

А.Ж. Жаналиева , Н.Н. Жаксылыков ,
М.О. Алтаева , Т.Б. Тленшин , М.Н. Мамаева* 

Университет Мирас, Шымкент, Казахстан

*e-mail: mmakbal85@mail.ru

ЦИФРОВОЙ СЛЕД ЛИЧНОСТИ: ПРОБЛЕМЫ ПРАВОВОЙ ИДЕНТИФИКАЦИИ В ЗАКОНОДАТЕЛЬСТВЕ РЕСПУБЛИКИ КАЗАХСТАН

Актуальность темы исследования определена необходимостью более глубокого анализа рисков и угроз, вызванных агрессивной цифровизацией жизни современного общества на фоне низкой информационной культуры общества и халатного отношения граждан к вопросам информационной безопасности.

В научной литературе появились некоторые исследования такого понятия как «цифровой след». Но они недостаточны с точки зрения обоснования необходимости внедрения данного понятия в проект Цифрового Кодекса Казахстана. В этой связи, представленное исследование направлено на то, что бы обратить внимание научной общественности, законодателя и правоприменителя к проблеме информационной безопасности личности в цифровой среде, которая, главным образом, обусловлена сохранением и возможностью незаконного использования информации, оставляемой субъектом в виртуальном пространстве при совершении им каких-либо действий в интернет-среде.

Цель исследования заключается в анализе современного подхода отечественного законодателя к понятию информационных обязанностей и ее составляющим с акцентом на понятие «цифрового следа» как составной информационно-правового статуса субъекта информационных правоотношений.

В результате проведенного нами исследования были сделаны реальные выводы о том, что требуется более пристальное внимание законодателя об ответственности за сбор и хранение личной информации, отслеживание действий личности в цифровой среде. Дано авторское понятие «цифрового следа личности». Обосновано, что действующее законодательство должно содержать не только этот термин, но и иметь целый блок положений о регулировании использования такого «цифрового следа». Обоснована позиция о том, что необходима огромная разъяснительная работа о информационной безопасности как важного приоритета национальной безопасности.

Ключевые слова: информация; информационная безопасность, цифровой след, цифровая личность, цифровой двойник, цифровой образ, цифровой профиль, сбор и хранение личной информации.

A.Zh. Zhanalieva, N.N. Zhaksylykov,
M.O. Altayeva, T.B. Tlenshin, M.N. Mamayeva*

Miras University, Shymkent, Kazakhstan

*e-mail: mmakbal85@mail.ru

Digital identity footprint: problems of legal identification in the legislation of the Republic of Kazakhstan

The relevance of the research topic is determined by the need for a deeper analysis of the risks and threats caused by the aggressive digitalization of modern society's life against the background of the low information culture of society and the negligent attitude of citizens to information security issues.

Some studies of such a concept as a "digital footprint" have appeared in the scientific literature. But they are not sufficient in terms of justifying the need to introduce this concept into the draft Digital Code of Kazakhstan. In this regard, the presented research is aimed at drawing the attention of the scientific community, legislators and law enforcement officers to the problem of personal information security in the digital environment, which is mainly due to the preservation and possibility of illegal use of information left by a subject in the virtual space when performing any actions in the Internet environment.

The purpose of the study is to analyze the modern approach of the Russian legislator to the concept of information obligations and its components, with an emphasis on the concept of "digital footprint" as an integral part of the information and legal status of the subject of information relations.

As a result of our research, we have drawn real conclusions that we need more attention from the legislator on the responsibility for collecting and storing personal information, tracking personal actions in the digital environment. The author's concept of the "digital footprint of personality" is given. It is justified that the current legislation should contain not only this term, but also have a whole set of provisions regulating the use of such a "digital footprint". The position that a huge amount of explanatory work is needed on information security as an important priority of national security is substantiated.

Keywords: information, information security, digital footprint, digital identity, digital double, digital image, digital profile, collection and storage of personal information.

А.Ж. Жаналиева, Н.Н. Жаксылыков,
М.О. Алтаева, Т.Б. Тленшин, М.Н. Мамаева*
Мирас университеті, Шымкент, Қазақстан
*e-mail: mmakbal85@mail.ru

Жеке тұлғаның цифрлық ізі: Қазақстан Республикасының заңнамасындағы құқықтық сәйкестендіру мәселелері

Зерттеу тақырыбының өзектілігі қоғамның ақпараттық мәдениетінің төмендігі және азаматтардың ақпараттық қауіпсіздік мәселелеріне немқұрайлы қарауы аясында қазіргі қоғамның өмірін агрессивті цифрландырудан туындаған тәуекелдер мен қауіптерді тереңірек талдау қажеттілігімен анықталады.

Ғылыми әдебиеттерде «сандық із» сияқты кейбір зерттеулер пайда болды. Бірақ олар Қазақстанның Цифрлық кодексінің жобасына осы тұжырымдаманы енгізу қажеттілігін негіздеу тұрғысынан жеткіліксіз. Осыған байланысты, ұсынылған зерттеу ғылыми қоғамның, заң шығарушының және құқық қолданушының назарын цифрлық ортадағы тұлғаның ақпараттық қауіпсіздігі мәселесіне аударуға бағытталған, бұл негізінен субъект интернет ортасында қандай да бір іс-әрекеттер жасаған кезде виртуалды кеңістікте қалдырған ақпаратты сақтау және заңсыз пайдалану мүмкіндігіне байланысты.

Зерттеудің мақсаты – отандық заң шығарушының ақпараттық міндет ұғымына және оның құрамдас бөліктеріне ақпараттық құқықтық қатынастар субъектісінің ақпараттық-құқықтық мәртебесінің құрамдас бөлігі ретінде «цифрлық із» ұғымына баса назар аударып, қазіргі көзқарасын талдау.

Біз жүргізген зерттеу нәтижесінде заң шығарушының жеке ақпаратты жинау және сақтау, цифрлық ортадағы жеке тұлғаның іс-әрекетін бақылау жауапкершілігі туралы мұқият назар аударуы қажет деген нақты тұжырымдар жасалды. «Тұлғаның сандық ізі» авторлық тұжырымдамасы берілген. Қолданыстағы заңнамада тек осы термин ғана емес, сонымен қатар осындай «цифрлық іздің» қолданылуын реттеу туралы ережелердің тұтас блогы болуы керек екендігі негізделген. Ұлттық қауіпсіздіктің маңызды басымдығы ретінде ақпараттық қауіпсіздік туралы үлкен түсіндіру жұмыстары қажет деген ұстаным негізделген.

Түйін сөздер: ақпарат, ақпараттық қауіпсіздік, сандық із, сандық тұлға, сандық егіз, сандық сурет, сандық профиль, жеке ақпаратты жинау және сақтау.

Введение

В результате развития информационных технологий в конце XX и начале XXI в. стала оцифровка многих процессов и создание цифровых копий в виртуальном пространстве. Многие считают, что первый уровень выходит проблема цифровой личности.

Понятие «цифровой личности» все еще не сформировано в полном объеме. Присутствуют различные подходы. Так, наиболее распространенным является мнение о том, что «цифровой человек» – это личность, переведенную в цифровую форму, которая составлена из записей, фрагментов данных и кусочков информации (Sartor, 2017). Поэтому появилось еще одно понятие «цифровой клон» (Sullivan, 2009) или цифровой двойник.

Вся цифровая система выстроена таким образом, что позволяет не только обмениваться данными и хранить их, но и отслеживать каждый IP-адрес, его операции как запрашиваемые, так и проводимые, местонахождение пользователя и прочее. Именно на этом выстроены различные системы анализа и прогнозирования, персонализированные рекомендации, диспетчерские решения и т. д. в основном выстроены в процесс маркировки данных и портрета данных. Если эти портреты не имеют границ и не ограничены, данные о личности людей, их взаимоотношениях, местонахождении, имуществе, эмоциях и т. д. окажутся сгруппированными различными способами и путями и станут определенными объектами, которые будут наблюдаться, анализироваться и просматриваться, а цифровые

граждане превратятся в «людей, которых можно вычислить цифрами» (Скиннер, 2019).

Обзор литературы

Демкин В.О. предложил такое понятие как «структура цифровой личности», которая, по его мнению, включает в себя три основных элемента: цифровой профиль, цифровой образ и цифровой след (Демкин, 2024).

Все эти три элемента занимают важное место в исследованиях современного информационного права. Более того, проблематика правового регулирования генезиса цифровой личности приобретает в настоящее время особую актуальность. Целый ряд международных нормативных актов посвящен попыткам регулирования статуса и защиты «цифровой личности» и трех ее составляющих.

В первую очередь это резолюция Совета ООН по правам человека от 16 июня 2012 г. A/HRC/RES/20/8, которая подтверждая права человека и основные свободы, закрепленные во Всеобщей декларации прав человека и в соответствующих международных договорах по правам человека, включая Международный пакт о гражданских и политических правах и Международный пакт об экономических, социальных и культурных правах, подтверждает, что те же права, которые человек имеет в офлайновой среде, должны также защищаться и в онлайн-среде (<https://www.riigiteataja.ee/>). Что, по сути, означает как само наличие цифровой личности, так и то, что она обладает теми же правами, что и личность в реалии.

Другая Резолюция Генеральной Ассамблеи ООН от 18 декабря 2013 г. A/RES/68/167 посвящена уже праву на неприкосновенность личной жизни в цифровой век указывает на то, что развитие информационных и коммуникационных технологии позволяет отслеживать, перехватывать и собирать информацию как правительствам, так и физическим и юридическим лицам, что может привести к нарушению или ущемлению прав человека, особенно права на неприкосновенность личной жизни (<https://undocs.org/ru>)

Вопросы информационной безопасности продолжают в целом ряде иных резолюции ООН. Так, важным является Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» в которой под-

черкивается, что информационно-коммуникационные технологий являются технологиями двойного назначения и могут использоваться как в законных, так и в злонамеренных целях, выражая обеспокоенность, что ряд государств занимается наращиванием потенциала в сфере ИКТ для военных целей, а использование ИКТ в будущих конфликтах становится все более вероятным. В этой связи ООН призывает государства предотвратить использование информационных ресурсов или технологий в преступных или террористических целях, подчеркивая важность уважения прав человека и основных свобод в сфере использования ИКТ путем принятия и реализации своих национальных юрисдикции. Но при этом подчеркивается, что именно государства несут главную ответственность за поддержание безопасной и мирной ИКТ-среды, но частный сектор, научные круги и организаций гражданского общества могли бы способствовать повышению эффективности международного сотрудничества (<https://docs.un.org/>).

Особо следует выделить Резолюцию Генеральной Ассамблеи ООН от 14 декабря 2022 года A/RES/77/150 «Использование информационно-коммуникационных технологий в целях устойчивого развития», которая вносит целый ряд рекомендации государствам, межгосударственным объединениям, бизнесу и научному сообществу по вопросам использования ИТК в целях устойчивого развития как отдельных государств, так и всего мира с учетом необходимости продвижения цифровой экономики.

В целом эти и иные рекомендации ООН лежат в основе действующего законодательства об информатизации и цифровизации членов-участников.

Вместе с тем, каждая страна принимая свое суверенное законодательство устнавливает свои принципы регулирования соответствующих общественных отношений.

Соответственно, наш отечественный опыт реализации действующего законодательства и необходимость его совершенствования также подлежат критическому анализу со стороны правоприменителей и особенно со стороны научно-го сообщества.

Методология

Методологическую основу исследования составляет совокупность общенаучных и специальных методов изучения явлений и процессов.

Представленное исследование осуществлено на основе анализа большого объема международных актов, рекомендации ООН, законов и нормативно-правовых актов Республики Казахстан, Китайской Народной Демократической Республики, Российской Федерации и ряда других стран.

Исследование также проводится на основе сравнительного анализа отечественного законодательного подхода в ретроспективе. А именно приводятся положения действующего законодательства и нормы предлагаемого уполномоченным органом РК проекта Цифрового кодекса с объяснением позиции и сравнением с новейшими течениями мирового опыта. Такой подход является эффективным и позволяет осуществить критический анализ казахстанских тенденций.

Особо следует отметить применение экспертных оценок специалистов в сфере ИИ и государственного управления, что позволяет получить не только нормативный, но и практический обзор поднимаемой проблемы.

Результаты и обсуждение

Основным заказчиком, обладателем цифровых данных является государство. Только оно обладает возможностью инициирования сбора информации по неограниченному кругу своих граждан, иностранцев и лиц без гражданства, контактирующих с ним. И практика показывает, что многие государства активно пользуются такой возможностью постепенно наращивая и расширяя как круг субъектов, так и виды требуемой информации. Такая информация в современных условиях подлежит цифровизации и постоянному (неограниченному) хранению.

Так, в качестве примера можно привести, например, новые требования Российской Федерации, которые вводят требования обязательной дактилоскопии при пересечении государственной границы (<https://online.zakon.kz/>). Подобные требования действуют и в целом ряде других стран, таких как США, Малайзия, ОАЭ, Китай и пр. И это лишь один из примеров сбора информации.

В отношении же своих собственных граждан государства запрашивают более широкий круг данных личного характера, которые, по сути, носят конфиденциальный, личный характер. И государство имеет на это право, как основной регулятор общественных отношений, несущий ответственность за безопасность. Таким образом формируется цифровой профиль каждой

личности. По мнению Демкина В.О. цифровой профиль – это «наиболее важная часть цифровой личности, представляющая собой совокупность персональных и иных связанных с ними данных индивида в виртуальном пространстве, содержащихся в информационных базах уполномоченных на их обработку субъектов» (Демкин, 2024).

Такой цифровой профиль содержится в специальных государственных системах, подлежащих безусловной защите. В отечественном законодательстве это законы РК «О национальной безопасности» от 6 января 2012 года № 527-IV, «О государственных секретах» от 15 марта 1999 года № 349-I, «Об информатизации» от 24 ноября 2015 года № 418-V, «О персональных данных и их защите» от 21 мая 2013 года № 94-V, «О государственных услугах» от 15 апреля 2013 года. Непосредственная детализация обеспечивается подзаконными актами уполномоченных органов, например такими как Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 406/НК «Об утверждении Правил сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг» и пр.

Но помимо данных, любое использование Интернета оставляет след, который позволяет не только проследить местоположение, финансовые или иные операции субъекта, но и многое другое. Так, А.Е. Жатканбаева отмечает, что «Цифровые следы» позволяют отслеживать не только действия или местонахождение лица, но и анализировать его предпочтения, просчитывать его поведение (это может использоваться как в негативном формате, так и в позитивном, например, как маркетинговое исследование и пр.). В итоге цифровой след создает цифровую репутацию человека (сейчас работодатель предпочитает принимать решение о трудоустройстве на основании соответствующего анализа цифровой репутации человека). Это неизбежный процесс, который получает все большее распространение, а в некоторых областях и предпочтение» (Жатканбаева, 2025). Более того, интеллектуальный анализ данных, основанный на технологиях ИИ, дает возможность по полученным сведениям прогнозировать и направлять поведение индивида и целых групп, ранжировать субъектов и оценивать их действия

Действительно, цифровой след как совокупность информации, оставляемой субъектом в виртуальном пространстве при совершении им

каких-либо действий в интернет-среде сегодня это очень важная составляющая жизнедеятельности современного человека. Не менее одной третьей жизни мы уже проводим в Интернете, перенеся в виртуальную среду ряд своих интересов, потребностей, вкусов и предпочтений. Поэтому вопросы правового регулирования использования информации о наших следах в Интернет-пространстве в современном мире имеет огромную роль.

Именно этот вопрос сегодня очень актуален с точки зрения информационной безопасности не только личности, но и общества в целом, тогда как опыт правового регулирования по данному вопросу ситуативен и бессистемен. Эти общественные отношения или носят фрагментарный характер или отсутствуют полностью.

Установлен правовой запрет на распространение информации о личных, персональных данных, но отсутствует твердая позиция о том носит ли информация об операциях, действиях в Интернете носит закрытый характер или может быть свободно использован бизнес или иных структур.

Следует понимать, что сам факт оставления цифрового следа в подавляющем большинстве случаев не осознается человеком. Это обусловлено тем, что взаимодействие с цифровой средой происходит в повседневном режиме и воспринимается как нейтральный и безопасный процесс. Это служит хорошей возможностью при расследовании преступлений или иных действиях государственных органов. Но вместе с тем, этот же факт играет и против интереса человека.

Фактически отсутствует понимание юридического статуса «цифрового следа». Что это за событие? Влечет ли оно за собой правовые последствия, если да, то когда и какие? Следует ли отнести цифровой след к конфиденциальной информации и можно ли обеспечить ее закрытость?

Эти обстоятельства обусловили широкую академическую дискуссию о проблемах обеспечения прав человека в «цифровом мире» – начиная с прикладных вопросов получения согласия субъекта на обработку его персональных данных и заканчивая глобальной угрозой массовой «цифровой слежки» со стороны правительств разных стран.

Ситуация усугубляется также тем, что «многие государства ... в последнее десятилетие ввели законодательное регулирование, регламентирующее особенности оборота тех или иных разновидностей цифровых следов. По этой

причине глобальная проблема, преломляясь через законодательство той или иной страны, неизбежно приобретает национальное измерение. Подходы, складывающиеся в отдельных государствах, отличаются своеобразием, в связи с чем их сравнительное исследование заслуживает отдельного обсуждения» (Мочалов, 2024). В таком многообразии вариантов решения проблемы Казахстану необходимо определиться.

Начнем с анализа технических характеристик цифрового следа, что, несомненно, позволит дать его правовую характеристику.

Так, по способу закрепления цифровые следы можно разделить на два вида: которые сохраняются только на пользовательском устройстве, с которым взаимодействует индивид и которые записываются в память носителей информации, не принадлежащих пользователю. Это имеет огромное значение в вопросе обеспечения конфиденциальности. В основном это зависит от того, подключено ли данное устройство к Интернету. Само подключение к Интернету означает высокий уровень утечки информации, что учитывается специалистами при обеспечении информационной безопасности.

Но большинство операции в современном мире простой человек осуществляет благодаря сотовым телефонам, что автоматически означает, что подавляющее большинство следов являются не конфиденциальными или с низким уровнем конфиденциальности.

Далее, по режиму доступа цифровые следы, передаваемые посредством сети Интернет, можно подразделить на следы ограниченного доступа (они доступны пользователю или ограниченному им кругу лиц) и общедоступные следы. Как правило режим доступности определяется самим владельцем устройств или страниц в социальных сетях, либо оговаривается при оказании тех или иных услуг, оказываемых посредством Интернета.

Определенная попытка решения этих задач предпринята в процессе разработки Цифрового кодекса, который был принят в работу Мажилисом Парламента (данные на сентябрь 2025 года).

Представленный проект устанавливает, что целью цифрового законодательства Республики Казахстан является определение правовых основ, задач и принципов, а также механизмов реализации единой государственной политики в цифровой среде (<https://online.zakon.kz/>).

Основными принципами государственной политики в цифровой сфере в числе других являются приоритет прав и свобод человека и

гражданина и безопасность личности, общества и государства.

Под приоритетом прав и свобод человека и гражданина понимается то, что развитие цифровых технологий, в том числе, с применением искусственного интеллекта, не должно умалять права и свободы человека и гражданина и государство обязано разрабатывать эффективные юридические гарантии защиты граждан от дискриминации при автоматизированной обработке данных, в том числе, с применением алгоритмов искусственного интеллекта. А под обеспечением безопасности в проекте отмечено, что государство, субъекты частного предпринимательства, иные организации обязаны принимать необходимые меры для оценки и предотвращения потенциальных рисков негативного воздействия развития и применения цифровых технологий на права и свободы человека, а также законные интересы общества, обеспечивать их этичное применение. И запрещается разрабатывать, и внедрять цифровые технологии, направленные на подрыв конституционного строя, общественного порядка, ущемление прав и свобод человека и гражданина.

В проекте обозначено, что защита объектов информатизации представляет собой комплекс правовых, организационных и технических мероприятий, направленных на сохранность объектов информатизации, предотвращение неправомерного и (или) непреднамеренного доступа и (или) воздействия на них и обеспечивается собственниками, владельцами и пользователями электронных информационных ресурсов.

Но при этом следует указать на то, что представленный проект Цифрового Кодекса – это попытка кодифицированного регулирования объединил в себе общественных отношений о цифровых услугах, об Цифровом (Электронном) правительстве, о ЭЦП, об информатизации, о персональных данных, об информатизации и связи.

Вместе с тем, данный проект является 2 представленным проектом. Первый проект 2024 года обозначил ряд цифровых прав субъектов персональных данных: право доступа к своим персональным данным; право на исправление неточных персональных данных; право на забвение; право на ограничение обработки, на переносимость данных, а также иные права.

Новый же проект, вынесенный на ознакомление, выделяют лишь право на идентичность и право на забвение. Право на идентичность озна-

чает право субъектов правоотношений в цифровой среде идентифицировать или не идентифицировать себя, за исключением случаев, когда обязанность идентифицировать себя установлена законами Республики Казахстан.

Право на забвение – право субъекта персональных данных требовать от собственника и (или) оператора базы персональных данных уничтожения своих персональных данных (<https://online.zakon.kz/>) Возможность удаления информации таких личных данных возникает тогда, когда эта информация стала неактуальной или является недостоверной.

Рассмотрим подробнее эти два права, так как каждое из них имеет прямое отношение к цифровому следу.

Идентичность в цифровом мире рассматривается как «активное цифровое изображение физического лица (гражданина), суть которого заключается в цифровом выражении воли, поведения и взаимоотношений физического лица (гражданина)», которое позволяет отслеживать цифровое воплощение естественного гражданина и цифровое выражение, которое несет в себе идентичность гражданина, логику действий, отношения прав и обязанностей в цифровой общественной жизни. Теоретическая реконструкция цифрового гражданина обеспечит важную теоретическую поддержку и ценностное руководство для построения цифрового правового государства (Ма Чаншань & Гун Нань, 2024).

В соответствии с проектом Цифрового кодекса, а в настоящее время Законом РК от 7 января 2003 года № 370-ІІ «Об электронном документе и электронной цифровой подписи» идентификация осуществляется специально уполномоченными органами по специальным правилам для физических лиц через индивидуальный идентификационный номер, а для юридических лиц – бизнес-идентификационный номер (<https://adilet.zan.kz>).

Проект устанавливает, что никто не может быть принужден к идентификации, за исключением случаев, установленных законами Республики Казахстан.

Идентичность в цифровом пространстве это очень важная составляющая уже с точки зрения безопасности. Если во взаимоотношениях в Электронным правительством или в вопросах банкинга вопросы цифровой идентификации более или менее ясны, то в других сферах никто не мешает тому или иному лицу создавать несколько аккаунтов или идентификаций с самым

разным имиджем, а также свободно взаимодействуют и выражают свое мнение в цифре.

Достоверная и единая система удостоверения цифрового гражданина – это важнейшее условие реальных отношений между цифровым правительством, бизнес-платформой и цифровым гражданином. В это вопросе важно на уровне законодательства обеспечить институциональное признание цифрового гражданина в публичном праве и права на цифровую личность в частном праве. В качестве примера следует привести опыт Китая, который на уровне закона устанавливает, что поставщики сетевых услуг при сборе личной информации должны получить на это согласие пользователя; поставщикам сетевых услуг запрещен сбор личной информации, не имеющей отношения к этим услугам; пользователь имеет право потребовать удаления информации о нем, а если она неверна – исправить ее. Одновременно с усилением защиты персональных данных была ликвидирована анонимность пользователей (<http://www.npc.gov.cn/>)

Но очень знаменательным является опыт Китая о том, что любой цифровой след, оставляемый ее гражданином, фиксируется, сохраняется и обрабатывается с помощью технологий искусственного интеллекта на Всекитайской объединенной и региональных платформах кредитной информации. Так, продаваемые в КНР смартфоны устанавливаются обязательные приложения, отслеживающие передвижение человека, его покупки, заказы, платежи, состояние здоровья, контакты, активность в соцсетях и Интернете и пр. При этом каждый смартфон привязан к его владельцу, личность которого идентифицирована. Для этого в 2010 г. всем пользователям мобильных телефонов пришлось зарегистрироваться под своим настоящим именем (Zhou, 2022).

Соответственно, такое признание должно обеспечиваться установлением определенного круга прав и обязанностей.

Кроме того, следует отметить, что в мировом пространстве различные страны используют различные подходы в том числе и в вопросах идентификации субъектов информационных правоотношений. Так, как и в реальном мире существуют «цифровые офшоры», позволяющие проходить регистрацию идентификационных кодов позволяющие не отслеживать их. Соответственно, такими услугами могут пользоваться Интернет-мошенники и иные преступные элементы, что также вызывает огромные риски и сомнения.

Представленный проект Цифрового кодекса помимо прочего предлагает также положение, в соответствии с которым владельцы цифровых систем и платформ обязаны по запросу субъекта правоотношений в цифровой среде удалить все цифровые данные и записи о таком субъекте, которые были предоставлены им добровольно, если иное не предусмотрено Законами Республики Казахстан.

Право на забвение уже действует в европейской правоприменительной практике. Оно выражено в Общем регламенте по защите данных (General Data Protection Regulation, далее – «GDPR» или «Регламент») и представлено достаточно широко. Данное право включает в себя право требовать исправления или уничтожения данных, обработанных с нарушением норм Регламента, право на отзыв своего согласия на их обработку и право требовать предоставления данных о себе в структурированном, повсеместно используемом и машиночитаемом формате соответственно (<https://itglobal.com/ru-kz/>)

Право на забвение в международном сообществе объективно связано с правом на неприкосновенность личной жизни. Вместе с тем, вся мировая общественность осознает, что «при формировании мощной цифровой памяти личная информация, попав в Сеть, остаётся там навсегда, как татуировка на теле человека. И право на забвение стало актом естественной самозащиты общественности (прежде всего в Европе) от всепроникающей власти Интернета (Wargo, 2009).

Российская Федерация в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» на цифровые следы, представляющие собой общедоступную информацию, в полной мере распространяется правовое регулирование распространения информации, а если цифровой след содержит запрещенную к распространению информацию, то доступ к ней может быть ограничен по требованию Роскомнадзора. Требование об удалении материала (страницы сайта) направляется владельцу сайта через провайдера хостинга (т. е. лица, предоставляющего вычислительную мощность для размещения сайта в Интернете), а в случае ее неудаления провайдер хостинга, а затем и оператор связи обязаны заблокировать доступ пользователей к соответствующей странице интернет-сайта. Ограничивать доступ к запрещенному пользовательскому контенту долж-

ны и владельцы социальных сетей (<https://www.consultant.ru/>).

Заключение

Подводя итоги, следует отметить следующие реалии настоящего времени:

1. международное сообщество пришло к пониманию потребности правового признания и регулирования «цифровой личности» и его прав и обязанностей в цифровом пространстве, о чем свидетельствует ряд рекомендаций ООН и опыт ЕС;

2. каждая страна стремится обеспечить регулирование данного вопроса через свою национальную информационную политику и политику защиты персональных данных, но с учетом общественного интереса;

3. в Республике Казахстан наблюдается значительное отставание по данному вопросу, а именно по признанию и введению в законодательство Казахстана таких понятий как «цифровой профиль» и «цифровой образ». Об этом

свидетельствует проведенный анализ проектов Цифрового Кодекса (первой и второй редакций);

4. тогда как дальнейшее отсутствие правового регулирования сбора и обработки информации, составляющей содержание цифрового следа личности, в Казахстане приведет к массовому нарушению прав и свобод человека.

Вклад авторов

А.Ж. Жаналиева: концептуализация, разработка методологии, научное руководство, редактирование и доработка текста. Н.Н. Жаксылыков: проведение исследования, сбор и обработка данных, формальный анализ, подготовка первоначального текста статьи. М.О. Алтаева: правовой анализ, работа с источниками, валидация результатов, редактирование текста. Т.Б. Тленин: подготовка визуальных материалов, интерпретация данных, редактирование текста. М.Н. Мамаева: управление проектом, привлечение финансирования, редактирование и доработка текста.

Литература

- Демкин, В. О. (2024). Цифровая личность и цифровой образ человека: характеристика и место понятий в системе смежных категорий. *RUDN Journal of Law*, 28(3), 512–527. <https://doi.org/10.22363/2313-2337-2024-28-3-512-527>
- Досье на проект Цифрового кодекса Республики Казахстан (апрель 2024 года). (2024). Получено 06 сентября 2025 г. с https://online.zakon.kz/Document/?doc_id=38933548&pos=1125;-45#pos=1125;-45
- Досье на проект Цифрового кодекса Республики Казахстан (сентябрь 2025 года). (2025). Получено 06 сентября 2025 г. с https://online.zakon.kz/Document/?doc_id=38933548&pos=43;-26#pos=43;-26
- Жатканбаева, А. Е. (2025). Конституционно-правовые основы информационной безопасности. В *Конституционализация права в Республике Казахстан: Эволюция, современное состояние и основные направления совершенствования законодательства: Сборник научных статей* (с. 121). Алматы: ТОО «Издательство Фортуна Полиграф».
- Закон об удостоверении личности резидентов (КНР). (2011). Получено 31 мая 2024 г. с http://www.npc.gov.cn/zgrdw/npc/xinwen/2011-10/31/content_1678466_2.htm
- Ма Чаншань, & Гун Нань. (2024). Формирование идентичности и защита прав цифрового гражданина в цифровом обществе. *Вестник Санкт-Петербургского университета. Право*, 15(2), 298–334. <https://doi.org/10.21638/spbu14.2024.201>
- Мочалов, А. Н. (2024). Цифровые следы человека и неприкосновенность частной жизни. *Антиномии*, 24(4), 164–189.
- Постановление Правительства Российской Федерации от 7 ноября 2024 года № 1510 «О проведении эксперимента по апробации правил и условий въезда и выезда из Российской Федерации иностранных граждан и лиц без гражданства» в период с 30 июня 2025 года до 30 июня 2026 года. (2024). https://online.zakon.kz/Document/?doc_id=33925087
- Приказ исполняющего обязанности Министра по инвестициям и развитию Республики Казахстан от 17 марта 2016 года № 281 «Об утверждении Правил регистрации, перерегистрации и аннулирования объектных идентификаторов в казахстанском сегменте объектных идентификаторов». (2016). Зарегистрирован в Министерстве юстиции Республики Казахстан 22 апреля 2016 года № 13615. <https://adilet.zan.kz/rus/docs/V1600013615>
- Резолюция Генеральной Ассамблеи ООН от 18 декабря 2013 г. A/RES/68/167 «Право на неприкосновенность личной жизни в цифровой век». (2013). Получено 06 сентября 2025 г. с <https://undocs.org/ru/A/RES/68/167>
- Резолюция, принятая Генеральной Ассамблеей 5 декабря 2018 года, A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». (2018). <https://docs.un.org/ru/A/RES/73/27>
- Резолюция Совета ООН по правам человека от 16 июня 2012 г. A/HRC/RES/20/8 «Поощрение, защита и осуществление прав человека в Интернете». (2012). Получено 06 сентября 2025 г. с <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/518012016001/consolide>
- Скиннер, К. (2019). *Человек цифровой. Четвертая революция в истории человечества, которая затронет каждого*.
- Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ (последняя редакция). (2006). https://www.consultant.ru/document/cons_doc_LAW_61798

General Data Protection Regulation (GDPR) – регламент по защите персональных данных, принятый Евросоюзом 25 мая 2018 года. (2018). Получено 06 сентября 2025 г. с <https://itglobal.com/ru-kz/company/glossary/gdpr/>

Sartor, G. (2017). Human rights and information technologies. В *The Oxford Handbook of Law, Regulation and Technology* (с. 424–450). <https://doi.org/10.1093/oxfordhb/9780199680832.013.79>

Sullivan, C. (2009). Digital identity – The legal person? *Computer Law & Security Review*, 25, 227–236. <https://doi.org/10.1016/j.clsr.2009.03.009>

Werro, F. (2009). The right to inform v. the right to be forgotten: A transatlantic crash. В *Liability in the Third Millennium: Liber Amicorum Gert Brüggemeier* (pp. 285–289). Baden-Baden.

Zhou, W. (2022). Digital citizenship in the era of meta-universe: Identity dilemma, practical logic and theoretical proof. *Dianzi Zhengwu [E-Government]*, 10, 62–74.

References

Demkin, V. O. (2024). Tsifrovaya lichnost i tsifrovoy obraz cheloveka: kharakteristika i mesto ponyatiy v sisteme smezhnykh kategoriy [Digital personality and digital image of a person: Characteristics and place of the concepts within related categories]. *RUDN Journal of Law*, 28(3), 512–527. <https://doi.org/10.22363/2313-2337-2024-28-3-512-527>

Dosye na proekt Tsifrovogo kodeksa Respubliki Kazakhstan (aprel 2024 goda) [Dossier on the draft Digital Code of the Republic of Kazakhstan (April 2024)]. (2024). Retrieved September 6, 2025, from https://online.zakon.kz/Document/?doc_id=38933548&pos=1125;-45#pos=1125;-45

Dosye na proekt Tsifrovogo kodeksa Respubliki Kazakhstan (sentyabr 2025 goda) [Dossier on the draft Digital Code of the Republic of Kazakhstan (September 2025)]. (2025). Retrieved September 6, 2025, from https://online.zakon.kz/Document/?doc_id=38933548&pos=43;-26#pos=43;-26

Zhatkanbaeva, A. E. (2025). Konstitutsionno-pravovyye osnovy informatsionnoy bezopasnosti [Constitutional and legal foundations of information security]. In *Konstitutsionalizatsiya prava v Respublike Kazakhstan: Evolyutsiya, sovremennoe sostoyaniye i osnovnyye napravleniya sovershenstvovaniya zakonodatelstva: Sbornik nauchnykh statey* [Constitutionalisation of law in the Republic of Kazakhstan: Evolution, current state and main directions of legislative improvement: Collection of scientific articles] (p. 121). Almaty: TOO “Izdatelstvo Fortuna Poligraf”.

Zakon ob udostoverenii lichnosti rezidentov [Law on identification of residents]. (2011). Retrieved May 31, 2024, from http://www.npc.gov.cn/zgrdw/npc/xinwen/2011-10/31/content_1678466_2.htm

Ma, Chanshan, & Gong, Nan. (2024). Formirovaniye identichnosti i zashchita prav tsifrovogo grazhdanina v tsifrovom obshchestve [Formation of identity and protection of the rights of a digital citizen in the digital society]. *Vestnik Sankt-Peterburgskogo universiteta. Pravo [Vestnik of Saint Petersburg University. Law]*, 15(2), 298–334. <https://doi.org/10.21638/spbu14.2024.201>

Mochalov, A. N. (2024). Tsifrovyye sledy cheloveka i neprikosновенност chastnoy zhizni [Digital traces of a person and privacy]. *Antinomii [Antinomies]*, 24(4), 164–189.

Postanovlenie Pravitelstva Rossiyskoy Federatsii ot 7 noyabrya 2024 goda No. 1510 “O provedenii eksperimenta po aprobatsii pravil i usloviy vyezda i vyezda iz Rossiyskoy Federatsii inostrannykh grazhdan i lits bez grazhdanstva” v period s 30 iyunya 2025 goda do 30 iyunya 2026 goda [Decree of the Government of the Russian Federation No. 1510 of 7 November 2024 “On conducting an experiment to test the rules and conditions of entry to and exit from the Russian Federation for foreign citizens and stateless persons” from June 30, 2025 to June 30, 2026]. (2024). https://online.zakon.kz/Document/?doc_id=33925087

Prikaz ispolnyayushchego obyazannosti Ministra po investitsiyam i razvitiyu Respubliki Kazakhstan ot 17 marta 2016 goda No. 281 “Ob utverzhdenii Pravil registratsii, pereregistratsii i annullirovaniya obyektnykh identifikatorov v kazakhstanskom segmente obyektnykh identifikatorov” [Order of the Acting Minister of Investments and Development of the Republic of Kazakhstan No. 281 of 17 March 2016 “On approval of the Rules for registration, re-registration and cancellation of object identifiers in the Kazakhstani segment of object identifiers”]. (2016). Registered in the Ministry of Justice of the Republic of Kazakhstan on April 22, 2016 No. 13615. <https://adilet.zan.kz/rus/docs/V1600013615>

Rezolyutsiya Soveta OON po pravam cheloveka ot 16 iyunya 2012 g. A/HRC/RES/20/8 “Pooshchreniye, zashchita i osushchestvleniye prav cheloveka v Internete” [UN Human Rights Council Resolution A/HRC/RES/20/8 of 16 June 2012 “The promotion, protection and enjoyment of human rights on the Internet”]. (2012). Retrieved September 6, 2025, from <https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/518012016001/consolide>

Rezolyutsiya Generalnoy Assamblei OON ot 18 dekabrya 2013 g. A/RES/68/167 “Pravo na neprikosновенност lichnoy zhizni v tsifrovoy vek” [UN General Assembly Resolution A/RES/68/167 of 18 December 2013 “The right to privacy in the digital age”]. (2013). Retrieved September 6, 2025, from <https://undocs.org/ru/A/RES/68/167>

Rezolyutsiya, prinyataya Generalnoy Assambley 5 dekabrya 2018 goda A/RES/73/27 “Dostizheniya v sfere informatizatsii i telekommunikatsiy v kontekste mezhdunarodnoy bezopasnosti” [UN General Assembly Resolution A/RES/73/27 of 5 December 2018 “Developments in the field of information and telecommunications in the context of international security”]. (2018). <https://docs.un.org/ru/A/RES/73/27>

Skinner, C. (2019). *Chelovek tsifrovoy. Chetvertaya revolyutsiya v istorii chelovechestva, kotoraya zatronet kazhdogo* [Digital human: The fourth revolution in human history that will affect everyone].

Federalnyy zakon “Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii” ot 27 iyulya 2006 g. No. 149-FZ (poslednyaya redaktsiya) [Federal Law of the Russian Federation No. 149-FZ of 27 July 2006 “On information, information technologies and information protection” (latest version)]. (2006). https://www.consultant.ru/document/cons_doc_LAW_61798

General Data Protection Regulation (GDPR) – reglament po zashchite personalnykh dannykh, prinyaty Evrosoyuzom 25 maya 2018 goda [General Data Protection Regulation – EU personal data protection regulation adopted on 25 May 2018]. (2018). Retrieved September 6, 2025, from <https://itglobal.com/ru-kz/company/glossary/gdpr/>

Sartor, G. (2017). Human rights and information technologies. In *The Oxford Handbook of Law, Regulation and Technology* (pp. 424–450). <https://doi.org/10.1093/oxfordhb/9780199680832.013.79>

Sullivan, C. (2009). Digital identity – The legal person? *Computer Law & Security Review*, 25, 227–236. <https://doi.org/10.1016/j.clsr.2009.03.009>

Werro, F. (2009). The right to inform v. the right to be forgotten: A transatlantic crash. In *Liability in the Third Millennium: Liber Amicorum Gert Brüggemeier* (pp. 285–289). Baden-Baden.

Zhou, W. (2022). Digital citizenship in the era of meta-universe: Identity dilemma, practical logic and theoretical proof. *Dianzi Zhengwu [E-Government]*, 10, 62–74.

Сведения об авторах:

Жаналиева Айгуль Жаналиевна – кандидат юридических наук, старший преподаватель юридического сектора Университета Мирас (Шымкент, Казахстан, e-mail: rasuli-77@mail.ru).

Жаксылыков Нуржан Нуртазаулы – кандидат юридических наук, старший преподаватель юридического сектора Университета Мирас (Шымкент, Казахстан, e-mail: marc33@mail.ru).

Алтаева Мадина Орынбековна – магистр, старший преподаватель юридического сектора Университета Мирас (Шымкент, Казахстан, e-mail: botashova.80@mail.ru).

Тленин Талгат Бахытулы – магистр, старший преподаватель юридического сектора Университета Мирас (Шымкент, Казахстан, e-mail: ttalgat_1979@mail.ru).

Мамаева Макбал Нуржановна – магистр, старший преподаватель юридического сектора Университета Мирас (Шымкент, Казахстан, e-mail: mtakbal85@mail.ru).

Information about the authors:

Zhanalieva Aigul Zhanalieva – PhD in Law, Senior Lecturer in the Law Sector at Miras University (Shymkent, Kazakhstan, e-mail: rasuli-77@mail.ru).

Zhaksylykov Nurzhan Nurtazauly – PhD in Law, Senior Lecturer in the Law Sector at Miras University (Shymkent, Kazakhstan, e-mail: marc33@mail.ru).

Altayeva Madina Orynbekovna – Master’s degree, Senior Lecturer in the Law Sector at Miras University (Shymkent, Kazakhstan, e-mail: botashova.80@mail.ru).

Tlenshin Talgat Bakhytuly – Master’s Degree, Senior Lecturer in the Law Sector at Miras University (Shymkent, Kazakhstan, e-mail: ttalgat_1979@mail.ru).

Mamayeva Makbal Nurzhanovna – Master’s degree, Senior Lecturer in the Law Sector at Miras University (Shymkent, Kazakhstan, e-mail: mtakbal85@mail.ru).

Авторлар туралы мәлімет:

Жаналиева Айгуль Жаналиевна – заң ғылымдарының кандидаты, Мирас университеті Құқық секторының аға оқытушысы (Шымкент, Қазақстан, e-mail: rasuli-77@mail.ru).

Жаксылыков Нуржан Нуртазаулы – заң ғылымдарының кандидаты, Мирас университеті Құқық секторының аға оқытушысы (Шымкент, Қазақстан, e-mail: marc33@mail.ru).

Алтаева Мадина Орынбековна – магистр, Мирас университеті Құқық секторының аға оқытушысы (Шымкент, Қазақстан, e-mail: botashova.80@mail.ru).

Тленин Талгат Бахытулы – магистр, Мирас университеті Құқық секторының аға оқытушысы (Шымкент, Қазақстан, e-mail: ttalgat_1979@mail.ru).

Мамаева Макбал Нуржановна – магистр, Мирас университеті Құқық секторының аға оқытушысы (Шымкент, Қазақстан, e-mail: mtakbal85@mail.ru).

Зарегистрирован: 15.09.2025

Принят: 20.03.2026