другими клиентами или способы расчета. Но из этой опасности не следует право скрыть всю информацию о заявителе. Нужно отделить содержание его записи от посторонних записей и от технического устройства системы. Задача состоит в достаточности ответа для осуществления права, а не в передаче ресурса, пригодного для самостоятельной коммерческой эксплуатации другим лицом.

В деле C-487/21 CRIF, решение от 4 мая 2023 года, лицо просило сведения о себе и копии содержащих их документов, а компания предоставила сводный перечень. Суд ЕС разъяснил, что статья 15(3) GDPR требует точного и понятного воспроизведения обрабатываемых персональных данных. Фрагменты документов и базы, а при необходимости целые документы, предоставляются, когда без них право нельзя эффективно осуществить. Ограничение статьи 15(4), включая коммерческую тайну, требует согласования интересов и выбора защищенного способа передачи, но не полного отказа в информации [12].

Правовой смысл такого подхода прост. Человек должен понять, какие сведения о нем использованы, а не получить только названия категорий. Одновременно ответ не должен раскрывать данные остальных клиентов. Для казахстанской практики предлагается сначала выделять относящийся к заявителю материал, затем проверять, понятен ли он без исключенных частей. Если в ответе остается только необъясненный код, формальное удаление чужих сведений еще не делает ответ достаточным. Если же запись понятна без соседних строк, оснований выдавать весь массив не возникает.

В действующем казахстанском Законе подпункт 1) пункта 1 статьи 24 уже предусматривает информацию о наличии, целях,

источниках, способах и сроках обработки. Подпункты 6)-7) пункта 2 статьи 25 требуют предоставить относящиеся к субъекту данные либо мотивированный отказ [4]. Поэтому создавать заново общую обязанность отвечать не нужно. Уточнения требует способ ответа при пересечении режимов: компания должна объяснить, какую часть не раскрывает, почему и каким способом можно предоставить положенную человеку информацию без избыточного раскрытия.

Для производной клиентской оценки важно не путать результат и способ его получения. Подпункт 2) пункта 4 статьи 43 Цифрового кодекса предусматривает в установленных законодательством случаях и порядке объяснение ключевых факторов полностью автоматизированного решения без раскрытия алгоритмов, исходного кода и охраняемой тайны [13]. Следовательно, не требуется выбирать между раскрытием всей программы и полным молчанием. Следует показать относящиеся к конкретному решению факторы в пределах установленного права. Изготовление компанией новой оценки не превращает ее автоматически в сведения, никак не относящиеся к оцененному человеку.

При этом доступ к своей информации не дает права потребовать любой предпочитаемый результат. Для требования об исправлении необходимо установить, что неверно: исходная запись, отнесение записи к человеку или использование уже исправленных сведений. Несогласие с прогнозом само по себе еще не доказывает фактической ошибки. Предлагается разделять исправление документально проверяемого факта и пересмотр решения на достоверных данных. Это сохраняет право клиента на проверку и не подменяет его правом самостоятельно назначить себе коммерческую оценку.

Теперь необходимо рассмотреть менее заметную, но важную проблему: может ли разрешение обладателя тайны легализовать использование сведений, которые первоначально попали к приобретателю без надлежащего основания? Для клиентской базы ответ касается не только двух компаний. Соглашение между ними может устранить спор о коммерческом использовании информации, однако права людей, чьи данные входят в базу, требуют отдельной

оценки. Именно здесь гражданско-правовой инструмент легко применить шире его назначения.

П. Самуэльсон критически оценивает идею свободно отчуждаемых прав собственности на персональную информацию и предлагает исследовать отдельные правила лицензирования и добросовестного обращения с тайной [14]. Полезна не замена личного права торговым титулом, а возможность точно ограничить цели и круг получателей. Лицензирование помогает договориться об использовании, но не должно превращаться в способ отказаться от чужих прав. Поэтому для клиентской базы важно определить, какие ограничения следуют из соглашения, а какие продолжают действовать независимо от воли его сторон.

Статья 1018 ГК РК содержит специальное решение. Пункт 2 связывает последствия для добросовестного приобретателя с получением им знания о незаконности использования. По пункту 3 суд, учитывая затраты такого приобретателя, может разрешить дальнейшее использование на условиях возмездной исключительной лицензии [3]. Однако этот способ разрешения спора относится к нераскрытой информации и отношениям с ее правомерным обладателем. Из него не следует, что суд разрешает любые действия со всеми категориями сведений внутри базы.

Предлагаемое толкование состоит в самостоятельной проверке личных прав. Если требуемое использование включает персональные данные, основание по профильному Закону должно быть установлено независимо от лицензионного разрешения. Уплата вознаграждения компании возмещает или согласует ее имущественный интерес, но не выражает волю клиентов. Это не означает запрета лицензировать смешанные массивы вообще. Возможно правомерное использование разрешенной части или иное допустимое предоставление, но состав и назначение такой части должны быть определены, а не предполагаться автоматически.

Правовой опорой служит и пункт 3 статьи 270 ГК, в котором обязательство не создает обязанностей для третьих лиц [2]. Договор между владельцем клиентской базы и приобретателем не может сам по себе обязать гражданина терпеть обработку, на которую у сторон нет основания. Для практики это означает необходимость

раздельных документов и объяснений: одно подтверждает отношения с обладателем тайны, другое - правомерность обращения с персональной составляющей. Они могут содержаться в общем комплекте, но должны отвечать на разные вопросы.

Чтобы исключить расширительное прочтение, предлагается дополнить пункт 3 статьи 1018 ГК предложением: «Разрешение дальнейшего использования нераскрытой информации, содержащей персональные данные, не заменяет правового основания их обработки и не ограничивает права субъектов персональных данных, предусмотренные законами Республики Казахстан». Это авторское предложение уточняет предел уже существующего исключения для добросовестного приобретателя и не вводит новую лицензию на персональные данные.

Зачем нужна такая оговорка, если профильный Закон уже действует? Она делает предел судебного разрешения видимым в той норме, на которую ссылается приобретатель. Суду легче отделить допустимое продолжение использования коммерческой информации от операций, нарушающих права клиентов. Получатель заранее понимает, что оплата лицензии не решает второй вопрос. Для теории это сохраняет различие имущественного разрешения и личного права, а для законодательства - согласует два существующих режима без создания общей собственности на сведения.

Предложение не основано на утверждении, будто казахстанские суды уже систематически обходят защиту клиентов через статью 1018. Подтвержденная подборка таких решений не установлена. Основание предложения иное, а именно в том, что совместное прочтение норм выявляет ситуацию, в которой предел специального разрешения нуждается в ясном объяснении. Доктринальное уточнение и доказанный массовый недостаток правоприменения - разные результаты исследования. Смешивать их для усиления аргумента нельзя.

М. Риш исследует причины защиты тайны на фоне свободы доступа к знаниям и отсутствия авторско-правовой охраны самих фактов [15]. Для настоящего вопроса это дополнительное ограничение. Договор о базе не должен создавать запрет на все

сведения о клиентах независимо от источника. Пункт 4 статьи 1018 ГК допускает самостоятельное правомерное получение тех же сведений [3]. Но независимость от обладателя тайны не означает независимости от субъекта персональных данных. Получатель должен подтвердить законность собственного способа сбора, а не только отсутствие копирования чужой базы.

При смене владельца бизнеса конфликт принимает другую форму. Покупателю важно сохранить клиентские отношения, однако условия передачи могут затронуть сведения, полученные для прежнего ограниченного назначения. Здесь особенно опасно считать включение базы в перечень активов достаточным основанием ее дальнейшего использования. Предмет сделки и правомерный объем передаваемой информации нужно определять одновременно. Иначе цена приобретенного бизнеса начинает ошибочно восприниматься как цена снятия всех ограничений на данные.

В официальном сообщении Генерального прокурора Техаса от 20 мая 2015 года об урегулировании RadioShack описано соглашение, достигнутое после медиации при продаже активов. Определенные категории клиентских сведений исключены из передачи, большая часть данных подлежала уничтожению, а новый получатель сохранял обязательства по прежней политике приватности. Для части электронных адресов установлены условия сохранения, дальнейшая продажа и передача ограничены [16]. Это содержание конкретного соглашения, а не универсальное судебное правило о банкротстве и не решение о признании всей базы коммерческой тайной.

Сравнительный вывод состоит в том, что сохранение хозяйственной ценности и ограничение состава передаваемых данных могут рассматриваться вместе. Для Казахстана из этого не следует переносить все условия американского соглашения или установленный там срок. Необходимо определить, какие данные нужны для правомерного продолжения отношений, какое основание относится к каждой операции и какие ограничения сохраняются у получателя. Клиентскую базу нельзя описывать только числом

записей, если разные части имеют разные условия дальнейшего использования.

Отдельной проверки требует сохранение информации после окончания договора. Пункт 2 статьи 1019 ГК допускает сохранение обязанности конфиденциальности после прекращения лицензии, если сведения остаются нераскрытыми и договором не предусмотрено иное [3]. Эта обязанность отвечает на вопрос, можно ли разгласить то, что стало известно. Она не является самостоятельным разрешением бесечно хранить все персональные записи. Продолжение хранения должно иметь основание по законодательству о данных, независимо от того, выгодно ли компании оставить ресурс закрытым.

Вопрос об отзыве согласия нельзя решать без предусмотренных законом ограничений. Пункт 2 статьи 8 Закона о персональных данных учитывает противоречие закону и неисполненное обязательство. Пункт 7 предусматривает прекращение обработки в течение пятнадцати рабочих дней, если она не требуется по законодательству, либо мотивированный отказ [4]. Поэтому неверны обе крайности - немедленно удалить все по любому требованию или сохранить весь массив под предлогом коммерческой тайны. Следует указать конкретное основание, состав остающихся сведений и допустимые операции.

Предлагается разграничивать обязанность сохранить определенный документ и возможность использовать его для новых деловых целей. Сохранение для исполнения закона или конкретного обязательства не должно без проверки превращаться в продолжение рекламного профилирования. Практическое решение - ограничить дальнейшие действия тем назначением, ради которого сведения остаются. Это не новая универсальная обязанность создать особую архивную систему, а способ объяснить предел уже существующего основания хранения.

Т. Фиа показывает риск чрезмерного расширения охраны при применении коммерческой тайны к неперсональным массивам [17]. Его исследование не разрешает напрямую спор о персональных данных, но помогает понять более узкую проблему, которая состоит в том, что сохранение тайны не должно превращаться в право

навсегда исключить любые иные притязания к ресурсу. В клиентской базе такое ограничение необходимо проверять и со стороны гражданина, и со стороны компании. Обезличивание одной части не доказывает свободу использования всех остальных записей, как и прекращение персонального режима не создает тайну автоматически.

Н. Пуртова и Г. ван Маанен критикуют попытку решать все задачи управления данными через их экономические характеристики [18]. В рассматриваемом споре этот аргумент имеет практическое значение, поскольку доказывает, что стоимость базы не показывает, какие операции с ней законны. Предлагается оценивать не один суммарный актив, а сохраняемую функцию каждой спорной части. Компания может объяснить ценность результата анализа, но ей все равно необходимо подтвердить допустимость использования связанных с ним записей о конкретных людях.

После утечки интересы компании и клиентов могут нарушаться одновременно, но требования остаются самостоятельными. В официальном сообщении о проверке ТОО «МФО Робокэш.кз» зафиксированы обнаружение утечки 5 марта 2024 года, административное реагирование и уведомление граждан [19]. В нем нет вывода о доказанном режиме коммерческой тайны всей базы, взыскании убытков компании или присуждении компенсации каждому клиенту. Источник позволяет изучать опубликованный результат проверки, но не дополнять его отсутствующей судебной мотивировкой.

Из такого эпизода для нашей темы следует необходимость двух самостоятельных объяснений. Компания, требующая возместить утрату коммерческого преимущества, показывает свой охраняемый интерес и относящиеся к нему потери. Гражданин обосновывает нарушение личного права и заявленное последствие. Они могут использовать часть общих фактов инцидента, но не подменять друг друга. Выплата компании не является выплатой клиентам, а размер базы не дает готовой формулы расчета индивидуального вреда.

Пункты 1 и 4 статьи 9 ГК различают пресечение нарушения и денежные требования, причем юридическое лицо не обладает

правом на возмещение морального вреда [2]. Поэтому в соглашении компаний необходимо точно указывать, чьи потери урегулированы. Оно не должно обозначать прекращение всех требований по инциденту, если права граждан не являются предметом правомерного представительства и самостоятельного разрешения. В то же время одна и та же потеря одного заявителя не подлежит повторному взысканию под разными названиями только из-за пересечения режимов.

Положительный для компании исход спора о тайне также не доказывает, что она исполнила все обязанности перед клиентами. Владелец базы может защищаться от неправомерного копирования и одновременно обязан отвечать на требования о собственных нарушениях обработки. Эти роли следует оценивать отдельно. Иначе признание компании потерпевшей от чужого действия превращается в необоснованное освобождение от ее обязанностей, а обнаружение нарушения у компании - в столь же необоснованное разрешение конкуренту использовать любой ее ресурс.

Для обычной работы предлагается закрепить порядок, при котором запрос клиента рассматривается по частям. Сначала определяется, какие сведения относятся к заявителю и какое право он осуществляет. Затем устанавливается, что необходимо исключить для защиты других лиц и действительно охраняемой информации. Наконец проверяется, позволяет ли оставшаяся часть понять ответ и воспользоваться правом. Такой порядок не требует раскрывать весь массив и не допускает закрывать все сведения одной отметкой о тайне.

В правилах предоставления информации можно использовать следующую формулировку: «Наличие в клиентской базе коммерческой тайны не является само по себе основанием для отказа субъекту в сведениях, предоставление которых предусмотрено законом. При ограничении объема ответа указываются его правовое основание и причины невозможности предоставить соответствующую часть. Сведения, доступ к которым не ограничен, предоставляются в понятной форме, позволяющей осуществить право без раскрытия избыточной информации о других

лицах». Это авторское предложение для конкретизации исполнения действующих статей 24-25 Закона, а не создание нового безусловного права на копию всей базы.

Польза этой формулировки в том, что спор становится проверяемым. Компания должна обосновать конкретное ограничение, а клиент понимает, какая часть ответа отсутствует и почему. Проверяющий орган или суд может сопоставить причину отказа с требуемыми сведениями. Для практики это уменьшает число формальных ответов, для законодательства - уточняет исполнение уже предоставленного права, для теории - сохраняет различие права на собственную информацию и права доступа к чужому ресурсу.

В договоре о предоставлении клиентского массива предлагается отдельно закреплять следующее: «Разрешение использовать нераскрытую информацию действует только в пределах прав передающей стороны. Получатель самостоятельно соблюдает применимые основания и ограничения обработки персональных данных. Стороны обеспечивают передачу относящихся к их исполнению требований об исправлении, ограничении обработки и прекращении доступа. Распределение обязанностей между сторонами не ограничивает предусмотренные законом права субъектов данных». Условие подлежит согласованию с предметом договора и не заменяет необходимых согласий и иных правовых оснований.

Такое условие нужно не для возложения всех последствий на приобретателя. Его назначение - определить границу обещанного предоставления и порядок действий, когда основание обработки меняется. Передающая сторона должна сообщить известные ограничения и исполнить собственные обязанности. Получатель не вправе прикрываться лицензией от проверки своих операций. Ни одна из сторон не должна обещать, что гражданин никогда не воспользуется предоставленным ему законом правом.

Предлагаемый подход не требует нового вида собственности на клиентскую базу. Достаточно последовательно ответить, какой интерес охраняется, кто имеет соответствующее право, какая операция разрешена и какое последствие устраняет установленное

нарушение. При продаже, лицензировании, доступе и удалении ответы будут различаться. Это различие нужно сохранять в договоре, ответе на обращение и судебном требовании, а не заменять общим обозначением «конфиденциальный массив».

Итак, режим коммерческой тайны и защита персональных данных могут охранять один информационный ресурс, но не дают одному участнику права распоряжаться всеми интересами остальных. Компания защищает доказанно охраняемое содержание и вправе устанавливать законные условия его использования. Гражданин сохраняет права на относящиеся к нему данные. Основание, достаточное для отношений двух компаний, необходимо проверить отдельно в отношении человека, а объем раскрытия человеку - отдельно в отношении чужих записей и тайны.

Таким образом, было исследовано соотношение прав организации на коммерчески ценную клиентскую базу и самостоятельных прав граждан, сведения о которых включены в нее. Определены, как разрешать требования о доступе, передаче, прекращении использования и сохранении информации без подмены одного правового основания другим. При этом были применены формально-юридический и сравнительно-правовой методы, анализ доктрины и опубликованных материалов практики. На основе сопоставления статьи 126, 270, 1017-1019 Гражданского кодекса Республики Казахстан, законодательство о персональных данных и статья 43 Цифрового кодекса, на материале решений Суда Европейского союза C-621/22 и C-487/21, урегулирования дела RadioShack и сообщения о проверке «Робокэш.кз» раскрыты пределы коммерческого использования и конфиденциальности. Обосновано, что согласие обладателя тайны или предоставленная добросовестному приобретателю лицензия не заменяют правового основания обработки данных клиентов. В свою очередь, право гражданина получить относящиеся к нему сведения не означает право на всю базу. В этой связи предлагаются уточнение пункта 3 статьи 1018 ГК, порядок мотивированного частичного предоставления информации и договорное условие о сохранении самостоятельных прав субъектов данных.

Главный результат исследования - понятная граница между имущественным разрешением и правомерностью обработки. Предложенное уточнение статьи 1018 исключает восприятие судебной лицензии как замены основания работы с персональными данными. Частичное мотивированное предоставление сведений позволяет совместить право клиента на информацию с охраной действительно закрытой части. Договорное условие сохраняет самостоятельность требований третьих лиц. Эти решения нужны не для увеличения количества формальностей, а для того, чтобы каждый участник заранее понимал предел своего права и способ его защиты.

Финансирование. Исследование подготовлено в рамках проекта ИРН AP23489796 «Проблемы регламентации правового режима больших данных (Big Data): отечественный и международный опыт», финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан.

Список использованных источников

1 Сулейменов, М. К. Понятие и способы защиты гражданских прав [Электронный ресурс] / М. К. Сулейменов // Параграф. - 2014. - 16 июня. - URL: https://prg.kz/document/?doc_id=33100058 (дата обращения: 05.05.2026).

2 Гражданский кодекс Республики Казахстан (Общая часть) : Кодекс Республики Казахстан от 27 декабря 1994 г. № 268-ХІІІ // Ведомости Верховного Совета Республики Казахстан. - 1994. - № 23–24 (приложение). - Электронная версия: ИПС «Әділет». - URL: <https://old.adilet.zan.kz/rus/docs/K940001000> (дата обращения: 07.05.2026).

3 Гражданский кодекс Республики Казахстан (Особенная часть) : Кодекс Республики Казахстан от 1 июля 1999 г. № 409 // Ведомости Парламента Республики Казахстан. - 1999. - № 16–17. - Ст. 642. - Электронная версия: ИПС «Әділет». - URL: <https://old.adilet.zan.kz/rus/docs/K990000409> (дата обращения: 10.05.2026).

4 О персональных данных и их защите : Закон Республики Казахстан от 21 мая 2013 г. № 94-V // Ведомости Парламента Республики Казахстан. - 2013. - № 7. - Ст. 35. - Электронная версия: ИПС «Әділет». - URL: <https://old.adilet.zan.kz/rus/docs/Z1300000094> (дата обращения: 29.06.2026).

5 Malgieri, G. Quasi-Property in Consumer Information: Trade Secrets and Consumer Rights in the Age of Big Personal Data / G. Malgieri // Proceedings of the 7th International Conference on Information Law and Ethics, ICIL 2016: Broadening the Horizons of Information Law and Ethics: A Time for Inclusion / ed. by M. Bottis,

E. Alexandropoulou. - Thessaloniki: University of Macedonia Press, 2017. - P. 376–400. URL: https://icil.gr/download.php?fен=years/2016/downloads/speakers/0049-malgieri-full_text-en-v1.pdf (дата обращения: 12.05.2026).

6 Омарова, А. Б. Способы защиты интеллектуальных продуктов на рынке товаров, работ и услуг в Республике Казахстан / А. Б. Омарова // Вестник КазНУ. Серия юридическая. - 2014. - № 2 (70). - С. 130–135. - URL: <https://bulletin-law.kaznu.kz/index.php/journal/en/article/download/245/242/483> (дата обращения: 15.05.2026).

7 Banterle, F. The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database sui generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis / F. Banterle // Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach? / ed. by M. Bakhoun, B. Conde Gallego, M.-O. Mackenrodt, G. Surblytė-Namavičienė. - Berlin ; Heidelberg: Springer, 2018. - P. 411–443. - DOI: 10.1007/978-3-662-57646-5_16. - URL: https://link.springer.com/chapter/10.1007/978-3-662-57646-5_16 (дата обращения: 18.05.2026).

8 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) [Электронный ресурс]: 15 April 1994 : Annex 1C to the Marrakesh Agreement Establishing the World Trade Organization // WTO Legal Texts / World Trade Organization. - 1994. - URL: https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm (дата обращения: 20.05.2026)

9 Nissenbaum, H. Privacy as Contextual Integrity / H. Nissenbaum // Washington Law Review. - 2004. - Vol.79, no.1. - P.119–158. URL: <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/> (дата обращения: 22.05.2026).

10 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. - 4 May. - P. 1–88. - URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (дата обращения: 25.05.2026).

11 Court of Justice of the European Union. Koninklijke Nederlandse Lawn Tennisbond v Autoriteit Persoonsgegevens [Электронный ресурс] : judgment of the Court of 4 October 2024, Case C-621/22. - ECLI:EU:C:2024:858. - URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0621> (дата обращения: 28.05.2026)

12 Court of Justice of the European Union. F.F. v Österreichische Datenschutzbehörde (CRIF) [Электронный ресурс] : judgment of the Court of 4 May 2023, Case C-487/21. - ECLI:EU:C:2023:369. - URL: <https://collab.dpa.gr/wp-content/uploads/2023/07/CJEU-C-487-21.pdf> (дата обращения: 31.05.2026).

13 Цифровой кодекс Республики Казахстан : Кодекс Республики Казахстан от 9 января 2026 г. № 255-VIII ЗРК // Казахстанская правда. - 2026. - 10 января. - № 5–6 (30634–30635). - Электронная версия: ИПС «Әділет». - URL: <https://old.adilet.zan.kz/rus/docs/K2600000255> (дата обращения: 03.06.2026).

14 Samuelson, P. Privacy as Intellectual Property? / P. Samuelson // Stanford Law Review. - 2000. - Vol. 52, no. 5. - P. 1125–1173. - DOI: 10.2307/1229511. URL: <https://www.law.berkeley.edu/center-article/privacy-as-intellectual-property/> (дата обращения: 06.06.2026).

15 Risch, M. Why Do We Have Trade Secrets? / M. Risch // Marquette Intellectual Property Law Review. - 2007. - Vol. 11, no. 1. - P. 1–76. URL: <https://scholarship.law.marquette.edu/iplr/vol11/iss1/1/> (дата обращения: 09.06.2026).

16 Office of the Attorney General of Texas. Attorney General Paxton Announces Agreement to Protect Consumer Privacy in RadioShack Case [Электронный ресурс]. - 2015. - 20 May. - Официальное сообщение об урегулировании спора после медиации. URL: <https://www.texasattorneygeneral.gov/news/releases/attorney-general-paxton-announces-agreement-protect-consumer-privacy-radioshack-case> (дата обращения: 12.06.2026).

17 Fia, T. Resisting IP Overexpansion: The Case of Trade Secret Protection of Non-Personal Data / T. Fia // IIC - International Review of Intellectual Property and Competition Law. - 2022. - Vol. 53, no. 6. - P. 917–949. - DOI: 10.1007/s40319-022-01204-8. URL: <https://link.springer.com/article/10.1007/s40319-022-01204-8> (дата обращения: 15.06.2026).

18 Purtova, N. Data as an economic good, data as a commons, and data governance [Электронный ресурс] / N. Purtova, G. van Maanen // arXiv. - 2023. - 18 April. - Version 2. - 57 p. - arXiv:2212.10244v2. - DOI: 10.48550/arXiv.2212.10244. URL: <https://arxiv.org/abs/2212.10244v2> (дата обращения: 19.06.2026).

19 Минцифры объявило результаты проверки в отношении ТОО «МФО Робокэш.кз» [Электронный ресурс] / Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан // Gov.kz. - [2024]. - Официальное сообщение. - Номер публикации: 740137. URL: <https://www.gov.kz/memleket/entities/maidd/press/news/details/740137?lang=ru> (дата обращения: 23.06.2026).

Омарова А.Б.

*Кандидат юридических наук, профессор
Школы прав и государственного управления
НАО «Университет Нархоз»*

ДОКАЗЫВАНИЕ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ ПРИ ЗАЩИТЕ МАССИВОВ ЦИФРОВЫХ ДАННЫХ

Проблема защиты коммерческой тайны может обнаружиться тогда, когда информация уже вышла из-под контроля компании. В интервью, опубликованном Ratel.kz 9 сентября 2025 года, эксперт

по корпоративной безопасности Игорь Чернов описал расследование в отношении сотрудника, который перешел к другому работодателю и забрал прежнюю базу данных, цифровой массив данных. По словам эксперта, обязательство о неразглашении было подписано, но компания не смогла подтвердить, что содержание базы составляло коммерческую тайну [1]. Номер дела и судебный акт не приведены. Поэтому этот материал используется как опубликованное практическое наблюдение, а не как установленная судом позиция.

Из описанного эпизода возникает конкретный вопрос - что должна доказать организация помимо самого копирования файла? Недостаточно показать, что база находилась на ее сервере и была полезна для бизнеса. Нужно установить, какие сведения охранялись, почему их неизвестность другим лицам имела коммерческое значение и как компания сохраняла конфиденциальность. Только после этого можно оценивать, нарушил ли ответчик соответствующее право. Иначе спор о тайне превращается в спор о любой информации, которую работодатель считает своей.

Для решения этого вопроса полезно различие между охраной и защитой гражданских прав. Охрана охватывает условия нормального осуществления права, включая организационные меры, а защита связана с его признанием, восстановлением и пресечением нарушения [2]. Применительно к цифровому массиву это означает, что порядок работы с информацией создается до спора, а после нарушения суд проверяет, существовал ли этот порядок и к каким сведениям он относился. Подготовка убедительного иска не заменяет мер, которые ранее не принимались.

Цель настоящего исследования - предложить понятный способ подтверждения коммерческой тайны в изменяемом массиве. В работе сопоставляются конкретные нормы и опубликованные судебные решения, отдельно оцениваются договоры и фактические меры охраны. Нормативные источники проверены на 27 сентября 2026 года. Зарубежные дела используются для сравнения юридических подходов, а не как обязательные для Казахстана решения. На основе отдельных эпизодов не делается вывод о результативности всей национальной судебной практики.

Предлагаемые правила ниже обозначаются как авторские предложения.

Начать необходимо с условий возникновения защиты. Пункт 1 статьи 126 ГК РК связывает ее с тремя обстоятельствами: 1) коммерческой ценностью информации вследствие неизвестности третьим лицам, 2) отсутствием свободного доступа на законном основании и принятием мер конфиденциальности. Пункт 1 статьи 1017 Особенной части ГК дополнительно указывает на правомерное обладание информацией, а пункт 2 исключает обязательность регистрации, свидетельства и иных подобных формальностей [3, 4]. Следовательно, охрана возникает не потому, что компания назвала файл секретным, но и не только после получения официального документа.

Здесь важно избежать противоположных ошибок. Первая - считать внутренний приказ достаточным подтверждением всех условий. Приказ выражает решение организации, но не показывает, были ли сведения доступны конкурентам и работали ли ограничения доступа. Вторая - отказать в защите из-за отсутствия конкретного штампа, не исследовав остальные доказательства. Надпись помогает предупредить получателя, но ее доказательственное значение следует отличать от обязательного условия возникновения права.

В том же интервью эксперт рекомендует использовать именно обозначение «коммерческая тайна», а не слово «конфиденциально» [1]. Как совет по организации документооборота точная маркировка полезна. Однако общий вывод, что иная надпись сама по себе лишает информацию защиты, не вытекает из названных положений ГК. Практический смысл этого различия прост, а именно организация должна объяснить содержание ограничения и подтвердить его действие. Суду, в свою очередь, необходимо оценить все обстоятельства, а не заменить такую оценку проверкой одного слова на документе.

Следующий вопрос - можно ли защищать сочетание сведений, отдельные элементы которого известны другим лицам. Для больших данных он особенно важен, поскольку предметом использования становится не изолированная запись, а ее связь с

другими записями. Подпункт «а» пункта 2 статьи 39 Соглашения ТРИПС допускает оценку секретности точного сочетания и расположения компонентов. Подпункты «b» и «с» сохраняют требования коммерческой ценности вследствие секретности и разумных мер ее охраны. Аналогичный подход закреплен в подпунктах «а»-«с» пункта 1 статьи 2 Директивы ЕС 2016/943 [5, 6].

М. Риш рассматривает основания охраны тайны на фоне свободы доступа к знаниям и отсутствия авторско-правовой монополии на сами факты [7]. Для нашего вопроса это важное предостережение, поскольку затраты на сбор информации объясняют интерес компании, но не позволяют закрыть для всех каждый использованный факт. Охраняемое преимущество следует искать в конкретном неизвестном сочетании, методе организации или непубличном содержании, а не в общем утверждении, что создание базы стоило денег.

Поэтому предлагается описывать предмет охраны в два шага. Сначала указывать, какую часть массива компания считает конфиденциальной. Затем объяснять, что в этой части неизвестно другим участникам соответствующей деятельности и какую пользу дает ее закрытость. Для практики это позволяет отделить защищаемое содержание от обычных реквизитов, общих технических решений и опубликованных сведений. Для теории такое разграничение важно потому, что предметом защиты становится определенный информационный интерес, а не физическое владение носителем.

Право США также прямо допускает охрану информационных подборок, но связывает ее с разумными мерами сохранения тайны и экономической ценностью неизвестности - это подпункты «А» и «В» пункта 3 § 1839 раздела 18 Свода законов США [8]. Названная конструкция полезна для сравнения. Она не позволяет сделать вывод, что любой объемный набор записей является тайной. Формат хранения расширяет возможный круг объектов, а условия охраны ограничивают его.

В деле *InteliClear, LLC v. ETC Global Holdings, Inc.* от 15 октября 2020 года спор касался логики и структуры базы для учета операций с ценными бумагами. Апелляционный суд Девятого округа США

счел достаточно конкретными представленные описания таблиц, столбцов, идентификаторов и их взаимосвязей для продолжения разбирательства. Учитывались шифрование и договорная конфиденциальность. Отказ в иске без полного судебного разбирательства был отменен, в том числе из-за преждевременного завершения дела до раскрытия доказательств [9, с. 9-16, 21]. Суд не присудил убытки и не установил окончательно неправомерное использование.

Смысл этого решения не в освобождении истца от обязанности раскрыть предмет требования. Компания представила конкретизацию, а не предложила суду самостоятельно искать секреты внутри всей системы. Вместе с тем суд не потребовал окончательного доказательства каждого элемента спора до получения необходимых материалов. Для Казахстана такой подход полезен как ориентир соразмерности: описание должно позволять ответчику возражать и суду проверять условия охраны, но не превращаться в требование заранее доказать все обстоятельства, доступные только другой стороне.

У изменяемой базы появляется дополнительная трудность, которая состоит в том, что описание сегодняшней версии не показывает, что находилось в ней в момент передачи. Поэтому предлагается связывать защищаемое содержание с датой, периодом или зафиксированным состоянием массива. Не обязательно хранить полную отдельную копию после каждого обновления. Можно сохранять сведения о составе полей, правилах включения записей и изменениях, позволяющих восстановить относящееся к спору состояние. Выбор способа зависит от устройства системы и того, что именно составляет тайну.

Такой подход решает две задачи. Он не позволяет включить в иск сведения, появившиеся уже после предполагаемого нарушения. Одновременно он не требует переоформлять весь режим из-за обычного обновления записей в заранее определенных границах. Существенное изменение содержания, новых источников или круга получателей требует отдельной проверки. Однократное описание базы не должно превращаться в бессрочное признание секретным всего, что компания когда-либо добавит в систему.

После определения предмета нужно объяснить его коммерческое значение. Здесь проблема возникает из-за смешения расходов на создание ресурса и ценности его неизвестности. Счета за оборудование, оплату труда и программное обеспечение подтверждают расходы. Они не показывают автоматически, какое преимущество получает конкурент, узнав спорные сведения. Поэтому предлагается дополнять финансовые документы объяснением конкретной деловой функции закрытой информации: какое решение она позволяет принять, какие затраты избежать или какие условия деятельности узнать.

При этом не требуется доказывать уже совершенную продажу тайны. Закон допускает потенциальную коммерческую ценность [3, ст. 126, п. 1]. Но потенциал должен быть объяснен применительно к определенному содержанию, а не ко всему информационному хозяйству компании. Существенны документы о фактическом использовании массива, его роли в работе, допустимых получателях и ограничениях. Такая проверка нужна, чтобы не приравнивать ценность любого рабочего файла к ценности, обусловленной именно секретностью.

Следующий этап касается реальных мер охраны. Пункты 2-3 статьи 28 Предпринимательского кодекса РК предусматривают определение доступа и условий обращения с тайной самим предпринимателем. Подпункты 1)-3) пункта 4 перечисляют возможные меры: определение защищаемой информации, ограничение доступа и учет получателей. Закон использует слова «могут включать», а пункт 6 отдельно допускает требование подписки о неразглашении [10]. Следовательно, перед нами не закрытый обязательный комплект документов. Отсутствие одного элемента не освобождает от оценки того, как охрана была организована в действительности.

Для цифрового массива предлагается проверять связь каждой меры с конкретным риском. Список допущенных работников показывает установленный круг лиц, но сам по себе не подтверждает, что доступ остальных был закрыт. Договор с подрядчиком закрепляет обязанность, но еще не показывает, кому он мог передавать сведения. Журнал операций помогает

восстановить использование, однако не заменяет ограничения доступа. Эти документы следует рассматривать вместе: каждый отвечает на свой вопрос, и ни один не доказывает весь режим автоматически.

Разумность мер нельзя оценивать только по тому, произошла ли утечка. Иначе любой удавшийся обход защиты задним числом означал бы отсутствие самой тайны. С другой стороны, наличие дорогой системы безопасности не оправдывает фактическую передачу защищаемого содержания без ограничений. Предлагается выяснять, какие меры действовали до события, кому они были известны и насколько соответствовали способу работы с данным массивом. Новые правила, принятые после обнаружения нарушения, полезны для будущего, но не доказывают прежнее состояние.

Передача данных внешнему исполнителю делает этот вопрос особенно заметным. Ш. Сандин в исследовании облачного хранения показывает значение условий передачи третьему лицу и предлагает различать передачу информации и раскрытие, разрушающее секретность [11]. Это авторский анализ американского регулирования, а не запрет использовать облачные услуги. Для казахстанского договора вывод более узкий: необходимо установить, что именно передается исполнителю, кому доступно содержание и какие ограничения сохраняются. Местонахождение сервера само по себе не отвечает на эти вопросы.

Практическое решение состоит в согласовании технических и договорных границ. В документах стоит различать хранение, администрирование и разрешенное использование содержания. Компания должна иметь возможность подтвердить, что техническое обслуживание не сопровождалось неограниченным правом исполнителя использовать сведения для своих задач. Это не требование запрещать все действия поставщика услуги. Его назначение - сделать понятным, какие действия согласованы, какие исключены и чем подтверждается соблюдение границы.

Проверка соглашения о неразглашении нужна отдельно, потому что обязательство адресата и охраняемый статус информации - разные юридические вопросы. Подпункт «b» пункта 1 § 2 немецкого

Закона о защите коммерческой тайны прямо требует соразмерных обстоятельствам мер конфиденциальности [12]. В казахстанском праве соответствующая оценка проводится по собственным нормам, рассмотренным выше. Иностранное условие не подменяет их, но позволяет проверить, не ограничивается ли заявитель представлением общего обещания вместо доказательств действующего режима.

Федеральный суд по трудовым спорам Германии в решении от 17 октября 2024 года по делу 8 AZR 172/23 отказал работодателю в требовании о запрете. В пунктах 24-28 отмечена неподтвержденность надлежащих мер охраны технических сведений. В пунктах 30-32 отдельно рассмотрена чрезмерно широкая бессрочная обязанность молчать обо всех внутренних вопросах компании, признанная недействительной по § 307(1) BGB. При этом пункт 31 допускает договорную охрану информации и за пределами законодательного понятия тайны [13]. Решение не объявляет недействительными все соглашения о неразглашении.

Два рассмотренных зарубежных дела дополняют друг друга. В IntelIClear предмет охраны был конкретизирован настолько, чтобы спор продолжился. В немецком деле проблема состояла в подтверждении мер и содержании договорного ограничения. Из этого предлагается сделать практический вывод, что сначала необходимо подготовить описание информации, затем доказательства ее охраны и только потом сопоставлять поведение адресата с обязательством. Один универсальный пункт «все сведения компании конфиденциальны» не решает три разные задачи.

Такое разграничение важно и для свободы дальнейшей работы человека. Предметом запрета должно быть неправомерное использование определенных сведений, а не любое применение приобретенного профессионального опыта. Для договорной практики предлагается прямо указывать, какие материалы и сведения подпадают под ограничение и почему обязанность сохраняется после прекращения отношений. Последоговорный запрет не следует выводить только из желания работодателя

исключить конкуренцию. Его основание, содержание и пределы подлежат отдельной правовой проверке.

Еще одна проблема возникает в клиентских массивах, где одновременно присутствуют интерес компании и права граждан. Пункты 1-2 статьи 11 Закона РК «О персональных данных и их защите» устанавливают самостоятельную обязанность сохранять конфиденциальность персональных данных ограниченного доступа. Подпункт 1) пункта 1 статьи 24 закрепляет право субъекта получать сведения об обработке [14]. Следовательно, отсутствие доказанного режима коммерческой тайны не означает свободу распространения клиентских данных. Обратный вывод также неверен: персональный характер записи сам по себе не доказывает коммерческую тайну организации.

Предлагается отдельно описывать защищаемые компанией деловые сведения и правовые основания обращения с информацией о гражданах. Это позволяет установить, какое требование относится к компании, а какое - к субъекту данных. Пометка о коммерческой тайне не должна служить объяснением отказа человеку в предусмотренной законом информации о нем. Но и осуществление такого права не предполагает свободной передачи ему всей клиентской базы с чужими сведениями. Необходимый объем раскрытия определяется содержанием конкретного права.

Законность происхождения также нельзя заменять последующим ограничением доступа. Пункт 1 статьи 1017 ГК адресован правомерному обладателю [4]. Пункт 7 статьи 17 Цифрового кодекса, в свою очередь, не признает открытыми данные, доступность которых возникла вследствие утечки, ошибки или противоправных действий [15]. Поэтому закрытый сервер и соглашение о неразглашении не устраняют первоначальную незаконность получения спорных сведений. В исследуемом массиве требуется определить затронутую часть и проверить остальные сведения отдельно, а не заранее объявлять законным либо незаконным весь ресурс.

После установления режима остается вопрос о самом нарушении. Ш. Сандин в работе о неправомерном получении информации обращает внимание на различия между

приобретением, последующим использованием и причиненным вредом [16]. Для гражданско-правовой оценки это означает необходимость отдельных доказательств. Запись о скачивании показывает техническое действие, но не объясняет его договорную цель. Сходство двух файлов подтверждает совпадение содержания, но не всегда объясняет происхождение совпадения. Правовой вывод требует связать технические сведения с установленным ограничением.

Пункт 4 статьи 1018 ГК РК прямо разрешает самостоятельное правомерное получение и использование тех же сведений [4]. Поэтому обладатель тайны не получает общего права запретить конкуренту прийти к такому же результату независимо. Для проверки возражения о самостоятельной разработке существенны источники, последовательность работы и материалы, подтверждающие происхождение результата. Предлагаемый подход защищает не только истца: он дает ответчику понятную возможность показать законность своих действий, не ограничиваясь голословным отрицанием.

При выявлении совпадений нужно объяснять, в чем их доказательственная сила. Значение может иметь сочетание непубличных элементов, последовательность записей или иная особенность, связанная с указанным истцом предметом охраны. Но само количество совпадений не заменяет проверки общих законных источников. Эксперт помогает установить технические обстоятельства, а вопрос о выполнении условий статьи 126 остается правовым. Передача всего массива эксперту с просьбой «найти коммерческую тайну» необоснованно переносит на него задачу заявителя и суда.

Отдельного рассмотрения требует состояние информации после передачи. Ш. Сандин в работе *A Typology of Disclosure* показывает, что разные виды раскрытия имеют разные правовые последствия и не всякое разглашение автоматически прекращает любые права на информацию [17]. Для рассматриваемой темы это означает необходимость установить объем и круг распространения. Получение копии ограниченным кругом лиц, публикация

отдельных полей и раскрытие всей структуры не должны описываться одним недифференцированным словом «утечка».

Пункт 4 статьи 1017 ГК связывает продолжение охраны с сохранением предусмотренных законом условий [4]. Поэтому для запрета будущего использования необходимо исследовать сохраняющийся предмет защиты. Для требования о последствиях уже совершенного нарушения значимы также обстоятельства соответствующего периода. Позднейшее изменение доступности не должно заменять анализ прежнего поведения. Но и первоначальный секретный статус не позволяет без дополнительного обоснования бесконечно запрещать использование сведений, которые впоследствии правомерно стали общедоступными.

Теперь необходимо связать существование тайны с конкретным способом защиты. Пункты 1 и 4 статьи 9 ГК РК различают пресечение нарушения и возмещение убытков [3]. Для денежного требования одной доказанной секретности недостаточно: нужно установить относящиеся к нему потери и их связь с нарушением. Для прекращения неправомерного использования важно точно определить запрещаемые действия и сведения. В пункте 3 статьи 1018 предусмотрено и специальное судебное решение для добросовестного приобретателя - дальнейшее использование на условиях возмездной исключительной лицензии [4]. Эти разные последствия нельзя заменять общим требованием «наказать за базу».

Практически это требует разделять доказательства режима и доказательства заявленного результата. Описание защищаемой части, ограничения доступа и коммерческое значение подтверждают наличие охраняемой позиции. Документы о конкретных потерях и действиях ответчика отвечают на другие вопросы. Такое разделение не увеличивает искусственно число препятствий для истца. Оно помогает заранее определить, каких материалов действительно недостает, и не принимать подтверждение одного обстоятельства за доказательство всего требования.

Само доказывание не должно превращаться в новое неконтролируемое раскрытие. Статья 72 ГПК РК закрепляет

обязанность сторон подтверждать основания требований и возражений, а часть 2 статьи 19 допускает закрытое рассмотрение для сохранения коммерческой и иной охраняемой тайны [18]. Следовательно, заинтересованному лицу нужно не только представить описание защищаемого содержания, но и своевременно поставить вопрос о порядке его исследования. При этом конфиденциальность не означает, что ответчик должен защищаться от полностью скрытого от него требования.

Возможный порядок состоит в отделении общего описания требования от относящегося к нему конфиденциального материала. Описание объясняет, какая информация спорна и почему она значима. Более подробный материал позволяет проверить заявленное содержание при установленных судом ограничениях. Избыточные сведения о других лицах следует исключать, если без них можно исследовать спор. Это предложение о применении существующих средств, а не о признании любого составленного истцом закрытого приложения достаточным доказательством.

Проведенный анализ позволяет сформулировать решение без нового всеобщего реестра коммерческой тайны. Организации предлагается заранее сохранять краткое описание защищаемого содержания, основание законного обладания, объяснение коммерческого значения и сведения о фактически действующих ограничениях. Для изменяемой базы добавляется способ определить ее относящееся к спору состояние. Все перечисленное может содержаться в действующих договорах, правилах доступа и технической документации. Не требуется создавать отдельный документ только ради нового названия.

Чтобы такой подход получил ясную законодательную опору, предлагается дополнить пункт 4 статьи 28 Предпринимательского кодекса РК новым подпунктом: «документирование содержания охраняемой части цифрового массива или сочетания сведений и существенных изменений, позволяющее определить предмет охраны и применяемые к нему ограничения доступа». Это авторское предложение. Оно добавляет один возможный способ охраны в существующий открытый перечень, а не вводит обязательную регистрацию всех баз.

Зачем нужно это дополнение? Действующая норма позволяет составлять перечень информации, но для меняющейся базы общее название в перечне не всегда помогает восстановить предмет спора. Предлагаемая формулировка показывает, что описывать можно часть и сочетание сведений, а изменение следует фиксировать в той мере, в какой оно влияет на предмет охраны. Для небольшой организации достаточно понятного описания и истории существенных изменений. Для сложной системы могут использоваться уже существующие технические средства. Смысл предлагаемого способа - определенность, а не одинаковый объем расходов.

Для судебного применения предлагается также следующее разъяснение. При оценке мер охраны нераскрытой информации учитываются ее содержание, условия использования и фактически действовавшие ограничения доступа. Отсутствие отдельной формы учета или специальной надписи само по себе не исключает защиту, если законом такая форма не установлена. Наличие надписи либо соглашения о неразглашении не освобождает от установления остальных условий правовой охраны. Это предлагаемое толкование, а не цитата из действующего постановления Верховного Суда.

Польза такого разъяснения состоит в устранении двух видов формализма. Компания не проигрывает спор только из-за отсутствия необязательной бумаги. Но она также не выигрывает его только потому, что такую бумагу составила. Для правоприменения это означает оценку реального содержания отношений. Для законодательства - сохранение предусмотренного статьей 1017 отсутствия регистрационных формальностей. Для гражданско-правовой теории - последовательное разграничение условия возникновения защиты и способа доказать, что это условие выполнено.

В договоре предлагается связывать конфиденциальность с определенным предоставлением. В частности предлагается включать следующую формулировку: «Стороны определяют охраняемые сведения в описании передаваемого массива, указывают разрешенные цели использования и круг допущенных получателей. Существенное изменение охраняемого содержания

или условий доступа доводится до получателя способом, позволяющим подтвердить уведомление». Эта формулировка предназначена для договорной работы и требует согласования с конкретным отношением. Она не позволяет односторонне изменить договор или ограничить права третьих лиц.

Такое условие нужно не для механического увеличения ответственности. Оно помогает адресату понять границу дозволенного до начала работы, а при споре - сопоставить полученное содержание с реально совершенным действием. Необходимо отдельно согласовать, что происходит с копиями после прекращения доступа и какие обязанности сохраняются на законном основании. Договор не должен обещать вечную секретность независимо от фактов. Он также не может исключать обязательное раскрытие сведений, прямо предусмотренное законом.

Наконец, предлагаемое описание не заменяет доказательств и не получает заранее установленной силы. Суд проверяет, существовал ли соответствующий документ в нужный период, согласуется ли он с системой доступа и относится ли к спорным сведениям. Подготовленная уже после конфликта справка может объяснять материалы, но не создает задним числом отсутствовавшие ограничения. Для компаний это означает необходимость организовать доказуемую охрану в обычной работе, а не пытаться восстановить все ее элементы только перед предъявлением иска.

Итак, центральная проблема заключается не в отсутствии названия для большого цифрового массива. Она состоит в способности связать определенное содержание с законным обладанием, коммерческой ценностью секретности и реальными мерами охраны в нужный момент. Предложенное решение - конкретное, обновляемое описание защищаемых сведений и подтверждение действующих ограничений. Это позволяет использовать существующий институт коммерческой тайны без признания всей информации компании исключительной собственностью и без введения ненужных регистрационных процедур.

Для практики результат выражается в понятном наборе вопросов к доказательствам. Для теории - в различении защищаемого интереса, договорной обязанности и последствий нарушения. Для законодательства - в точечном уточнении способа описания динамического массива и в отказе от формальной оценки по одному штампу или соглашению. Такая защита имеет определенные границы: она препятствует неправомерному использованию доказанно охраняемых сведений, но не закрывает законные источники, самостоятельную работу и осуществление прав других лиц.

Финансирование. *Исследование подготовлено в рамках проекта ИРН AP23489796 «Проблемы регламентации правового режима больших данных (Big Data): отечественный и международный опыт», финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан.*

Список использованных источников

1. Калашникова, А. Игорь Чернов: Защита коммерческой тайны - это национальная безопасность Казахстана [Электронный ресурс] : интервью / А. Калашникова // Ratel.kz. - 2025. - 9 сентября. - URL: https://ratel.kz/outlook/igor_chernov_zaschita_kommercheskoj_tajny_eto_natsionalnaja_bezopasnost_kazahstana (дата обращения: 03.10.2026).
2. Сулейменов, М. К. Понятие и способы защиты гражданских прав [Электронный ресурс] / М. К. Сулейменов // Параграф : информационная система. - 2014. - 16 июня. - URL: https://prg.kz/document/?doc_id=33100058 (дата обращения: 03.10.2026).
3. Гражданский кодекс Республики Казахстан (Общая часть) : от 27 декабря 1994 г. № 268-ХІІІ // Ведомости Верховного Совета Республики Казахстан. - 1994. - № 23–24 (приложение). - Электронный текст в ИПС «Әділет». - URL: https://old.adilet.zan.kz/rus/docs/K940001000_ (дата обращения: 03.10.2026).
4. Гражданский кодекс Республики Казахстан (Особенная часть) : от 1 июля 1999 г. № 409-І // Ведомости Парламента Республики Казахстан. - 1999. - № 16–17. - Ст. 642. - Электронный текст в ИПС «Әділет». - URL: https://old.adilet.zan.kz/rus/docs/K990000409_ (дата обращения: 03.10.2026).
5. Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) [Электронный ресурс] : Annex 1C to the Marrakesh Agreement Establishing the World Trade Organization : 15 April 1994 // World Trade Organization : official website. - Art. 39. - URL: https://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm (дата обращения: 03.10.2026).

6. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure // Official Journal of the European Union. - 2016. - L 157, 15 June. - P. 1–18. - URL: <https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng> (дата обращения: 03.10.2026).

7. Risch, M. Why Do We Have Trade Secrets? / M. Risch // Marquette Intellectual Property Law Review. - 2007. - Vol. 11, no. 1. - P. 1–76. - URL: <https://scholarship.law.marquette.edu/iplr/vol11/iss1/1/> (дата обращения: 03.10.2026).

8. United States Code [Электронный ресурс]. Title 18. Crimes and Criminal Procedure. § 1839. Definitions // Legal Information Institute, Cornell Law School : electronic collection of federal law. - URL: <https://www.law.cornell.edu/uscode/text/18/1839> (дата обращения: 03.10.2026).

9. United States Court of Appeals for the Ninth Circuit. IntelIClear, LLC v. ETC Global Holdings, Inc. [Электронный ресурс] : opinion of 15 October 2020, no. 19-55862. - 2020. - 21p. - Official electronic publication. - URL: <https://cdn.ca9.uscourts.gov/datastore/opinions/2020/10/15/19-55862.pdf> (дата обращения: 03.10.2026).

10. Предпринимательский кодекс Республики Казахстан : от 29 октября 2015 г. № 375-V ЗРК // Ведомости Парламента Республики Казахстан. - 2015. - № 20-III. - Ст. 112. - Электронный текст в ИПС «Әділет». - URL: <https://old.adilet.zan.kz/rus/docs/K1500000375> (дата обращения: 03.10.2026).

11. Sandeen, S. K. Lost in the Cloud: Information Flows and the Implications of Cloud Computing for Trade Secret Protection / S. K. Sandeen // Virginia Journal of Law & Technology. - 2014. - Vol. 19, no. 1. - P. 1–103. - URL: <https://open.mitchellhamline.edu/facsch/405/> (дата обращения: 03.10.2026).

12. Gesetz zum Schutz von Geschäftsgeheimnissen (Geschäftsgeheimnisgesetz - GeschGehG) : vom 18. April 2019 // Bundesgesetzblatt. - 2019. - Teil I. - S. 466. - Amtliche elektronische Fassung auf Gesetze im Internet. - URL: <https://www.gesetze-im-internet.de/geschgehg/BJNR046610019.html> (дата обращения: 03.10.2026).

13. Bundesarbeitsgericht. Geschäftsgeheimnisse - Geheimnisschutz - Unterlassung [Электронный ресурс] : Urteil vom 17. Oktober 2024, 8 AZR 172/23. - 2024. - ECLI:DE:BAG:2024:171024.U.8AZR172.23.0. - Amtliche elektronische Veröffentlichung. - URL: <https://www.bundesarbeitsgericht.de/entscheidung/8-azr-172-23/> (дата обращения: 03.10.2026).

14. О персональных данных и их защите : Закон Республики Казахстан от 21 мая 2013 г. № 94-V // Ведомости Парламента Республики Казахстан. - 2013. - № 7. - Ст. 35. - Электронный текст в ИПС «Әділет». - URL: <https://old.adilet.zan.kz/rus/docs/Z1300000094> (дата обращения: 03.10.2026).

15. Цифровой кодекс Республики Казахстан : от 9 января 2026 г. № 255-VIII ЗРК // Казахстанская правда. - 2026. - 10 января. - № 5–6 (30634–30635). - Электронный текст в ИПС «Әділет». - URL: <https://old.adilet.zan.kz/rus/docs/K2600000255> (дата обращения: 03.10.2026).

16. Sandeen, S. K. Out of Thin Air: Trade Secrets, Cybersecurity, and the Wrongful Acquisition Tort / S. K. Sandeen // Minnesota Journal of Law, Science & Technology. - 2018. - Vol. 19, no. 2. - P. 373–404. - DOI 10.24926/15529541.3802. - URL: <https://scholarship.law.umn.edu/mjlst/vol19/iss2/3/> (дата обращения: 03.10.2026).

17. Sandeen, S. K. A Typology of Disclosure / S. K. Sandeen // Akron Law Review. - 2021. - Vol. 54, no. 3. - P. 657–687. - URL: <https://ideaexchange.uakron.edu/akronlawreview/vol54/iss3/5/> (дата обращения: 03.10.2026).

18. Гражданский процессуальный кодекс Республики Казахстан : от 31 октября 2015 г. № 377-V ЗРК // Ведомости Парламента Республики Казахстан. - 2015. - № 20-VI. - Ст. 114. - Электронный текст в ИПС «Әділет». - URL: <https://old.adilet.zan.kz/rus/docs/K1500000377> (дата обращения: 03.10.2026).

Иноятова С.Ф.

и.о.профессора сектора Гражданского права ТГЮУ, д.ю.н.

ORCID: <https://orcid.org/0009-0007-3975-3172>

DOI10.47689/2181-1415-vol5-iss4/S-pp219-228

ПРАВОВЫЕ МЕХАНИЗМЫ ЗАЩИТЫ ЖЕНЩИН ОТ ПРИТЕСНЕНИЯ И НАСИЛИЯ И РАСШИРЕНИЯ ИХ ВОЗМОЖНОСТЕЙ В ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

Одной из значимых проблем на сегодняшний день, стоящих перед Республикой Узбекистан является защита прав женщин от всех форм дискриминации и насилия. Домашнее насилие — это не только одна из самых распространённых, сложных и травмирующих жизненных ситуаций, но и одно из наиболее частых нарушений прав человека. Долгое время домашнее насилие воспринималось как «личное дело» частных лиц, однако современная концепция прав человека предоставляет возможности изменить это восприятие, рассматривая проблему как общественную, требующую решения на уровне всего общества. Так, например, бывший Генеральный Секретарь ООН Пан Ги Мун в 2016 году в своём послании, посвящённом Международному дню ликвидации насилия в отношении женщин, который отмечается ежегодно 25 ноября, подчеркнул, что, наконец, растёт глобальное признание того факта,

что насилие в отношении женщин и девочек представляет собой нарушение прав человека, создаёт масштабную угрозу для общественного здравоохранения и является серьёзным препятствием на пути устойчивого развития [1]. Необходимо особо подчеркнуть, что права женщин закрепляют социально-экономический, гражданский и политический статус женщин, они направлены на обеспечение защиты женщин от гендерной дискриминации. Права женщин входят в число основных прав человека и закреплены в многочисленных международных конвенциях, договорах, резолюциях, декларациях и программах действий в области прав человека.

Основным источником по защите прав женщин в мировом сообществе является Конвенция Организации Объединенных Наций о ликвидации всех форм дискриминации в отношении женщин (далее - Конвенция). Данная Конвенция является основополагающим документом, выделившим права женщин в отдельную категорию. Конвенция определяет дискриминацию в отношении женщин как любое различие, исключение или ограничение по признаку пола, которое направлено на ослабление или сводит на нет признание, пользование или осуществление женщинами, независимо от их семейного положения, на основе равноправия мужчин и женщин, прав человека и основных свобод в политической, экономической, социальной, культурной, гражданской или любой другой области [2]. Согласно статье 2 Конвенции правовые механизмы защиты женщин от дискриминации должны не только декларировать конституционный принцип равноправия мужчин и женщин, но и принимать соответствующие законодательные и другие меры, включая санкции, запрещающие любые формы дискриминации в отношении женщин. Обращая внимание государств на то, что дискриминация в отношении женщин характерна для традиционного патриархального уклада общества, в статье 5 Конвенции регламентировано, что страны-участницы должны принять меры правового регулирования, направленные на изменение социальных и культурных моделей поведения мужчин и женщин с целью искоренения предрассудков и стереотипов, основанных на идее

неполноценности или превосходства одного из полов. Конвенция устанавливает обязанность государств обеспечить равные гражданские, политические, экономические и социальные права мужчин и женщин и напрямую налагает на государства обязательство принимать все соответствующие меры для ликвидации дискриминации в отношении женщин со стороны не только государственных органов, но и любого физического и юридического лица. Ратифицируя Конвенцию, государства-участники берут на себя обязательства не только установить формальное правовое равенство между женщинами и мужчинами, но также принимать меры для обеспечения реального осуществления женщинами своих прав наравне с мужчинами [3].

Республика Узбекистан уделяет особое внимание обеспечению защиты прав женщин, к примеру, наша страна одной из первых в Центральной Азии ратифицировала конвенции ООН «О ликвидации всех форм дискриминации в отношении женщин», «Об охране материнства», «О дискриминации в области труда и занятий». В целях контроля за соблюдением государствами положений Конвенции был также учреждён Комитет по ликвидации дискриминации в отношении женщин (далее – Комитет). Конвенция устанавливает специальный механизм контроля за выполнением норм государством-участником в рамках договора на основании подачи периодических отчётов [2]. С момента присоединения Узбекистана к Конвенции в Комитет по ликвидации дискриминации в отношении женщин представлены 6 национальных докладов:

- 2000 г. – первый национальный доклад;
- 2004 г. – второй-третий национальные доклады;
- 2008 г. – четвертый национальный доклад;
- 2014 г. – пятый национальный доклад;
- 2019 г. – шестой национальный доклад.

Безусловно, такие доклады позволяют оценить прогресс в реализации обязательств по Конвенции, выявить существующие проблемы и предложить рекомендации для их решения.

В 2017-2019 годах в республике принято значительное количество нормативно-правовых актов, направленных на обеспечение и защиту прав женщин. К примеру, в сфере повышения

роли женщин в социально-политической жизни страны был принят Указ Президента Республики Узбекистан №5325 от 02.02.2018 г. «О мерах по коренному совершенствованию деятельности в сфере поддержки женщин и укрепления института семьи». Данный указ предоставляет возможность в корне изменить работу Комитета женщин Узбекистана, а также ряда государственных органов и общественных организаций. Во исполнение указа было создано более 46 тысяч женских первичных организаций в министерствах и ведомствах, предприятиях и организациях, органах самоуправления граждан, воинских частях и учебных заведениях, трудовых коллективах, а также был учрежден Общественный фонд по поддержке женщин и семьи, который расширил возможности Комитета женщин для оказания эффективной и продуктивной помощи женщинам, находящимся в тяжелой жизненной ситуации [3]. Принятие 2 сентября 2019 года Закона Республики Узбекистан «О гарантиях равных прав и возможностей для женщин и мужчин» свидетельствует о стремлении государства укрепить правовые основы для обеспечения гендерного равенства. В данном нормативно-правовом акте были впервые закреплены и даны конкретные определения таким понятиям, как «прямая дискриминация по признаку пола» и «косвенная дискриминация по признаку пола», введена обязательная гендерно-правовая экспертиза нормативно-правовых актов, направленная на выявление их несоответствия принципам гендерного равенства, возможных рисков дискриминационного характера в процессе их применения, разработку рекомендаций по устранению выявленных норм, допускающих прямую или косвенную дискриминацию по признаку пола. Согласно данному закону, женщины и мужчины имеют равные права избирать и быть избранными в представительные органы власти. Более того, установлено, что государство принимает соответствующие меры по обеспечению женщинам возможности на равных условиях с мужчинами и без какой-либо дискриминации занимать руководящие должности в государственных органах в соответствии со своими способностями и профессиональной подготовкой. Выше приведенный законодательный акт подтверждает обязательство страны по созданию равных условий

для мужчин и женщин в различных сферах жизни, включая трудовые, социальные и политические права. Закон направлен на устранение дискриминации по половому признаку, закрепление равных прав и возможностей, а также создание механизмов для защиты этих прав. Закон также подчеркивает важность государственной политики в поддержке женщин, их участия в общественной жизни страны.

Следует отметить, что в сфере защиты женщин от насилия принято Постановление Президента Республики Узбекистан №3827 от 02.07.2018года «О мерах по совершенствованию системы социальной реабилитации и адаптации, а также профилактики семейно-бытового насилия», которым утверждена целая программа мер по совершенствованию социальной реабилитации и адаптации, и системы профилактики семейно-бытового насилия. Большой реформой на пути обеспечения защиты прав женщин, а также инкриминирования домашнего насилия стало принятие и вступление в силу Закона Республики Узбекистан «О защите женщин от притеснений и насилия» 2 сентября 2019года. Документ регулирует отношения в области защиты женщин от притеснений и насилия в быту, на рабочих местах, в образовательных учреждениях и в иных местах. Нормативно-правовой акт направлен на утверждение в обществе атмосферы нетерпимого отношения к любым проявлениям насилия в отношении женщин. В нем дана четкая характеристика ряду терминов, среди которых, такие термины, как «притеснение», «насилие», а также виды насилия «психологическое насилие», «физическое насилие», «половое насилие», «экономическое насилие», «жертва притеснения и насилия», «охранный ордер» и другие. Предусмотрена организация работы горячих телефонных линий для жертв притеснений и насилия, определен порядок их деятельности, введено понятие специальных центров реабилитации [2]. Основными направлениями государственной политики в области защиты женщин от притеснения и насилия определены:

разработка и реализация гендерной политики, государственных программ и стратегий в области защиты женщин от притеснения и насилия;

повышение в обществе правового сознания и правовой культуры;

создание эффективных организационно-правовых механизмов для предупреждения, выявления, пресечения притеснения и насилия в отношении женщин;

принятие мер по устранению причин и условий, способствующих притеснению и совершению насилия в отношении женщин;

обеспечение сотрудничества государственных органов, органов самоуправления граждан, негосударственных некоммерческих организаций и других институтов гражданского общества в целях предупреждения притеснения и насилия в отношении женщин.

Таким образом, современная правовая политика Республики Узбекистан в сфере защиты женщин от притеснения и насилия характеризуется переходом от формирования базовых законодательных гарантий к развитию комплексного механизма профилактики, ответственности, судебной защиты и социальной реабилитации. Если в 2019 году основное внимание уделялось законодательному закреплению понятия насилия и созданию института охранного ордера, то последующие реформы расширили административные и уголовно-правовые механизмы защиты, усилили судебные гарантии, усовершенствовали порядок выдачи охранного ордера и расширили систему социальной поддержки. Вместе с тем судебная практика показывает, что проблемы реализации сохраняются: значительная доля дел прекращается в связи с примирением, а большинство потерпевших в исследованной выборке не имели адвоката. Это свидетельствует о необходимости дальнейшего совершенствования не только законодательства, но и практики его применения.

Отдельные официально озвученные данные также позволяют оценить применение административной и уголовной ответственности. По информации, распространённой со ссылкой на пресс-секретаря Верховного суда Республики Узбекистан, за январь–октябрь 2024 года по статье 59 Кодекса об административной ответственности к ответственности были привлечены 15 427 человек: 9 210 лицам назначен штраф, а 6 217

лицам — административный арест. За тот же период по статье 126 Уголовного кодекса были осуждены 399 человек, из которых 126 получили наказание в виде лишения свободы, 255 — наказания, не связанные с лишением свободы, а 18 лицам назначено условное осуждение.

Гендерная характеристика потерпевших в исследованных судебных материалах подтверждает, что семейное насилие в подавляющем большинстве случаев затрагивает женщин: из 882 потерпевших 833 человека, или 94,4 %, составляли женщины. При этом 96,1 % потерпевших в проанализированных делах не имели адвоката. В 859 делах (97,4 %) семейное насилие было связано с умышленным причинением телесных повреждений, а 737 случаев (83,1 %) произошли в жилых помещениях, где совместно проживали супруги. В шести проанализированных делах семейное насилие привело к смерти потерпевшего.

Показательной является современная судебная практика по статье 126¹ Уголовного кодекса. Согласно исследованию ПРООН, с момента введения уголовной ответственности за семейное (бытовое) насилие судами по уголовным делам было рассмотрено 1 454 таких дела, в том числе 459 дел в 2023 году и 995 дел в 2024 году. В рамках исследования были проанализированы 882 судебных документа, отобранных из дел о семейном (бытовом) насилии. По результатам анализа 501 дело (56,8 %) было прекращено в связи с примирением сторон, тогда как по 381 делу (43,2 %) были вынесены обвинительные приговоры [3].

Изменения законодательства сопровождаются значительным объёмом выявляемых случаев притеснения и насилия и расширением практики применения охранных ордеров. Согласно информации, представленной Узбекистаном в материалах Комитета ООН по ликвидации дискриминации в отношении женщин, в 2023 году было выявлено 40 055 случаев притеснения и насилия в отношении женщин, при этом 39 263 женщинам были выданы охранные ордера. Приведённые показатели свидетельствуют одновременно о значительном масштабе выявляемых случаев и о широком использовании механизма охрannого ордера как инструмента оперативной защиты.

Современная статистика и судебная практика

Наиболее поздние изменения, актуальные на 2026 год, предусмотрены Законом Республики Узбекистан от 1 июля 2026 года № ЗРУ-1156. В Закон «О защите женщин от притеснения и насилия» внесены положения, предоставляющие специальным центрам право обращаться в суды с заявлениями, жалобами и исками в защиту прав и законных интересов пострадавших от притеснения и насилия и их несовершеннолетних детей без уплаты государственной пошлины. Также размещение жертвы в специальном центре является основанием для выдачи листка временной нетрудоспособности на период пребывания в центре, но не более чем на один месяц.

В 2025 году защита пострадавших от семейного (бытового) насилия была усилена также в семейном и жилищном законодательстве. Законом Республики Узбекистан от 9 апреля 2025 года № ЗРУ-1053 статья 40 Семейного кодекса дополнена положением, согласно которому суд по требованию лица, пострадавшего от семейного (бытового) насилия, не назначает срок для примирения. Кроме того, в Жилищный кодекс внесена норма, позволяющая при определённых спорах о пользовании жилым помещением предусмотреть предоставление другой равноценной жилой площади либо оплату арендной платы [4].

Важным этапом стало принятие Закона Республики Узбекистан от 21 октября 2024 года № ЗРУ-978, которым были усилены меры защиты от семейного (бытового) насилия в отношении детей. В частности, соответствующие положения об административной и уголовной ответственности были распространены на случаи семейного (бытового) насилия в отношении детей, а также уточнены отдельные процессуальные гарантии по делам данной категории [5].

Дополнительные меры социальной защиты были предусмотрены Постановлением Президента Республики Узбекистан от 10 мая 2024 года № ПП-175 «О дополнительных мерах по совершенствованию оказания социальных услуг лицам, пострадавшим от притеснения и насилия». Документ предусматривает совершенствование системы реабилитации и адаптации пострадавших, развитие взаимодействия органов

внутренних дел с центрами социальных услуг «Инсон» и внедрение коррекционных программ для лиц, совершивших либо склонных к совершению притеснения и насилия.

В 2024 году механизм защиты пострадавших был дополнительно усовершенствован. Постановлением Кабинета Министров Республики Узбекистан от 26 августа 2024 года № 529 предусмотрена возможность получения охрannого ордера посредством Единого портала интерактивных государственных услуг. Инспектор профилактики выдаёт охранный ордер в течение 24 часов с момента выявления ситуации притеснения и насилия либо угрозы их совершения. С 1 декабря 2024 года предусмотрена также возможность выдачи охрannого ордера по инициативе инспектора профилактики в случаях, когда ситуации притеснения и насилия выявляются два и более раза в течение одного календарного года [2].

Закон № ЗРУ-829 также расширил предусмотренные законодательством формы защиты. В частности, было введено понятие «преследование», охватывающее совершаемые против воли жертвы действия по её поиску, установлению контакта, посещению места работы, учёбы или проживания, в том числе посредством телекоммуникационных сетей и Интернета. Кроме того, в Уголовный кодекс была введена статья 141³, устанавливающая ответственность за распространение без согласия лица фотографий и (или) видеозаписей обнажённого тела либо половых органов, а также за угрозу распространения таких материалов. Существенно усилен и механизм охрannого ордера: при сохранении угрозы его действие может быть продлено судом на срок до одного года.

Одним из наиболее существенных нововведений 2023 года стало дополнение Уголовного кодекса Республики Узбекистан статьёй 126¹, устанавливающей уголовную ответственность за семейное (бытовое) насилие. Норма охватывает, в частности, воспрепятствование осуществлению права на собственность, образование, здравоохранение или труд, умышленное повреждение имущества и личных вещей, унижение чести и достоинства, запугивание и изоляцию от близких родственников, а также различные виды умышленного причинения телесных повреждений

в отношении супруга, бывшего супруга, лица, совместно проживающего на основе единого хозяйства, либо лица, имеющего общего ребёнка. Параллельно в Кодекс об административной ответственности была введена статья 59² «Семейное (бытовое) насилие», предусматривающая ответственность за соответствующие деяния, если они не содержат признаков преступления.

После принятия в 2019 году Закона Республики Узбекистан «О защите женщин от притеснения и насилия» законодательство Республики Узбекистан претерпело существенные изменения, направленные на усиление гарантий защиты женщин от различных форм насилия, совершенствование механизмов профилактики и повышение эффективности привлечения виновных лиц к ответственности. Особое значение в этом отношении имеет Закон Республики Узбекистан от 11 апреля 2023 года № ЗРУ-829 «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан в связи с дальнейшим совершенствованием системы надежной защиты прав, свобод и законных интересов женщин и детей». Данным законом были внесены изменения в Уголовный кодекс, Кодекс об административной ответственности и Закон «О защите женщин от притеснения и насилия», что существенно расширило механизмы правовой защиты женщин и детей.

Принятие 2 сентября 2019 года Закона «О защите женщин от притеснений и насилия» в Узбекистане свидетельствует о том, что государство признает проблему насилия в отношении женщин как одну из приоритетных и активно работает над ее решением на законодательном уровне. Этот закон демонстрирует стремление обеспечить правовую защиту женщин от различных форм насилия и притеснений, создать механизмы для предотвращения подобных действий, а также предоставить пострадавшим от насилия доступ к правовой и социальной помощи. Принятие данного закона также указывает на готовность государства защищать права женщин, гарантировать им безопасность и поддерживать принципы равенства и справедливости в обществе. Как отмечает Уполномоченный Олий Мажлиса Республики Узбекистан по правам

человека (Омбудсмен) «в соответствии со статьей 3 Конвенции о ликвидации всех форм дискриминации в отношении женщин, к которой Республика Узбекистан присоединилась в 1995 году, государства-участники обеспечивают, всестороннее развитие и прогресс всех женщин, в частности, в политической, социальной, экономической и культурной сферах, принимают все необходимые меры, в том числе законодательные, и сегодня это реализовано в нашем законодательстве. В национальном законодательстве, прежде всего, принята Конституция в новой редакции, а также законы специального характера, гарантирующие права женщин в соответствии с международными стандартами и ряд нормативно-правовых актов. В частности, Конституция Республики Узбекистан и Закон Республики Узбекистан «О гарантиях равных прав и возможностей женщин и мужчин» обеспечивают гарантии недискриминации по признаку пола и равных прав и возможностей для женщин и мужчин. Кроме того, Закон о защите женщин от притеснения и насилия содержит нормы, касающиеся обеспечения прав, свобод и законных интересов женщин, защиты их от угнетения и насилия».

Каждый год во всем мире проводится кампания «16 дней активизма против гендерного насилия», направленная на привлечение внимания общественности к проблеме насилия в отношении женщин и девочек. Кампания начинается 25 ноября – в Международный день борьбы за ликвидацию насилия в отношении женщин, и заканчивается 10 декабря, в международный день прав человека. Говоря о видах насилия в отношении женщин и девочек, в основном подразумевается физическое, психологическое, и сексуальное насилие. Однако существует и экономическое насилие женщин. Согласно статье 3 Закона Республики Узбекистан «О защите женщин от притеснений и насилия» экономическое насилие проявляется путем ограничения экономических возможностей и зависимости от мужчин, проявляющееся в виде удержания заработной платы, лишения доступа к финансовым ресурсам, контроль над имуществом, а также ограничение возможности в получении качественного образования и работы. Выявление и предотвращение экономического насилия в отношении женщин

является одной из приоритетных задач Узбекистана на пути к устойчивому развитию. Согласно открытым статистическим данным за последние 5 лет число женщин-предпринимателей в Узбекистане удвоилось. Безусловно это положительная тенденция, свидетельствующая о том, что женщины становятся все более активными и самостоятельными в бизнес-сфере. На сегодняшний день 40% предпринимателей в стране составляют женщины. Данного результата удалось добиться благодаря ряду государственных программ, направленных на создание безопасной среды для женщин, включая финансовую. В целях защиты экономических прав женщин государство активно поощряет женщин в запуске startup проектов и бизнеса путем предоставления льгот и преференций при уплате налогов. На сегодняшний день женщинам предоставляется финансовая поддержка в виде беспроцентных кредитов с льготным периодом в 10 лет. В качестве примера стоит привести Государственный целевой фонд по поддержке женщин, за счет средств которого финансируется целый ряд мероприятий для малообеспеченных женщин, начиная с финансирования бизнес инициатив, заканчивая предоставлением социальной защиты. Особое внимание уделяется развитию знаний, умений и навыков женщин, организации обучающих семинаров посредством Агентства по работе махаллабай и развитию предпринимательства. Налажена деятельность моноцентров «Ишга мархамат», которые обучают профессиям, преподают иностранные языки, оценивают квалификацию и помогают с трудоустройством женщин, оказавших жертвами домашнего насилия, а также находящихся в социально уязвимом положении. Особого внимания заслуживает практика внедрения «Женских тетрадей», которые служат сильным механизмом поддержки женщин по разным направлениям. В частности, тетради охватывают предоставление социальной защиты, обеспечение жилой площадью на льготных условиях, а также вопросы финансового содействия через трудоустройство и помощь в запуске бизнес инициатив.

Несомненно, государство осознает проблемы экономического насилия и принимает меры для ее предотвращения. Однако важно продолжать усилия в данном направлении. В первую очередь

необходимо повысить правовую грамотность среди населения, особенно женщин и девочек, об их правах и возможностях, которые предоставляет государство. В этом плане учитывается роль институтов гражданского общества, таких как средства массовой информации, органов государственной власти на местах и махаллинского комитета и государственного комитета по делам семьи и женщин [6].

Резюмируя вышеизложенное, хотим отметить, что защита прав женщин от притеснений и насилия, а также создание условий для их равноправного участия в общественной и экономической жизни, имеют важное значение для построения справедливого и развитого гражданского общества. Принятие Законов Республики Узбекистан «О защите женщин от притеснений и насилия» и «О гарантиях равных прав и возможностей для женщин и мужчин», являются важными шагами на пути к гендерному равенству и обеспечению защиты прав женщин. Однако для достижения полноценного успеха необходимо продолжать работу над эффективным применением этих законов, развивать программы поддержки и реабилитации женщин, ставших жертвами насилия, а также содействовать их активному участию в предпринимательской деятельности. Расширение возможностей для женщин в бизнесе не только способствует их экономической независимости, но и вносит значительный вклад в социально-экономическое развитие страны в целом.

Финансирование. Научная статья подготовлена в рамках программно-целевого финансирования по научным и (или) научно-техническим программам на 2025-2027 годы, направленная на реализацию проекта ИРН BR28713695 «Теоретические и методологические основы сотрудничества семьи и общества по проблемам насилия в отношении женщин и девочек-подростков», финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан.

Список использованных источников

1. Secretary-General's message for the International Day to End Violence Against Women and Girls // United Nations Secretary-General. URL:

<https://www.un.org/sg/en/content/sg/statement/2016-11-25/secretary-generals-message-international-day-end-violence-against>.

2. Постановление Президента Республики Узбекистан от 10 мая 2024 года № ПП-175 «О дополнительных мерах по совершенствованию оказания социальных услуг лицам, пострадавшим от притеснения и насилия». <https://lex.uz/uz/docs/6916641>

3. Cusack S., Timmer A.S.H. Gender stereotyping in rape cases: The CEDAW Committee's decision in *Vertido v The Philippines* // *Human Rights Law Review*. 2011. Vol. 11. Is. 2. P. 329–342

4. Антонова Ю.А. Дискриминация по признаку пола // Создание правовой среды для защиты от дискриминации по признакам этнической принадлежности, пола и возраста. Концепция развития российского законодательства: сб. материалов. М.: Новая юстиция, 2011.

5. Поленина С.В. Гендерное равенство. Проблема равных прав и равных возможностей мужчин и женщин. М.: Аспект Пресс, 2005.

6. Шведова Н.А. Гендерное равенство в России в XXI в. в контексте международных обязательств: прогресс или упущенные возможности? // *Женщина в российском обществе*. 2011. № 3. С. 23.

Иноятова С.Ф.

и.о.профессора сектора Гражданского права ТГЮУ, д.ю.н.

ORCID: <https://orcid.org/0009-0007-3975-3172>

DOI10.47689/2181-1415-vol5-iss4/S-pp219-228

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ ЗАЩИТЫ НОВЫХ ОБЪЕКТОВ ГРАЖДАНСКИХ ПРАВ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ И РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Цифровая трансформация экономики и общества кардинально изменила структуру объектов гражданского оборота, что ставит перед правовой наукой и практикой принципиально новые вызовы. Появление блокчейн-технологий, искусственного интеллекта, токенизации активов и виртуальной реальности создало категорию правовых объектов, «которые не укладываются в традиционную дихотомию вещных и обязательственных прав» [1]. Правовая защита таких объектов порождает «необходимость переосмысления

классических доктрин гражданского права и выработки новых механизмов, адаптированных к специфике цифровых активов» [1].

Анализ современной практики и законодательных инициатив позволяет выделить следующие категории новых объектов гражданских прав, «каждая из которых обладает уникальными характеристиками:

1) криптоактивы и токены: включая криптовалюты (Bitcoin, Ethereum), стейблкоины (USDT, USDC), utility токены и governance токены;

2) невзаимозаменяемые токены (NFT): цифровые сертификаты собственности на уникальные активы, от цифрового искусства до виртуальной недвижимости и игровых предметов;

3) результаты деятельности систем искусственного интеллекта: сгенерированный контент, алгоритмы машинного обучения, автономные программные агенты;

4) цифровые двойники и метавселенная-активы: виртуальная недвижимость, аватары, цифровые предметы в виртуальных мирах;

5) токенизированные традиционные активы: цифровые представления акций, облигаций, товаров и недвижимости» [1].

Основной проблемой правового регулирования новых объектов является их промежуточное положение между традиционными категориями собственности. Комиссия по правовым реформам Англии и Уэльса в 2023 году выявила, что «цифровые активы не подпадают под классические категории *things in possession* (материальные вещи) и *things in action* (права требования), что создает правовую неопределенность для их владельцев» [1]. В ответ на это британский парламент в сентябре 2024 года принял *Property (Digital Assets etc) Bill*, вводящий третью категорию персональной собственности специально для цифровых активов.

Современная правовая доктрина выработала несколько концептуальных подходов к защите новых объектов гражданских прав. Наиболее влиятельной является теория «цифровых прав собственности» [1], в рамках которой обоснована необходимость распространения традиционных принципов собственности на цифровые активы через призму исключительности, контроля и

передаваемости. «Альтернативный подход предлагает концепция “функциональной собственности” Angela Walch, согласно ей права на цифровые активы должны определяться их экономической функцией, а не формальными характеристиками» [2].

В современной правовой доктрине разработан ряд теорий и научных взглядов, связанных с защитой новых объектов, самой разработанной из которых является **концепция правовой субъектности цифровых объектов**. В этих теориях рассматривается «влияние цифровизации на традиционные представления о правосубъектности и анализируются различные подходы к определению правового статуса ИИ» [2].

Особый научный интерес представляет также и **теория расширенной собственности**, где «основными точками обсуждения являются современные подходы к пониманию собственности в контексте гражданского права». Данная концепция позволяет выработать правильный подход в восприятии новых объектов гражданского права на базе традиционной собственности.

Далее заслуживает особого внимания **концепция цифровых прав**. Теории, разработанные в рамках указанной концепции посвящаются «анализу цифровых технологий как объектов юридической науки и возникающих в связи с ними правовых вопросов» [3] и вопросам, «связанным с субъектами цифровых правоотношений и их правовым статусом» [3].

Также существует **теория правового саморегулирования**, где «представлены идеи саморегулирования в сфере цифровой экономики и правовые подходы к ним» [4].

Особого внимания заслуживает **теория трансграничного регулирования цифровых активов**, в рамках которой проводится «сравнительный анализ правового статуса цифровых активов в различных юрисдикциях».

Данные теории предоставляют углубленный анализ и различные подходы к правовой защите новых объектов гражданских прав в условиях цифровизации.

Сложность определения способов защиты новых объектов гражданских прав основывается на таких факторах, как: отсутствие единообразного правового регулирования, так как многие новые

объекты остаются вне правового поля или регулируются фрагментарно; наличие юрисдикционных сложностей, ведь цифровые активы и интеллектуальная собственность часто выходят за пределы одной страны; ограниченность механизмов правоприменения, выражающаяся в сложности доказательств правонарушений в цифровой среде; наличие этических и моральных вопросов, а именно – правового статус объектов, созданных искусственным интеллектом или биотехнологиями.

Несомненно, вышеупомянутые объекты имеют специфические свойства, отличающие их от традиционных объектов гражданского оборота, что требует разработки особых механизмов их защиты. Если традиционные способы защиты, применяющие к тем или иным традиционным объектам гражданских прав, изучены в той или иной степени и, более того, нашли свое отражение в действующем законодательстве, то касательно новых объектов гражданских прав выработка научной парадигмы находится только на начальном этапе. Учеными делаются попытки сформировать и сгенерировать общие подходы защиты, которые могут показать себя как эффективное средство восстановления нарушенного права относительно новых объектов.

Проведенное исследование правовой природы новых объектов и классического познания способов защиты гражданских прав позволило нам сделать выводы, что защита новых объектов гражданских прав может осуществляться ее гражданско-правовыми способами – в судебной или иной альтернативной форме.

Говоря о **гражданско-правовых способах защиты**, важно отметить, что к новым объектам гражданских прав гражданское законодательство позволяет применение таких традиционных способов защиты прав собственников и правообладателей, как:

- признание права – подтверждение права собственности или иных вещных прав на новый объект;
- возмещение убытков – взыскание компенсации за незаконное использование или причинение ущерба;
- компенсация морального вреда – защита нематериальных прав, таких как репутация;

-иск о запрете действий, нарушающих право – судебная защита от противоправных действий;

-пресечение недобросовестной конкуренции – защита инновационных разработок от копирования и незаконного использования.

В связи с отсутствием четкого регулирования в некоторых областях новых объектов гражданских прав судебная практика играет ключевую роль в их защите. В этом контексте важным представляется:

-разработка специализированных судебных процедур, направленных на защиту новых объектов гражданских прав;

-создание специализированных судов (например, судов по интеллектуальной собственности);

-введение цифровых механизмов судебной защиты (электронное правосудие, блокчейн-технологии в судопроизводстве).

При этом, осознавая необратимое развитие технологии во всем мире, наряду с традиционными способами, новые объекты гражданских прав требуют гибких инструментов защиты. По нашему мнению, таковыми могут выступать: институт **международного коммерческого арбитража**, как эффективный способ для защиты прав в международных коммерческих спорах; **инновационные механизмы саморегулирования** – кодексы поведения, корпоративные стандарты, внутренние регламенты компаний; **технологическая защита**, т. е. использование смарт-контрактов, блокчейн-регистрации и цифровых сертификатов.

Особую сложность в защите цифровых активов представляют вопросы идентификации и доказательства права собственности. «В отличие от традиционных активов, цифровые объекты существуют в децентрализованных сетях, что затрудняет установление их местонахождения и юрисдикции. Дело *Hermès v. Rothschild* (2022–2024) стало знаковым для определения границ интеллектуальной собственности в контексте NFT, поскольку суд должен был решить, может ли NFT, содержащий изображение сумки Hermès, нарушать авторское право бренда» [5].

Судебная практика США 2024 года значительно повлияла на развитие правовой защиты цифровых активов. Дело SEC v. Ripple Labs завершилось частичной победой Ripple: суд постановил, что токен XRP сам по себе не является ценной бумагой, однако определенные сделки с ним могут квалифицироваться как сделки с ценными бумагами. Штраф в размере 125 млн долларов оказался значительно меньше требуемых SEC 2 млрд. Не менее важным стало дело против Uniswap Labs, где суд отклонил коллективный иск, признав различие между пользовательским интерфейсом протокола и базовыми смарт-контрактами, что укрепило принцип децентрализации в DeFi.

Защита новых объектов гражданских прав осуществляется через комплекс традиционных и инновационных правовых механизмов. К традиционным способам, адаптированным для цифровой среды, относятся:

- признание права собственности через блокчейн-записи и криптографические доказательства;
- возмещение убытков с учетом волатильности цифровых активов и методов их оценки;
- компенсация морального вреда при нарушении цифровой репутации и персональных данных;
- судебные запреты на основе технических возможностей блокирования транзакций;
- защита от недобросовестной конкуренции в сфере токенизации и протоколов DeFi.

Особенностью защиты цифровых активов является широкое использование технологических механизмов защиты. Смарт-контракты позволяют автоматизировать исполнение соглашений и предотвращать определенные виды нарушений, мультиподписные кошельки обеспечивают коллективный контроль над активами, а time-lock механизмы предотвращают несанкционированные транзакции. Развиваются также механизмы децентрализованного арбитража, такие как Kleros и Aragon Court, которые используют криптоэкономические стимулы для разрешения споров без участия традиционных судебных органов.

Международный коммерческий арбитраж становится предпочтительным способом разрешения споров, связанных с цифровыми активами, благодаря своей гибкости и специализации. Сингапурский международный арбитражный центр (SIAC) разработал специальные правила для криптоспоров, а Лондонский международный арбитражный суд (LCIA) создал экспертную панель по блокчейн-технологиям. Преимуществами арбитража в данной сфере являются конфиденциальность разбирательства, возможность выбора арбитров с техническими компетенциями и признание решений в рамках Нью-Йоркской конвенции 1958 года.

Трансграничный характер цифровых активов создает существенные проблемы для определения применимого права и юрисдикции. Децентрализованные сети «не имеют географической привязки, что создает коллизии между различными правовыми системами» [1]. Показательным является дело Do Kwon (Terraform Labs), где одновременно расследования ведут США, Южная Корея и Сингапур, что приводит к конфликту юрисдикций и различным правовым оценкам одних и тех же действий. Европейский союз пытается решить эту проблему через регулирование Markets in Crypto-Assets (MiCA), которое устанавливает единые правила для 27 стран ЕС, но вопросы взаимодействия с третьими странами остаются открытыми. [6]

Правоприменительная практика выявляет серьезные пробелы в механизмах защиты цифровых активов. Типичным примером является сложность возврата украденных криптоактивов: в отличие от традиционных банковских переводов, блокчейн-транзакции необратимы, что делает неэффективными традиционные способы защиты. Дело FTX/Alameda Research показало недостаточность существующих механизмов корпоративного управления для криптобирж: потери клиентских средств в размере 8 млрд долларов стали возможными из-за отсутствия надлежащего разделения активов и контроля рисков. Восстановление активов в таких случаях осложняется международным характером операций и использованием криптосмешивающих сервисов.

Для решения проблем правовой неопределенности многие юрисдикции внедряют «регуляторные sandbox –

экспериментальные правовые режимы для тестирования инновационных финансовых продуктов. Великобритания в 2024 году запустила Digital Securities Sandbox (DSS) – первую инфраструктуру финансового рынка, созданную в рамках полномочий Financial Services and Markets Act 2023» [3]. Аналогичные инициативы реализуются в Сингапуре через Project Guardian и в Швейцарии через DLT Act, что позволяет компаниям тестировать новые продукты в контролируемой среде с временными послаблениями регуляторных требований.

Анализ существующих механизмов защиты выявляет их системные недостатки. Во-первых, традиционные способы защиты, разработанные для материальных объектов, неадекватны специфике цифровых активов: невозможность физического изъятия, мгновенность и необратимость транзакций, глобальный характер операций. Во-вторых, технологические способы защиты (смарт-контракты, мультиподпись) имеют ограниченную эффективность из-за уязвимостей в коде и возможности социальной инженерии. В-третьих, отсутствие унифицированных международных стандартов создает регуляторный арбитраж и затрудняет трансграничное правоприменение. [7]

На основе анализа международного опыта и выявленных проблем представляется целесообразным внедрение следующих механизмов правовой защиты новых объектов гражданских прав:

1. Создание специализированной правовой категории для цифровых активов по образцу британского Property (Digital Assets etc) Bill, что обеспечит правовую определенность без необходимости кардинального пересмотра существующих институтов собственности.

2. Внедрение технологически нейтрального регулирования, которое фокусируется на функциях и рисках, а не на конкретных технологиях, что обеспечит адаптируемость к будущим инновациям.

3. Развитие гибридных механизмов защиты, сочетающих правовые и технологические инструменты: использование оракулов для связывания смарт-контрактов с правовыми решениями, внедрение механизмов технического арбитража с правовой силой.

Эффективная защита цифровых активов невозможна без международной координации. Перспективным представляется создание многосторонних соглашений по аналогии с Гаагской конвенцией о международном похищении детей, но адаптированных для цифровых активов [10]. Такие соглашения должны включать механизмы взаимного признания судебных решений, процедуры трансграничного замораживания активов и стандарты доказательства права собственности на цифровые активы. Первые шаги в этом направлении делает Financial Action Task Force (FATF), разработавшая стандарты для криптосервисов, однако этого недостаточно для комплексного решения проблемы. [9]

Защита новых объектов гражданских прав находится на стадии активного формирования, что создает как возможности, так и риски для правовых систем. Опыт 2024 года показывает, что наиболее успешными являются юрисдикции, которые сочетают правовые инновации с технологической экспертизой и международным сотрудничеством. Для Республики Узбекистан критически важно не отставать от этих тенденций, поскольку промедление в регулировании может привести к оттоку инновационных проектов и инвестиций в более прогрессивные юрисдикции. Вместе с тем поспешное регулирование без учета международного опыта и технологических особенностей может затормозить развитие цифровой экономики, что делает необходимым сбалансированный подход, основанный на глубоком анализе зарубежного опыта и активном взаимодействии с международными экспертными сообществами.

Финансирование. Научная статья подготовлена в рамках программно-целевого финансирования по научным и (или) научно-техническим программам на 2025-2027 годы, направленная на реализацию проекта ИРН BR28713695 «Теоретические и методологические основы сотрудничества семьи и общества по проблемам насилия в отношении женщин и девочек-подростков», финансируемого Комитетом науки Министерства науки и высшего образования Республики Казахстан.

Список использованных источников

1. Law Commission. Digital assets – Law Commission Report. 2023.
2. Property (Digital Assets etc) Bill. UK Parliament. 2024.
3. Norton Rose Fulbright. 2024 FinTech Outlook. 2024.
4. Law Commission. Digital assets – Law Commission Report. 2023.
5. Fairfield J. Virtual Property // Boston University Law Review. 2005. Vol. 85. P. 1047; Indiana Legal Studies Research Paper No. 35.
6. Walch A. The Path of the Blockchain Lexicon (and the Law) // Review of Banking & Financial Law, 2017, March 24. No. 713. P. 36.
7. Никитенко С.В. Концепции правосубъектности искусственного интеллекта // Научные междисциплинарные исследования. 2020. № 2-2. URL: <https://cyberleninka.ru/article/n/kontseptsii-pravosubektnosti-iskusstvennogo-intellekta> (дата обращения: 31.03.2025).
8. Савельев В.А. Проблема разделенной собственности и современная теория российского гражданского права // Журнал российского права. 2008. № 4(136). URL: <https://cyberleninka.ru/article/n/problema-razdelennoy-sobstvennosti-i-sovremennaya-teoriya-rossiyskogo-grazhdanskogo-prava> (дата обращения: 31.03.2025).
9. Панин В.В. Развитие научных представлений о собственности в экономической теории // ОНВ. 2006. № 10(49). URL: <https://cyberleninka.ru/article/n/razvitie-nauchnyh-predstavleniy-o-sobstvennosti-v-ekonomicheskoy-teorii> (дата обращения: 31.03.2025).
10. Банакас С., Петров Д.А., Попондопуло В.Ф., Силина Е.В. Цифровые отношения как предмет правового исследования // Вестник Санкт-Петербургского университета. 2023. С. 492–509. DOI: 10.21638/spbu14.2023.213.

Петрова А.

*Магистрант 1 курса специальности «Юриспруденция»
Университет «Narxoz»*

АЛГОРИТМИЧЕСКИЕ ДОКАЗАТЕЛЬСТВА В СУДЕБНОМ ПРОЦЕССЕ: ПРАВОВЫЕ РИСКИ И ПЕРСПЕКТИВЫ РЕГУЛИРОВАНИЯ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Данная исследование посвящено правовым проблемам использования алгоритмических доказательств, формируемых с применением технологий искусственного интеллекта и обработки больших данных, в условиях цифровизации судебной системы. Особое внимание уделяется вопросам их допустимости,

относимости, достоверности и процессуальной проверяемости в уголовном и гражданском судопроизводстве. В работе анализируется современное состояние правового регулирования в Республике Казахстан, выявляются пробелы в процессуальном законодательстве, связанные с отсутствием специальных норм, определяющих правовой статус и порядок использования результатов, формируемых алгоритмическими системами. Подчеркиваются правовые риски, возникающие при включении таких данных в доказательственную базу, включая неопределенность критериев их оценки и сложности процессуальной верификации. Проводится сравнительно-правовой анализ подходов Европейского союза, основанных на риск-ориентированной модели регулирования искусственного интеллекта. Формулируются предложения по совершенствованию национального законодательства, направленные на обеспечение правовой определенности, процессуальной надежности и надлежащей оценки алгоритмических доказательств в судебном процессе.

Современное развитие информационно-коммуникационных технологий сопровождается последовательной и масштабной цифровизацией государственных и общественных институтов, включая систему правосудия, деятельность правоохранительных органов и механизмы государственного управления. Конституционно-правовые основы функционирования государственной власти в условиях цифровой трансформации опираются на общие положения Основного закона Республики Казахстан, закрепляющего принципы правового государства и верховенства права [1]. Дальнейшее развитие процессуальной среды осуществляется в рамках уголовно-процессуального регулирования, которое определяет базовые требования к допустимости и оценке доказательств в судебном процессе [2]. В условиях цифровизации значительное влияние на формирование доказательственной базы оказывает развитие цифровых данных и алгоритмических технологий, что также отражено в нормах цифрового законодательства, регулирующего обработку и использование информации в электронной форме [5]. Особую роль

в трансформации правовой системы играет внедрение технологий искусственного интеллекта и автоматизированной обработки данных, которые постепенно интегрируются в правоприменительную практику. При этом уголовное законодательство устанавливает общие рамки правовой оценки деяний, совершенных с использованием цифровых технологий и информационных систем, что опосредованно влияет на развитие цифрового доказывания [3]. В целом формирование цифровой среды правосудия осуществляется также в рамках законодательства об информатизации, закрепляющего основы функционирования информационных систем и цифровых платформ в государственном управлении [4]. В совокупности данные нормативные акты формируют институциональную основу цифровой трансформации, в рамках которой технологии искусственного интеллекта и обработки больших данных становятся неотъемлемым элементом современной доказательственной деятельности. Искусственный интеллект представляет собой совокупность алгоритмических методов и моделей машинного обучения, предназначенных для обработки больших массивов информации, выявления закономерностей и формирования аналитических выводов [7; 8]. Такие технологии находят применение при анализе электронных документов, цифровых следов, аудио- и видеоматериалов, а также иных источников информации, используемых в процессе доказывания.

Роль алгоритмических систем в доказательственной деятельности

Применение алгоритмических систем в современной доказательственной деятельности обусловлено общими процессами цифровой трансформации правосудия и направлено на повышение эффективности обработки значительных объемов информации, поступающей в рамках уголовного и гражданского судопроизводства. Использование технологий искусственного интеллекта и методов автоматизированного анализа данных позволяет существенно ускорить проведение первичной обработки доказательственного материала, включая систематизацию электронных документов, анализ цифровых следов, аудио- и

видеоматериалов, а также иных источников информации, имеющих значение для установления обстоятельств дела [5]. С точки зрения процессуального права подобные технологии выступают в качестве инструментов оптимизации доказательственного процесса, позволяя участникам судопроизводства более оперативно выявлять релевантные сведения и формировать предварительные аналитические выводы. При этом их использование не подменяет традиционные процессуальные формы доказывания, закрепленные в уголовно-процессуальном законодательстве Республики Казахстан, включая требования относимости, допустимости и достоверности доказательств [2]. В то же время результаты работы алгоритмических систем все чаще фактически интегрируются в доказательственную базу по делу, оказывая влияние на формирование внутреннего убеждения суда и оценку совокупности доказательств. В этой связи особую актуальность приобретает вопрос правовой квалификации результатов, формируемых с использованием искусственного интеллекта. В научной доктрине отсутствует единообразный подход к определению их процессуальной природы: часть исследователей рассматривает такие результаты как самостоятельный вид цифровых доказательств, обладающих специфической формой выражения и происхождения, в то время как другая позиция исходит из того, что алгоритмические системы следует рассматривать исключительно как техническое средство получения, обработки и интерпретации доказательственной информации [7].

Уголовное и гражданское процессуальное законодательство Республики Казахстан традиционно исходит из классической модели доказательств, предполагающей наличие проверяемого источника информации и возможности его процессуальной верификации [2]. Однако специфика алгоритмически сформированных данных заключается в том, что их происхождение и логика формирования могут быть опосредованы сложными математическими моделями и методами машинного обучения, что усложняет их традиционную процессуальную оценку. Дополнительную сложность представляет отсутствие в действующем законодательстве специальных норм, регулирующих

правовой статус результатов функционирования алгоритмических систем, что фактически оставляет данный вопрос на усмотрение судебной практики. В результате формируется неоднородность подходов к оценке таких данных, что может снижать предсказуемость правоприменения и влиять на единообразие судебных решений. Таким образом, роль алгоритмических систем в доказательственной деятельности следует рассматривать как вспомогательную и инструментальную, однако с выраженной тенденцией к их постепенной институционализации в рамках цифрового правосудия. Это обуславливает необходимость дальнейшего развития правового регулирования, направленного на формирование специальных процессуальных стандартов использования алгоритмических технологий в доказывании, включая вопросы их допустимости, проверяемости и оценки в совокупности с иными доказательствами [3; 5].

Проблематика допустимости и проверяемости алгоритмических доказательств

Одной из ключевых проблем внедрения алгоритмических систем в доказательственную деятельность является их соответствие фундаментальным требованиям доказательственного права. В уголовном и гражданском процессе Республики Казахстан к таким требованиям традиционно относятся относимость, допустимость, достоверность, а также возможность процессуальной проверки и оценки доказательств в их совокупности [2; 3]. В условиях цифровизации данные критерии приобретают повышенную значимость, поскольку именно они обеспечивают баланс между технологическими возможностями обработки информации и процессуальными гарантиями участников судопроизводства. Существенные трудности возникают при оценке доказательств, сформированных с использованием искусственного интеллекта и алгоритмических систем, поскольку их происхождение связано с применением сложных математических моделей, методов машинного обучения и анализа больших массивов данных [7; 8]. Это объективно затрудняет установление прямой и однозначной связи между исходной информацией и конечным результатом, представляемым в суде. Особую проблему

представляет вопрос процессуальной проверяемости таких данных. В классической модели доказывания суд должен иметь возможность установить источник доказательства, условия его получения и механизм формирования. Однако в случае алгоритмических систем значительная часть обработки информации осуществляется автоматически, что усложняет воспроизведение логики получения результата в традиционном процессуальном понимании. Дополнительную сложность создает феномен алгоритмической непрозрачности, при котором внутренняя логика формирования результата может быть недоступна для полного анализа участниками процесса и даже специалистами, осуществляющими его оценку. В результате ограничивается возможность полноценной процессуальной верификации доказательственной информации, что непосредственно влияет на ее оценку судом [5]. Данные обстоятельства могут оказывать влияние на реализацию принципов уголовного и гражданского судопроизводства, включая состязательность сторон, равноправие участников процесса и обеспечение справедливого судебного разбирательства, закрепленных в процессуальном законодательстве Республики Казахстан [1; 2]. Кроме того, отсутствие единых методологических подходов к оценке алгоритмически сформированных данных усиливает неопределенность в правоприменительной практике. В аналогичных ситуациях суды могут приходить к различным выводам относительно допустимости и достоверности таких доказательств, что снижает предсказуемость судебных решений и единообразие правоприменения. Отдельного внимания заслуживает вопрос качества исходных данных, используемых при формировании алгоритмических моделей. Неполнота, искажения или нерепрезентативность обучающих выборок способны существенно повлиять на конечные результаты анализа и привести к снижению их достоверности [6]. В тесной связи с этим находится проблема алгоритмической предвзятости, проявляющаяся в воспроизведении или усилении существующих статистических либо социальных искажений, содержащихся в данных или структуре модели [6]. В совокупности указанные проблемы свидетельствуют о необходимости разработки специальных

процессуальных стандартов оценки цифровых и алгоритмических доказательств, адаптированных к условиям современной цифровой трансформации судебной системы.

Международная судебная практика и эволюция подходов к оценке алгоритмических доказательств

В последние годы судебная практика различных государств демонстрирует устойчивую тенденцию к признанию цифровых и алгоритмически сформированных данных в качестве допустимых доказательств при условии соблюдения требований их достоверности, относимости и процессуальной проверяемости. При этом ключевой проблемой остается адаптация традиционных правил доказывания к новым формам информации, формируемым с использованием технологий искусственного интеллекта и автоматизированных систем анализа данных. В правовом порядке Соединенных Штатов Америки значительное развитие получила практика применения цифровых доказательств, включая данные, полученные с использованием алгоритмов анализа и автоматизированных систем обработки информации. В ряде судебных решений американские суды исходят из того, что допустимость таких доказательств определяется через общие критерии надежности методологии, воспроизводимости результатов и возможности их процессуальной проверки в рамках установленных стандартов доказательственного права (в частности, стандартов Daubert) [7]. При этом суды уделяют особое внимание вопросу верификации алгоритмически полученных данных и возможности их оспаривания сторонами процесса. В государствах Европейского союза формируется более централизованный и нормативно детализированный подход к оценке цифровых доказательств, что связано с развитием регулирования в сфере искусственного интеллекта и цифровых данных. Практика Суда Европейского союза и национальных судов государств-членов показывает, что при оценке цифровых доказательств особое значение придается принципам прозрачности, контролируемости и соблюдения прав человека в процессе обработки данных [4]. Например, в делах, связанных с использованием данных массового цифрового мониторинга и зашифрованных коммуникаций, суды ЕС

допускают использование цифровых доказательств при условии соблюдения процессуальных гарантий и возможности их последующей судебной проверки. Отдельного внимания заслуживает развитие подходов Европейского суда по правам человека, который в своей практике подчеркивает необходимость обеспечения справедливого судебного разбирательства при использовании технически сложных доказательств, включая данные, полученные с применением автоматизированных систем. В частности, акцент делается на соблюдении принципа «равенства оружия» и возможности сторон оспаривать представленные доказательства, независимо от их технической природы [1]. Сравнительный анализ показывает, что как в США, так и в Европейском союзе формируется единый вектор развития доказательственного права, направленный на интеграцию цифровых и алгоритмических данных в традиционную систему доказательств при одновременном усилении процессуальных гарантий их проверки. В этом контексте международная практика оказывает значительное влияние на формирование новых стандартов допустимости цифровых доказательств, которые постепенно трансформируют классическую модель доказательственного процесса. Дополнительно следует отметить, что развитие цифровых доказательств в международной практике сопровождается постепенной выработкой единых подходов к их процессуальной оценке, основанных на сочетании технической проверяемости и правовых гарантий справедливого судебного разбирательства. В ряде государств усиливается тенденция к признанию алгоритмически обработанных данных допустимыми доказательствами при условии соблюдения требований их достоверности, воспроизводимости и возможности независимой экспертной проверки. Особое значение при этом приобретает подход, согласно которому цифровые и алгоритмические доказательства не рассматриваются как абсолютно автономный вид доказательств, а оцениваются в совокупности с традиционными доказательственными средствами. Такой подход позволяет снизить процессуальные риски, связанные с использованием сложных технологических систем, и обеспечить баланс между

инновационным развитием правосудия и сохранением классических принципов доказательственного права. Сравнительный анализ показывает, что международная практика постепенно смещается в сторону интеграции цифровых доказательств в традиционную доказательственную систему при одновременном усилении требований к их проверяемости и прозрачности. Это формирует основу для дальнейшей гармонизации национальных правовых систем и выработки единых стандартов оценки алгоритмически сформированных данных. В этих условиях особую актуальность приобретает необходимость адаптации национального законодательства к международным тенденциям цифрового правосудия, включая внедрение специальных процессуальных механизмов оценки и контроля цифровых доказательств, полученных с использованием технологий искусственного интеллекта.

Перспективы развития правового регулирования алгоритмических доказательств в Республике Казахстан

Современное развитие цифровых технологий и расширение использования алгоритмических систем в судебной и правоохранительной деятельности актуализируют необходимость формирования комплексного правового регулирования доказательств, полученных с применением искусственного интеллекта. Существующая нормативная база Республики Казахстан, включающая положения Конституции, уголовно-процессуального законодательства, а также законодательства о цифровизации и информатизации, создает общие основы регулирования цифровой среды, однако не формирует специализированных процессуальных механизмов оценки алгоритмически сформированных доказательств [1; 2; 4; 5]. В этих условиях перспективным направлением развития правовой системы является институционализация цифровых и алгоритмических доказательств как самостоятельной категории доказательственной информации. Такая институционализация предполагает не только закрепление их правового статуса, но и формирование специальных процессуальных требований к их получению, проверке и оценке в рамках уголовного и гражданского судопроизводства. Особое

значение приобретает необходимость нормативного определения критериев допустимости и относимости подобных доказательств, а также установления процедур их процессуальной верификации [2].

Важным направлением совершенствования законодательства выступает внедрение принципа технологической прозрачности и объяснимости алгоритмических систем, используемых в доказательственной деятельности. Несмотря на то что действующее законодательство не содержит прямого закрепления данных принципов, их внедрение представляется необходимым условием обеспечения процессуальных гарантий участников судопроизводства и реализации принципов состязательности и равноправия сторон [1]. Дополнительно целесообразным является развитие института специализированной цифровой экспертизы, направленной на оценку алгоритмов и моделей искусственного интеллекта, используемых при формировании доказательственной информации. Такая экспертиза должна обеспечивать проверку корректности функционирования алгоритмических систем, а также оценку достоверности полученных с их помощью результатов, что позволит повысить уровень доверия к цифровым доказательствам в судебной практике [6]. Сравнительно-правовой анализ показывает, что международные правовые порядки постепенно движутся в сторону усиления регуляторных требований к использованию искусственного интеллекта в юридически значимых процессах, включая судебную деятельность. В частности, подход Европейского союза, основанный на риск-ориентированной модели регулирования, демонстрирует необходимость сочетания технологического развития с усилением процессуальных гарантий и механизмов контроля за алгоритмическими системами [4]. В долгосрочной перспективе развитие национального законодательства Республики Казахстан в данной сфере должно быть направлено на формирование устойчивой правовой модели цифрового правосудия, в которой алгоритмические доказательства займут институционально определенное место, а их использование будет сопровождаться четкими процессуальными гарантиями, обеспечивающими баланс между эффективностью правосудия и защитой прав участников судебного процесса.

Проведенное исследование показывает, что внедрение алгоритмических систем и технологий искусственного интеллекта в доказательственную деятельность является закономерным этапом цифровой трансформации судебной системы Республики Казахстан. Развитие цифровых технологий расширяет технические возможности получения и обработки доказательственной информации [2; 5]. Вместе с тем правовое регулирование остается фрагментарным и не учитывает специфику алгоритмически сформированных данных. Действующее процессуальное законодательство продолжает опираться на традиционную модель доказательств, что создает правовую неопределенность при их оценке в судебной практике [2]. Основные проблемы связаны с отсутствием единых критериев оценки, сложностью верификации и недостаточной определенностью правового статуса таких данных, что усиливает зависимость от судебного усмотрения и снижает единообразие практики [3]. В Европейском союзе формируется более детализированный риск-ориентированный подход, основанный на принципах прозрачности, документируемости и контролируемости алгоритмических систем [4]. Этот опыт может быть использован для дальнейшего совершенствования национального регулирования. Перспективным направлением является разработка специальных процессуальных норм, закрепляющих статус алгоритмических доказательств, условия их допустимости и стандарты оценки [1; 3]. В целом дальнейшее развитие института цифровых и алгоритмических доказательств должно быть направлено на обеспечение баланса между технологической эффективностью и соблюдением фундаментальных принципов справедливого судебного разбирательства, закрепленных в правовой системе Республики Казахстан.

Список использованных источников

1. Конституция Республики Казахстан (от 30 августа 1995 года, с изменениями и дополнениями по состоянию на 19.09.2022 г.;
2. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V ЗРК (с изменениями и дополнениями).

3. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК (с изменениями и дополнениями).
4. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК.
5. Цифровой кодекс Республики Казахстан от 9 января 2026 года № 255-VIII.
6. Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings (E-Evidence Regulation).
7. Russell S., Norvig P. *Artificial Intelligence: A Modern Approach*. - Pearson, 2021.
8. Goodfellow I., Bengio Y., Courville A. *Deep Learning*. - Cambridge: MIT Press, 2016.
9. European Commission. *Artificial Intelligence Act (AI Regulation Framework)*. - 2024.

Рузиназаров Ш.Н.

*Доктор юридических наук, профессор,
академик Туранской академии наук
<https://orcid.org/0000-0001-8550-9276>
E-mail: sh.ruzinazarov@mail.ru*

ПАРАДИГМА ЧАСТНОГО ПРАВА В ЦИФРОВУЮ ЭПОХУ: СООТНОШЕНИЕ ЦИФРОВОГО И ГРАЖДАНСКОГО ПРАВА

Статья посвящена исследованию трансформации парадигмы частного права в условиях цифровизации общественных отношений и развитию концептуальных подходов к определению места цифрового права в современной правовой системе. Рассматриваются теоретические и практические проблемы соотношения цифрового и гражданского права, анализируются существующие научные подходы к пониманию цифрового права как самостоятельной отрасли, комплексного правового института либо составной части частного права. Особое внимание уделяется влиянию цифровых технологий, искусственного интеллекта, цифровых платформ, смарт-контрактов, цифровых активов и технологий распределенного реестра на содержание гражданско-

правовых отношений, а также трансформации традиционных институтов договорного, обязательственного и вещного права. На основе сравнительно-правового анализа международного опыта и современных тенденций развития законодательства обосновывается вывод о том, что цифровое право не подменяет гражданское право, а представляет собой новый этап его эволюции, обусловленный цифровой трансформацией экономики и общества. Предлагаются концептуальные направления совершенствования частноправового регулирования, предусматривающие модернизацию гражданского законодательства, формирование единых принципов регулирования цифровых правоотношений и обеспечение баланса между инновациями, автономией воли участников гражданского оборота и эффективной защитой их прав в цифровой среде.

В настоящее время одними из важных факторов, изменяющих фундаментальные устои во всех сферах жизни общества, выступают процессы, обозначаемые термином «цифровизация». Внедрение современных цифровых технологий происходит в том числе и в частно- правовую сферу. Цифровая трансформация двояко воздействует на систему права. С одной стороны, информационно-коммуникационные технологии проникают в сферу правового регулирования, тем самым информатизируя право, с другой стороны - прогрессирование в целом правовой системы государства способствует как развитию существующих в системе права отраслей права, так и, возможно, формированию новой отрасли-цифрового права. В данном контексте одной из важных проблем мировых правовых систем являются изучение парадигма частного права в цифровую эпоху. В настоящее время право и цифровые технологии стали не только объектом фундаментальных исследований, но и сферой законодательства, учебной дисциплиной и областью правоприменительной практики. Генезис цифровизации общественных отношений уходит в глубокую историю - к эпохе Восточного Возрождения, в частности к научному учению Аль-Хорезми об алгоритмах. Сущность современной реальности заключается в том, что право невозможно представить без цифровых технологий [1]. Учение Аль-Хорезми об алгоритмах является фундаментальной гносеологической основой

формирования цифрового государства и права. Особенно важно, что алгоритмы играют ключевую роль в трансформации современной правовой системы и являются важнейшим ресурсом науки и технологий.

Самое главное соотношение цифрового и гражданского права имеет важное научно-практическое значение. Несмотря на то, что понятие “цифровое право” отсутствует в законодательстве Республики Узбекистан, и практически отсутствуют научные и прикладные исследования в данной сфере, данный термин иногда встречается в ряде исследований ученых-юристов [2]. Цифровые права - права человека, заключающиеся в праве людей на доступ, использование, создание и публикацию цифровых произведений, доступ и использование компьютеров и иных электронных устройств, а также коммуникационных сетей, в частности, к сети интернет [3]. Так, А. А. Карцхия, выделяя цифровое право в качестве самостоятельной отрасли, мотивирует это тем, что широко используемые цифровые технологии обусловили формирование отдельной отрасли права, которая «автономно регулирует общественные отношения в сфере цифровизации вне зависимости от иных отраслей, используя свои способы регулирования процессов жизненного цикла в экономике, политике, праве, в предпринимательских правоотношениях» [4]. В этом усматривается весьма прагматичный западный подход, базирующийся на представлении о необходимости специального регулирования системы общественных отношений в определенной сфере «в силу того, что они встречаются в практике с констатируемой частотой» [5]. этой связи нельзя не вспомнить Н. К. Ренненкампа, который отмечал: «Не должно думать, что система права может быть вполне законченной и постоянной: каждое время и государства понимают по-своему значение, границы и соотношение частей права» [6]. Наконец, нельзя не признать, что некоторые правоотношения существуют только в условиях особой цифровой среды, которая заметно видоизменяет характер взаимодействия их участников, иногда фактически создавая новую реальность, для которой характерны «бесконечное существование; синхронизация с реальностью; отсутствие ограничений по количеству одновременно

подключившихся пользователей; собственная полноценно функционирующая экономика; интеграция цифрового и реального мира, публичные и частные платформы, частные и общедоступные сети; беспрецедентная совместимость данных, контента, активов, предметов, которые можно передавать между виртуальными мирами (трансплатформенность); наполненность контентом и опытом широкого круга пользователей в виде индивидуальных или коллективных участников» [7]. Очевидно, что это обстоятельство не может долго игнорироваться ни законодателем, ни правоприменителем. Причем подобная трансформация правоотношений отмечается достаточно давно и изначально связывалась с развитием Интернета, что обусловило появление категорий «интернет-право» [8], «киберправо» и «сетевое право» [9]. Позднее стали говорить о платформенном праве [10] и праве цифровых технологий [11]. Фактически все они используются как синоним цифрового права и базируются на смешении традиционных и «новых правовых институтов и положений, появившихся и развившихся именно в связи с Интернетом», что объективно поднимает вопрос о месте соответствующих правовых норм в системе права. Ряд ученых считают, что цифровое право должно выступать в качестве подотрасли информационного права [12], в том числе вследствие того, что «цифровые права, регулируемые в Гражданском кодексе РФ, можно считать частным случаем информационно-коммуникативных прав» [14]. Из этого очевидного факта в доктрине выводятся два принципиально разных положения. Одно из них, базируясь на представлении о том, что новая форма не меняет содержания, заключается в том, что цифровые отношения могут иметь различную отраслевую принадлежность, а следовательно, оснований для выделения цифрового права как отрасли нет [15]. В то же время неоднородность правоотношений дает основание говорить о комплексном характере цифрового права. И если одни ученые видят в подобном подходе решение проблемы отраслевого деления, то другие опасаются стирания границ между публичным и частным правом [16]. Проблема заключается в неоднозначной оценке самой идеи существования комплексных отраслей, высказанной В. К.

Райхером и поддержанной рядом ученых [17]. До сих пор диапазон мнений варьируется от оценки данной категории как плодотворной до ее отрицания как неоправданного подхода, недоразумения, способствующего «размыванию» системы права, а также ведущего к путанице понятий, усложнению и без того сложных проблем [18]. Термин «международное цифровое право» в российской международно-правовой литературе и в официальных нормативных актах пока не встречается. Нет его и в международных договорах, в актах международных организаций, в научных работах зарубежных юристов-международников [19].

Определенная компетенция относительно вопросов цифровой проблематики имеется у некоторых –многих– международных организаций: ООН, ЮНЕСКО, ВОИС, ВТО, ЮНСИТРАЛ, ОБСЕ, ОЭСР и др. В рамках ВОИС, например, осуществляется управление двумя десятками соглашений, связанных с авторским и патентным правом, статусом фонограмм, компьютерных программ и т. д.

В рамках ЕС принимаются соответствующие директивы:

Директива ЕС 2018/1673 о борьбе с отмыванием денег и т. п. Борьбой с использованием в преступных целях цифровых технологий на международном уровне озабочены и разнообразные параорганизации: Группа-7, БРИКС и другие, – принимающие рекомендательные и декларативные акты. Группа-7, например, приняла Декларацию об ответственном поведении государств в киберпространстве (2017); на совещании министров иностранных дел Г-7 было принято «Динарское заявление об инициативе за нормы в киберпространстве» (2019).

Многие акты, касающиеся цифровой сферы, принимаются на разного рода частных конференциях: так, известные и авторитетные «Азиломарские принципы» были приняты в США на международной конференции разработчиков программ искусственного интеллекта (2017). Подобного рода акты не являются правовыми, но оказывают постепенное воздействие на международное правосознание, благодаря которому впоследствии формулируются и продвигаются нормы национального или международного права. В рамках Комиссии ООН по праву международной торговли –ЮНСИТРАЛ– приняты Типовые

законы: об электронной торговле (1996); об электронных подписях (2001). В рамках СНГ принят «Модельный закон об основах регулирования Интернета» (2011). Эти факты показывают пример еще одного правового инструмента регулирования цифровой среды: через разработанные типовые законы для внутренних правовых систем государств происходит постепенная унификация национальных законодательств в том или ином вопросе.

Цифровое право является новой комплексной отраслью права, обладающей собственным предметом правового регулирования. Следовательно, цифровое право представляет собой совокупность межотраслевых правовых институтов. Оно выступает как система общеобязательных, формально определенных и гарантированных государством норм, регулирующих общественные отношения, возникающие при использовании цифровых данных и цифровых технологий. Механизм правового регулирования общественных отношений в цифровой среде, прежде всего, связан с их информационной природой и проявляется в цифровой форме - в виде действий с цифровыми данными и связанной с ними информацией.

Предмет цифрового права включает, *во-первых*, общественные отношения, возникающие при поиске, получении, представлении, распространении информации, а также при реализации иных субъективных цифровых прав, связанных с данными в цифровой форме и цифровыми технологиями. *Во-вторых*, он охватывает цифровые отношения, возникающие в процессе указанных действий с использованием цифровых технологий, а также связанные с ними отношения по реализации субъективных цифровых прав. В зарубежных странах цифровое право уже признано в качестве учебной дисциплины, что требует определения его места в национальной правовой системе. В условиях цифровой трансформации образования особое значение приобретает повышение эффективности преподавания юридических дисциплин, включая цифровое право. Одной из актуальных задач является формирование теории и методики преподавания данной новой комплексной отрасли. Цифровое право - это одна из самых современных отраслей права. В мире все более отчетливо

проявляется регулирование отношений, связанных с информационно-коммуникационными технологиями. Цифровой суверенитет и цифровая безопасность становятся неотъемлемыми атрибутами государства и признаками его независимости. Цифровизация изменяет содержание правового регулирования гражданско-правовых отношений и способствует появлению новых отраслей права, обусловленных потребностями виртуальной реальности. В связи с этим возникает необходимость анализа современных тенденций внедрения ИКТ в гражданское право и создания соответствующей законодательной базы. Цифровые технологии вносят новые изменения в правовую природу гражданского оборота. Понимание социальной роли цифрового права становится объективной необходимостью для эффективного регулирования таких отношений. Цифровое право регулирует отношения, возникающие при использовании цифровых технологий, и включает нормы, обеспечивающие передачу, обработку и распространение информации, а также реализацию субъективных прав в цифровой среде.

Анализ научных источников позволяет выделить несколько подходов: Согласно *первому*, цифровое право не является самостоятельной отраслью из-за недостаточной разработанности доктринальной и законодательной базы.

Второй подход признает возможность формирования новой отрасли права на основе существующих нормативных актов.

Третий подход подчеркивает роль саморегулирования в цифровой среде и необходимость включения принципов, формируемых цифровыми платформами.

Исходя из этого, цифровое право можно определить как отрасль права, регулируемую общественные отношения, возникающие в цифровой среде при использовании цифровых технологий.

Как научная дисциплина, цифровое право представляет собой совокупность концепций и идей о роли права в процессе цифровизации и трансформации механизмов правового регулирования. В научной литературе также подчеркивается, что цифровое право сталкивается с рядом проблем, связанных с

быстрым развитием цифровой среды. Правовая система зачастую не успевает за технологическими изменениями. Это противоречие может быть преодолено либо созданием принципиально новой правовой системы, либо адаптацией существующих норм. Цифровая реальность охватывает такие объекты, как искусственный интеллект, Big Data, IT-проекты и другие элементы цифровой среды. Среди ученых существуют различные взгляды на регулирование цифровых отношений. Например, М. К. Сулейменов отмечает риски разработки законопроектов технологами без учета правовой системы. Американский футуролог Рэй Курцвейл прогнозирует, что в будущем цифровые технологии кардинально изменят общество, включая автоматизацию труда и трансформацию правовых систем. В то же время подчеркивается, что использование искусственного интеллекта не создает самостоятельных субъектов права - юридические отношения по-прежнему возникают между людьми и организациями.

Следовательно, развитие цифровых технологий приводит к трансформации традиционных гражданско-правовых отношений и формированию новых - цифровых правоотношений. Вопрос о природе цифрового права и его месте в системе права представлен в литературе крайне противоречиво. С одной стороны, утверждается, что цифровизация стирает грани между отраслями, формирует цифровое право как комплексную отрасль или институт права (Р.Б. Головкин); с другой - процесс формирования цифрового права представляет собой цифровизацию права, его отраслей; отношения, составляющие предмет цифрового права, тесно связаны с отношениями, выступающими предметом регулирования иных отраслей права (В.В. Блажеев). Существует также позиция, в соответствии с которой цифровое право - это не особое подразделение в системе права, а цифровая форма частных и публичных общественных отношений, с характерными для них методами регулирования, в том числе и саморегулирования, т.е. цифровая форма традиционных общественных отношений (С. Банакас, Д.А. Петров, Т.Я. Хабриева, Н.Н. Черногор и др.). Ф. Истербрук отрицает самостоятельность киберправа как отрасли, аргументируя это тем, что, во-первых, отсутствует предметное

единство норм; во-вторых, трансграничным характером цифровой среды и возникающей сложностью определения юрисдикции конкретного государства; в-третьих, наличием собственных механизмов принуждения в цифровой среде - методы «свободного рынка» Диаметрально противоположной позиции придерживается профессор Л. Лессиг, который признает существование киберправа, так как существует код, протокол, сетевой стандарт, веб-дизайн как специфические источники («законы»); киберпространство необходимо нуждается в правовом регулировании в новом режиме. Более точным, является понимание *цифрового права как комплексного межотраслевого образования*. Цифровое право состоит из действующих правовых норм, регулирующих отношения, связанные с поиском, получением, передачей, производством и распространением цифровых данных, а также с применением цифровых информационных технологий. Эти нормы находятся в документах разной отраслевой принадлежности. Например, регулирование технологий искусственного интеллекта требует одновременной реализации как норм публичного права для обеспечения безопасности, защиты персональных данных, так и частноправовых норм, направленных на защиту имущественных интересов, интеллектуальных прав, возмещения вреда, как в рамках национальной, так и международной (общей и региональной) правовых систем.

Перспектива цифрового права - в новых формах социального, технического и правового регулирования, а не в адаптации цифровых технологий к правовой среде. Проблема должна решаться на всех типах и уровнях правовых семей и систем. Цифровое право можно рассматривать как искусственно создаваемый социобиотехнический регуляторный механизм, основанный на совокупности набора средств, способов и методов различной природы, который призван упорядочивать, контролировать и развивать отношения в цифровой среде. Кодекс позволит комплексно урегулировать многие институты цифрового права. Стоит отметить формирование самостоятельного предмета цифрового права, включающего отношения, например, по владению, пользованию и распоряжению цифровой

собственностью, цифровыми активами; личные неимущественные права; в сфере медицины, образования; по оптимизации бизнес-процессов; по предупреждению и пресечению нарушений, складывающихся в этой сфере и т.д. Цифровое право обладает специфическим методом правового регулирования, сочетающим императивные (в публичных цифровых институтах, национальных и международных отношений) и диспозитивные (цифровая собственность, регулирование смарт-контрактов) компоненты. В силу специфики цифрового пространства и его постоянного развития нецелесообразно устанавливать жесткие императивные рамки правового регулирования (за исключением вопросов национальной безопасности и безопасности конкретного лица и пр.). Охват публичных и частных институтов обуславливает наличие органически взаимосвязанных способов воздействия: дозволений, предписаний, запретов, рекомендаций, поощрений и других. Представляется обоснованным регулирование общественных отношений в цифровом пространстве посредством так называемого «мягкого права», а также различных форм саморегулирования. Глобальность цифровых технологий говорит о трансграничном характере отношений в данной сфере и выходе за юрисдикцию одного определенного государства. При разграничении юрисдикции в цифровом пространстве возникает проблема применения национальных правовых механизмов за пределами государственных границ, что ограничит право гражданина Республики Узбекистан на поиск и получение информации решением зарубежного органа власти, принятого в зарубежной юрисдикции на основании зарубежных источников права.

Цифровой кодекс является законодательной основой науки и образования в сфере цифрового права. Системный научный и сравнительно-правовой анализ показывает, что готового образца Модельного цифрового кодекса не существует кроме, Цифрового кодекса Республики Киргизстан. В рамках СНГ разработаны основы модельного законодательства. В этой связи научное сообщество, законодатели и правоприменительная практика внимательно следят за законодательными инициативами в данной сфере. Идеи

кодификации законодательства в области цифровизации активно обсуждаются в таких странах, как Россия, Китай, Япония, Индия, Узбекистан, Казахстан, Азербайджан и Молдова. В частности, в Италия в 2005 году был принят аналог цифрового кодекса - Кодекс цифрового управления (Codice dell'Amministrazione Digitale). Во Франция в 2016 году принят Закон «О цифровой республике». В Германия действует Закон «О содействии развитию электронного управления» (2009). В Великобритания в 2017 году принят Закон «О цифровой экономике». В США в 2002 году принят Закон «Об электронном правительстве». Хотя в Китай кодификация цифрового законодательства в строгом смысле не проведена, достигнута его консолидация. В Индия в 2023 году принят Закон «О цифровой Индии». Сингапур является одной из стран-пионеров в сфере цифрового законодательства, где развитие осуществляется через государственные программы. Близким к полной кодификации является Цифровой кодекс Кыргызстан, принятый в 2024 году и вступающий в силу в 2026 году. Аналогичные кодексы разрабатываются в Азербайджан и Казахстан. В связи с этим необходимо не только наблюдать за данным процессом, но и приступить к разработке проекта Цифрового кодекса Узбекистан с привлечением ведущих ученых и экспертов. Процесс разработки цифрового кодекса отличается от традиционных кодексов и требует согласования с действующими нормами. В случае успешной апробации его нормы могут быть включены в систему кодифицированного законодательства.

В мае 2025 года в Узбекистан был представлен проект регулирования онлайн-платформ, включающий элементы европейского законодательства (DSA) и британского закона Online Safety Act.

Анализ зарубежного законодательства показывает, что регулированию подлежат следующие сферы: обработка и защита цифровых данных; защита персональных данных; цифровая трансформация государственного управления; управление ИКТ; телекоммуникации; электронная подпись; информационные ресурсы; цифровые услуги и экосистемы; информационная безопасность; электронная коммерция; искусственный интеллект и

др. Изучение зарубежного опыта позволит эффективно разработать национальный Цифровой кодекс. Унификация цифрового законодательства направлена на гармонизацию правовых норм в сфере цифровых технологий, трансграничного обмена данными, электронной идентификации и электронной подписи. Основная цель - создание единого правового пространства, обеспечивающего свободное обращение цифровых товаров и услуг независимо от границ государств.

Цифровое право представляет собой субъективное гражданское право в отношении цифрового объекта, подтверждаемое записями в информационной системе. В проекте Гражданского кодекса Узбекистан предусматривается закрепление норм о цифровых правах. При формировании образовательных стандартов необходимо учитывать предмет, метод и систему цифрового права. Также важно разработать научно-методологическую концепцию цифрового права. В мире уже сформированы различные научные школы в области цифрового права, цифровой экономики и искусственного интеллекта, опыт которых следует использовать.

Целесообразно учитывать Модельный закон «О цифровых правах», принятый Межпарламентской Ассамблеей СНГ 14 апреля 2023 года № 55-12, а также тенденции кодификации в развитых странах. Кроме того, важно привлекать мнения зарубежных ученых, экспертных сообществ и университетов, а также учитывать позиции национальных заинтересованных организаций. Разработка научно обоснованной концепции цифрового права станет важной основой для формирования квалификационных требований и образовательных стандартов в данной сфере.

Цифровая трансформация общественных отношений обуславливает необходимость системного обновления частноправового регулирования и, прежде всего, переосмысления роли Гражданского кодекса Республики Узбекистан как основного кодифицированного акта частного права. В этих условиях принципиальное значение приобретает вопрос о том, должна ли цифровизация осуществляться посредством формирования автономного массива «цифрового права» либо преимущественно

посредством последовательной адаптации и развития гражданско-правовых конструкций.

Для Республики Узбекистан данный вопрос необходимо рассматривать с учетом принадлежности национальной правовой системы к романо-германской правовой традиции, для которой характерны верховенство закона, кодификация, системность отраслевого регулирования, нормативная определенность и иерархическая взаимосвязь источников права. В такой системе кодекс выполняет не только функцию систематизации законодательства, но и формирует внутреннюю архитектуру соответствующей отрасли права. Поэтому цифровая трансформация частного права не должна приводить к разрушению его кодификационного ядра и возникновению параллельных, конкурирующих систем регулирования. В связи с этим методологически обоснованным представляется исходить из положения о том, что цифровизация частного права представляет собой не замещение гражданского права цифровым правом, а его функциональную трансформацию применительно к цифровой среде. Изменению подвергаются прежде всего способы реализации гражданских прав и обязанностей, формы заключения и исполнения сделок, юридическая фиксация фактов, характеристики отдельных объектов гражданских прав и механизмы защиты нарушенных прав. При этом фундаментальные начала гражданского права - равенство участников, автономия воли, свобода договора, имущественная самостоятельность, добросовестность и судебная защита - сохраняют свое системообразующее значение. Именно поэтому Гражданский кодекс должен рассматриваться как нормативное ядро цифровой трансформации частного права, а специальные цифровые нормы - как его функциональное развитие и конкретизация.

Кодификационная природа Гражданского кодекса предполагает не простое объединение отдельных норм, а их концептуальное и системное согласование. Поэтому внесение цифровых положений в гражданское законодательство должно осуществляться с учетом внутренней структуры Кодекса, единства понятийного аппарата и взаимосвязи общих и специальных норм. Уже сложившаяся практика цифровизации законодательства

Республики Узбекистан показывает необходимость такого подхода. В частности, законодательство об электронной коммерции непосредственно связывает электронные договоры с требованиями Гражданского кодекса, тем самым подтверждая приоритет гражданско-правовой основы над специальным цифровым регулированием. Аналогичным образом электронный документ и электронная цифровая подпись получили юридическое признание посредством специального законодательства, но их использование происходит в общей системе юридически значимых отношений. Следовательно, формирование цифрового частного права должно строиться на принципе кодификационной преемственности: новые цифровые конструкции должны включаться в систему гражданского права без нарушения его фундаментальных категорий. Это требует прежде всего пересмотра тех положений Гражданского кодекса, которые непосредственно связаны с юридическими фактами, формой сделок, объектами гражданских прав, обязательствами, ответственностью и способами защиты гражданских прав. При этом цифровая трансформация не означает, что каждая технологическая конструкция должна получать самостоятельный гражданско-правовой статус. Необходимо разграничивать **технологическую форму и юридическое содержание** соответствующего отношения. Например, электронная форма является способом выражения воли, смарт-контракт - технологическим механизмом автоматизации исполнения договорных условий, а цифровой актив - возможным объектом имущественных отношений. Поэтому юридическая квалификация должна основываться не на названии технологии, а на ее правовой функции. Такой функциональный подход особенно важен для кодифицированного законодательства, поскольку позволяет обеспечить его технологическую устойчивость и избежать чрезмерной зависимости правовых норм от быстро изменяющихся технических решений.

Методологической основой взаимодействия Гражданского кодекса и специального цифрового законодательства должен выступать принцип *lex generalis – lex specialis*. Однако его применение требует определенных ограничений. Гражданский

кодекс выполняет функцию общего регулятора частноправовых отношений, а специальные цифровые нормы применяются к отношениям, специфика которых обусловлена использованием цифровых технологий. При этом специальная норма не должна автоматически вытеснять общую норму гражданского права. Приоритет специального регулирования допустим лишь тогда, когда оно непосредственно охватывает соответствующее отношение и устанавливает специальный правовой режим. Во всех остальных случаях должны применяться общие положения Гражданского кодекса. Таким образом, наиболее рациональной является следующая конструкция: Гражданский кодекс -общая нормативная основа - специальное цифровое регулирование - конкретизация - субсидиарное применение Гражданского кодекса. Это позволяет обеспечить одновременно специализацию регулирования и единство частного права. В данном цивилистическом контексте самостоятельный Цифровой кодекс, если вопрос о его создании ставится законодателем, не должен рассматриваться как автономная альтернатива Гражданскому кодексу. Его нормативное содержание должно быть функционально связано с гражданско-правовыми принципами и институтами. В противном случае существует риск нормативной фрагментации и возникновения коллизий между двумя кодифицированными массивами.

Особое значение в условиях цифровой трансформации приобретает концепция **smart regulation - умного регулирования**. Ее применение к частному праву предполагает изменение самой логики законодательного воздействия: государство должно регулировать не каждую технологическую инновацию, а только те отношения и риски, которые требуют юридического вмешательства. Для гражданского права это особенно важно, поскольку его фундаментальной особенностью является автономия участников оборота. Избыточная императивность способна ограничивать свободу договора, препятствовать появлению новых бизнес-моделей и снижать адаптивность законодательства к технологическим изменениям. В связи с этим smart regulation в сфере частного права следует основывать на нескольких

взаимосвязанных принципах: необходимости, пропорциональности, риск-ориентированности, технологической нейтральности, минимизации регуляторной нагрузки и последующей оценки эффективности регулирования. Следовательно, smart regulation должно рассматриваться как методологический механизм постоянной адаптации Гражданского кодекса к цифровым изменениям, а не как основание для бесконечного увеличения количества специальных нормативных актов.

С точки зрения частноправовой кодификации цифровая трансформация Гражданского кодекса Республики Узбекистан должна концентрироваться на тех институтах, которые непосредственно подвергаются воздействию цифровых технологий. В первую очередь речь идет о совершенствовании положений о сделках и их форме, включая электронное заключение договоров и автоматизированное выражение воли. Вторым направлением является определение правового режима новых цифровых объектов и имущественных прав. Третье направление связано с использованием цифровых технологий при исполнении обязательств, включая автоматизированное исполнение и смарт-контракты. Четвертое - с развитием цифровых способов подтверждения юридически значимых обстоятельств и защиты гражданских прав. При этом цифровая трансформация должна осуществляться не изолированно по каждому институту, а **системно**, поскольку изменение одной гражданско-правовой категории неизбежно влияет на другие элементы правоотношения. Например, признание нового цифрового объекта объектом гражданских прав должно сопровождаться определением его оборотоспособности, способов отчуждения, защиты, наследования и ответственности за нарушение соответствующих прав. Аналогично признание смарт-контракта юридически значимым механизмом требует решения вопросов о выражении воли, действительности сделки, ошибке, нарушении обязательства и способах защиты. Именно поэтому цифровая модернизация должна проводиться посредством **сквозного кодификационного анализа**, а не посредством фрагментарного внесения отдельных цифровых терминов и норм.

Таким образом, для Республики Узбекистан наиболее обоснованной представляется модель цифровой трансформации частного права, основанная на сохранении Гражданского кодекса в качестве системообразующего кодифицированного акта и развитии специального цифрового регулирования в функциональной связи с его принципами и институтами. В рамках романо-германской правовой традиции цифровизация должна обеспечивать не разрушение кодификационной структуры, а ее адаптацию к новым формам гражданского оборота. Основным методологическим ориентиром при этом должны выступать кодификационная системность, единство понятийного аппарата, технологическая нейтральность, функциональная дифференциация общих и специальных норм и принцип *lex generalis – lex specialis*. В свою очередь, *smart regulation* позволяет обеспечить необходимую динамичность цифрового частного права без утраты его правовой определенности. Его значение заключается в том, чтобы специальное регулирование вводилось только при наличии объективной потребности и соответствовало уровню создаваемого цифрового риска. Поэтому цифровая трансформация Гражданского кодекса Республики Узбекистан должна рассматриваться как непрерывный процесс кодификационной адаптации частного права, при котором стабильные фундаментальные категории сохраняются, а способы их реализации приспособляются к цифровой среде. В конечном счете оптимальная модель может быть выражена следующим образом: Гражданский кодекс - кодификационное нормативно-правовая база; цифровое законодательство - специальный функциональный уровень; *smart regulation* - метод их адаптации; технологическая нейтральность - гарантия устойчивости; системность - критерий целостности частного права. Именно такая модель позволяет обеспечить баланс между стабильностью кодифицированного гражданского законодательства и динамикой цифровой экономики, не допуская ни консервации устаревших правовых конструкций, ни чрезмерной фрагментации национального частного права.

Цифровой кодекс должен выступать специализированным продолжением Гражданского кодекса, а не его заменой. Следует

использовать смешанную модель взаимодействия, обеспечивающую баланс между универсальностью и технологической конкретизацией. Необходимо обеспечить системную согласованность и унификацию понятий, чтобы исключить правовые коллизии. Практическая реализация норм Цифрового кодекса должна учитывать опыт зарубежных стран и стран СНГ, в частности концептуальные подходы Киргизии, Азербайджана и Казахстана. Важным является создание методологических основ цифрового права, включающих образовательные стандарты, квалификационные требования и научное сопровождение. Правильное соотношение Гражданского и Цифрового кодексов позволит создать эффективную, гибкую и технологически адаптированную систему частного права, способную регулировать цифровую экономику, электронные услуги и трансграничный оборот цифровых активов. Цифровое право формируется как комплексная межотраслевая система, регулирующая общественные отношения, возникающие в цифровой среде, и требует систематизации на уровне кодифицированного акта. Единого универсального Модельного цифрового кодекса не существует, однако в рамках СНГ уже сформированы модельные правовые основы (Информационный кодекс, модельные законы), что создает предпосылки для национальной кодификации. Зарубежная практика демонстрирует разнообразие подходов: от частичной кодификации и консолидации норм до принятия специализированных цифровых законов (ЕС, Великобритания, США и др.). Кодификация цифрового законодательства является объективной тенденцией, обусловленной ростом цифровых отношений, развитием искусственного интеллекта, платформенной экономики и трансграничного обмена данными. Цифровые правоотношения трансформируют традиционные гражданско-правовые институты, включая сделки, объекты прав, способы их защиты и доказательства. Гражданский кодекс сохраняет базовую (системообразующую) роль, однако он не способен в полном объеме охватить динамику цифровых отношений.

Под цифровизацией, с одной стороны, понимается система перехода процесса подготовки юристов на качественно новую

образовательную платформу, учитывающую процессы цифровизации во всех сферах современного общества; с другой стороны, - система подготовки специалистов в области юриспруденции с широким использованием цифровых технологий, информационных ресурсов и возможностей интернет-пространства. В условиях цифровой трансформации успешность подготовки современных юридических кадров непосредственно связана с рациональным использованием и гармоничным сочетанием в образовательном процессе традиционных и инновационных цифровых технологий, в том числе технологий искусственного интеллекта. Особое значение в юридическом клиническом и дуальном образовании, в частности при преподавании цифрового права, имеют рациональные функции и полномочия преподавателя по контролю за образовательным процессом. Студент юридического высшего образовательного учреждения обязан усваивать знания, в установленные сроки выполнять все учебные занятия, предусмотренные учебным планом и образовательной программой юридического высшего образовательного учреждения, строго соблюдать устав, правила внутреннего распорядка, а также нормы этики и поведения юридического высшего образовательного учреждения.

В процессе преподавания дисциплины «Цифровое право» преподаватель обладает рядом прав в сфере педагогическое мастерство преподавателя, включая осуществление контроля за получением и усвоением студентами знаний; оценивание знаний студентов на семинарских и практических занятиях в соответствии с требованиями модульной системы, исходя из принципов клинического и дуального образования; применение воспитательного и этического воздействия; а при необходимости - инициирование производства по вопросу привлечения студента к дисциплинарной ответственности в соответствии с требованиями правил этики и поведения университета. Во-вторых, в отличие от прошлого, сфера изучения тех или иных дисциплин студентами, обучающимися в области юриспруденции, постоянно расширяется. Если ранее студент получал знания преимущественно из учебников, учебных пособий и соответствующих нормативно-правовых актов,

то с внедрением в образовательный процесс информационно-коммуникационных технологий появилась возможность широко использовать глобальную сеть Интернет, научные статьи на различных иностранных языках, зарубежное законодательство, международно-правовые документы, материалы правоприменительной практики, а также практику международного коммерческого арбитража и третейских судов. В этой связи следует отметить значительный объем работы, проведенной в сфере зарубежных цифровых правовых источников, направленной на то, чтобы студенты могли при минимальных затратах труда получать больше результатов в процессе приобретения и закрепления знаний по цифровому праву, а также формирования соответствующих профессиональных компетенций, умений и навыков. В-третьих, в условиях развития цифровых технологий одной из наиболее заметных проблем совершенствования юридического образования с применением принципов клинического и дуального образования является поиск новых методов и моделей обучения и приобретения профессиональных юридических знаний и навыков. Требуется разработка комплексной инновационной модели профессиональной подготовки и переподготовки юристов на основе клинического и дуального образования. Данная модель должна включать следующие элементы: разработку новых концептуальных и организационно-управленческих подходов к формированию системы профессиональной подготовки юристов на основе принципов клинического и дуального образования с учетом цифрового гражданского оборота и цифровой реальности во всех сферах развития общества; создание новых направлений (специализаций, профилей) юридического образования; качественное обновление содержательных компонентов юридического клинического и дуального образования, прежде всего в направлении развития цифровых компетенций студентов юридических высших образовательных учреждений. Необходимо также предложить и внедрить новые компетенции и сформировать новый стандарт компетентностного подхода, ориентированный на подготовку корпуса юристов, способных осуществлять профессиональную деятельность в сфере правового регулирования

цифровых отношений и функционировать в условиях развитой правовой экосистемы. Профессорско-преподавательский состав, а также учебно-вспомогательные и тьюторские работники должны обладать высоким уровнем подготовки в области осуществления сетевого электронного взаимодействия, создания цифрового контента для онлайн-клинического и дуального образования, оценки и развития предметных компетенций.

В цифровую эпоху очный, дистанционный, виртуальный и интерактивный форматы обучения требуют формирования и использования в образовательном процессе ресурсов цифрового клинического и дуального образования. Необходимо создать качественно новую современную методическую основу организации образовательного процесса на принципах клинического и дуального образования в условиях цифровых технологий. Она должна включать онлайн-курсы и консультации по клиническому и дуальному образованию, гипермедийные учебники открытого доступа, системы тренингов и тестирования, игровые (ролевые) интернет-приложения, системы вопросов и ответов, образовательные чат-боты и другие цифровые инструменты. Вместе с тем при оценке перспектив широкого внедрения цифровых технологий в юридическое клиническое и дуальное образование существует определенный риск, на который обращает внимание ряд специалистов: чрезмерное приоритетное использование цифровых технологий в юридическом клиническом и дуальном образовании может осуществляться за счет классических, традиционных методов обучения. Между тем именно в системе подготовки юристов значение традиционных подходов трудно переоценить. На наш взгляд, именно это является одной из наиболее актуальных проблем современного юридического клинического и дуального образования. Еще одной проблемой системы юридического образования является отсутствие либо недостаточность необходимого количества учебных дисциплин в рамках отдельного раздела профессиональной подготовки, который условно можно назвать «Цифровые технологии в юридической деятельности», в действующих государственных образовательных стандартах. Действующий стандарт клинического и дуального образования

предусматривает лишь отдельные дисциплины, что совершенно недостаточно в условиях цифровизации сферы профессиональной юридической деятельности.

Исходя из этого, можно сделать вывод о том, что совершенствование системы подготовки юристов должно основываться на гармоничном сочетании традиционных методов, способов и средств обучения с современными методами, основанными на эффективном использовании цифровых технологий. Кроме того, в современной системе юридического клинического и дуального образования, использующей потенциал цифровых технологий, существует еще один весьма важный аспект, который ярко проявляется во взаимосвязи юридической науки, юридического образования и юридической практики (деятельности).

В заключение следует отметить, что в условиях цифровой реальности будущие юристы в процессе профессионального обучения в системе юридического клинического и дуального образования должны эффективно использовать соответствующие научные, практические и правовые источники и формироваться как зрелые специалисты, отвечающие требованиям современности.

Цифровые технологии, в том числе технологии искусственного интеллекта, являются важным фактором совершенствования взаимодействия преподавателя и студента в процессе глубокого освоения теоретических и практических знаний, рационального и целенаправленного использования возможностей информационно-коммуникационных технологий. При этом наиболее важным является то, что независимо от того, какие современные инструменты используются в цифровой и технологической среде, подготовка специалистов должна обеспечивать глубокое освоение теоретических и практических знаний и навыков, соответствующих требованиям стандартов юридического клинического и дуального образования. Именно это должно рассматриваться в качестве одного из ключевых факторов подготовки квалифицированного специалиста-юриста, способного эффективно осуществлять профессиональную деятельность в условиях цифровой

трансформации и широкого применения технологий искусственного интеллекта.

В данном контексте тенденции цифровизации всех сфер общественной жизни создают объективные предпосылки для отраслевого обособления цифрового права. Потенциал, заложенный в цифровых технологиях, способен не только существенно трансформировать имеющиеся, но и создать принципиально новые отношения, что не позволяет согласиться с утверждением о том, что их применение обуславливает лишь новую форму их существования. В целом возможность рассмотрения цифрового права в качестве комплексной отрасли права прежде всего связывается: 1) со спецификой составляющих его предмет отношений, возникновение и существование которых невозможно без применения тех или иных цифровых технологий; 2) с особенностями метода их регулирования, характеризующегося сочетанием императивного и диспозитивного регулирования, законодательной регламентации при сохранении значительной роли саморегулирования и необходимости учета специфики национальной юрисдикции в интернет-пространстве; 3) с формированием особой, обусловленной спецификой киберпространства системы принципов построения соответствующих отношений.

Таким образом можно сделать вывод о том, что умная модель развития законодательства заключается не в замене Гражданского кодекса Цифровым, а в их системном сосуществовании, при котором Цифровой кодекс выступает как специализированное продолжение и развитие гражданско-правового регулирования в условиях цифровой трансформации частного права.

Список использованных источников

1. Турдалиев М. П. Правовой понятия и сущности цифровое право в практике Узбекистан и Россия// Oriental Renaissance: Innovative, educational, natural and social sciences (E)ISSN:2181-1784 www.oriens.uz SJIF 2023 = 6.131 / ASI Factor = 1.7 3(1), Jan., 2023 Городов О.А. О месте цифрового права в системе российского права// <https://elibrary.ru/item.asp?id=46255534>

2. Столбова Ю. М. Цифровое право как комплексная отрасль публичного и частного, международного и национального права: дискуссионные проблемы// https://elib.utmn.ru/jspui/bitstream/ru-tsu/35050/1/Lapzgo_2024_350_354.pdf

Саранкина Н.Д. Цифровое право - отрасль, подотрасль или институт права? //Сборник материалов межвузовской научно-практической конференции с международным участием "Юриспруденция 2.0 : новый взгляд на право" Год издания: 2019 Издательство: Изд-во РУДН.

3.Lucchi, Nicola, Access to Network Services and Protection of Constitutional Rights: Recognizing the Essential Role of Internet Access for the Freedom of Expression (February 6, 2011). Cardozo Journal of International and Comparative Law (JICL), Vol. 19, No. 3, 2011, Available at SSRN: <https://ssrn.com/abstract=1756243>

4.Карцхия А. А. Цифровые права и правоприменение // Мониторинг правоприменения. 2019. № 2 (31). С. 45.

5.Талапина Э. В. Сравнительное цифровое право: становление и перспективы // Журнал российского права. 2021. № 9. С. 21.

6.Ренненкампф Н. К. Юридическая энциклопедия. Киев, 1913. С. 214.

7.Нигматзянова Д. А. NFT как основа экономики метавселенных // Право и бизнес. 2022. № 4. С. 26–31

8.См.: Даниленков А. В. Интернет-право. М. : Юстицинформ, 2014.

9.См.: Голоскоков Л. В. О сущности сетевого права // Сетевое право и финансы : сборник науч. трудов / Академия бюджета и казначейства ; отв. ред. А. П. Альбов. М., 2011. С. 8.

10.См.: Lobel O. The Law of the Platform // Minnesota Law Review. 2016. 137. P. 87–153 ; Алтухов А. В., Ершова И. В., Кашкин С. Ю. Платформенное право как драйвер развития инноваций // Предпринимательское право. 2020. № 4. С. 17–24.

11.См.: Зыкова О. А. Природа цифрового права и его соотношение со смежными правовыми категориями // Цивилист. 2023. № 1. С. 12–21.

12.Рожкова М. А. Является ли цифровое право отраслью права и ожидать ли появления цифрового кодекса? // Хозяйственное право. 2020. № 4. С. 3–12.

13.См.: Городов О. А. Цифровое право как подотрасль информационного права // Право и цифровая экономика. 2021. № 1. С. 36–43 ; Танимов О. В., Шевченко А. Р. Цифровое право: основные сущностные аспекты // Российская юстиция. 2019. № 10. С. 6–9.

14.Нестеров А. В. Цифровое право против информационного кодекса // Юрист. 2021. № 11. С. 8–12.

15.См.: Банакас С., Петров Д. А., Попондопуло В. Ф., Силина Е. В. Цифровые отношения как предмет правового исследования // Вестник Санкт-Петербургского университета. Право. 2023. № 14 (2). С. 496–497.

16.Талапина Э. В. Сравнительное цифровое право: становление и перспективы // Журнал российского права. 2021. № 9. С. 25.

17.См.: Райхер В. К. Общественно-исторические типы страхования. М. ; Л., 1947. С. 190 ; Иоффе О. С., Шаргородский М. Д. Вопросы теории права. М., 1961. С. 361–362 ; Толстой Ю. К. О теоретических основах кодификации гражданского законодательства // Правоведение. 1957. № 1. С. 42–45 ; Алексеев С. С. Проблемы теории права : курс лекций. Свердловск, 1972. Т. 1. С. 146.

18.См.: Красавчиков О. А. Система права и система законодательства: гражданско-правовой аспект// Правоведение. 1975. № 2. С. 65 ; Тонков Е. Е., Синенко В. С. Комплексные отрасли права: плодотворная идея или отказ от формальной определенности в правовой науке? // Вестник ВГУ. Серия «Право». 2016. № 2. С. 74.

19.Шумилов В. М. Международное цифровое право как отрасль международного права//<https://inlibrary.uz/index.php/digiteclaw/article/view/137655>

Сейтжан А. А.

Құқық магистрі

*Нархоз Университетінің құқықтану және мемлекеттік
басқару мектебінің ассистент профессоры
ainash.seitzhan@narхоз.kz*

ЖАСАНДЫ ИНТЕЛЛЕКТ НЕГІЗІНДЕ ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ҚЫЛМЫСТЫҚ ЗАҢНАМАСЫНЫҢ ТЕРМИНОЛОГИЯЛЫҚ ДЕРЕКТЕР БАЗАСЫН ҚҰРУ

Мақалада Қазақстан Республикасының қылмыстық заңнамасындағы қазақ және орыс тілдеріндегі терминдерді жинақтайтын, салыстыратын және тексеретін интеллектуалды терминологиялық деректер базасының тұжырымдамасы ұсынылады. Зерттеудің мақсаты - құқықтық ұғым, термин, анықтама және заң нормасындағы қолданыс арасындағы байланысты машиналық өңдеуге жарамды түрде көрсету. Деректер базасын қалыптастыру үшін нормативтік мәтіндерді автоматты алу, терминдерді тану, контекстік сәйкестікті есептеу және сараптамалық валидациялау кезеңдері негізделді. Жасанды интеллект сарапшының шешімін алмастырмайды; ол ықтимал сәйкессіздіктерді белгілейтін және дәлелді тексеруді жеделдететін көмекші құрал ретінде қарастырылады. Ұсынылған модель заң мәтіндерінің лингвистикалық теңтүпнұсқалылығын бағалауға, терминдерді біріздендіруге және өзгерістер тарихын бақылауға мүмкіндік береді.

Қылмыстық заңның тілі құқықтық айқындық қағидатына тікелей ықпал етеді. Бір ұғымның қазақ және орыс мәтіндерінде

әртүрлі мағыналық көлемде берілуі құқық нормасын түсіндіру кезінде қайшылық туғызуы мүмкін. Қазақстан Республикасының Қылмыстық кодексі қылмыстық жауаптылықтың негіздерін, қылмыстық құқық бұзушылықтардың түрлерін және олар үшін қолданылатын құқықтық ықпал ету шараларын белгілейді [1]. Сондықтан кодексте қолданылатын әрбір термин тек тілдік бірлік емес, құқықтық салдары бар ұғымдық белгі болып саналады. «Құқықтық актілер туралы» заң құқықтық актілерді әзірлеу, қабылдау, жариялау және мониторингтеу тәртібін реттейді. Заңнамалық актілер жобаларының қазақ және орыс тілдеріндегі мәтіндерінің теңтүпнұсқалығына ғылыми лингвистикалық сараптама жүргізу де осы реттеу аясында көзделген [2]. Қылмыстық заңнамаға енгізілетін өзгерістер саны мен мәтіндік нұсқалардың көлемі артқан сайын терминдерді қолмен салыстыру көп уақыт алады. Мұндай жағдайда жасанды интеллект терминдерді іздеу, контекст бойынша топтау және ықтимал айырмашылықтарды алдын ала анықтау міндеттерін атқара алады.

Зерттеудің мақсаты - қылмыстық заңнаманың терминологиялық деректер базасын құрудың мазмұндық және технологиялық моделін ұсыну. Зерттеу нысаны ретінде Қылмыстық кодекстің қазақ және орыс тілдеріндегі ресми мәтіндері алынады. Зерттеу пәнін терминдердің нысаны, мағынасы, құқықтық анықтамасы, контексті және тілдер арасындағы сәйкестігі құрайды. Жұмыста салыстырмалы-құқықтық, терминологиялық, құрылымдық-модельдеу және мәтінді автоматты өңдеу әдістері қолданылады.

Ұсыныстың ғылыми жаңалығы құқықтық терминологияны екі тілдегі сөздер тізімі ретінде емес, нұсқалары уақыт бойынша өзгертін байланысқан деректер жүйесі ретінде модельдеуден көрінеді. Қолданыстағы электрондық мәтіннен терминді табу жеткіліксіз: оның қандай ұғымды білдіретінін, сол ұғымның өзге нормада қалай аталғанын және аудармада мағыналық компоненттердің сақталғанын анықтау қажет. Осыған байланысты база корпустық лингвистика, терминография және құқықтық сараптама тәсілдерін бір ортада біріктіреді.

Зерттеудің практикалық маңызы үш қолдану сценарийімен анықталады. Біріншіден, заң жобасын әзірлеуші жаңа терминді бұрынғы қолданыстармен салыстыра алады. Екіншіден, лингвист-сарапшы екі тілдегі нормалардың мағыналық көлемін тексереді. Үшіншіден, зерттеуші белгілі бір ұғымның редакциялар бойынша өзгеруін бақылайды. Нәтижесінде база терминологиялық шешімді іздеу уақытын қысқартуға және сараптамалық қорытындының дәлелдік негізін көрсетуге қызмет етеді.

Терминологиялық деректер базасының ұғымдық негізі стандарты терминологиялық жұмысты ұғымдарды және олардың атауларын жүйелі жинау, сипаттау, өңдеу мен ұсынуға бағытталған қызмет ретінде қарастырады. Стандарт объект, ұғым, анықтама және белгілеу арасындағы байланысты ажыратуды талап етеді [3]. Осы қағида құқықтық деректер базасында «термин» өрісімен шектелмеу керектігін көрсетеді. Мысалы, бір атау әртүрлі баптарда бірдей жазылғанымен, оның құқықтық қызметі мен мағыналық шекарасы контекске байланысты өзгеруі ықтимал.

Базаның негізгі бірлігі термин емес, ұғымдық жазба болуы тиіс. Әр жазбаға қазақша және орысша атау, нормативтік анықтама, бап пен тармаққа сілтеме, мәтіндік контекст, терминнің салалық санаты, күшіне ену мерзімі және редакция нұсқасы тіркеледі. Бұған қоса, терминнің мәртебесі көрсетіледі: дәл сәйкестік, шартты сәйкестік, көпмағыналылық немесе сараптаманы қажет ететін нұсқа. Мұндай құрылым бір терминнің барлық қолданысын біріктіріп, өзгеріс енгізілген кезде бұрынғы редакцияны сақтауға мүмкіндік береді.

Деректердің бастапқы көзі ретінде тек ресми жарияланған және бақылаулы күйде сақталатын нормативтік мәтіндер пайдаланылуға тиіс. «Әділет» ақпараттық-құқықтық жүйесіндегі екі тілдегі мәтіндер бірегей құжат нөмірі мен редакция күні бойынша сәйкестендіріледі [1]. Базаға ғылыми мақалалардан немесе түсіндірме сөздіктерден алынған анықтамалар енгізілген жағдайда, олардың нормативтік емес мәртебесі бөлек белгіленеді. Бұл шешім ресми норма мен доктриналық түсіндірмені араластыруға жол бермейді.

Терминдерді жіктеу де алдын ала бекітілген өлшемдерге сүйенуі керек. Базада жалпы құқықтық терминдер, тек қылмыстық

құқыққа тән атаулар, қылмыс құрамының белгілері, жаза түрлері, субъектіні сипаттайтын атаулар және бағалау ұғымдары бөлек белгіленеді. Бағалау ұғымдарына қатысты контекст ерекше маңызды, өйткені олардың мазмұны сот практикасы мен нақты норманың мақсаты арқылы нақтылануы мүмкін. Жіктеу машиналық модельге ұқсас жазылатын, бірақ қызметі бөлек бірліктерді шатастырмауға көмектеседі.

Әр жазбада дереккөздің тұтастығын тексеретін техникалық белгі болғаны жөн. Құжат жүктелген кезде оның нұсқасы, алынған уақыты және мәтіннің бақылау сомасы тіркеледі. Кейін ресми мәтін жаңартылса, жүйе бұрынғы жазбаны өшірмей, жаңа редакциямен байланыстырады. Осы тәсіл зерттеудің қай нормативтік нұсқаға сүйенгенін қалпына келтіруге және ұсыныстың ескі редакциядан алынбағанын тексеруге мүмкіндік береді.

Қазақстанда жасанды интеллектіні дамытудың 2024–2029 жылдарға арналған тұжырымдамасы деректер сапасын, технологиялық инфрақұрылымды және жауапты қолдануды жүйелі дамытуды көздейді [4]. Қылмыстық заңнама терминологиясының базасын құру осы бағытпен үйлеседі, бірақ заң саласының тәуекелі жоғары болғандықтан, автоматтандыру нәтижесі міндетті сараптамалық бақылаудан өтуі керек.

Бірінші кезеңде ресми құжаттардан құрылымдық корпус жасалады. Бағдарлама кодекс мәтінін бап, бөлік, тармақ және редакция күні бойынша бөледі. Қазақ және орыс нұсқалары құжат реквизиттері мен құрылымдық нөмірлері арқылы жұптастырылады. Екінші кезеңде табиғи тілді өңдеу моделі термин-кандидаттарды анықтайды. Ол тұрақты сөз тіркестерін, анықтамалық конструкцияларды және құқықтық мағынасы жиі қайталанатын атауларды белгілейді. Үшінші кезеңде көптілді модель екі тілдегі үзінділердің контекстік жақындығын есептейді. Төмен сәйкестік көрсеткіші қате бар екенін дәлелдемейді; ол сарапшы тексеруі қажет фрагментті ғана көрсетеді.

Төртінші кезеңде ұғымдар графы құрылады. Онда жалпы және арнайы ұғымдар, синонимдер, ескірген атаулар және өзара сілтемелер көрсетіледі. Мысалы, жалпы ұғым мен қылмыстың нақты құрамын білдіретін атауды бір деңгейге қоюға болмайды.

Бесінші кезеңде заңгер мен лингвист ұсынылған жұпты тексеріп, шешімін электрондық хаттамаға енгізеді. Расталған жазбалар модельді кейін қайта баптау үшін сапалы оқу дерегіне айналады.

Жүйе сапасы кемінде төрт өлшеммен бағалануы тиіс. Біріншісі - терминді танудың дәлдігі: модель белгілеген бірліктердің қаншасы нақты құқықтық термин екені тексеріледі. Екіншісі - толықтық: сарапшы тандаған терминдердің қаншасын жүйе тапқаны есептеледі. Үшіншісі - тілдер арасындағы сәйкестік: қазақша атаудың орысша баламамен бір құқықтық ұғымды білдіру дәрежесі бағаланады. Төртіншісі - түсіндірмелілік: жүйе күмәнді белгі қойған кезде оған негіз болған бапты, контексті және салыстыру белгісін көрсетуі керек.

Жасанды интеллектіні қолданудың негізгі тәуекелі - ықтималдық қорытындыны құқықтық ақиқат ретінде қабылдау. Тілдік модель сенімді көрінетін, бірақ нормативтік мәтінде жоқ терминді ұсынуы немесе тарихи редакцияларды араластыруы мүмкін. Бұған жол бермеу үшін модель тек бекітілген корпус шегінде жұмыс істеп, әр ұсыныс бастапқы мәтінге сілтемемен берілуі қажет. Нұсқаларды бақылау, әрекеттер журналын жүргізу және рөлдік қолжетімділік те міндетті талаптар болуы тиіс. Деректер базасы заңды ресми түсіндіру құралы емес; оның нәтижесі ғылыми және сараптамалық жұмысқа арналған көмекші ақпарат ретінде ұсынылады.

Алгоритмдік бейтараптық мәселесі де ескеріледі. Егер оқу дерегінде орыс тіліндегі мәтін басым болса, модель қазақша терминдердің сөзжасамдық және синтаксистік ерекшеліктерін дұрыс бағаламауы мүмкін. Сондықтан екі тілдегі корпус көлемі мен сапасы теңгеріліп, қазақ тілінің морфологиялық талдау құралдары жеке тексерілуге тиіс. Сарапшылар арасындағы келісім коэффициентін өлшеу де пайдалы: ол бағалау өлшемдерінің қаншалықты анық екенін көрсетеді.

Техникалық архитектураны үш қабатқа бөлу орынды. Деректер қабаты нормативтік мәтіндерді, редакцияларды және сараптамалық шешімдерді сақтайды. Өңдеу қабаты мәтінді сегменттеу, морфологиялық талдау, терминдерді тану және семантикалық салыстыру модульдерінен тұрады. Қолданбалы қабат іздеу мен

салыстыру интерфейсін, ескерту жүйесін және есептерді қалыптастыру құралын қамтиды. Қабаттарды бөлу алгоритм өзгерген кезде нормативтік деректер мен бұрынғы сараптамалық шешімдердің сақталуын қамтамасыз етеді.

Модельді бағалау үшін алдын ала белгіленген бақылау жиынтығы қажет. Оған әртүрлі бөлімдерден алынған терминдік жұптар, дәл баламалар, ішінара сәйкес атаулар және әдейі енгізілген қайшылық мысалдары қосылады. Бұл жиынтықты модельді баптау деректерінен бөлек сақтау керек. Нәтиже әр жаңартудан кейін бірдей өлшемдермен тексерілсе, жүйенің сапасы шынымен жақсарғанын немесе белгілі бір терминдер тобы бойынша төмендегенін байқауға болады.

Деректер базасын енгізу моделі Жобаны кезең-кезеңімен іске асыру ұсынылады. Алдымен Қылмыстық кодекстің Жалпы бөлімі негізінде пилоттық корпус жасалады. Бұл бөлімдегі негізгі ұғымдар Ерекше бөлім нормаларын түсіндіру үшін тірек қызметін атқарады. Пилот барысында деректер сызбасы, терминді тану ережелері және сараптамалық интерфейс тексеріледі. Кейін база Ерекше бөліммен, қылмыстық заңнамаға өзгеріс енгізетін актілермен және Жоғарғы Соттың тиісті нормативтік қаулыларымен толықтырылуы мүмкін.

Пайдаланушы интерфейсін термин бойынша іздеу, екі тілдегі контексті қатар көрсету, редакцияларды салыстыру және сараптамалық ескерту енгізу функцияларын қамтуы керек. Ашық бөлік пайдаланушыларға тек расталған жазбаларды ұсынады. Сарапшыларға арналған бөлік күмәнді сәйкестіктерді қарауға, дәлел қосуға және шешім тарихын көруге мүмкіндік береді. Деректерді JSON немесе XML сияқты құрылымдық форматта экспорттау ғылыми зерттеулер мен өзге құқықтық ақпараттық жүйелерде қайта пайдалануға жағдай жасайды.

Базаның тиімділігі терминдер саны арқылы ғана өлшенбеуі керек. Негізгі көрсеткіштерге анықталған мағыналық қайшылықтар, сараптамаға жұмсалған уақыттың өзгеруі, түзетілген терминдік жұптар және жаңартылған редакцияны базаға енгізу мерзімі жатады. Пилот аяқталғаннан кейін тәуелсіз заңгерлер мен лингвистер іріктемелі тексеру жүргізіп, қате оң және қате теріс

нәтижелерді бағалауы қажет. Осы бағалау негізінде модельдің шекті көрсеткіштері мен сараптамалық регламент нақтыланады.

Жасанды интеллект негізіндегі терминологиялық деректер базасы қылмыстық заңнаманың қазақ және орыс тілдеріндегі мәтіндерін жүйелі салыстыруға арналған инфрақұрылым бола алады. Оның ғылыми құндылығы терминді жеке сөз ретінде емес, құқықтық ұғым, анықтама, контекст және редакция тарихы бірлігінде сипаттауымен байланысты. Автоматты талдау қайшылықты өздігінен шешпейді, бірақ үлкен мәтін көлемінен сарапшы назарын қажет ететін орындарды жылдам табады.

Ұсынылған модельді іске асыру үшін үш шарт маңызды: ресми дереккөздерге сүйену, әр автоматты ұсыныстың түсіндірілетін болуын қамтамасыз ету және соңғы шешімді заңгер-лингвист сарапшыларға қалдыру. Осы талаптар сақталса, база заң терминологиясын үйлестіру, мәтіндердің лингвистикалық теңтүпнұсқалылығын бағалау және қылмыстық заңнаманың сапасын арттыру жұмыстарын деректерге негізделген деңгейге көшіреді.

Қаржыладыру. *Мақала Қазақстан Республикасы Ғылым және жоғары білім министрлігі Ғылым комитеті қаржыландыратын BR 24993217 «Қазақстан Республикасының қылмыстық құқық саласындағы заң терминологиясын үйлестіру және заң мәтіндерінің лингвистикалық теңтүпнұсқалылығы» жобасын іске асыруға бағытталған 2024–2026 жылдарға арналған ғылыми және (немесе) ғылыми-техникалық бағдарламалар бойынша бағдарламалық-нысаналы қаржыландыру шеңберінде дайындалды.*

Әдебиеттер тізімі

1. Қазақстан Республикасының Қылмыстық кодексі: 2014 жылғы 3 шілдедегі № 226-V ҚРЗ. «Әділет» ақпараттық-құқықтық жүйесі. URL: <https://adilet.zan.kz/kaz/docs/K1400000226> (қаралған күні: 28.09.2026).
2. Құқықтық актілер туралы: Қазақстан Республикасының 2016 жылғы 6 сәуірдегі № 480-V ҚРЗ Заңы. «Әділет» ақпараттық-құқықтық жүйесі. URL: <https://adilet.zan.kz/kaz/docs/Z1600000480> (қаралған күні: 28.09.2026).
3. ISO 704:2022. Terminology work - Principles and methods. Geneva: International Organization for Standardization, 2022.
4. Жасанды интеллектті дамытудың 2024–2029 жылдарға арналған тұжырымдамасын бекіту туралы: Қазақстан Республикасы Үкіметінің 2024

жылғы 24 шілдедегі № 592 қаулысы. URL: <https://adilet.zan.kz/kaz/docs/P2400000592> (қаралған күні: 28.09.2026).

5. ISO 1087:2019. Terminology work and terminology science - Vocabulary. Geneva: International Organization for Standardization, 2019.

6. Devlin J., Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding // Proceedings of NAACL-HLT. 2019. P. 4171–4186.

Смагулова Т. С.

LL.M., докторант 3 курса, УО «Каспийский общественный университет», г. Алматы, Республика Казахстан

Порохов Е. В.

Директор НИИ финансового и налогового права, доктор юридических наук, профессор ВШП «Әділет» УО «Каспийский общественный университет», г. Алматы, Республика Казахстан

УКЛОНЕНИЕ ОТ УПЛАТЫ АЛИМЕНТОВ КАК ФОРМА ЭКОНОМИЧЕСКОГО НАСИЛИЯ: ПОЗИТИВНЫЕ ОБЯЗАТЕЛЬСТВА ГОСУДАРСТВА И РОЛЬ НАЛОГОВЫХ ОРГАНОВ В ИХ РЕАЛИЗАЦИИ

Экономическое насилие в семье выражается в контроле одного из партнёров над доходами и имуществом другого, в препятствиях к трудоустройству и в отказе участвовать в общих расходах. В отличие от физического насилия, оно редко оставляет видимые следы и долгое время воспринималось как частное дело семьи. Вместе с тем именно финансовая зависимость нередко удерживает женщину в насильственных отношениях и лишает её возможности самостоятельно обеспечивать себя и детей. Признание экономического насилия самостоятельным видом бытового насилия отражает сложившееся в современном праве понимание насилия в семье как явления, не ограничивающегося физическим воздействием на личность. Вместе с тем в правоприменительной практике и в научной литературе экономическое насилие анализируется преимущественно применительно к периоду совместного проживания супругов, когда один из них

непосредственно распоряжается общими денежными средствами и имуществом. Период, наступающий после фактического прекращения брачных отношений, остаётся значительно менее изученным, хотя в этот период уязвимость женщины нередко не снижается, а наоборот возрастает.

Расторжение брака не прекращает экономический контроль автоматически, а во многих случаях лишь видоизменяет механизм его осуществления. В период совместной жизни контроль носит непосредственный характер и выражается в распоряжении семейным бюджетом, ограничении доступа к банковским счетам или препятствовании трудоустройству. После прекращения брака эти инструменты утрачивают значение, однако сохраняется правовая связь между бывшими супругами, основанная на алиментном обязательстве родителя перед ребёнком. Уклонение от уплаты алиментов, занижение официального дохода и намеренное затягивание исполнения судебного акта позволяют должнику сохранять влияние на материальное положение женщины и детей. В результате правовой институт, призванный обеспечить интересы ребёнка, приобретает функцию средства давления, а взыскательница, добиваясь исполнения алиментного обязательства, вынуждена поддерживать длительное взаимодействие с лицом, от контроля которого она стремилась освободиться.

В зарубежной научной литературе намеренное уклонение от уплаты алиментов рассматривается как одна из форм постсепарационного экономического насилия, то есть продолжающегося причинения финансового вреда бывшему партнёру после расставания [1; 2]. В одном из качественных исследований, проведённых в США, более 75 % опрошенных женщин, переживших насилие в браке, сообщили, что после расставания бывшие мужья удерживали алименты, медицинскую страховку и другие базовые выплаты, которые ранее согласились производить [2; 3]. Австралийская исследовательница К. Натальер обращает внимание на то, что подобное поведение поддерживается устройством самих государственных процедур взыскания, и потому называет его экономическим насилием, которому содействует государство [1].

Для настоящего исследования особое значение имеет положение детей. В подростковом возрасте расходы на содержание ребёнка возрастают за счёт затрат на образование, здоровье и повседневные нужды, и отсутствие поддержки второго родителя ощущается особенно остро. Недостаток средств в семье может сужать образовательные возможности детей и усиливать их зависимость от окружения, а ситуация, в которой отец безнаказанно уклоняется от содержания, способна формировать у ребёнка представление о допустимости экономического давления в семейных отношениях. Поэтому проблема неуплаты алиментов относится не только к сфере гражданско-правовых обязательств, но и к профилактике насилия в отношении женщин и девочек.

В Казахстане эта проблема носит массовый характер. По данным Комитета принудительного исполнения Министерства юстиции, в первом полугодии 2026 года на исполнении находилось 329 513 производств о взыскании алиментов в отношении 232 758 должников, из которых 96,7 % составляют мужчины. По итогам первого полугодия 2026 года задолженность по исполнительным производствам, по которым алименты не выплачиваются вовсе, составила 19 млрд тенге, тогда как в 2024 году она составляла 16,7 млрд тенге, а в 2025 году 18,2 млрд тенге [4]. Преобладание мужчин среди должников позволяет сделать вывод, что неисполнение алиментных обязательств следует рассматривать как проблему, затрагивающую главным образом матерей, самостоятельно воспитывающих детей, и имеющую выраженное гендерное измерение.

Комитет принудительного исполнения Министерства юстиции отмечает, что одной из причин задолженности служит сокрытие реальных доходов, когда должник формально указывает минимальную заработную плату и именно от неё рассчитываются алименты [5]. В 2026 году Министерство юстиции объявило о начале интеграции с Министерством труда и социальной защиты населения и Министерством финансов для получения сведений о доходах и контрактах должников [5]. В то же время идея создания государственного алиментного фонда не получила поддержки, поскольку её реализация потребовала бы расходов

республиканского бюджета [6]. Тем самым вопрос о том, как обеспечить реальное взыскание алиментов без прямых бюджетных затрат, смещается в сферу налогового администрирования и межведомственного информационного обмена. Этот вопрос лежит на пересечении семейного права, налогового права и законодательства об исполнительном производстве и пока остаётся наименее изученным в отечественной юридической науке.

Цель статьи состоит в том, чтобы определить содержание позитивных обязательств государства в сфере взыскания алиментов и роль налоговых органов в их реализации. На основе анализа казахстанского законодательства, правовых позиций Конституционного Суда и практики Верховного Суда Республики Казахстан, а также зарубежного опыта предлагаются меры по совершенствованию правового регулирования. Научная новизна работы заключается в том, что налоговые органы рассматриваются как самостоятельный участник механизма исполнения позитивных обязательств государства по защите ребёнка и матери от постсепарационного экономического насилия.

Причина, по которой сокрытие дохода оказывается столь действенным способом уклонения от уплаты алиментов, кроется в самом механизме определения их размера. Кодекс Республики Казахстан «О браке (супружестве) и семье» (далее – КоБС) закрепляет долевого порядок определения размера алиментов. При отсутствии соглашения между родителями на содержание одного ребёнка взыскивается четверть заработка и (или) иного дохода, двух детей – одна треть, трёх и более детей – половина (п. 1 ст. 139 КоБС). В отдельных случаях суд вправе установить алименты в твёрдой денежной сумме. Это возможно, если родитель имеет нерегулярный или меняющийся доход, получает его в натуральной форме, применяет специальный налоговый режим либо выехал на постоянное место жительства за пределы Республики Казахстан (п. 1 ст. 141 КоБС) [7]. Эффективность долевого порядка как способа обеспечить надлежащее содержание ребёнка, однако, напрямую зависит от того, насколько полно и достоверно установлен фактический доход плательщика, от которого исчисляется доля. Если реальный доход скрыт, уплата доли от минимальной

заработной платы позволяет должнику формально исполнять обязанность и при этом фактически уклоняться от надлежащего содержания ребёнка.

Уклонение от уплаты алиментов в казахстанской доктрине и законодательстве рассматривается лишь как неисполнение гражданско-правовой обязанности, а не как проявление экономического насилия, требующее от государства активных мер защиты. В практическом отношении единственным массовым источником сведений о доходах должника служат данные налогового учёта, однако правовой режим их использования для целей взыскания алиментов не сформирован. Конституционный Суд Республики Казахстан констатировал, что расчёт алиментов и задолженности предпринимателей регламентирован лишь актом рекомендательного характера, а налоговая декларация, предназначенная для расчётов с бюджетом, не отражает реальных материальных возможностей родителя [8]. Отсюда возникает вопрос о том, в какой мере государство, располагая налоговыми данными, обязано использовать их для защиты ребёнка и матери и какие правовые механизмы для этого необходимы.

Ответ на первую часть этого вопроса дают международные обязательства Республики Казахстан. Обязанность государства в алиментной сфере не ограничивается невмешательством в отношения родителей и детей. Конвенция о правах ребёнка возлагает основную ответственность за обеспечение условий жизни ребёнка на родителей (п. 2 ст. 27), но при этом обязывает государства-участников принимать все необходимые меры для обеспечения восстановления содержания ребёнка родителями или другими лицами, несущими за него финансовую ответственность (п. 4 ст. 27) [9]. Данная норма закрепляет позитивное обязательство в его классическом понимании. Государство отвечает не за поведение конкретного должника, а за наличие и действенность механизма, обеспечивающего реальное взыскание.

Этот вывод подкрепляется позицией Комитета по ликвидации дискриминации в отношении женщин, который раскрывает обязательства государств через обязанности уважать, защищать и осуществлять права женщин на недискриминацию и на

возможность пользоваться равенством (п. 9 Общей рекомендации № 28) [10]. Применительно к экономическим последствиям распада семьи Комитет указывает, что женщины, как правило, несут более значительные экономические потери после развода, а домохозяйства, возглавляемые женщинами, чаще оказываются в бедности (пп. 1, 4 Общей рекомендации № 29). Руководящим принципом Комитет называет равное распределение между сторонами экономических выгод и издержек, связанных с отношениями и их прекращением (п. 45). Достижение фактического равенства, по мнению Комитета, требует от государства оценивать не только содержание закона, но и последствия его применения (п. 8) [11]. Если формально нейтральная норма о долевых алиментах позволяет отцу, скрывающему доход, переложить почти всё бремя содержания ребёнка на мать, государство допускает именно тот результат, от которого его предостерегает Комитет.

На национальном уровне аналогичный подход выражен в практике Конституционного Суда Республики Казахстан. Сославшись на ст. 27 Конвенции о правах ребёнка, Суд указал на необходимость пересмотра законодательства об исчислении и взыскании алиментов и совершенствования механизма исполнения соответствующих судебных актов [12]. Закон Республики Казахстан от 30 декабря 2025 года № 245-VIII «О профилактике правонарушений» сохранил экономическое насилие в числе видов бытового насилия и определяет его как умышленное лишение человека жилья, пищи, одежды, имущества, средств, на которые он имеет предусмотренное законами Республики Казахстан право (подп. 28 ст. 1) [13]. Этому определению по своему содержанию отвечает и умышленное лишение ребёнка средств, право на получение которых основано на алиментном обязательстве родителя. Вместе с тем законодатель не соотнёс понятие экономического насилия с нормами алиментного законодательства. В результате систематическое уклонение от содержания ребёнка не рассматривается ни как основание для применения мер профилактики, ни как обстоятельство, учитываемое при оценке риска насилия в семье. Тем самым неуплата алиментов, даже подтверждённая материалами исполнительного производства,

рассматривается лишь как неисполнение имущественной обязанности, а не как проявление экономического насилия, требующее профилактического реагирования.

Поскольку позитивное обязательство государства заключается в обеспечении реального взыскания, ключевым инструментом его исполнения становятся налоговые данные. Налоговый кодекс Республики Казахстан от 18 июля 2025 года № 214-VIII относит к налоговой тайне любые полученные налоговым органом сведения о налогоплательщике, если иное не установлено законом (п. 1 ст. 45). Из предусмотренных Налоговым кодексом случаев предоставления налоговой тайны без согласия налогоплательщика к алиментным отношениям применимы два. Суд вправе получить такие сведения при рассмотрении иска о взыскании алиментов, поскольку должник является стороной по делу (подп. 2 п. 6 ст. 45), а судебный исполнитель может использовать их в находящемся у него исполнительном производстве для исчисления алиментов и задолженности по ним (подп. 3 п. 6 ст. 45). Обмен сведениями может осуществляться посредством интеграции информационных систем (п. 7 ст. 45) [14].

Следовательно, режим налоговой тайны сам по себе не препятствует использованию налоговых данных для взыскания алиментов. Проблема заключается в порядке доступа к ним. Сведения предоставляются по отдельному запросу и лишь в рамках уже возбуждённого исполнительного производства или судебного спора, а интеграция информационных систем законом допускается, но не является обязательной. Кроме того, налоговый орган располагает сведениями только о задекларированных и учтённых доходах, поэтому запрос сам по себе не позволяет выявить доход, скрытый от налогообложения. Взыскательница, в свою очередь, не вправе получить эти сведения без согласия должника и может добиваться их предоставления лишь через суд или судебного исполнителя.

Не менее значим вопрос о том, какие налоговые данные служат базой исчисления алиментов. Перечень видов заработной платы и (или) иного дохода, из которых производится удержание алиментов на содержание несовершеннолетних детей, утверждённый приказом

Министра юстиции Республики Казахстан от 24 декабря 2014 года № 372, охватывает широкий круг доходов, включая заработную плату, пенсии, пособия и иные выплаты [15]. Наибольшую сложность с точки зрения исчисления алиментов представляют доходы от предпринимательской деятельности без образования юридического лица. В отличие от заработной платы, алименты с которой удерживает работодатель, размер дохода индивидуального предпринимателя определяется на основании его собственной налоговой отчётности, и именно здесь налоговые данные становятся непосредственной базой расчёта.

Порядок исчисления алиментов с доходов индивидуального предпринимателя, как установил Конституционный Суд, определён лишь Методическими рекомендациями, утверждёнными приказом Министра юстиции от 31 марта 2017 года № 345 [8]. Рекомендации отсылают к данным налоговой декларации, упрощённой декларации или расчёта стоимости патента [8; 16]. Конституционный Суд обратил внимание на то, что декларация создаётся для фискальных целей, то есть для исчисления налоговых обязательств перед государством. Её содержание зависит от избранной государством налоговой политики, в рамках которой часть прибыли может не подлежать отражению в силу преференций. Следовательно, ориентация на декларационные данные при определении размера алиментов не исключает занижения причитающегося ребёнку содержания [8].

Стоит отметить, что проблема здесь глубже, чем простая неполнота сведений. Налоговое и алиментное правоотношения преследуют разные цели. В первом законное уменьшение налоговой базы за счёт льгот поощряется государством, тогда как во втором то же уменьшение дохода прямо сокращает размер содержания ребёнка. Более того, при опоре на декларацию у предпринимателя возникает двойной стимул занижать заявляемый доход, поскольку это одновременно снижает и налоговую нагрузку, и сумму алиментов. Использование фискального документа для целей, которым он изначально не служит, неизбежно переносит на алиментные отношения логику налоговой оптимизации, несовместимую с приоритетом интересов ребёнка.

Законодатель признал применение специальных налоговых режимов основанием для взыскания алиментов в твёрдой денежной сумме (п. 1 ст. 141 КоБС) [7]. Однако, как разъяснил Верховный Суд, такое требование заявляется по инициативе получателя алиментов [17], и именно он, в соответствии с общим правилом о распределении бремени доказывания (ст. 72 ГПК РК) [18], должен обосновать наличие соответствующих оснований.

Возможности налогового органа ограничены и объёмом собираемой информации. Всеобщее декларирование доходов и имущества могло бы дать государству более полное представление о доходах граждан, однако в соответствии с принятыми поправками граждане, не вошедшие в первые три этапа декларирования, освобождены от представления деклараций, за исключением владельцев зарубежных активов, лиц, приобретавших имущество на сумму свыше 20 000 МРП, и лиц, получавших доходы, облагаемые самостоятельно [19]. Такое решение оправданно с точки зрения снижения нагрузки на добросовестных граждан. Однако в результате большинство должников по алиментам остаются вне системы декларирования, и налоговый орган располагает сведениями об их доходах лишь в той мере, в какой их представляют налоговые агенты.

Недостаток сведений о доходе снижает и эффективность мер ответственности. Уголовная ответственность по ст. 139 Уголовного кодекса Республики Казахстан наступает за неисполнение родителем более трёх месяцев обязанности по уплате средств на содержание несовершеннолетних детей, назначенных решением суда [20]. Должник, регулярно перечисляющий долю от официальной минимальной заработной платы, эту обязанность формально исполняет. В 2025 году к административной ответственности были привлечены 4 824 должника, а к уголовной 380 [5], что несопоставимо с общим числом должников. Таким образом, санкции направлены против открытой неуплаты, но не затрагивают случаи сокрытия дохода.

Практическое значение обозначенной проблемы подтверждается материалами судебной практики, опубликованными Верховным Судом Республики Казахстан. Так,

еще в 2010 году суд обязал жителя города Актау ежемесячно выплачивать на содержание ребенка алименты в размере одной четверти от всех видов его дохода вплоть до достижения ребенком совершеннолетия. Спустя более десяти лет, в 2023 году, частным судебным исполнителем была рассчитана задолженность по алиментным обязательствам, сумма которой составила порядка 50 млн тенге. При проверке имущественного положения должника было установлено, что с 2003 года он был зарегистрирован в качестве индивидуального предпринимателя и работал с применением специального налогового режима на основе упрощенной декларации. Сведения налоговых органов показали, что за отдельные периоды с 2010 по 2016 год, а также с 2020 по 2022 год им был задекларирован доход, превышающий в совокупности 200 млн тенге. Должник не согласился с рассчитанной суммой и оспорил действия судебного исполнителя. Специализированный межрайонный административный суд Мангистауской области требования не поддержал, указав, что при определении алиментной задолженности необходимо исходить из фактически полученного дохода предпринимателя, сведения о котором содержатся в его налоговой отчетности. Принятый судебный акт впоследствии был оставлен без изменения судами апелляционной и кассационной инстанций [21; 22].

Рассмотренное дело позволяет обратить внимание на две существенные проблемы правоприменения. Первая связана с обменом информацией между государственными органами и участниками исполнительного производства. Несмотря на наличие у налоговых органов сведений о значительных доходах должника, алиментное обязательство продолжительное время оставалось неисполненным. Размер накопившейся задолженности был установлен только после обращения судебного исполнителя к данным налоговой отчетности. Такая ситуация свидетельствует о недостаточной эффективности действующего порядка информационного взаимодействия, при котором необходимые сведения о доходах должника используются преимущественно после их истребования, а не передаются для целей исполнения алиментных обязательств в системном порядке.

Второй аспект касается определения дохода индивидуального предпринимателя для расчета алиментов. В рассматриваемом споре суд принял за основу сведения, указанные самим должником в налоговой декларации, и признал их достаточными для определения размера его обязательств. В конкретной ситуации это обеспечило защиту интересов ребенка, поскольку в отчетности были отражены существенные доходы. Вместе с тем подобный механизм не всегда способен гарантировать объективный результат: если предприниматель указывает доход в меньшем размере, расчет алиментов исключительно по налоговой декларации может не соответствовать его фактическому материальному положению. Именно поэтому декларационные сведения целесообразно рассматривать не как единственный, а как один из источников оценки реальной платежеспособности должника, что согласуется с правовой позицией Конституционного Суда [8].

Британский подход к обеспечению алиментных обязательств основан на передаче основной части соответствующих полномочий от судов специализированному государственному органу. Такая система начала формироваться после принятия Закона о содержании детей 1991 года (Child Support Act 1991) [23]. С декабря 2012 года эти функции выполняет Служба содержания детей (Child Maintenance Service), созданная в структуре Министерства труда и пенсий вместо прежнего Агентства по алиментам на детей (Child Support Agency) [24]. Значение этой модели было подтверждено и судебной практикой. В деле *R (Kehoe) v Secretary of State for Work and Pensions* Палата лордов пришла к выводу, что родитель, совместно проживающий с ребенком, не может самостоятельно обращаться в суд за взысканием образовавшейся задолженности, поскольку обязанность по ее принудительному взысканию возложена на государственный орган [25]. Мать обратилась в Европейский суд по правам человека, посчитав, что у неё отняли право на защиту в суде. Однако в 2008 году Европейский суд с этим не согласился и признал такой порядок допустимым (*Kehoe v. the United Kingdom*) [26]. Отсюда следует вывод, что британская модель исходит из того, что передача государству функции взыскания

предполагает и возложение на него основной ответственности за эффективность исполнения алиментного обязательства.

Определение размера выплат построено преимущественно на информации о доходах, которой располагает Налоговая и таможенная служба Великобритании (HM Revenue and Customs, HMRC). Служба содержания детей получает необходимые сведения напрямую из налоговой системы, а данные о текущем заработке используются лишь тогда, когда расхождение с ранее учтенным доходом достигает установленного порога в 25 % [27]. Такой механизм сокращает возможность произвольного изменения плательщиком сведений, используемых для расчета алиментов. Если имеются основания полагать, что часть доходов скрывается, к проверке могут быть привлечены сотрудники специального подразделения, занимающегося финансовыми расследованиями [28].

Служба содержания детей обладает и собственными инструментами принудительного исполнения. В частности, взыскание может производиться непосредственно из заработной платы либо денежных средств, находящихся на банковских счетах должника, без предварительного обращения в суд [23; 28]. При устойчивом уклонении от исполнения обязательств законодательство допускает применение более строгих мер, включая ограничение права управления транспортным средством или использования паспорта на основании судебного решения [23; 28]. Дополнительным направлением развития системы стал Закон 2023 года о взыскании алиментов в случаях домашнего насилия (Child Support Collection (Domestic Abuse) Act 2023), предусматривающий возможность организации выплат через государственную службу в случаях домашнего насилия, чтобы получатель алиментов не был вынужден непосредственно взаимодействовать с плательщиком. Однако в действие этот закон пока не введен [24; 29].

Опыт Великобритании демонстрирует комплексный подход к обеспечению исполнения алиментных обязательств, при котором ключевая роль отводится государственным институтам. Размер подлежащих уплате средств определяется с использованием

официальной информации о доходах плательщика, содержащейся в налоговых базах, а компетентный орган наделён полномочиями самостоятельно применять предусмотренные законом меры взыскания. Для Казахстана особое значение имеет возможность непосредственного информационного взаимодействия между органами, обеспечивающими исполнение алиментных обязательств, и налоговыми органами. Такой механизм позволил бы устанавливать фактическое материальное положение должника на основании объективных государственных данных и тем самым снижать риск намеренного занижения либо сокрытия доходов.

В Германии регулирование алиментных отношений основано на сочетании норм частного, процессуального и публичного права. Германское гражданское уложение (*Bürgerliches Gesetzbuch, BGB*) возлагает на родителей несовершеннолетних детей усиленную обязанность по их содержанию, предполагающую использование всех имеющихся возможностей для исполнения алиментных обязательств (абз. 2 § 1603 BGB). Одновременно § 1605 BGB предусматривает обязанность родственников раскрывать сведения о своих доходах и имущественном положении, если такая информация необходима для определения размера содержания [30]. Процессуальные гарантии закреплены в Законе о производстве по семейным делам и делам добровольной юрисдикции от 17 декабря 2008 года (*Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit, FamFG*). В соответствии с § 235 FamFG суд вправе потребовать от участника дела сведения о доходах, а при их непредставлении — получить необходимые данные от работодателя, органов социального страхования, страховых организаций и финансовых органов. По ходатайству другой стороны такое истребование становится обязанностью суда (абз. 1, 2 § 236 FamFG) [31]. Таким образом, получение информации о доходах должника обеспечивается непосредственно судебным механизмом, а не возлагается исключительно на получателя алиментов.

Публично-правовой уровень германской модели образует Закон об обеспечении содержания детей одиноких матерей и отцов посредством авансирования алиментов (*Unterhaltsvorschussgesetz*,

UVG). По этому закону государство выплачивает ребёнку содержание, если второй родитель его не предоставляет, а требование к должнику переходит к государству. Согласно § 6 UVG, уполномоченный орган вправе получать от финансовых органов информацию о месте проживания должника, его занятости и доходах. Кроме того, через Федеральное центральное налоговое ведомство (Bundeszentralamt für Steuern) могут быть установлены сведения о принадлежащих ему банковских счетах. По обращению родителя, совместно проживающего с ребёнком, соответствующий орган также передаёт ему имеющиеся данные о должнике, включая информацию, полученную от работодателя и о банковских счетах (абз. 1, 2, 5–7 § 6 UVG) [32].

С 1 июля 2017 года порядок авансирования был существенно расширен. Возрастная граница получения выплат повышена с 12 до 18 лет, а прежнее ограничение срока их получения в 72 месяца отменено. В результате увеличилось как число детей, имеющих право на авансирование, так и продолжительность выплат [33]. Однако обратное взыскание остаётся малоэффективным. По данным федерального министерства по делам семьи, в 2024 году государство выплатило около 3,2 млрд евро, а вернуть от должников удалось лишь 17 % этой суммы [34]. В июле 2026 года федеральный министр по делам семьи объявила о намерении снизить возрастную границу получения авансирования с 18 до 16 лет, что вызвало возражения объединений родителей-одиночек [35]. Для настоящего исследования это обстоятельство показательно, поскольку сокращение поддержки затрагивает именно подростков. Германский опыт демонстрирует, что государственное авансирование надёжно защищает ребёнка, но требует значительных бюджетных расходов и не решает проблемы сокрытия дохода должником. Поэтому наибольший интерес для Казахстана представляет не сам институт авансирования, а сопровождающие его информационные механизмы.

В России возникла та же проблема, что и в Казахстане, а именно вопрос о том, следует ли при исчислении алиментов с доходов индивидуального предпринимателя учитывать понесённые им расходы. Этот вопрос рассмотрел Конституционный Суд

Российской Федерации по жалобе предпринимателя, применявшего упрощённую систему налогообложения. Судебный пристав-исполнитель запросил в налоговом органе его налоговые декларации и рассчитал задолженность по алиментам из всей суммы полученного дохода, не вычитая расходов, связанных с ведением предпринимательской деятельности. В Постановлении от 20 июля 2010 года № 17-П Конституционный Суд признал такой подход недопустимым и указал, что подтверждённые документами расходы предпринимателя должны вычитаться из дохода, с которого удерживаются алименты [36]. Иначе алименты исчислялись бы с сумм, которые фактически не составляют доход предпринимателя, поскольку были потрачены на ведение бизнеса.

Впоследствии эта позиция была закреплена в Постановлении Правительства Российской Федерации от 2 ноября 2021 года № 1908, утвердившем перечень видов доходов, из которых удерживаются алименты. Согласно перечню, доход предпринимателя определяется за вычетом расходов, если они подтверждены документами [37]. Для Казахстана российский опыт важен в двух отношениях. Во-первых, он показывает возможное решение спорного вопроса о базе исчисления алиментов, сохраняющего свою актуальность, как свидетельствует спор из г. Актау. Во-вторых, в России соответствующее правило закреплено обязательным нормативным правовым актом, тогда как в Казахстане аналогичный вопрос решается лишь методическими рекомендациями, которые, как указал Конституционный Суд Республики Казахстан, не обеспечивают необходимой правовой определённости [8].

Исходя из результатов анализа, представляется обоснованным следующий комплекс предложений по совершенствованию законодательства Республики Казахстан.

Первое предложение касается закрепления в законе базы исчисления алиментов с доходов индивидуального предпринимателя. Оно направлено на устранение правовой неопределённости, выявленной Конституционным Судом РК в Постановлении № 46-НП, при которой на практике основной базой расчёта фактически служит налоговая декларация [8; 21].

Предлагается дополнить ст. 140 КоБС пунктом, согласно которому при общеустановленном режиме налогообложения алименты исчисляются с дохода предпринимателя за вычетом документально подтверждённых расходов, связанных с предпринимательской деятельностью, и уплаченных налогов, а при специальных налоговых режимах, не предполагающих ведения учёта расходов, с дохода, отражённого в налоговой отчётности, который может быть уменьшен на сумму расходов, связанных с предпринимательской деятельностью, при их подтверждении первичными документами. Основой предложения служит российский опыт, где аналогичное правило выработано Конституционным Судом и закреплено обязательным нормативным актом [36; 37]. Реализация предложения сделает расчёт алиментов понятным для обеих сторон и позволит выполнить рекомендацию Конституционного Суда Республики Казахстан.

Второе предложение направлено на переход от запросного к автоматическому обмену налоговой информацией. Оно устраняет недостаток, наглядно проявившийся в споре о взыскании алиментов с предпринимателя из г. Актау, задолженность которого была определена лишь спустя более десяти лет после вынесения судебного акта, хотя налоговые органы всё это время располагали сведениями о его доходах [21; 22]. Предлагается дополнить п. 6 ст. 45 Налогового кодекса Республики Казахстан нормой, обязывающей органы государственных доходов автоматически передавать в информационную систему исполнительного производства сведения о должниках по алиментам (о регистрации в качестве индивидуального предпринимателя, смене налогового режима, трудоустройстве к новому работодателю и представлении налоговой отчётности). Одновременно в Законе Республики Казахстан «Об исполнительном производстве и статусе судебных исполнителей» следует закрепить обязанность судебного исполнителя при получении таких сведений пересчитать размер алиментов и задолженности по ним. Основой предложения служит британская модель, в которой закон обязывает налоговые органы передавать службе по взысканию алиментов сведения о доходах должника, а размер алиментов рассчитывается непосредственно на

основе этих данных [23; 27]. Аналогичная обязанность налоговых органов сообщать сведения о доходах должника закреплена и в германском законодательстве [32].

Техническая возможность такого обмена в Казахстане уже предусмотрена п. 7 ст. 45 Налогового кодекса РК, а Министерство юстиции объявило о начале соответствующей интеграции [5]. Предлагаемая норма придаст этой интеграции правовую основу и определит её объём. Особенностью казахстанской системы является то, что принудительное исполнение осуществляют не только государственные, но и частные судебные исполнители, которые не являются государственными служащими. Поэтому при передаче им сведений, составляющих налоговую тайну, необходимо обеспечить защиту этих сведений от неправомерного использования. Для этого передача должна осуществляться только через информационную систему исполнительного производства. Доступ к сведениям следует ограничить алиментными производствами, находящимися у конкретного судебного исполнителя, а каждое обращение к ним фиксировать в системе. За незаконное разглашение таких сведений судебный исполнитель должен нести ответственность в соответствии с законодательством о персональных данных [38]. При соблюдении этих условий мера позволит своевременно корректировать размер алиментов и исключит многолетние расхождения между налоговыми сведениями и расчётом задолженности.

Третье предложение направлено на восполнение информационного пробела, возникшего после сужения всеобщего декларирования [19]. Предлагается установить в Налоговом кодексе РК обязанность лиц, имеющих задолженность по алиментам свыше трёх месяцев, представлять декларацию о доходах и имуществе (форма 270.00) за весь период существования задолженности. Одновременно в ст. 141 КоБС следует закрепить, что непредставление такой декларации или выявленное в ней несоответствие между доходами и приобретённым имуществом является основанием для взыскания алиментов в твёрдой денежной сумме. Прямого аналога этой меры в изученных правовых порядках нет, однако она основана на общем для них принципе, согласно

которому сведения о доходе обязан раскрыть сам плательщик алиментов. В Великобритании служба по взысканию алиментов вправе требовать от плательщика сведения о доходах, а за их непредставление установлена ответственность [23]. В Германии родственники обязаны предоставлять друг другу сведения о доходах, необходимые для определения алиментов (§ 1605 BGB) [30]. В Казахстане такая мера может быть введена без значительных затрат, поскольку система электронного декларирования уже действует. Обязанность возникает при задолженности свыше трёх месяцев, что совпадает с порогом уголовной ответственности по ст. 139 Уголовного кодекса РК [20], и прекращается после её погашения, поэтому не возлагает на должника чрезмерного бремени. Риск указания в декларации недостоверных сведений снижается благодаря возможности сопоставить их с данными о зарегистрированном имуществе должника и банковских операциях. В результате налоговый орган и суд получают сведения о доходах именно тех лиц, которые уклоняются от уплаты алиментов.

Четвёртое предложение касается процессуального положения получателя алиментов. Действующее законодательство возлагает на получателя алиментов бремя доказывания дохода должника, не предоставляя при этом доступа к налоговым сведениям. Предлагается закрепить в ст. 141 КоБС право истца заявить при подаче иска ходатайство об истребовании сведений о доходах ответчика из органов государственных доходов. Суд обязан удовлетворить такое ходатайство, если ответчик не представил добровольно сведения о доходах в установленный судом срок. Основой служит § 236 Закона Германии о производстве по семейным делам (FamFG), обязывающий суд по ходатайству стороны запрашивать сведения о доходах у налоговых органов [31].

Предлагается также установить, что при существенном расхождении между задекларированным доходом должника и его расходами или приобретённым имуществом суд вправе определить доход исходя из официально установленных налоговыми и другими уполномоченными органами в соответствующих актах и документально подтвержденных данных о доходах и расходах должника, если должник не докажет иное. Это правило опирается на

германский подход, согласно которому родитель обязан использовать для содержания ребёнка все доступные ему средства [30], но в казахстанских условиях основанием для определения дохода судом в целях исчисления алиментов должны служить документально подтверждённые и доказанные уполномоченными органами объективные расхождения в имущественном положении должника.

Наконец, по образцу абз. 7 § 6 Закона Германии об авансировании алиментов (UVG) [32] взыскательнице целесообразно предоставить право получать от судебного исполнителя сведения о доходах должника для проверки правильности расчёта алиментов при условии сохранения их конфиденциальности. Реализация этих мер уравнивает взыскателя и должника в процессуальных правах сторон гражданского процесса и исполнительного производства и лишит должника информационного преимущества в споре.

Проведённое исследование позволяет сделать вывод о том, что уклонение от уплаты алиментов не сводится исключительно к неисполнению имущественной обязанности и может рассматриваться как форма постсепарационного экономического насилия, затрагивающего интересы ребёнка и родителя, на которого фактически возлагается основное бремя его содержания. Эффективность исполнения алиментных обязательств во многом определяется своевременным установлением реального дохода должника и возможностью получения соответствующей информации судом и судебным исполнителем. Законодательство Республики Казахстан предусматривает использование налоговых данных при взыскании алиментов, однако запросный порядок их получения, ограниченность сведений, содержащихся в налоговой отчётности, а также отсутствие нормативно закреплённого порядка определения доходов отдельных категорий плательщиков снижают эффективность действующего механизма. Анализ зарубежного опыта подтверждает значимость прямого межведомственного обмена информацией и активного участия государства в обеспечении надлежащего содержания ребёнка. В этой связи совершенствование порядка определения дохода должника,

автоматизация передачи налоговых сведений и расширение процессуальных возможностей получателя алиментов способны повысить результативность взыскания и обеспечить более полную реализацию позитивных обязательств государства по защите женщин и детей от экономического насилия.

Список использованной литературы

1. Natalier K. State Facilitated Economic Abuse: A Structural Analysis of Men Deliberately Withholding Child Support // *Feminist Legal Studies*. – 2018. – Vol. 26, № 2. – P. 121–140. – DOI: 10.1007/s10691-018-9376-1. – URL: <https://www.sci-hub.ru/10.1007/s10691-018-9376-1>.
2. Kaittila A., Hakovirta M., Kainulainen H. Types of Economic Abuse in Postseparation Lives of Women Experiencing IPV: A Qualitative Study from Finland // *Violence Against Women*. – 2024. – Vol. 30, № 2. – P. 426–444. – DOI: 10.1177/10778012221127727. – URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC10775644/>.
3. Toews M. L., Bermea A. M. «I Was Naive in Thinking, „I Divorced This Man, He Is Out of My Life“»: A Qualitative Exploration of Post-Separation Power and Control Tactics Experienced by Women // *Journal of Interpersonal Violence*. – 2017. – Vol. 32, № 14. – P. 2166–2189. – DOI: 10.1177/0886260515591278. – URL: <https://www.semanticscholar.org/paper/32f9e7688cf58cde40ca19cf130af5444b2195b1>.
4. Антонова С. Родители задолжали детям 19 миллиардов тенге по алиментам [Электронный ресурс] // *Tengrinews.kz*. – 2026. – 26 августа. – URL: https://tengrinews.kz/kazakhstan_news/roditeli-zadoljali-detyam-19-milliardov-tenge-po-alimentam-607001/.
5. Дюсенгулова Р. Налоговая начнёт проверять реальные заработки казахстанцев – кого коснутся новые меры [Электронный ресурс] // *Tengrinews.kz*. – 2026. – 26 марта. – URL: https://tengrinews.kz/kazakhstan_news/nalogovaya-nachnt-proveryat-realnyie-zarabotki-kazahstantsev-595610/.
6. Долг перед детьми: как работает система взыскания алиментов в РК [Электронный ресурс] // *Kazinform*. – 2026. – 3 марта. – URL: <https://www.inform.kz/ru/chto-stoit-za-sporami-ob-alimentah-35c25d>.
7. О браке (супружестве) и семье: Кодекс Республики Казахстан от 26 декабря 2011 года № 518-IV (с изм. и доп.) [Электронный ресурс] // ИПС «Әділет». – URL: <https://adilet.zan.kz/rus/docs/K1100000518>.
8. О рассмотрении на соответствие Конституции Республики Казахстан подпункта 11) пункта 1 Перечня видов заработной платы и (или) иного дохода, из которых производится удержание алиментов на содержание несовершеннолетних детей, утвержденного приказом Министра юстиции Республики Казахстан от 24 декабря 2014 года № 372: нормативное постановление Конституционного Суда Республики Казахстан от 28 июня 2024 года № 46-НП [Электронный ресурс] // ИПС «Әділет». – URL: <https://adilet.kz/ru/laws/o-rassmotrenii-na-sootvetstvie-konstitutsii-respubliki-28-06-2024-no-46-np/>.

9. Конвенция о правах ребенка: принята резолюцией 44/25 Генеральной Ассамблеи ООН от 20 ноября 1989 года [Электронный ресурс] // Организация Объединенных Наций. – URL: https://www.un.org/ru/documents/decl_conv/conventions/childcon.shtml.

10. Committee on the Elimination of Discrimination against Women. General recommendation No. 28 on the core obligations of States parties under article 2 of the Convention on the Elimination of All Forms of Discrimination against Women: CEDAW/C/GC/28. – Geneva: UN, 16 December 2010 [Электронный ресурс] // UN Digital Library. – URL: <https://digitallibrary.un.org/record/711350?v=pdf>.

11. Committee on the Elimination of Discrimination against Women. General recommendation on article 16 of the Convention on the Elimination of All Forms of Discrimination against Women (Economic consequences of marriage, family relations and their dissolution): CEDAW/C/GC/29. – New York: UN, 30 October 2013 [Электронный ресурс] // UN Digital Library. – URL: <https://digitallibrary.un.org/record/764504?v=pdf>.

12. О рассмотрении на соответствие Конституции Республики Казахстан абзацев второго, третьего и четвертого пункта 29 нормативного постановления Верховного Суда Республики Казахстан от 29 ноября 2019 года № 6 «О применении судами законодательства при рассмотрении дел, связанных с взысканием алиментов»: нормативное постановление Конституционного Суда Республики Казахстан от 24 декабря 2024 года № 58-НП [Электронный ресурс] // ИПС «Әділет». – URL: <https://adilet.kz/ru/laws/o-rassmotrenii-na-sootvetstvie-konstitutsii-respubliki-24-12-2024-no-58-np/>.

13. О профилактике правонарушений: Закон Республики Казахстан от 30 декабря 2025 года № 245-VIII (с изм. и доп.) [Электронный ресурс] // ИПС «Әділет». – URL: <https://adilet.zan.kz/rus/docs/Z2500000245>.

14. Налоговый кодекс Республики Казахстан: Кодекс Республики Казахстан от 18 июля 2025 года № 214-VIII (с изм. и доп.) [Электронный ресурс] // ИПС «Әділет». – URL: <https://adilet.zan.kz/rus/docs/K2500000214>.

15. Об утверждении перечня видов заработной платы и (или) иного дохода, из которых производится удержание алиментов на содержание несовершеннолетних детей: приказ Министра юстиции Республики Казахстан от 24 декабря 2014 года № 372 (с изм. и доп.) [Электронный ресурс] // ИПС «Әділет». – URL: <https://adilet.kz/ru/laws/ob-utverzhdenii-perechnya-vidov-zarabotnoy-platy-i-ili-inogo-24-12-2014-no-372/>.

16. Методические рекомендации по исполнению исполнительных документов о взыскании алиментов: утв. приказом Министра юстиции Республики Казахстан от 31 марта 2017 года № 345. – Текст в открытых правовых базах не опубликован; существование и содержание пункта 6 подтверждены в нормативном постановлении Конституционного Суда Республики Казахстан от 28 июня 2024 года № 46-НП. – URL: <https://adilet.zan.kz/rus/docs/S2400000046>.

17. О применении судами законодательства при рассмотрении дел, связанных с взысканием алиментов: нормативное постановление Верховного

Суда Республики Казахстан от 29 ноября 2019 года № 6 (с изм. и доп.) [Электронный ресурс] // ИПС «Әділет». – URL: <https://adilet.zan.kz/rus/docs/P190000006S>.

18. Гражданский процессуальный кодекс Республики Казахстан от 31 октября 2015 года № 377-V (с изм. и доп.). – Ст. 72 [Электронный ресурс] // ИПС «Әділет». – URL: <https://adilet.zan.kz/rus/docs/K1500000377>.

19. Всеобщее декларирование: ретроспективные изменения с 2025 года. Обзор ключевых поправок [Электронный ресурс] // PRO1C.kz. – 2025. – 1 сентября. – URL: <https://pro1c.kz/news/zakonodatelstvo/vseobshchee-deklarirovanieretrospektivnye-izmeneniya-s-2025-goda-obzor-klyuchevykh-popravok/>.

20. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изм. и доп.). – Ст. 139 [Электронный ресурс] // ИПС «Әділет». – URL: <https://adilet.zan.kz/rus/docs/K1400000226>.

21. О взыскании задолженности по алиментам с индивидуального предпринимателя, г. Актау [Электронный ресурс] // ҚР ЖОҒАРҒЫ СОТЫ: официальный Telegram-канал Верховного Суда Республики Казахстан. – 2025. – URL: https://t.me/Jogargy_sot/4596.

22. Суд подтвердил 50-миллионный долг жителя Актау по алиментам [Электронный ресурс] // Turan Times. – 2025. – 26 февраля. – URL: <https://turantimes.kz/regions/57911-sud-podtverdil-50-millionnyj-dolg-zhitelja-aktau-po-alimentam.html>.

23. Child Support Act 1991 (с. 48) (as amended) [Электронный ресурс] // legislation.gov.uk. – URL: <https://www.legislation.gov.uk/ukpga/1991/48/contents>.

24. Forrester J. Reforming the Child Maintenance Service: Lords Public Services Committee report [Электронный ресурс] // House of Lords Library. – 2026. – 29 May. – URL: <https://lordslibrary.parliament.uk/reforming-the-child-maintenance-service-lords-public-services-committee-report/>.

25. R (Kehoe) v Secretary of State for Work and Pensions [2005] UKHL 48 (House of Lords, 14 July 2005) [Электронный ресурс] // UK Parliament. – URL: <https://publications.parliament.uk/pa/ld200506/ldjudgmt/jd050714/kehoe-2.htm>.

26. Kehoe v. the United Kingdom, application no. 2010/06: judgment of the European Court of Human Rights, 2008 [Электронный ресурс] // HUDOC. – URL: <https://hudoc.echr.coe.int/eng?i=001-81653>.

27. The Child Support Maintenance Calculation Regulations 2012 (SI 2012/2677). – Regs. 34–36 [Электронный ресурс] // legislation.gov.uk. – URL: <https://www.legislation.gov.uk/uksi/2012/2677/part/4/chapter/1>.

28. Foley N. Child maintenance arrears and enforcement: Research Briefing CBP-7774 [Электронный ресурс]. – London: House of Commons Library, 2024. – 21 November. – URL: <https://researchbriefings.files.parliament.uk/documents/CBP-7774/CBP-7774.pdf>.

29. Child Support Collection (Domestic Abuse) Act 2023 (с. 24) [Электронный ресурс] // legislation.gov.uk. – URL: <https://www.legislation.gov.uk/ukpga/2023/24>.

30. Bürgerliches Gesetzbuch (BGB). – §§ 1603, 1605 [Электронный ресурс] // Gesetze im Internet. – URL: https://www.gesetze-im-internet.de/bgb/__1603.html.

31. Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) vom 17. Dezember 2008. – §§ 235, 236 [Электронный ресурс] // Gesetze im Internet. – URL: https://www.gesetze-im-internet.de/famfg/__236.html.

32. Gesetz zur Sicherung des Unterhalts von Kindern alleinstehender Mütter und Väter durch Unterhaltsvorschüsse oder -ausfallleistungen (Unterhaltsvorschussgesetz). – § 6 [Электронный ресурс] // Gesetze im Internet. – URL: https://www.gesetze-im-internet.de/uhvorschg/__6.html.

33. Deutscher Bundestag. Drucksache 19/4019 vom 27.08.2018: Antwort der Bundesregierung [zum Unterhaltsvorschuss] [Электронный ресурс]. – URL: <https://dserver.bundestag.de/btd/19/040/1904019.pdf>.

34. Nur 17 Prozent von Unterhaltsschuldnern wiedergeholt: Staat zahlt 3,2 Milliarden Euro Unterhaltsvorschuss [Электронный ресурс] // Der Tagesspiegel. – 2025. – 12. August. – URL: <https://www.tagesspiegel.de/politik/nur-17-prozent-von-unterhaltsschuldnern-wiedergeholt-staat-zahlt-32-milliarden-euro-unterhaltsvorschuss-14163887.html>.

35. Keine Kürzung beim Unterhaltsvorschuss!: Pressemitteilung vom 13.07.2026 [Электронный ресурс] // Verband alleinerziehender Mütter und Väter e.V. – URL: <https://vamv.de/de/presse/pressemitteilungen/keine-kurzung-beim-unterhaltsvorschuss/>.

36. По делу о проверке конституционности подпункта «з» пункта 2 Перечня видов заработной платы и иного дохода, из которых производится удержание алиментов на несовершеннолетних детей, в связи с жалобой гражданина Л. Р. Амаякяна: постановление Конституционного Суда Российской Федерации от 20 июля 2010 года № 17-П [Электронный ресурс] // ГАРАНТ.РУ. – URL: <https://www.garant.ru/hotlaw/federal/269543/>.

37. О перечне видов заработной платы и иного дохода, из которых производится удержание алиментов на несовершеннолетних детей, и признании утратившими силу некоторых актов и отдельных положений некоторых актов Правительства Российской Федерации: постановление Правительства Российской Федерации от 2 ноября 2021 года № 1908 [Электронный ресурс] // Официальный интернет-портал правовой информации. – URL: <http://publication.pravo.gov.ru/Document/View/0001202111030047>.

38. О персональных данных и их защите: Закон Республики Казахстан от 21 мая 2013 года № 94-V (с изм. и доп.) [Электронный ресурс] // ИПС «Әділет». – URL: <https://adilet.zan.kz/rus/docs/Z1300000094>.

Тлепбергенов О.Н.
Әл-Фараби атындағы Қазақ ұлттық университеті
Қазақстан заңгерлер одағының мүшесі,
Қазақстан Республикасы, Алматы қ.
E-mail: tlepbergenov.kz@mail.ru

ҰЛТТЫҚ ҚҰҚЫҚТЫҚ САНА, РУХАНИ ДАМУ ЖӘНЕ ҚЫЛМЫСТАН САҚТАНДЫРУДЫҢ ӨЗАРА СҰРАҚТАРЫ ЖАЙЛЫ

Ұлттық психология мен ұлттық құқықтық сананың дағдылар мен салт-дәстүрлері - құқықтық нормалардың мәніне ерекше серпін серіп отырғаны жасырын емес. Қазақ билер сотының тамаша шешімдері мен дала заңының өркениеттіліктің өрісінен алыс емес, қайта мәндес, мазмұндас екендігін дәлелдеуде қазақ заңгерлерінің еңбектерінің құндылығы мәңгілік. Құқықтық қатынастар мен қылмыстық саясат субъектілерінің мүдде, мұқтаждықтары және олардың қажеттілік деңгейі – тұлғаның құқықтық санасына тәуелді. Құқықтық сана – Қазақстан Республикасы азаматтарының жалпы құқықтық мәртебесіне қатысты азаматтық, идеологиялық, құқықтық пайымдарының, көпбағытты көзқарастарының, пікірлерінің, ішкі бағаларының жүйесін құрайтын санасының бір түрі. Құқықтық сананың жоғары болуы қоғамдағы демократиялық құндылықтарды жете түсінуді ғана емес, барлық жариялылық бағытындағы үдерістерді жеделдетуді, жалпы бүкіл қоғамды демократияландыруды әлеуметтік әділеттік қағидасы негізінде жүргізуді қамтамасыз етеді.

Қылмыстық-құқықтық сана – қылмыстық – құқықтық қатынас және қылмыстық саясат субъектілерінің қылмысқа және онымен күреске қатысты қажетті ой – пікір, пайымдаулары, оң ықпалды мұқтаждықтары мен жасалған қылмысқа құқықтық таным арқылы берілген кәсіби және қоғамдық баға деген көзқарасымызды көрсетеміз. Бұл пікіріміз, қылмыстан сақтандыру саласындағы қылмыстық саясаттың төмендегідей маңызды тұстарына мынадай талдау жасауымызға себеп болып отыр:

- құқықтық қатынас субъектілерінің, мемлекет және қоғам қайраткерлерінің тұлғалық қасиеттері, олардың білім – білік өресінің талапқа сайлылығы, отансүйгіштігі, мемлекеттік қызмет пен қызметтік міндеттердің жауаптылығын сезіне білуі – мемлекеттік талап қана емес, құқықтық қажеттілік;

- қылмыстық саясаттың маңызды субъективтік факторы - бұл қылмыстан сақтандыру қызметіндегі: адам, азамат, тұлға. Тұлға – қоғамның маңызды мәселелеріне кәсіби салауатты көзқарасын білдіретін, үздіксіз ізденумен қайратты құлшыныстың нәтижесінде қоғамдық ортадан маңызды рольді иемденген адам;

- қоғамдық сананың құрамдас элементтері ретінде құқықтық сананың, құқықтық – идеологияның, құқықтық психологияның қалыптасу ерекшелігі мен дағдылану тәртібі, сондай – ақ қылмыстық саясат субъектілерінің саяси шешімдері мен әрекеттері – қылмыстық саясаттың субъективтік факторларының негізгі белгілері мен тұлғаның рухани тұрпатын көрсетеді.

Қазақ билері де қылмыстық саясаттың өзіндік нысанының авторлары. Мал ұрлығы, жесір, жер дауы – билер тарапынан тиянақты да тұрақты өз шешімін тауып отырған. Қазақ халқының би-шешендері ерекше тұлғалар санатына жатады. Олардың ерекшелігі – бойындағы елді аузына қаратып, жедел шешімдер қабылдау қасиеті басқа халықтарда өте сирек кездескен. Біздің заманымыздан бұрын II-III ғасырлардағы Мәнді би, Елсау би, Оңқай би, Майқы би тәрізді қадым заманның дара да дана билерінің құқықтық ойлары бүгінге келіп жетті. Қазақтың бас биі Майқы би Мәнұлының:

Халқыңды билеместен бұрын өз орданды биле.

Орданды жұмған жұдырықтай берік ұстасан

Халық ешқайда қашпайды.

Хан өздігінен өлім жазасын қолданбасын.

Өлім жазасын шешетін халықтың өзі болсын дей келе,

Парақор биге ісің түспесін

Сараң үйге кісің түспесін – деп, мүліктік қатынастарға қатысты:

Момынның ақысы зәлімге кетпес, кетсе де ұжмаққа қолы жетпес [1, 15 б.] – деген халық басқару, сот билігі, сыбайлас жемқорлықпен, меншікке деген пайдақорлық-озбырлық, зорлық

қылмыстарының қауіптілігін меңзеген ғұлама сөздері – ұрпаққа мұра, адастырмас бағыт.

Зерттеудің осы тұсынан қылмыстық саясаттың мазмұнын белгілейтін объективті және субъективті факторлардың негізгілеріне тоқталайық.

Қылмыстық саясаттағы объективті және субъективті факторлар – бұл адам мәселесі, оның даму, мінез, қоршаған ортаға деген бейімділігі мен көзқарастары. Қылмыстық саясаттың негізі, оның жасалу жолдары- философияның, әлеуметтанумен, идеологияның негізі – адам болмысынан бастау алады. Адамның жеке тұлғасы мен оның адами қасиеттері адамның біртұтас келбетін қалыптастырады, сөйтіп, адам қоғамды түсінуге бейімделе бастайды. Мемлекеттік тұрпаттың зайырлығына қарамастан адам өмірінде олардың діни сенімі зор роль атқарып келеді. Қоғамдық өмірдегі субъективті және объективті факторлардың қолданылуы мен оның түрлі мәнге ие болуы – құқықтық экономика мен саясатқа әсерінің нысанын үлгілейді. Мысалы, ағылшындардың құқық жүйесіндегі соттық прецеденттердің ролі, құлиеленушілік құқықтың классикалық сипатына тән Рим құқығының нормалары Еуропа құрлығының құқықтық жүйесінің әлі күнге құрамдас элементі ретінде белгілі. Құқықтық мемлекетті құру сатысындағы Қазақстанның қылмыстық саясаты – дербес мәнге, көп қырға ие болды. Мемлекеттің даму кезеңімен құқықтың пайда болуы да қарайлас, оның себебіне мемлекет пен құқықтың тарихи кезеңдері негізгі қоғамдық-экономикалық формациялар мен өндірістік қатынастардың дамуының табиғи кезеңдеріне сай келеді. Құқықтық мемлекет ретіндегі Қазақстанның қылмыстық саясаты – жетекші Еуропа мемлекеттерінің революцияға дейінгі және Кеңестік қылмыстық саясаттың дағдылы әдістері мен қарама-қайшылықтарын, маңызды тұстарын ескерген, өзара қайшылықты, бәсекелес екі жүйенің (социализм мен капитализм) өзіне тән әдістері мен ерекшеліктерін құрамына сіңірген, үздіксіз дамудың келесі кезеңіндегі күрделі, мемлекеттік мүдделі әрекеттердің кешенді жиынтығы. Қазақстанның қылмыстық саясатының объективті көрінісін біз төмендегі ерекшеліктерін ескере отырып, былай ұсынамыз:

- қылмыстық саясаттың дамуы - әлеуметтік айқындылықтарға яғни, экономика және саясат, өндірістік және саяси қатынастардың дамуына тікелей байланысты;

- әлеуметтік жүйедегі Қазақстанның қылмыстық саясаты – түрлі кезең қылмыстық саясатының құқықтық жалғасы болып табылғанмен, қоғам дамуының жаңа заңдылықтарымен құнарландырылған – қылмыстық саясаттың жаңа түрі;

- Қазақстанның қылмыстық саясатының дамуының негізгі ағымдары – қоғам мүшелерінің негізгі құқықтары мен бостандықтарын, мүдделерін қорғау жолындағы қызметтің үрдісінен көрініс табады. Бұл жерде теория мен тәжірибенің қарама-қайшылығының тұстары даму үрдісінің бағыттарын тежеп отырғандығы жасырын емес;

- Қазақстанның қылмыстық саясатының ұлттық және өркениетті негіздерін – Қазақ билерінің кесімді шешімдері мен дала заңының ұлттық нұсқалары (Жеті жарғы т.б.) және де шетелдік нұсқалардың үздік тұстары құрайды;

- Қазақстанның қылмыстық саясаты - әлеуметтік даму заңдылығына орай, тұрақты, қатаң сипатқа ие емес, бірақ та оның дамуының тарихи кезеңдері - дөрекі материалдық нысаннан рухани нысанға ойысып бара жатқаны назар аудартады.

Сонымен қатар, биылғы жылы Астана қаласында өткен әлемдік және дәстүрлі діндер көшбасшыларының III съезі жиырмадан астам ел мен бірқатар діни ұйымдардың басын қосып, бұл құрамда БҰҰ, ЕҚЫҰ, ЮНЕСКО сынды беделді ұйымдардың өкілдері де болды. Съезд барысында Ислам діні тарапынан Мысыр, Индонезия, Кувейт, Сауд Арабиясы өкілдері мен Христиан конфессиясы тарапынан римдік католиктер, орыс православтары, англикандық, константинопольдік православтар, армяндық апостольдік шіркеу, бүкіләлемдік лютерандық федерация, иудаизм делегациялары қатысып, әлемдік дін тақырыбына қатысты біраз мәселелерді талқылады. Мемлекеттік нысан зайырлы ретінде танылып отырса да, азаматтарды қылмыстан сақтандыруда діни уағыздар мен дінбасылардың әсері қоғамымызда ерекше орын алып отырғандығын атап өту керек.

Діни сенім көп жағдайда адамды қылмыстан сақтандырушы да фактор екендігі жасыруға болмайды. «Құран - әрі адамзаттың тәрбиешісі. Құранның басты мақсаты – адам баласының жан-тәнін кірден арылтып, рухына ғайыптық қанат тағып, жәннатқа лайық ету. Асылында, Құраннан тәлім-тәрбие алған адам рухының бұл дүниесі де жәннатқа ұқсас. Өйткені адамның жан дүниесі мен болмысын тәрбиелеуде ең кемел әдісті адамды жоқтан жаратқан Аллаһ Тағала ғана біледі. Ендеше, Құран – адамзаттың жалғыз тәрбиешісі» [2, 18 б.]. Бұған біз, қылмыстан сақтандыру мен қылмыстың жолын кесудегі діни нандырудың ықпалының да белгілі дәрежедегі күші бар деген пікір ғана қосамыз. Қылмыстылықтың кей аумақтарда ұлттық қауіпсіздікке тигізіп отырған қауіп мемлекеттің зайырлы, құқықтық сипатына нұқсан келтіруде. Бұл жағдай Қазақстан Халықтары Ассамблеясының биылғы XV съезінде мемлекет басшысы Н.Ә. Назарбаев дін істері жөніндегі агенттік құрудың қажеттілігі туындап отырғанын атап көрсетті. Біздің ойымызша, құрылатын дін істері жөніндегі агенттік адамдардың діни бағыт бойынша адасушылығының алдын алып қана қоймай, Қазақстан Мұсылмандары Діни басқармасының да жұмысын бір жолға қоюға атсалысатын болар еді. Бұл мәселелердің шешілмеуі қазіргі таңдағы бірқатар ТМД елдеріндегі шиеленісті жағдайлар мен балқан, ирак төңірегінде қалыптасқан келеңсіз құбылыстардың бізде де туындауына негіз болуы мүмкін. Өкінішке орай, қордаланған кемшіліктерден пайда болған бұл қауіп көздері адам өмірі мен құқығын қорғауды қиындатып қана қоймай, ең төменгі сатыға ысырып тастады. Рухани өркендеу - Қазақстанның нигилистік көзқарасқа қарсы азаматтарының құқықтық білім мен қоғамдық құндылықтарды бағалау, оқу барысында тапқан ортақ қазынасы. Құқықтық мәдениет – тұлғаның жүріс – тұрысының ізгілігі мен оның пікірлерінің – өзге қоғам мүшелеріне түрткі салуынан басталады. Құқықтық мәдениеттің қалыптасуына немесе құқықтық мәдениетті тұлғаның ой – пікіріне қарсылық білдіру – қылмыстың жасалуының ізгілікке қарсы бейқұқықтық негізі. Жұмыссыздықты жою немесе Қазақстан азаматтарының жұмыспен қамтылуы – қылмыстың өрістеуіне немесе деңгейінің төмендеуіне тікелей әсері бар құбылыс. Қазақтың бас ақыны Абай Құнанбайұлының:

«Қазақтың біріне – бірінің қаскүнем болмағының, жалпы жалған қылмыстық қудалаудың негізгі себебіне жалқаулықты, қайратсыздықты, ақылсыздықты, надандықты» жатқыза отырып, билікке жету жолындағы адамдыққа жат әрекеттердің тізімін өзінің ғұламалы ғибраттарында жеткілікті көрсеткен [3, 11-12 бб.].

Қоғамдық дамудың объективті факторы – бұл біздің ойымызша, адам санасының жартылай тәуелді жағдайлар мен қатынастардың күрделі сипатты иеленуі: объективті фактор - әлеуметтік саяси, идеологиялық қатынастардың көрінісі бола отырып, қоғамның басым бөлігінің өз мүддесі үшін күресінің әдіс-тәсілдерінің жиынтығынан құралады. Объективті факторлардың қалыптасу қайнар көздеріне: сыртқы көріністерінің адам санасына жағымдылығы, қылмыстық ахуалдың тұрақтылығы, адам мен құқық қорғау органдарының «құқықтық» бірлікте болуы, қоғам мүшелерінің әрекетінен – адамгершілік, әдет, ізгілік, эстетикалық мәннің байқалып отыруы жатады. Объективті фактор – қоғамдық санадан, оның саналық деңгейінен мән сапасына ие болады. Қоғамдық сана – адамның рухани жұптасуы, олардың ізгілік байланыстарының өнімі.

Адам өмірі, сауаттылығы оның көзқарас көкжиегінің кеңдігі, танымның теңдігі, бойында болашақ немесе бүгінгі тұлғалардың қасиеттерінің ара-кідік кездесуі – объективті және субъективті факторлардың күрделігіне жол ашады. Субъективті фактор – бұл субъектінің әлеуметтік – саяси, рухани қызметінің жиынтығынан, бағыты мен міндетінен қалыптасады. Субъективті фактор - қоғамдық дамудың индикаторы ретінде құқықтық мемлекет құрудағы тұлғаның белсенділігі мен оның мақсаттарының маңызының өлшемін анықтайды және тәртіптің мықтылығына деген адамдық үлестің өлшемін жасайды. Толықтыра айтсақ, қоғамдық қажеттіліктер негізінде туындайтын субъективті фактор дегеніміз – адам әрекеті мен қызметінің әлеуметтік, идеологиялық, саяси мәнмен ұштасуы және адамның шынайы қажеттіліктерінің тізімі. Сондай-ақ – объективті факторлардың жоғарыдағы тұжырымдарын қуаттай отырып, объективті фактор – оның ішінде қылмыстық саясатқа тікелей қатысты объективті фактор дегеніміз – субъективті факторлардың басқа сипатты иеленуі, сондай-ақ

әлеуметтік күштердің, мүдделердің үздіксіз қақтығысуының қоғамдық бейнесі деген көзқарасымызды ғылыми даудың талқысына саламыз.

Заң ғылымы әдебиеттерінде қылмыстық саясаттың экономика, саясат, идеологиялық және қоғамдық дамудың басқа да бірқатар факторларымен біріккен жүйелесуі қарастырылмаған. Бұл құбылыстар қылмыстық саясаттың әлеуметтік мәнін ашу кезінде жағдай деп талқыланады. Шындығында экономика мен саясат – қылмыстық саясаттың қалыбын ғана қалыптастырып қоймай, оның мәндік белгілерінің түпкі өзегіне де жатады. Қылмыстық саясат қылмыспен күрестегі мемлекеттік басқару мен қылмыстылыққа құқықтық әсер етудегі мемлекеттік басымдық берудің нысаны. Қылмыспен күрестің үздіксіздігі, жүйелілігі, оның элементтерінің толықтығы (саяси – құқықтық қатынас, құқықтық норма, құқықтық сана, құқықтық идеология, қылмыстық саясат субъектісінің өкілетті әрекеті) ғана – қылмыстылықпен күресте, одан сақтандырудағы мемлекеттің жеңісін жасайды.

Сонымен қатар Абайдың рухани мұрагері Шәкәрімнің:

Адамның айуаннан айласы мол,

Қит етсе, қиянатқа қояды қол.

Мейірім, ынсап, ақ пейіл, адал еңбек –

Бұл төртеуін кім қылса, шын адам сол – деген рубаяттары - иманның бағасына құн бере отырып, қазіргі заманауи қылмыстық саясаттың тынысымен үндесетіндігі – даусыз ақиқат [4, 10 б.].

Жұмыссыздықтың қоғамға қауіптілігі оның қылмыстың өршуіне бастау болатындығынан ғана емес, бұл фактордың адамды қалыпты дамудан ажыратып қана қоймай, келелі мәселелерді талқылауға қатысу мүмкіндігін шектеу арқылы бүкіл адамдық болмысты игі құбылыстарға қарсы қоюынан да байқалады. Сондықтан да еліміздегі шетелдік жұмысшыларды отандық кадрлармен біртіндеп алмастыру арқылы мемлекеттегі тыныштық пен келісімді сақтаудың маңызын арттыруға, барша Қазақстандықтарды еңбекқорлық пен табандылыққа тәрбиелеуге болады. Ал бұл Қазақстан азаматтарын «қылмыстың негізгі қасиеті болып табылатын қоғамға қауіптіліктен», сондай-ақ, қауіпті әрекеттен, бастамадан, ойдан алыстату деген сөз [5, 3 б.].

Қаржыландыру. Ғылыми мақала Қазақстан Республикасы Ғылым және жоғары білім министрлігі Ғылым комитеті қаржыландыратын, 2024-2026 жылдарға арналған ғылыми және (немесе) ғылыми-техникалық бағдарламалар бойынша бағдарламалық-нысаналы қаржыландыру аясында, BR28713695 «Әйелдер мен жасөспірім қыздарға қатысты зорлық-зомбылық мәселелері бойынша отбасы мен қоғамның ынтымақтастығының теориялық және әдіснамалық негіздері» жобасын іске асыру шеңберінде дайындалды

Әдебиеттер тізімі

1. Төрекұл Н. Даланың дара ділмарлары. - Алматы: ЖШС «Қазақстан баспа үйі», 2001. - 592 б.
2. Исаұлы М. Құран кімнің сөзі? – Алматы: «Алтын қалам», 2004 – 252 б.
3. Абай. Қара сөз. Поэмалар. – Алматы: Ел, 1993. - 272 б.
4. Шәкәрім. Иманым. – Алматы: «Арыс», 2000. - 321 б.
5. Богомяков Ю.С. Роль субъективных признаков деяния в установлении объекта умышленных преступлений. Вопросы эффективности борьбы с преступностью и совершенствования законодательства. Тематический сборник. – УФА, 1975. - № 1. – С.3-12.

«IT LAW FORUM: ЖАСАНДЫ ИНТЕЛЛЕКТ,
ЦИФРЛАНДЫРУ ЖӘНЕ ҮЛКЕН ДЕРЕКТЕР -
ҚҰҚЫҚТЫҢ ЖАҢА ШЕКАРАЛАРЫ»

V ЖЫЛ САЙЫНҒЫ ФОРУМ

МАТЕРИАЛДАРЫ
2026 ж. 16 маусым

МАТЕРИАЛЫ

V ЕЖЕГОДНОГО ФОРУМА

«IT LAW FORUM: ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ,
ЦИФРОВИЗАЦИЯ И БОЛЬШИЕ ДАННЫЕ -
НОВЫЕ ГРАНИЦЫ ПРАВА»

16 июня 2026 г.

Подписано в печать 30.10.2026г.
Формат 60х84^{1/16}. Бумага офсетная 80гр/м².
Усл.печ.л.23. Гарнитура «Times».

Отпечатано в ТОО «Tandem-2»



NARXOZ
UNIVERSITY