

СРАВНИТЕЛЬНЫЙ АНАЛИЗ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ О ПЕРСОНАЛЬНЫХ ДАННЫХ США И РОССИЙСКОЙ ФЕДЕРАЦИИ В СФЕРЕ ИХ ИЗБЫТОЧНОГО СБОРА

Е.Д. Мартинес Моралес

Белорусский государственный экономический университет

Аннотация

Данная работа проводит сравнительный анализ нормативно-правовых актов, регулирующих обработку персональных данных, в Соединенных Штатах Америки и Российской Федерации. Основное внимание в статье уделяется эффективности рассматриваемых нормативов в предотвращении избыточного сбора персональной информации. Целью исследования является изучение различий и сходств в нормативных подходах к защите персональных данных, оценка эффективности мер по предотвращению неправомерного и избыточного сбора информации о физических лицах. Работа предполагает оценку соответствия нормативов принципам пропорциональности и необходимости в процессе сбора персональных данных.

Ключевые слова: персональные данные, избыточный сбор персональных данных о субъекте, обработка персональных данных в США, обработка персональных данных в Российской Федерации, риски и последствия при избыточном сборе персональных данных.

Современный мир стал свидетелем взрывного роста объема персональных данных, собираемых и обрабатываемых государственными органами и частными компаниями. Подобный рост вызвал серьезные вопросы в сфере защиты частной жизни и личной безопасности граждан. Персональные данные о гражданах используются не только для оказания необходимых им услуг, но и в коммерческих, медицинских, исследовательских и многих других целях. С ростом объемов собираемой информации возникает риск её избыточного сбора. Подобная тенденция становится угрозой нарушения принципа невмешательства в частную жизнь и значительно сужает наши личные границы.

Для решения данного вопроса и выстраивания «границ» обработки персональных данных в различных странах введены нормативно-правовые акты по ограничению и регулированию степени подобного вмешательства. Однако их эффективность в предотвращении избыточного сбора персональных данных может существенно различаться. Таким образом, именно анализ законодательства различных стран поможет найти верный и наиболее безопасный подход к регулированию сбора и использования персональной информации для Республики Беларусь.

Использование персональных данных в США

В США регулирование персональных данных разрознено и включает в себя несколько законов на федеральном уровне и уровне штатов. Главным федеральным актом является Закон о конфиденциальности в сфере

здравоохранения (HIPAA) и Закон о конфиденциальности потребителей (CCPA) в Калифорнии.

Важно отметить, что в США нет единого закона о защите персональных данных, вместо этого существует фрагментированная система правил, регулирующих определенные аспекты сбора, хранения и использования персональных данных.

Один из ключевых федеральных законов, касающихся персональных данных в США – это Закон о конфиденциальности медицинских записей (Health Insurance Portability and Accountability Act, HIPAA), который регулирует обработку медицинских данных и обеспечивает их конфиденциальность.

Еще одним важным актом является Закон о кредитных отчетах (Fair Credit Reporting Act, FCRA), который регулирует сбор, хранение и распространение информации о кредитной истории потребителей.

Согласно данному закону, перед тем как организация запросит кредитный отчет потребителя, она обязана его уведомить и получить согласие на проведение подобной проверки. Потребители, в свою очередь, вправе отказать в предоставлении согласия. Если последние отказываются, то организация не может запросить их кредитный отчет и должна исходить из доступной информации.

Стоит отметить, что в американском федеральном законодательстве определяются только обязанности госорганов в сфере защиты персональных данных, не затрагивая частные компании. Нормы, регулирующие обработку персональных данных частными компаниями, принимают на уровне штатов. Например, в штате Калифорния в 2020 году принят закон, регулирующий правила сбора данных и работы с ними. По этому закону физическое лицо, использующее услуги интернет-компаний, имеет право знать:

- какую информацию о нем собирает интернет-компания;
- с какой целью компании собирает эти сведения;
- каким образом данные будут использованы.

В дальнейшем субъект имеет право запретить передачу своих персональных данных третьим лицам, либо вообще требовать уничтожения таких данных.

Таким образом можно заметить, что регулирование персональных данных в США основывается на прозрачности и добровольной согласованности действий объекта персональных данных и оператора. Это означает, что компании обязаны предоставлять информацию о том, как они используют персональные данные самим физическим лицам и заручаться прежде всего их согласием и одобрением. В такой ситуации, регулирование объема собираемых персональных данных, их обработка и хранение со стороны органов государственного управления уходят на второй план, ведь основная заинтересованность в охране частной жизни лежит на самих субъектах персональных данных. Вместе с тем, практический опыт показывает, что подхода «добровольной согласованности» недостаточно и

требуется принятие новых более консолидированных законов, которые ужесточат правила обработки персональных данных.

Использование персональных данных в Российской Федерации

В Российской Федерации регулирование персональных данных осуществляется на федеральном уровне и основывается на Федеральном законе «О персональных данных» от 27.07.2006 № 152-ФЗ в редакции от 06.02.2023 № 8-ФЗ, а также на других законах и подзаконных актах.

В Федеральном законе «О персональных данных» от 27.07.2006 № 152-ФЗ прописаны принципы осуществления обработки информации ограниченного доступа, в частности персональных данных, обязанности оператора, осуществляющего такую обработку, а также права субъекта персональных данных. Согласно тексту данного закона, основной его целью является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну [1, с.30].

Следует отметить, что с течением времени российское законодательство о персональных данных подвергалось изменениям и дополнениям, например, введен в действие Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» от 29.07.2017 № 242-ФЗ (и его последующих поправок), который направлен на регулирование применения информационных технологий в сфере охраны здоровья в России. Вышеуказанным законом внедряется использование электронных медицинских документов для хранения и обмена информацией о пациентах, устанавливаются правила обработки персональных данных в медицинских целях, а рассматривается вопрос телемедицины и удаленного медицинского консультирования.

Регламентирование отношений, возникающих при сборе, хранении и обработке персональных данных вытекает из негативных последствий, к которым приводят неправильные сбор и хранение персональных данных. Так, в октябре 2020 года Одинцовский городской суд Московской области вынес обвинительный приговор в отношении гражданина А., который, являясь специалистом офиса продаж ООО «Русская Телефонная Компания», действуя из корыстных побуждений, осуществил неправомерный доступ к персональным данным клиентов (фамилии, имена, отчества, адреса регистрации, серии и номера паспортов, номера лицевого счетов, сведения об остатках денежных средств на абонентских номерах), фотографировал и передавал их третьему лицу за вознаграждение. Давая юридическую оценку, суд квалифицировал его действия как неправомерный доступ к компьютерной информации с использованием служебного положения и сбор сведений, составляющих коммерческую тайну и их разглашение. Судом было назначено наказание в виде 2 лет 6 месяцев условного лишения свободы, с испытательным сроком три года. Таким образом, фактически гражданин А. не понёс существенного наказания за свои действия. К тому же, если юридическое лицо, сотрудником которого он являлся, не проявит должной

степени ответственности и просто наймёт другого работника, подобная ситуация не исключена в последующем. Каким образом могут быть использованы украденные данные и какие последствия возникнут для их обладателей, в данной ситуации никого не интересует, даже если это способствует правонарушению [2, с.118-123].

Случаи утечки персональных данных вынуждают задуматься о целесообразности и необходимости их сбора субъектами хозяйствования, так как не каждая компания сможет обеспечить надлежащее хранение и использование собранных персональных данных. Более того, зачастую собранные персональные данные избыточны и напрямую противоречат принципам пропорциональности и необходимости.

Не так давно крупнейший российский онлайн-рынок Wildberries объявил о введении ограничений для неподтвержденных пользователей, которые теперь обязаны предварительно оплатить свои заказы. Это подтверждение осуществляется путем связи с банком "Тиньков" или использования Госуслуг.

Пользователи, пытаясь подтвердить свои аккаунты, были удивлены тем, что Wildberries требует полный доступ к их учетным записям на Госуслугах, включая все хранимые там личные данные.

Теперь услуги маркетплейса доступны для «неподтвержденных пользователей» только с полной предоплатой товара [3].

В действиях маркетплейса четко видны признаки избыточного сбора персональных данных его пользователей.

Таким образом, сравнительный анализ нормативно-правовых актов о персональных данных в США и России показал, что стандарты и подходы могут значительно различаться. Важно учитывать, что эффективность законодательства зависит не только от его строгости, но и от мер по его соблюдению и контролю. В будущем, практическое использование принятых правовых актов и обмен опытом поможет улучшить защиту персональных данных на глобальном уровне. Однако в настоящий момент, вопрос избыточного сбора персональных данных становится общемировой проблемой и представляет серьезные риски с точки зрения нарушения приватности и безопасности физических лиц:

во-первых, повышается возможность утечки персональных данных: чем больше данных собирается, тем больше возможностей для взлома систем их хранения;

во-вторых, возникает риск злоупотребления данными. Так, избыточные данные могут быть использованы для массового маркетинга, таргетированной рекламы или даже мошенничества;

в-третьих, появляется сложность в управлении персональными данными. Так как обработка и управление большим объемом избыточных данных увеличивает риск ошибок со стороны ответственного лица.

Список использованных источников:

1. Исаев, А. С. Правовые основы организации защиты персональных данных: учеб. пособие / А.С. Исаев, Е. А. Хлюпина // СПб. : НИУ ИТМО, 2014. – 106 с.
2. Рязанова, Е. Н. Ответственность за распространение персональных данных как способ противодействия правонарушениям в сфере информационно-коммуникационных технологий / Е. Н. Рязанова // Вестник Санкт-Петербургского университета МВД России. – 2022. – № 3 – С. 118–123.
3. Публицистическая статья: Wildberries ввел авторизацию через «Госуслуги»: чего боятся пользователи [Электронный ресурс] // hi-tech. – Режим доступа: <https://hi-tech.mail.ru/news/59210-wildberries-vvel-avtorizaciyu-cherez-gosuslugi-chego-boyatsya-polzovateli/?ysclid=ln1pjz6zdz61505803/>. – Дата доступа: 01.12.2023.
4. Пазюк, А. Защита персональных данных: введение в проблематику: учебное пособие / А. Пазюк, М. Соколова. – Минск : Альтера, 2015. – 116 с.
5. Privacy's Blueprint: The Battle to Control the Design of New Technologies / Woodrow Hartzog // Academic Trade, 2018. – 384 p.
6. Data Protection Laws and Regulations USA 2023 / JD F. Paul Pittman, JD Andrew Hamm, Abdul Hafiz [Электронный ресурс] // Global Legal Group. – Режим доступа: <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa>. – Дата доступа: 01.12.2023.