

ОБ ОТДЕЛЬНЫХ ПРАКТИЧЕСКИХ ВОПРОСАХ ПРИМЕНЕНИЯ ЗАКОНОДАТЕЛЬСТВА

о персональных данных в условиях цифровой трансформации

УДК 341/349



ПОЛЕЩУК Д. Г.,

кандидат юридических наук, доцент, юрист, доцент кафедры международного права факультета международных отношений Белорусского государственного университета

АННОТАЦИЯ

В век цифровых технологий увеличиваются объемы обработки личной информации, а вместе с ними повышается и значение их защиты. В 2021 году в Республике Беларусь сформировано комплексное законодательство о персональных данных, на протяжении нескольких лет прошедшее практическую апробацию. С учетом планируемой в текущем году подготовки законопроекта по вопросам защиты персональных данных в статье исследуются отдельные проблемные аспекты действующего правового регулирования, предлагаются перспективные направления его совершенствования.

Ключевые слова: персональные данные, законодательство, цифровые технологии, видеонаблюдение, искусственный интеллект, обработка, согласие.

В условиях расширения использования информационно-коммуникационных и других цифровых технологий в современном обществе

значение защиты персональных данных трудно переоценить. Неправомерные действия в отношении персональных данных называются в числе основных угроз в Концепции национальной безопасности Республики Беларусь, утвержденной решением Всебелорусского народного собрания от 25 апреля 2024 г. № 5 (п. 29), а Концепция правовой политики Республики Беларусь, утвержденная Указом Президента Республики Беларусь от 28 июня 2023 г. № 196, ориентирует на своевременную актуализацию законодательства и совершенствование практики обработки персональных данных (подп. 41.13 п. 41).

Система защиты персональных данных в республике сложилась и достаточно успешно функционирует, что иллюстрируют ежегодные опубликованные отчеты специального уполномоченного органа – Национального центра защиты персональных данных (далее – НЦЗПД) [1]. С момента вступления в силу Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» (далее – Закон № 99-З) и других правовых актов, направленных на его реализацию, прошло более четырех лет, за указанный период со стороны НЦЗПД и организаций республики нарабатана значительная практика применения

нового законодательства, включающая многообразие разъяснений, рекомендаций, образовательных и профилактических мероприятий. С позиции актуальных национальных интересов это позволяет оценить эффективность отдельных его положений и определить точечные векторы дальнейшего развития. В текущем году п. 27 плана подготовки проектов законодательных актов на 2026 год, утвержденного Указом Президента Республики Беларусь от 18 ноября 2025 г. № 400, предусмотрена разработка законопроекта «Об изменении законов по вопросам защиты персональных данных».



Следует отметить, что со времени начала подготовки и принятия Закона № 99-3 произошел целый ряд событий, оказывающих влияние на общественные отношения в информационной сфере. Среди них можно назвать, в частности, проведение республиканского референдума и дополнение ст. 28 Конституции Республики Беларусь нормой о создании государством условий для защиты персональных данных и безопасности личности и общества при их использовании; существенное изменение геополитической обстановки в мире и усиление неправомерного санкционного давления на Республику Беларусь и Российскую Федерацию; масштабирование применения технологий искусственного интеллекта (далее – ИИ); повышение роли общественно опасных посягательств, действующих цифровую среду, в структуре национальной (более 30 %) и транснациональной организованной преступности [2].

Цифровая трансформация – 4-й приоритет Программы социально-экономического развития Республики Беларусь на 2026–2030 годы, утвержденной решением Всебелорусского народного собрания от 19 декабря 2025 г. № 1, направления которой явно включают обработку персональных данных. В то же время Конституционный Суд Республики Беларусь констатирует опережение общественных отношений в цифровой сфере по сравнению с нормативно-правовым регулированием, ориентируя на адаптацию нормотворчества и правоприменения к новым

социально-экономическим реалиям в целях достижения баланса между развитием инновационных технологий и защитой гарантированных прав и свобод человека и гражданина [3, п. 6].

Совокупность указанных факторов позволяет говорить о предпосылках к научному осмыслению порядка обращения с личной информацией на основе накопленного практического опыта и динамики цифровых преобразований в обществе. В последние годы внимание к исследуемой тематике усилилось и непосредственно к вопросам защиты персональных данных в отдельных аспектах обращались такие белорусские ученые-правоведы и сотрудники НЦЗПД, как Абламейко М. С., Гаев А. А., Гавриленко А. И., Городецкая М. А., Диско В. И., Лосев В. В., Пырко И. А., Саванович Н. А., Шакель Н. В., Швед Н. А. и др.

Не претендуя на исключительность, позволим себе тезисно выразить авторский взгляд на комплекс практических вопросов применения законодательства о персональных данных в контексте особенностей национальной правовой системы и ожидаемых обществом изменений.

1. Совершенствование понятийного аппарата и правового режима отдельных категорий персональных данных.

На пространстве ЕАЭС, несмотря на развитие трансграничных информационных потоков, Соглашение о защите персональных данных, выступающее одним из приоритетов проработки инициатив в рамках реализации цифровой повестки ЕАЭС (решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12), пока еще не выработано, фактически переносится регулирование исследуемых аспектов только на национальный уровень. Проведенный анализ показывает, что используемая в Законе № 99-3 терминология сформирована на основе зарубежного опыта правового регулирования и устоявшихся международных стандартов в исследуемой сфере, среди которых нормы модельного закона СНГ от 29 ноября 2018 г. «О персональных данных», Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. № 108 и известного Общего регламента по защите персональных данных Европейского союза (далее – GDPR)¹ [4].

¹ Имеет экстерриториальный характер действия и может затрагивать интересы белорусских субъектов хозяйствования (ст. 3 GDPR).

Вместе с тем отдельные положения отечественного регулирования в этой части, по нашему мнению, могут быть уточнены. Уместно заметить, что Концепция правовой политики требует *взвешенно подходить к использованию зарубежного опыта регулирования общественных отношений* и предлагать нововведения, если они отвечают государственным и общественным интересам, учитывают национальные традиции (абз. 7 п. 36).

Так, одним из новых понятий в белорусском законодательстве является «*биометрические персональные данные*» (абз. 2 ст. 1 Закона № 99-3) – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение и др.). Перечень информации о человеке открытый, и на практике нередко происходит отнесение к такой категории персональных данных любых изображений лиц на фотографиях, в т. ч. отсканированных копий. Однако при внимательном изучении признаков биометрических персональных данных такой вывод является не совсем верным. Ключевым аспектом выступает «уникальность идентификации» человека, которая реально возможна при использовании необходимых для этого технических средств. Подход вытекает из модельного закона СНГ (ст. 2), GDPR (абз. 51 преамбулы), и, по всей видимости, разделяется НЦЗПД [5]. Соответственно, в целях исключения неоднозначного толкования данного понятия его определение предлагается дополнить прямым указанием на применение при уникальной идентификации *технических средств*.

В целом, относимые Законом № 99-3 к специальным персональным данным категории биометрических и генетических персональных данных представляют собой «особо чувствительную информацию» о человеке, противоправные действия с которой в век цифровых технологий могут причинить существенный и необратимый вред как самой личности, так и членам ее семьи. В связи с этим на долгосрочную перспективу видится оправданным *выделение отдельного правового режима* таких персональных данных, включая определение оптимального перечня случаев их обработки без согласия гражданина, дополнительных гарантий реализации его прав при возможной обработке указанной информации, специальных норм об ответственности за умышленные

незаконные действия с ними. Мнение о целесообразности формулирования специальных регулятивных норм Закона № 99-3 в данной части высказывалось и другими авторами [6, с. 86–87], а возможность установления государством дополнительных условий, в т. ч. ограничений, в отношении обработки генетических данных, биометрических данных или данных о здоровье предусмотрена и в GDPR (§ 4 ст. 9) [4].

Абзац 7 ст. 1 Закона № 99-3 содержит понятие «*общедоступные персональные данные*» – персональные данные, распространенные самим субъектом персональных данных либо с его согласия или распространенные в соответствии с требованиями законодательных актов. Определяемый термин используется только при описании правовых оснований обработки специальных персональных данных без согласия гражданина, когда он сам делает такие сведения общедоступными (абз. 2 п. 2 ст. 8 Закона № 99-3). При этом в описании правовых оснований обработки любых иных персональных данных употребляется уже иная формулировка: «*в отношении распространенных ранее персональных данных*» (абз. 19 ст. 6 Закона № 99-3). Полагаем, в целях обеспечения большей правовой определенности употребление терминологии, касающейся соответствующей категории персональных данных, должно быть согласованным.

Кроме того, учитывая возникающие на практике сложности с обеспечением правомерности обработки общедоступных персональных данных операторами, а также развитие технологий больших данных (Big Data), представляется целесообразным определить особенности правового режима такой категории информации в отдельной статье Закона № 99-3 (например, закрепить механизм подтверждения законности обработки данных; непосредственно указать критерии недопустимости формирования на основе сбора общедоступных персональных данных информационных ресурсов и др.).

В любом случае совершенствование правового режима отдельных категорий персональных данных и информации о частной жизни должно учитывать актуальную позицию Конституционного Суда Республики Беларусь относительно запрета на изменение цифровыми технологиями социально-биологической природы человека, необходимости комплексной и системной защиты персональных данных от противоправного использования [3, п. 6].

2. Определение порядка обработки персональных данных при осуществлении видеонаблюдения.

Законом № 99-З не предусмотрены особенности обработки персональных данных при осуществлении видеонаблюдения, в связи с чем практика применения законодательства в этой части формируется на основе разъяснений НЦЗПД [7] и отдельных комментариев [8; 9]. Однако возникающие в деятельности операторов вопросы относительно использования такого вида обработки персональных данных и опасения граждан, выраженные в наличии соответствующих жалоб [1], указывают на потенциал закрепления в законодательстве более четких правовых норм, регулирующих видеонаблюдение.

В настоящее время в качестве общих правовых оснований обработки персональных данных в связи с видеонаблюдением, как правило, выделяются:

- *выполнение обязанностей (полномочий), предусмотренных законодательными актами* (абз. 20 ст. 6, абз. 17 п. 2 ст. 8 Закона № 99-З) (например, обеспечение функционирования средств системы видеонаблюдения за состоянием общественной безопасности, созданной Указом Президента Республики Беларусь от 28 ноября 2013 г. № 527);

- *обработка в процессе трудовой (служебной) деятельности субъекта персональных данных в случаях, предусмотренных законодательством* (абз. 8 ст. 6, абз. 3 п. 2 ст. 8 Закона № 99-З) (например, при обеспечении производственно-технологической, исполнительской и трудовой дисциплины (п. 2 ч. 1 ст. 55 Трудового кодекса Республики Беларусь) – на строительных площадках, работах с материальными ценностями или непрерывным обслуживанием клиентов);

- *согласие гражданина* (например, в рамках использования нанимателем при организации пропускного режима видеонаблюдения с видеораспознаванием лиц при одновременном наличии у работников иного способа входа в здание).

В то же время при отсутствии специальных положений Закона № 99-З остаются явно дискуссионными вопросы организации видеонаблюдения в товариществах собственников и садовых товариществах, в т. ч. применительно к иным гражданам, посещающим принадлежащие им объекты, перечни мест, в которых видеонаблюдение

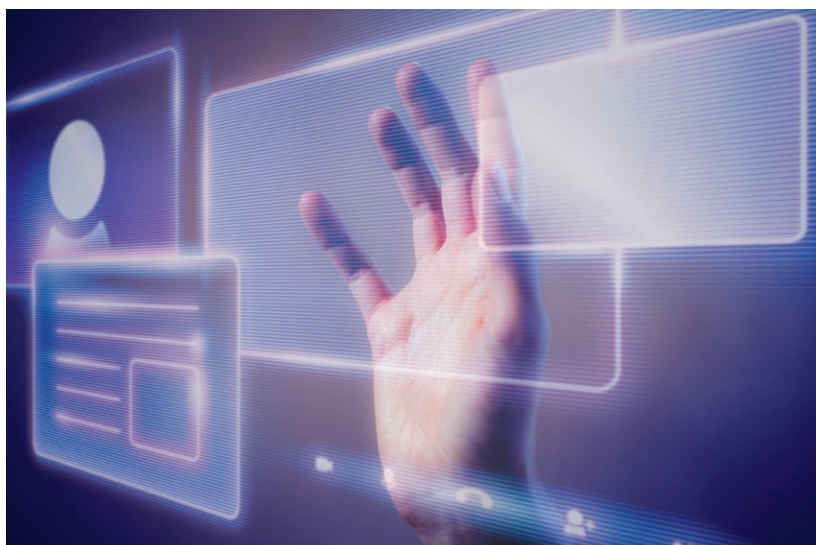
запрещено, порядок информирования об осуществлении видеонаблюдения и срок хранения полученной информации.

3. Регулирование обработки персональных данных с использованием ИИ.

ИИ в различных вариациях все больше находит применение в повседневной жизни граждан и бизнес-процессах организаций. С точки зрения защиты персональных данных это образует дополнительные риски операторов и уполномоченных лиц, поскольку в данном контексте обработка персональных данных может носить равно как «теневой» характер (например, осуществляться работниками организации не только без согласия граждан, но и без ведома ее руководства), так и трансграничный (когда данные могут размещаться на серверах, территориально расположенных в государствах с ненадлежащим уровнем защиты прав субъектов, нарушая тем самым правила ст. 9 Закона № 99-З).

Тем не менее ИИ становится неотъемлемым элементом цифровой экономики, предопределяет конкурентные преимущества организаций и даже отдельных государств, вынуждая идти на поиск компромиссов и разумного баланса между цифровизацией и обеспечением национальной безопасности.

Сложившаяся ситуация формирует предпосылки к рассмотрению необходимости отражения в Законе № 99-З норм, направленных на установление гарантий защиты персональных данных и прав их субъектов при использовании ИИ. Так, в соответствии со ст. 22 GDPR субъект данных *должен иметь право не подпадать под действие решения, основанного исключительно на автоматической обработке*, включая формирование профиля, которое порождает юридические последствия в отношении него или существенно воздействует на него [3]. Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных присутствуют и в Федеральном законе Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ст. 16) [10]. Более того, разрабатываемый в России законопроект об основах государственного регулирования ИИ предусматривает обязанности информировать клиентов об использовании ИИ при реализации товаров и оказании услуг, а также уведомлять граждан в случае применения



ИИ для принятия автономных решений в отношении их [11].

4. Оптимизация правовых оснований обработки персональных данных.

Правовые основания обработки персональных данных без согласия гражданина описаны в ст. 6 и п. 2 ст. 8 Закона № 99-3. Анализ показывает, что значительная их часть связана с реализацией государственно-властных полномочий в рамках различных сфер (областей) государственной деятельности (осуществление правосудия, государственного контроля (надзора), пенсионного обеспечения, проведение государственных статистических наблюдений и др.). В связи с этим по мере повышения правовой культуры в области защиты персональных данных в долгосрочной перспективе видится возможным объединить аналогичные по характеру правовые основания обработки персональных данных в рамках единой формулировки, например, «обработка необходима для выполнения государственно-властных полномочий, предусмотренных законодательством». Соответствующий подход встречается в европейском праве (п. (е) § 1 ст. 6 GDPR) [4] и, по нашему мнению, позволяет исключить определенную детализацию, упростить изложение общих по характеру правовых норм.

Также в целях совершенствования нормотворческой техники и обеспечения однозначного понимания нормативных предписаний предлагается согласовать формулировки сходных правовых оснований обработки персональных данных без согласия граждан, содержащиеся в ст. 6 и 8 Закона № 99-3 (например, при рассмотрении вопросов,

связанных с гражданством Республики Беларусь, предоставлением статуса беженца, дополнительной защиты, убежища и временной защиты в Республике Беларусь; для осуществления административных процедур).

Дискуссионным видится вопрос уточнения такого случая обработки персональных данных без согласия граждан, как получение персональных данных оператором на основании договора, заключенного (за-

ключаемого) с субъектом персональных данных, в целях совершения действий, установленных этим договором (абз. 15 ст. 6 Закона № 99-3). Заметим, что такое основание не применимо к обработке специальных персональных данных, например, о здоровье (ст. 8 Закона № 99-3).



На практике возникают сложности с определением правовых оснований обработки персональных данных, когда в договоре указывается *выгодоприобретатель* (например, один супруг оформляет страховой полис на другого). В этом случае, поскольку указание на него в абз. 15 ст. 6 Закона № 99-3 отсутствует, фактически возникает необходимость оформления согласия выгодоприобретателя на обработку персональных данных. Тем не менее следует обратить внимание, что в законодательстве России при формулировании аналогичного основания обработки персональных данных указание на выгодоприобретателя имеется (с определенными ограничениями в т. ч. касательно несовершеннолетних) (п. 5 ч. 1 ст. 6) [10], а в GDPR нет.

Важное место среди правовых оснований обработки персональных данных занимают *цели осуществления законной профессиональной деятельности журналиста и (или) деятельности средства массовой информации* (далее – СМИ), направленные

на защиту определенного общественного интереса (абз. 17 ст. 6 Закона № 99-3). Указанная норма носит более усеченный характер по сравнению с полномочиями журналиста и СМИ в подп. 4.7 п. 4 ст. 34, ст. 40 Закона Республики Беларусь от 17 июля 2008 г. № 427-3 «О средствах массовой информации», которые применительно к персональным данным они вправе реализовать на другом основании – абз. 20 ст. 6 Закона № 99-3 (выполнение обязанностей (полномочий), предусмотренных законодательными актами).

Не меняя сложившихся на практике подходов, но учитывая значение СМИ (особенно сетевых) в современном обществе и усиление внимания граждан к своей личной информации, на основе баланса конституционных прав на неприкосновенность частной жизни и на свободу информации (ст.ст. 28, 33 и 34 Конституции Республики Беларусь) полагаем в ст. 6 Закона № 99-3 следует рассмотреть возможность закрепления более всеобъемлющей формулировки правовых оснований обработки персональных данных без согласия граждан журналистами и СМИ. Кроме того, с учетом популярности среди молодежи, возможно, имеет смысл непосредственно обозначить *правовые рамки обработки персональных данных блогерами*, которые монетизируют свой контент и, соответственно, попадают под сферу действия Закона № 99-3 (ст. 2).

Выполнение обязанностей (полномочий), предусмотренных законодательными актами (абз. 20 ст. 6, абз. 17 п. 2 ст. 8 Закона № 99-3), выступает одним из распространенных и системообразующих оснований обработки персональных данных в белорусском законодательстве и правоприменительной практике (например, оно касается рассмотрения обращений граждан и юридических лиц, осуществления административных процедур, предоставления характеристик в отношении бывших работников, выполнения требований по обеспечению кибербезопасности информационных ресурсов и т. д.). В пункте (с) § 1 ст. 6 GDPR также присутствует названное правовое основание (обработка необходима для соблюдения юридической обязанности, объектом которой является контролер), однако оно не касается обработки, осуществляемой органами государственной власти при выполнении ими своих задач (для этого применим указанный нами ранее п. (е) § 1 ст. 6 GDPR) [4]. Есть оно и в аналогичном законе России (п. 2 ч. 1 ст. 6) [10].

Исходя из практики, его правильное применение требует отражения соответствующих обязанностей (полномочий) на уровне отраслевого законодательного акта или вытекающего из него подзаконного акта (например, постановление Совета Министров Республики Беларусь от 29 апреля 2010 г. № 645 «О порядке функционирования интернет-сайтов государственных органов и организаций» (далее – ПСМ № 645)). При этом необходимость указания в таком акте на обработку персональных данных без согласия граждан отсутствует. Поэтому в контексте проводимой на постоянной основе в республике ревизии законодательства является оправданным исключение избыточных положений нормативных правовых актов в данной части.

В то же время одним из проблемных вопросов, связанных с применением исследуемого основания, является размещение информации на интернет-сайтах различных организаций (например, сведения о руководстве, новостной контент и т. д.). В отношении государственных органов и государственных организаций возможность размещения определенной информации, в т. ч. и персональных данных, на интернет-сайтах урегулирована, в частности, ПСМ № 645, принятым в развитие Указа Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет», и Кодексом Республики Беларусь об образовании (ст.ст. 19, 55). В деятельности иных организаций, по нашему мнению, возможность размещения персональных данных в сети Интернет может базироваться, как правило, только на связи с трудовой функцией работника (например, специалист по работе с клиентами, пресс-секретарь) (абз. 8 ст. 6 Закона № 99-3) или же на согласии гражданина. Полагаем, данный вопрос нуждается в практическом осмыслении в целях определения понятных и сбалансированных правовых оснований распространения персональных данных на интернет-сайтах и иных интернет-ресурсах организаций независимо от форм собственности.

5. Уточнение обязанностей оператора.

Обязанности оператора, установленные ст. 16 Закона № 99-3, в основном корреспондируют правам субъектов персональных данных (ст.ст. 10–15). Одной из обязанностей является внесение изменений в персональные данные, которые являются неполными, устаревшими или неточными, за исключением случаев, когда иной порядок внесения

изменений в персональные данные установлен законодательными актами либо если цели обработки персональных данных не предполагают последующих изменений таких данных (абз. 6 ст. 16 Закона № 99-З). Вместе с тем, поскольку отдельные элементы указанной обязанности закреплены и в п. 4 ст. 11 Закона № 99-З (право на изменение персональных данных), усматривается целесообразность уточнения соответствующих положений.

Принимая во внимание значение кибербезопасности и цифровой экономики в современном обществе, а также положения Государственной программы «Цифровая Беларусь» на 2026–2030 годы, утвержденной постановлением Совета Министров Республики Беларусь от 30 декабря 2025 г. № 793, предлагается рассмотреть возможность исключения обязанности республиканского органа государственного управления размещать на своем официальном сайте в сети Интернет *информацию об информационных ресурсах (системах), содержащих персональные данные, владельцем которых он является*. В рамках поставленных в государстве задач по повышению качества данных государственных информационных ресурсов для поддержки принятия управленческих решений по экономическим, социальным и иным вопросам развития государства, внедрению технологии ИИ, сохранение указанной обязанности в представленной редакции видится формальным и избыточным.

6. Совершенствование мер по обеспечению защиты персональных данных.

В статье 17 Закона № 99-З сформирован ряд обязательных мер по обеспечению защиты персональных данных (п. 3–5). Отдельные дополнительные меры, связанные с защитой персональных данных, закреплены и в Указе Президента Республики Беларусь от 28 октября 2021 г. № 422 «О мерах по совершенствованию защиты персональных данных» (далее – Указ № 422) (подп. 3.2, 3.3, 3.5 и 3.6 п. 3).

За их несоблюдение предусмотрена административная ответственность по специальной норме ч. 4 ст. 23.7 Кодекса Республики Беларусь об административных правонарушениях.

В целом Закон № 99-З предлагает отвечающий современной зарубежной практике *риск-ориентированный подход* к обеспечению защиты персональных данных. Оператор (уполномоченное лицо) самостоятельно определяет состав и перечень мер, необходимых и достаточных для выполнения обязанностей по обеспечению защиты

персональных данных, с учетом требований Закона № 99-З и иных актов законодательства (п. 2 ст. 17). В совокупности это и оценивает НЦЗПД в ходе проверочных мероприятий [1].



В рамках реализации одной из своих профилактических функций (абз. 7 п. 7 Положения о Национальном центре защиты персональных данных, утвержденного Указом № 422) порядок применения мер по обеспечению защиты персональных данных активно разъясняется НЦЗПД. Однако, учитывая центральное место данных вопросов в механизме реализации законодательства о персональных данных и ужеработанную правоприменительную практику, усматривается целесообразность конкретизации и расширения соответствующих регулятивных положений на законодательном уровне. Видится, что меры по обеспечению защиты персональных данных должны быть понятными и сбалансированными, а их реализация не должна отвлекать значительные ресурсы от осуществления операторами (уполномоченными лицами) их основной деятельности.

Одной из первостепенных мер по обеспечению защиты персональных данных выступает назначение оператором (уполномоченным лицом), являющимся государственным органом, юридическим лицом Республики Беларусь, иной организацией, структурного подразделения или лица, *ответственного за осуществление внутреннего контроля за обработкой персональных данных* (абз. 2 п. 3 ст. 17 Закона № 99-З). В мировой практике такое лицо именуется инспектором по защите персональных данных, или кратко – DPO (Data Protection Officer). DPO может являться сотрудником контролера или обрабатывающего данные лица, или он может выполнять задачи на основе договора об оказании услуг (ст. 37 GDPR) [4].

Белорусское законодательство прямо не предусматривает возможность передачи функции по осуществлению внутреннего контроля за обработкой персональных данных третьему лицу, и данная проблематика являлась одной из обсуждаемых тем на площадке Белорусского юридического форума

«Право в современном мире» в декабре 2025 г. [12]. С учетом зарубежного опыта правового регулирования и незначительной штатной численности отдельных организаций представляется оправданным предоставить возможность передачи осуществления такой функции третьим лицам по договору, например, субъектами малого предпринимательства (коммерческими организациями со средней численностью работников за календарный год до 100 человек включительно).

В контексте требования п. 33 Концепции обеспечения суверенитета Республики Беларусь в сфере цифрового развития до 2030 года, утвержденной постановлением Совета Министров Республики Беларусь от 31 декабря 2024 г. № 1074, о том, что при разработке программного обеспечения необходимо учитывать требования законодательства о персональных данных, также предлагается рассмотреть возможность предоставления указанной функции «центрам кибербезопасности» и «офисам цифровизации» государственных органов и организаций, созданных в соответствии с указами от 14 февраля 2023 г. № 40 «О кибербезопасности» и от 29 ноября 2023 г. № 381 «О цифровом развитии». Это позволит выполнять внутренний контроль за обработкой персональных данных на более профессиональном уровне, сконцентрировав имеющиеся трудовые ресурсы государственных органов и организаций на реализации ими своих основных функций публичного характера.

Законодательство о персональных данных нередко ассоциируется со всевозможными *политиками обработки персональных данных* (абз. 3 п. 3 ст. 17 Закона № 99-3), но специальные законодательные требования к их составлению не предусмотрены. С момента вступления в силу Закона № 99-3 НЦЗПД неоднократно давались развернутые рекомендации по составлению документов, определяющих политику оператора (уполномоченного лица) в отношении обработки персональных данных, в т. ч. с ориентиром на их разработку для видеонаблюдения и обработки файлов cookie. Исходя из терминологии Закона № 99-3, издание политики не является обязательным для государственных органов, которые действуют в соответствии с положениями специальных нормативных правовых актов о них, хотя на практике имело место и выполнение указанной меры. Более того, отдельные организации с точки зрения реализации мер по защите персональных данных

ограничиваются лишь изданием таких документов, придавая всей проводимой работе исключительно формальный характер.

Учитывая разносторонний характер деятельности операторов (уполномоченных лиц), а также тот факт, что политика обработки персональных данных, на наш взгляд, в большей степени является элементом реализации требования прозрачности их обработки (п. 6 ст. 4 Закона № 99-3), чем реальных практических мер по защите персональных данных, возможно, следовало бы установить минимальные (типовые) требования к таким политикам на подзаконном уровне и даже сузить перечень операторов (уполномоченных лиц), обязанных их составлять (ограничиваясь лишь теми субъектами, информацию о деятельности которых в связи с обработкой персональных данных гражданам получить может быть затруднительно, а также случаями обработки данных с применением цифровых технологий, например, видеоаналитики и файлов cookie).



Одной из непоименованных в Законе № 99-3, но зачастую рекомендуемых к выполнению на практике мер по обеспечению защиты персональных данных называется *ведение реестра обработки персональных данных*. Основываясь на обязанности оператора по предоставлению гражданам информации, касающейся обработки их персональных данных (п.п. 1–3 ст. 11 Закона № 99-3), и подп. 3.5 п. 3 Указа № 422, который уже обязывает операторов-организаций устанавливать и поддерживать в актуальном состоянии отдельную информацию об обработке персональных данных (перечни информационных ресурсов и уполномоченных лиц, категории данных и сроки их хранения), на законодательном уровне, вероятно, можно было бы формализовать требование по ведению некоторыми операторами такого реестра с минимальным набором информации.

В завершение нельзя не обратить внимание, что как GDPR (ст. 25), так и принятый в СНГ 18 апреля 2025 г. модельный закон «О технологиях искусственного интеллекта» обязывает исследователей, разработчиков, производителей технологий ИИ соблюдать требования «проектируемой конфиденциальности»,

имплементированные в национальном законодательстве о персональных данных, путем создания технологических продуктов и решений, позволяющих обеспечить конфиденциальность и защиту персональных данных по умолчанию (ст. 26).

На основании изложенного можно констатировать, что белорусское законодательство о персональных данных с момента начала его комплексного развития в 2021 году прошло апробацию практикой с учетом имеющегося международного и зарубежного опыта, особенностей национальной правовой системы и ускорения развития цифровых технологий. Это позволило выделить ряд направлений совершенствования Закона № 99-З и связанных с ним нормативных правовых актов, ориентированных на усиление правовой определенности норм, регулирующих общественные отношения в информационной сфере, укрепление конституционного права на неприкосновенность частной жизни и информационной безопасности в целом.

Список источников

1. Отчет о деятельности НЦЗГД за 2025 год // Официальный сайт НЦЗГД. – 2026. – URL: <https://cpd.by> (дата обращения: 21.03.2026).
2. В 2026 году удельный вес киберпреступлений в структуре преступности составляет почти 40 процентов // SB.BY Беларусь сегодня. – 2026. – URL: <https://www.sb.by/articles/v-2026-godu-udelnyy-ves-kiberprestupleniy-v-strukture-prestupnosti-sostavlyayet-pochti-40-protentov.html> (дата обращения: 21.03.2026).
3. О состоянии конституционной законности в Республике Беларусь : решение Конституционного Суда Республики Беларусь от 12 марта 2026 г. № ПР-9/2026 // ЭТАЛОН: информ.-поисковая система (дата обращения: 21.03.2026).
4. General Data Protection Regulation (GDPR) // Complete Guide to GDPR Compliance. – 2026. – URL: <https://gdpr.eu/tag/gdpr/> (date of access: 21.03.2026).
5. Постатейный комментарий к Закону Республики Беларусь «О защите персональных данных» // Официальный сайт НЦЗГД. – 2026. – URL: <https://cpd.by> (дата обращения: 21.03.2026).
6. Абламейко, М. С. Биометрические персональные данные и дипфейки: правовой аспект / М. С. Абламейко, Н. В. Шакель // Право.by. – 2024. – № 3. – С. 79–87.
7. Разъяснения законодательства о персональных данных (о порядке осуществления видеонаблюдения в многоквартирных жилых домах) / Официальный сайт НЦЗГД. – 2026. – URL: <https://cpd.by> (дата обращения: 21.03.2026).

8. Хомич, М. В. Устанавливаем видеонаблюдение в организации: как не нарушить законодательство о персональных данных (актуально на 10.02.2026) / М. В. Хомич // iLex: информ. правовая система (дата обращения: 21.03.2026).

9. Полещук, Д. Г. Видеонаблюдение и видеосъемка как обработка персональных данных / Д. Г. Полещук // Актуальные проблемы гражданского права. – 2023. – № 2. – С. 32–48.

10. О персональных данных: Федер. закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ : с изм. от 24 июня 2025 г. // КонсультантПлюс. Россия : справ. правовая система (дата обращения: 21.03.2026).

11. Закон о регулировании ИИ могут принять в России // Sputnik Беларусь. – 2026. – URL: <https://sputnik.by/20260318/zakon-o-regulirovanii-ii-mogut-prinyat-v-rossii-1105364694.html> (дата обращения: 21.03.2026).

12. Защита персональных данных: кто эффективнее – человек или технологии? Итоги секции Белорусского юридического форума // Белорусский республиканский союз юристов. – 2026. – URL: <https://union.by> (дата обращения: 21.03.2026).

Материал поступил в редакцию 07.04.2026

D. G. POLESHCHUK

On Some Practical Issues of Applying Personal Data Legislation in the Context of Digital Transformation

Alongside with increasing the volume of personal information processing in the age of digital technologies, the importance of its protection is growing up accordingly. Comprehensive legislation on personal data formed up in the Republic of Belarus in 2021, have undergone practical testing over several years. Taking into account the planned drafting of a bill on personal data protection this year, this article is examining certain problematic aspects of the current legal framework and suggesting promising areas for its improvement.

Keywords: *personal data, legislation, digital technologies, video surveillance, artificial intelligence, processing, consent.*

Рецензент: ДУБКО М. А.,
кандидат юридических наук, доцент, главный
советник экспертно-правового управления
Государственного секретариата Совета
Безопасности Республики Беларусь