47. ЦИФРОВЫЕ ПОДПИСИ И ИХ РОЛЬ В ЦИФРОВОЙ ТРАНСФОРМАЦИИ БИЗНЕСА И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Цымбал Н.О., Михайловская М.С.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Орлова Е.И. – старший преподаватель

В условиях развития информационных технологий, цифровизации государства возникают проблемы с использованием информации, поступающей в глобальную сеть. Персональные данные лиц используются ими практически при любых действиях в сети Интернет, что порождает риск злоупотребления и незаконной обработки данной информации. При незаконной обработке персональных данных нарушаются основные права и свободы человека, что приводит к неблагоприятным последствиям в жизни общества и государства. В данной статье предпринята попытка исследовать основные проблемы обработки и защиты персональных данных в сети Интернет. Сделаны выводы о дальнейшем развитии законодательства в данной сфере.

В XXI веке фундаментом практически любой сферы жизни стала информация. Необходимость внедрения информационных технологий является одним из основополагающих направлений развития государства, так как они способствуют ускорению, упрощению различных процессов населения, государственных органов и государства в целом.

Внедрение информационных технологий приобретает глобальные масштабы, охватывая все сферы жизни общества и государства, что позволяет говорить об информатизации, происходящей при осуществлении каких-либо действий данными субъектами. Под цифровизацией в узком смысле понимается преобразование информации в цифровую форму, которое в большинстве случаев ведёт к снижению издержек и появлению новых возможностей. Цифровизацию в широком смысле можно рассматривать как тренд эффективного мирового развития только в том случае, если цифровая трансформация информации отвечает следующим требованиям: она охватывает производство, бизнес, науку, социальную сферу и обычную жизнь граждан; сопровождается лишь эффективным использованием; её результаты доступны пользователям преобразованной информации; ею пользуются не только специалисты, но и рядовые граждане [1, с. 46].

Несмотря на достаточное количество преимуществ цифровизации, существуют вопросы, связанные с появлением новых способов контроля и управления, где персональные данные выступают инструментом. В современных «цифровых» условиях возникает проблема, которая состоит в том, что при любых взаимодействиях человека и информационных технологий появляется «цифровой след» данного лица.

В процессе цифровизации большинство привычных нам процедур приобретает электронный формат, например, подача заявлений в государственные органы, обращение в медицинские учреждения, оформление заказов в интернет-магазинах, регистрация на сайтах государственных органов и другие. Так, при осуществлении таких действий персональные данные населения попадают в глобальную сеть Интернет и обрабатываются в электронном формате. Исходя из этого, возникает вопрос о защите персональных данных.

В соответствии с Законом Республики Беларусь «О защите персональных данных» персональные данные – любая информация, относящаяся к идентифицированному физическому лицу или физическому лицу, которое может быть идентифицировано. Безусловно, возможность использования персональных данных должна быть одобрена лицом, чьи персональные данные будут обрабатываться. Закон «О защите персональных данных» раскрывает понятия «субъект персональных данных» и «оператор». В частности, субъект персональных данных – физическое лицо, в отношении которого осуществляется обработка персональных данных. В свою очередь, оператор – государственный орган, юридическое лицо Республики Беларусь, иная организация, физическое лицо, в том числе индивидуальный предприниматель, самостоятельно или совместно с иными указанными лицами организующие и осуществляющие обработку персональных данных.

Право на защиту персональных данных – основополагающее право человека, в особенности, в век информационных технологий. Отсутствие гарантии на защиту личной информации порождает нарушение других, фундаментальных прав человека.

Традиционным способом защиты персональных данных выступает согласие физического лица на действия с его персональными данными. Данный способ с каждым днем становится менее действенным в виду того, что люди должным образом не реагируют на просьбы о согласии на использование их данных и ставят определенные отметки на всплывающих окнах различных Интернет-сайтов [2, с. 117]. Итогом этого служит отсутствие контроля за персональными данными субъекта и возрастание рисков незаконного использования информации.

Таким образом, возникают проблемы использования персональных данных в сети Интернет, которые обусловлены их попаданием в сеть при отсутствии согласия субъекта на такие действия и отсутствием эффективных способов получения компенсации, в виду незаконного использования личной информации субъекта.

Также сложно говорить об отказе в обороте персональных данных в сети Интернет. При этом механизмы выявления незаконного использования персональных данных субъектов развиты достаточно слабо и неэффективно. Отсутствуют четко сформированные подходы по обеспечению механизма защиты персональных данных в глобальной сети, при условии количества обработки информации в данной среде. Необходим пересмотр уже устоявшихся «классических» механизмов защиты персональных данных.

Возникает вопрос о создании типовой формы пользовательского соглашения, а также необходимость в конкретизации сроков и целей хранения персональных данных субъектов [3, с. 18].

Стоит отметить, что в рамках сети Интернет, взаимодействие оператора и субъекта персональных данных может выходить за пределы одного государства, это говорит о необходимости в разработке правового регулирования на более высоком уровне [4, с. 47]. В виду сложностей, как политических, так и социально-экономических данное предложение достаточно затруднительно в реализации, поэтому первоначально необходима разработка более эффективных способов выявления правонарушений и преступлений в отношении персональных данных в сети Интернет на государственном уровне.

Существует острая необходимость в реализации механизмов криптографической защиты и анонимизации данных в сети Интернет, так как субъекты персональных данных ежедневно оставляют свой «цифровой след» в глобальной сети, позволяющий использовать личную информацию в незаконных целях. Данный механизм должен быть реализован как на уровне хранения, так и передачи данных. Это включает использование шифрования для данных, передаваемых по сети, а также анонимизации информации, которая не требуется для выполнения функциональных задач. Важно внедрить такие технологии, как публичные и частные ключи для аутентификации пользователей и обеспечения конфиденциальности данных.

Кроме того, важным шагом в реализации решения является обязательное обучение пользователей и повышение их осведомленности о рисках, связанных с цифровым следом, а также интеграция механизмов двухфакторной аутентификации и защищенных каналов связи для предотвращения доступа к данным со стороны третьих лиц.

В итоге, внедрение таких технологий и стандартов защиты персональных данных будет способствовать снижению рисков незаконного использования информации и обеспечению большей безопасности для пользователей в глобальной сети.

Список использованных источников:

1.Халин, В.Г. Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски / В.Г. Халин, Г.В. Чернова // Управленческое консультирование. – 2018. – № 10. – С. 46–63.

2.Лачина, Е.А. Проблемы защиты персональных данных в сети «Интернет» / Е.А. Лачина, И.А. Кузнецова, Е.В. Носова // Ученые записки. – 2021. – №1(37). – С. 116–121.

3.Дмитриева, Е.Г. Проблемы защиты персональных данных в цифровом мире и пути их решения / Е.Г. Дмитриева //Право и бизнес. – 2021. – № 3. – С. 18–20.

4.Семенов, Е.Ю. Проблемы правового регулирования автоматизированной обработки общедоступных персональных данных / Е.Ю. Семенов, Е.С. Лысенко // Вестник Уфимского юридического института МВД России. – 2021. – С. 47–52.