

Некоторые вопросы защиты информационных прав работника

Аннотация. С развитием цифровых технологий особую актуальность приобретает проблема защиты информационных прав работника. В большинстве стран право на защиту информационных прав рассматривается как фундаментальное, поскольку в соответствии с европейским подходом выводится из права на защиту частной жизни. На международном и наднациональном уровнях различается защита персональных данных вообще и защита данных при автоматизированной обработке, именно последняя и подвергается все более детальной регламентации. В статье рассматриваются некоторые вопросы, связанные с правовым опосредованием оборота и защиты информационных прав работников в условиях повсеместной информатизации и цифровизации. Рассмотрены положения о защите информационных прав работников в Казахстане и некоторых зарубежных странах. Изучена деятельность уполномоченного органа по защите персональных данных, выявлены пробелы в правовом регулировании защиты информационных прав. Автором статьи также даны определенные выводы в сфере защиты трудовой информации работников.

Ключевые слова: обработка и защита персональных данных, информационное право, работник, работодатель, место работы.

DOI: <https://doi.org/10.32523/2616-6844-2022-140-3-72-80>

Введение

Актуальность проблемы правовой регламентации информационной безопасности, как информационного ресурса, во время стремительного развития цифрового общества и процессов цифровизации, несомненно, растет. При этом ее важнейший аспект - достижение оптимального баланса между объективными трансформациями государства и общества и частными потребностями наемных работников в обеспечении личного пространства в пределах правового механизма оборота и защиты информационных прав - остается все еще проблемным. И все это может быть достигнуто при условии соблю-

дения конституционного принципа приоритетности прав и свобод человека и гарантированной неприкосновенности частной жизни, личной и семейной тайны, защиты чести, достоинства и имени, производного от международных стандартов обеспечения прав и свобод человека и гражданина.

В казахстанском трудовом праве в настоящее время формируется новый институт: право на информацию субъектов трудового права и ее защита.

Право на информацию в трудовом праве включает в себя целый ряд правомочий, таких как: 1) правомочие на доступ к информации; 2) правомочие на обработку информации (хранение, комбинирование, передача,

распространение или другое использование). В качестве самостоятельного выделяется правомочие на защиту трудовых информации, что реализуется в рамках охранительного правоотношения [1].

Современные технологии позволяют работодателям в беспрецедентном масштабе использовать персональные данные в рамках осуществления своей деятельности. В связи с этим они должны обеспечить и высокий уровень их защиты на основе надежной правовой основы в области защиты информационных прав работников.

Методы

Теоретические исследования вопросов защиты информационных прав субъектов трудового права проводились путем изучения трудов ученых и сравнительно-правового анализа законодательства.

Обсуждение

Вследствие повсеместного сбора и, соответственно, возрастающей угрозы безопасности персональных данных в некоторых государствах принимаются законы, предоставляющие определенным лицам контрольные функции по части сбора, обработки и передачи персональных данных государственными и частным организациям. Так, согласно данным отчета Freedom House за 2018 год, в пятнадцати странах законы о защите данных находятся на рассмотрении и в тридцати пяти странах аналогичные законы уже приняты и действуют [2].

Положения законов о защите персональных данных, которые действуют в таких странах, как Аргентина, Бразилия и Индонезия, во многом очень схожи с европейским Общим регламентом о защите данных (GDPR), вступившим в силу в 2018 году. Принятие в разных странах законодательных актов, установивших правовой режим информационных ресурсов, стало основой для формирования комплексной отрасли права – информационного права, в предмет которой входят общественные

отношения, связанные с правовым регулированием оборота информации, ее созданием, хранением, обработкой и использованием на основе коммуникационных технологий, ее защитой [3].

Информационные права граждан закреплены в Международном пакте о гражданских и политических правах [4], который обязателен в 168 странах, в том числе и в Казахстане. Статьи 17-21 данного Пакта относятся к защите информационных прав личности. Информационные права содержатся в некоторых статьях (ст.ст.10-39) Конституции Республики Казахстан [5], которые напрямую не регулируют вопросы обеспечения защиты информационных прав личности, но выступают как базовые положения.

Одним из фундаментальных правовых актов в области защиты информационных прав граждан является Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан» (ст.18, ст.22-24) [6]. Различные аспекты правового регулирования информационных отношений закреплены в Законе РК от 16 ноября 2015 года № 401-V «О доступе к информации» [7].

Впервые с учетом международных стандартов 21 мая 2013 года в Казахстане был принят Закон «О персональных данных и их защите» [8], основным приоритетом которого является «обеспечение защиты прав и свобод человека и гражданина при сборе и обработке его персональных данных» (ст.2). Данный закон регулирует общественные отношения именно в сфере персональных данных и определяет правовые основы деятельности, связанные с защитой персональных данных. К сожалению, положения данного закона не получили развития в действующем Трудовом Кодексе Республики Казахстан (далее – ТК РК), где мы не находим статей, посвященных персональным данным и их защите. Есть только упоминание о праве работника на обеспечение защиты данных, хранящихся у работодателя (пп.24 п.2 ст.23 ТК РК). Эти «упоминания» и ссылки на законодательство о персональных данных и их защите, на наш взгляд, не реша-

ют всех проблем защиты именно трудово-вой информации, которая, безусловно, имеет свою специфику.

Обязанность работодателя защищать информационные права работника включает в себя защиту персональных данных работника именно в сфере трудовых отношений, а именно: информацию о работнике, о его профессиональной квалификации, деловых и профессиональных качествах, но ни коим образом не должна касаться его личной и семейной жизни. И в целях исключения неоправданного расширения сведений о работнике именно в ТК РК следует установить перечень сведений, которые запрещено требовать от работника.

Имеющиеся в настоящее время в стране проблемы утечки персональных данных, согласно данным Министерства цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан, свидетельствуют о наличии целого ряда проблем [9].

Каждый государственный орган, как владеющий базами данных, должен самостоятельно нести ответственность за хранение персональных данных в своих базах и соблюдать положения по использованию и секретности имеющейся там информации.

Помимо проблем утечки личной информации важны следующие аспекты:

1) ответственность за нарушение соответствующих норм. Здесь речь идет об увольнении руководителя отделения, отвечающего за сбор и хранение персональных данных. В настоящее время в Казахстане отсутствует правовая статистика по защите персональных данных, в связи с чем также необходимо развивать культуру защиты персональных данных, особенно работодателями, в том числе путем сообщения об утечках информации самому работнику [10], что позволит выстроить доверительные отношения и воспринимать всерьез ответственность по сбору, обработке и хранению персональных данных;

2) конфиденциальность информационных сведений о работнике. Если защита данных — это защита от несанкционированного доступа, то конфиденциальность информа-

ционных сведений — это авторизованный доступ. Защита информационных данных работника — это, по сути, техническая проблема, тогда как конфиденциальность данных является правовой (юридической). Многие протоколы защиты секретности информации все еще являются уязвимыми для уполномоченных лиц, которым данная информация доступна. Бремя ответственности указанных лиц, скорее всего, связано с законом о конфиденциальности, а не с технологиями [11];

3) технологические возможности субъектов для сотрудничества. Касательно защиты информационных сведений возникают вопросы о том, кто имеет доступ и ведет контроль безопасности сбора, обработки и хранения информации о работнике, полученной при помощи различных приборов (к примеру, камеры видеонаблюдения).

В настоящее время все государственные органы и организации работают или владеют различными объектами информатизации и базами данных в силу того, что ими оказываются электронные услуги и, соответственно, имеется доступ к персональным данным граждан. Для того, чтобы их деятельность и техническая инфраструктура всегда соответствовали требованиям информационной безопасности, и они были максимально защищены как от возможных хакерских атак, так и от внутренних угроз, в Казахстане определен уполномоченный орган, осуществляющий госконтроль в области обеспечения информационной безопасности - Министерство цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан.

В соответствии с Предпринимательским кодексом РК от 29 октября 2015 года №375-V ЗРК, уполномоченным органом в области информационной безопасности проводятся профилактический контроль и внеплановые проверки, которые позволяют выявлять несоответствия требованиям информационной безопасности в деятельности государственных органов и организаций [12].

При обнаружении фактов незаконного сбора или утечки персональных данных, а также нарушения правил использования элек-

тронной цифровой подписи (ЭЦП) граждане могут обратиться в уполномоченный орган любым удобным и доступным для него способом, позволяющим зарегистрировать обращение (в электронном виде, на бумажном носителе, посредством почты или портала «Электронного правительства», путем направления обращения на блог руководителя, электронного письма на ведомственную электронную почту и т.п.). По обращению граждан и юридических лиц уполномоченный орган, в целях установления факта правонарушения и привлечения к ответственности, имеет право начать проверку в отношении нарушителя, возбудить административное дело и привлекать к ответственности за нарушения, предусмотренные статьями 79, 639, 640 и 641 КоАП РК.

Круг лиц и организаций, заинтересованных либо так или иначе участвующих в процессах, связанных с защитой персональных данных, является очень большим. Несмотря на наличие профильных ведомств, курирующих надзорных органов и других задействованных участников информационного процесса по сбору, обработке, хранению, уничтожению личных данных, важно понимать, что, по сути, следует отразить все существующие государственные органы и их комитеты, департаменты и отделы, поскольку у каждого института власти есть как минимум одна база данных, с которой они работают. Это означает, что защита информационных прав работников должна превратиться в то самое связующее звено, которое позволит гармонично взаимодействовать государственным органам друг с другом и с обществом, повысить уровень доверия и коммуникаций, что является неотъемлемой частью цифрового общества, создание которого предусмотрено Законом РК «О персональных данных и их защите». Согласно данным, приведенным на сайте Комитета по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан, «вопросы защиты оставлены на усмотрение собственников и операторов персональных данных (владельцев интернет-ре-

сурсов, интернет-магазинов, кредитных бюро, микрофинансовых организаций, работодателей и др.)» [13]. При этом технические требования по защите информации в информационных системах, содержащих персональные данные, установлены почему-то только для государственных органов.

Согласно данным Комитета по информационной безопасности, осуществление контроля за применением закона о защите персональных данных и контроля за соблюдением требований по их защите станут главными звеньями работы по защите персональных данных. Однако ныне существующая практика не позволяет решать системные проблемы, поскольку откладывает решение наиболее важных проблем на более поздний срок, в т. ч. обучение кадров, создание правовой и информационной культуры, и прежде всего, во всем государственном аппарате. Впрочем, и увольнение (за ненадлежащее хранение, утечку информации и др.) не может оставаться единственным способом наказания за нарушение законодательства, так как оно нуждается в четких механизмах привлечения к ответственности. Поскольку персональные данные подлежат защите и ее гарантом выступает именно государство, все занимающиеся так или иначе вопросами защиты персональных данных должны соответствовать выработанным техническим и юридическим параметрам.

Цифровая трансформация в трудовых отношениях приносит очевидные преимущества как работодателям, так и работникам и лицам, ищущим работу, с точки зрения новых возможностей трудоустройства, повышения производительности, улучшения условий труда и новых способов организации работы, а также повышения качества предоставляемых услуг. В целом, при правильной организации и защите информационных прав сторон трудовых отношений это может привести к росту занятости и сохранению рабочих мест.

Результаты

В нормах казахстанского права не имеется полного перечня общедоступных пер-

сональных данных и конкретной правовой регламентации сбора и обработки общедоступных сведений. В связи с чем работодателям необходимо заранее получать согласие работников на обработку общедоступных данных, поскольку цели, для осуществления которых сведения личного характера оказались общедоступными, могут и не совпадать с заявленными целями организации по сбору и обработке персональных данных.

При постановке вопросов представительства на дачу согласия и его отзыва на сбор и обработку личных сведений работников необходимо учитывать, что согласие на сбор и обработку личной информации может предоставить лишь собственник. В действующих национальных нормах не предусмотрена возможность предоставления права реализовать указанные действия третьими лицами по доверенности. Такое право есть лишь у законного представителя, т.е. лица, который может представлять интересы физического лица в государственных органах, так как опекаемый лично не может непосредственно реализовать свои права и нести обязанности из-за недостижения восемнадцатилетнего возраста либо специфики физического состояния. Поэтому считаем, что работодатели должны учитывать данное обстоятельство, а законодатель должен предусмотреть возможность предоставления согласия на обработку персональных данных работника по доверенности.

Как отмечено, в ТК РК общие требования к обработке персональных данных работника установлены нормами, регулирующими обязанности работодателя по сбору, обработке и защите персональных данных. Более того, каждый работодатель должен определить четкий порядок сбора, обработки и защиты персональных данных посредством принятия локального акта и ознакомить с ним всех работников. При этом работодатель должен ограничить доступ к личным сведениям работников и нести ответственность за это лиц. Одновременно данные лица должны получать доступ только к тем персональным данным, которые им необходимы для осуществления своих должностных функций на

условиях обязательного соблюдения режима конфиденциальности.

В месте выполнения работы собирается много данных, хотя оно не всегда находится в центре внимания управления данными. Вопросы прав на данные, сбора, доступа и совместного использования остаются нерешенными, что влияет на конфиденциальность сведений работников, их карьерную мобильность и качество работы. То же самое касается необходимости обеспечения защиты коллективных прав, поскольку, согласно данным глобальной благотворительной организации Luminate, «регулирующие органы продолжают уделять внимание защите отдельных лиц или, в лучшем случае, защищенных классов, таких как люди определенного пола, возраста, этнической принадлежности или сексуальной ориентации». Хотя это чрезвычайно важно, но недостаточно для того, чтобы предоставить работникам и работодателям, их представителям настоящую свободу действий.

Пандемия COVID-19 открыла новые источники данных в месте выполнения работы благодаря сбору сведений о состоянии здоровья и дистанционной работе. Данные Gartner показывают, что количество работников, использующих инструменты онлайн-сотрудничества, удвоилось до 80% с 2019 по 2021 год [14].

Обычно данные о работниках собираются во время приема на работу и во время работы (с помощью средств связи, человеко-машинного интерфейса, датчиков и т.д.). Эти данные, относящиеся к работнику, создают ценность для работодателя (особенно в целях повышения производительности труда). В реальной жизни возможности работников ограничены из-за технологической сложности, отсутствия прозрачности, а также отсутствия способов отстаивать свои индивидуальные и коллективные права на личные и коллективные сведения.

Рамочное соглашение европейских социальных партнеров по цифровизации (принято в 2020 г.) предусматривает, что представители работников могут участвовать в вопросах, касающихся согласия, защиты конфиденциальности и наблюдения, в соответствии с Об-

щим регламентом защиты данных (GDPR) [16]. Однако GDPR касается только доступа к личным данным. Это ограничение, поскольку предполагаемые и наблюдаемые данные, которые в значительной степени собираются на рабочем месте, не подпадают под это определение. Правовая база также размыта в отношении «конфиденциальных данных», которые включают расовое или этническое происхождение субъекта данных, политические взгляды, религиозные убеждения, членство в профсоюзах, здоровье, сексуальную ориентацию и генетические или биометрические данные. Работодатели могут использовать такие данные в сфере трудовых отношений без ограничений.

Данное рамочное соглашение направлено на:

- повышение осведомленности и улучшение понимания работодателями, работниками и их представителями возможностей и проблем в сфере труда, возникающих в результате цифровой трансформации;

- обеспечение правовой основы для поощрения, руководства и помощи работодателям, работникам и их представителям в разработке мер и действий, направленных на использование возможностей цифровых технологий и решение проблем, с учетом существующих инициатив, практики и коллективных соглашений;

- поощрение партнерского подхода между работодателями, работниками и их представителями;

- поддержание развития ориентированного на человека подхода к интеграции цифровых технологий в сфере труда для повышения производительности.

В этих условиях баланс сил смещается в сторону работодателя, который, располагая дополнительной информацией, может изменить оплату труда и условия труда или принять решение об увольнении. Например, в августе Xsolla (российская компания, занимающаяся электронными платежами) уволила 150 сотрудников на основе результатов анализа больших данных. По данным Guardian, работники по уходу на дому в американском

штате Арканзас не получили заработную плату в полном объеме из-за сбоя электронной проверки посещения через приложение AuthentiCare (приложение, отслеживающее ежедневную работу, физическое местоположение и часы работы) [16].

Чтобы заслужить, а потом и удержать доверие работников, работодатель должен защищать не базы данных, а сами данные о работнике. Технологии не стоят на месте, постоянно появляются новые механизмы идентификации, и работодателю следует быть в курсе подобных инноваций. При этом также необходимо законодательно урегулировать средства получения и обработки персональных данных работников на стадии их разработки, а не только реализации.

Заключение

Текущая система защиты персональных данных ограничена определенными типами данных, состоит из дачи согласия в качестве правовой основы для передачи персональных данных и не полностью охватывает проблемы, связанные с местом работы, что не может полностью реализовать права работников на их данные с точки зрения содержания, обращения и контроля над обработкой и совместным использованием.

Считаем необходимым пересмотр и обновление правил защиты персональных данных для конкретных отраслей с учетом их специфики. Они могут быть сосредоточены на конкретных группах работников и позволить более активное их участие, а также работодателей за счет расширения охвата всех соответствующих типов персональных данных, а также объема их передачи.

Подводя итог, отметим, что в настоящее время имеются различные способы создания правового режима по защите персональных данных. Важно понимать, что разработка и принятие профильного закона, делегирование полномочий либо создание специального органа, продвижение вперед в индексах интернет-свободы или кибербезопасности – это только начало долгих усилий по созда-

нию устойчивой цифровой экосистемы. Для Казахстана, который проходит процесс массовой цифровизации с целью интеграции в глобальные информационные процессы, помимо законодательных и других инициатив, нужных для регламентации данной отрасли, важно сосредоточить усилия на повышении осведомленности работников о необходимости защиты персональных данных и продвижении культуры цифровых прав посредством углубления знаний и формирования цифровой грамотности работников.

Список литературы

1. Лушников А.М. Курс трудового права. - М., 2009 – 210 с.
2. Adrian Shahbaz, "Freedom on the Net 2018. The Rise of Digital Authoritarianism," Freedom House, 2018. [Электрон. ресурс] // <https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism> (дата обращения 15.07.2022).
3. Воробьева О.А., Полякова Ю.А. Информационное право: Электронное учебно-методическое пособие. - Тольятти, Изд-во ТГУ, 2020. - С. 48.
4. Международный пакт о гражданских и политических правах (Нью-Йорк, 16 декабря 1966 г.) // https://online.zakon.kz/Document/?doc_id=1010760.
5. Конституция Республики Казахстан (принята на республиканском референдуме 30 августа 1995 года) (с изменениями и дополнениями по состоянию на 08.06.2022 г.) [Электрон. ресурс] // https://online.zakon.kz/document/?doc_id=1005029 (дата обращения 15.07.2022);
6. Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан» (с изменениями и дополнениями по состоянию на 16.11.2020 г.) [Электрон. ресурс] // https://online.zakon.kz/Document/?doc_id=31106860 (дата обращения 15.07.2022).
7. Закон РК от 16 ноября 2015 года № 401-V «О доступе к информации» [Электрон. ресурс] // https://online.zakon.kz/Document/?doc_id=39415981 (дата обращения 15.07.2022).
8. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 01.07.2021 г.) [Электрон. ресурс] // https://online.zakon.kz/Document/?doc_id=31396226 (дата обращения 15.07.2022).
9. Гусарова А., Джаксылыков С. Защита персональных данных в Казахстане: статус, риски и возможности // Фонд «Сорос-Казахстан», 2020 // https://www.soros.kz/wp-content/uploads/2020/04/Personal_data_report.pdf.
10. Защита персональных данных в Казахстане: неработающий закон и осторожное движение к GDPR, Soros Foundation Kazakhstan, June 4, 2019. [Электрон. ресурс] <https://www.soros.kz/ru/personal-data-protection-in-kz/> (дата обращения 15.07.2022).
11. Rick Robinson, "Data Privacy vs Data Protection," IPS Watch Blog, January 20, 2020. [Электрон. ресурс] // <https://blog.ipswitch.com/dataprivacy> (дата обращения 15.07.2022).
12. Кодекс Республики Казахстан от 29 октября 2015 года № 375-V «Предпринимательский кодекс Республики Казахстан» (с изменениями и дополнениями по состоянию на 06.07.2021 г.) [Электрон. ресурс] // https://online.zakon.kz/Document/?doc_id=38259854 (дата обращения 15.07.2022).
13. Защита персональных данных (Data Protection Agency). [Электрон. ресурс] // <http://isdpm.dai.gov.kz/ru/page/zaschita-personalnykh-dannykh-data-protection-agency> (дата обращения 15.07.2022).
14. Employers hold too much power over information [Электрон. ресурс] // <https://www.weforum.org/agenda/2021/09/workplace-data-rights-regulation/> (дата обращения 15.07.2022).
15. Рамочное соглашение европейских социальных партнеров по цифровизации [Электрон. ресурс] // https://www.buinessurope.eu/sites/buseur/files/media/reports_and_studies/2020-06-22_agreement_on_digitalisation_-_with_signatures.pdf (дата обращения 15.07.2022).
16. Работодатели обладают слишком большой властью над информацией. Работники должны заявить о своих правах на данные [Электрон. ресурс] // <https://www.weforum.org/agenda/2021/09/workplace-data-rights-regulation/> (дата обращения 15.07.2022).

Сырлыбаева Ф.М.

Л.Н. Гумилев атындағы Еуразиялық ұлттық университеті, Астана, Қазақстан

Жұмыскерлердің ақпараттық құқықтарын қорғаудың кейбір мәселелері

Аңдатпа. Цифрлық технологиялардың дамуымен байланысты жұмыскерлердің ақпараттық құқықтарын қорғау мәселесі ерекше өзекті болып отыр. Көптеген елдерде азаматтардың жеке ақпарат құқықтарын қорғау негізгі болып саналады, өйткені еуропалық көзқарасқа сәйкес, ол жеке өмірді қорғау құқығынан туындайды. Халықаралық және ұлттан жоғары деңгейлерде жалпы жеке деректерді қорғау және автоматтандырылған өңдеу кезінде деректерді қорғау ерекшеленеді, дәл осы соңғысы барған сайын егжей-тегжейлі реттеуге жатады. Мақалада кеңінен ақпараттандыру мен цифрландыру жағдайында жұмыскерлердің ақпараттық құқықтары мен айналымын құқықтық реттеуге қатысты кейбір мәселелер талқыланды. Қазақстандағы және кейбір шет елдердегі жұмыскерлердің ақпараттық құқықтарын қорғау туралы ережелер қарастырылды. Дербес деректерді қорғау саласындағы уәкілетті органның қызметі зерделенді, жеке ақпараттық құқықтарды қорғауды құқықтық реттеудегі олқылықтар анықталды. Мақала авторы жұмыскерлердің еңбекпен байланысты жеке ақпараттарын қорғау саласында да белгілі бір тұжырымдар жасаған.

Кілт сөздер: жеке деректерді өңдеу және қорғау, ақпарат туралы заң, қызметкер, жұмыс беруші, жұмыс орны.

F.M. Syrlybaeva

L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

Some issues of protection of employee information rights

Abstract. With the development of digital technologies, the problem of protecting the information rights of an employee is of particular relevance. In most countries, the right to the protection of information rights is regarded as fundamental, because, in accordance with the European approach, it is derived from the right to the protection of privacy. At the international and supranational levels, there is a distinction between the protection of personal data in general and the protection of data in automated processing, it is the latter that is subject to more and more detailed regulation. The article discusses some issues related to the legal mediation of the circulation and protection of the information rights of workers in the context of widespread informatization and digitalization. The article considers provisions for the protection of information rights of employees in Kazakhstan and some foreign countries. There have been studied activities of the authorized body for the protection of personal data, and gaps in the legal regulation of the protection of information rights in the article. The author of the article also gave certain conclusions in the field of protection of labor information of workers.

Keywords: processing and protection of personal data, information law, employee, employer, place of work.

References

1. Lushnikov A.M. Kurs trudovogo prava. - M., 2009 – 210 s.
2. Adrian Shahbaz, "Freedom on the Net 2018. The Rise of Digital Authoritarianism," Freedom House, 2018. [Elektron. resurs] // <https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism> (accessed: 15.07.2022).
3. Vorob'yova O.A., Polyakova YU.A. Informacionnoe pravo: Elektronnoe uchebno-metodicheskoe posobie. - Tol'yatti, Izd-vo TGU, 2020. - S. 48.
4. Mezhdunarodnyj pakt o grazhdanskij i politicheskij pravah (N'yu-Jork, 16 dekabrya 1966 g.) // https://online.zakon.kz/Document/?doc_id=1010760.
5. Konstituciya Respubliki Kazahstan (prinyata na respublikanskom referendumе 30 avgusta 1995 goda) (s izmeneniyami i dopolneniyami po sostoyaniyu na 08.06.2022 g.) [Elektron. resurs] // https://online.zakon.kz/document/?doc_id=1005029 (accessed: 15.07.2022);

6. Закон Respubliki Kazahstan ot 6 yanvarya 2012 goda № 527-IV «O nacional'noj bezopasnosti Respubliki Kazahstan» (s izmeneniyami i dopolneniyami po sostoyaniyu na 16.11.2020 g.) [Elektron. resurs] // https://online.zakon.kz/Document/?doc_id=31106860 (accessed: 15.07.2022).
7. Закон RK ot 16 noyabrya 2015 goda № 401-V «O dostupe k informacii» [Elektron. resurs] // https://online.zakon.kz/Document/?doc_id=39415981 (accessed: 15.07.2022).
8. 8. Закон Respubliki Kazahstan ot 21 maya 2013 goda № 94-V «O personal'nyh dannyh i ih zashchite» (s izmeneniyami i dopolneniyami po sostoyaniyu na 01.07.2021 g.) [Elektron. resurs] // https://online.zakon.kz/Document/?doc_id=31396226 (accessed: 15.07.2022).
9. Gusarova A., Dzhaksylykov S. Zashchita personal'nyh dannyh v Kazahstane: status, riski i vozmozhnosti // Fond «Soros-Kazahstan», 2020 // https://www.soros.kz/wp-content/uploads/2020/04/Personal_data_report.pdf.
10. Zashchita personal'nyh dannyh v Kazahstane: nerabotayushchij zakon i ostorozhnoe dvizhenie k GDPR, Soros Foundation Kazakhstan, June 4, 2019. [Elektron. resurs] <https://www.soros.kz/ru/personal-data-protection-in-kz/> (accessed: 15.07.2022).
11. Rick Robinson, "Data Privacy vs Data Protection," IPS Watch Blog, January 20, 2020. [Elektron. resurs] // <https://blog.ipswitch.com/dataprivacy> (accessed: 15.07.2022).
12. Kodeks Respubliki Kazahstan ot 29 oktyabrya 2015 goda № 375-V «Predprinimatel'skij kodeks Respubliki Kazahstan» (s izmeneniyami i dopolneniyami po sostoyaniyu na 06.07.2021 g.) [Elektron. resurs] // https://online.zakon.kz/Document/?doc_id=38259854 (accessed: 15.07.2022).
13. Zashchita personal'nyh dannyh (Data Protection Agency). [Elektron. resurs] // <http://isdp.mdai.gov.kz/ru/page/zaschita-personalnykh-dannykh-data-protection-agency> (accessed: 15.07.2022).
14. Employers hold too much power over information [Elektron. resurs] // <https://www.weforum.org/agenda/2021/09/workplace-data-rights-regulation/> (accessed: 15.07.2022).
15. Ramochnoe soglasenie evropejskih social'nyh partnerov po cifrovizacii [Elektron. resurs] // https://www.buinesseuropa.eu/sites/buseur/files/media/reports_and_studies/2020-06-22_agreement_on_digitalisation_-_with_signatures.pdf (accessed: 15.07.2022).
16. Rabotodateli obladayut slishkom bol'shoj vlast'yu nad informaciej. Rabotniki dolzhny zayavit' o svoih pravah na dannye [Elektron. resurs] // <https://www.weforum.org/agenda/2021/09/workplace-data-rights-regulation/> (accessed: 15.07.2022).

Сведения об авторе:

Сырлыбаева Ф.М. – докторант кафедры гражданского, трудового и экологического права Евразийского национального университета им. Л.Н. Гумилева, ул. Сатпаева, 2, Астана, Казахстан.

Syrlybayeva F.M. – Ph.D. student, Department of the civil, labor, and ecological law, L.N. Gumilyov Eurasian National University, 2 Satpayeva str., Astana, Kazakhstan.