УДК 340.132:342.7:347.121.2
DOI: 10.36979/1694-500X-2024-24-11-80-85

НЕКОТОРЫЕ АСПЕКТЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ

М.У. Алияскарова

Аннотация. Исследуются правовое регулирование безопасности личной информации и некоторые аспекты, связанные с ними. В последние годы проблеме безопасности личной информации уделяется значительное внимание в связи с увеличением числа киберпреступлений, которые происходят по всему миру. Личная информация определяется как любая информация, относящаяся к идентифицированному или поддающемуся идентификации физическому лицу: идентификационный номер, данные о местоположении, онлайн-идентификатор или любой другой фактор, специфичный для физической, физиологической, генетической, ментальной, экономической, культурной или социальной идентичности этого физического лица. Анализируется круг отношений, который включается исследователями в сферу информационной безопасности личности. Делается вывод, что для гармоничного развития института информационной безопасности личности необходимо усиление внетехнических, социально направленных мер и стимулов.

Ключевые слова: информационная безопасность личности; национальная безопасность; идентификация; защита информации; доктрина информационной безопасности; кибербезопасность.

ЖЕКЕ МААЛЫМАТ КООПСУЗДУГУН УКУКТУК ЖӨНГӨ САЛУУНУН АЙРЫМ АСПЕКТИЛЕРИ

М.У. Алияскарова

Аннотация. Макалада жеке маалыматтын коопсуздугун укуктук жөнгө салуу жана ага байланыштуу айрым аспектилер каралат. Акыркы жылдары дүйнө жүзү боюнча болуп жаткан кибер кылмыштардын көбөйүшүнө байланыштуу жеке маалыматтын коопсуздугу маселесине олуттуу көңүл бурулууда. Жеке маалымат катары аныкталган же идентификациялануучу адамга тиешелүү ар кандай маалымат, идентификациялык номер, жайгашкан жери жөнүндө маалымат, онлайн идентификатор же ошол адамдын физикалык, физиологиялык, генетикалык, психикалык, экономикалык, маданий же социалдык иденттүүлүгүнө мүнөздүү болгон башка факторлор аныкталат. Бул макалада жеке маалыматтын коопсуздугун укуктук жөнгө салуу, ошондой эле ага байланыштуу актуалдуу аспектилер каралат. Изилдөөчүлөр тарабынан инсандык маалыматтык коопсуздук чөйрөсүнө киргизилген мамилелердин чөйрөсү талданат. Инсандын маалыматтык коопсуздук институтун гармониялуу өнүктүрүү үчүн техникалык, социалдык багыттагы чараларды жана стимулдарды күчөтүү зарыл деген тыянак чыгарылды.

Түйүндүү сөздөр: жеке маалымат коопсуздугу; улуттук коопсуздук; идентификация; маалыматты коргоо; маалыматтык коопсуздук доктринасы; киберкоопсуздук.

CERTAIN ASPECTS OF THE LEGAL REGULATION OF PERSONAL INFORMATION SECURITY

M.U. Aliyaskarova

Abstract. The article examines the legal regulation of the security of personal information and explores some aspects related to this. In recent years, the issue of personal information security has received considerable attention due to the increase in the number of cybercrimes that occur around the world. Personal information is defined as any information

relating to an identified or identifiable individual, identification number, location data, online identifier or any other factor specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual. This article examines the legal regulation of the security of personal information, as well as relevant aspects related to it. The circle of relations that researchers include in the sphere of personal information security is analyzed. It is concluded that for the harmonious development of the institute of information security of the individual, it is necessary to strengthen non-technical, socially oriented measures and incentives.

Keywords: personal information security; national security; identification; information protection; information security doctrine; cybersecurity.

Безопасность личной информации вызывает все большую озабоченность в связи с растущим числом утечек данных и кибератак по всему миру. Правовое регулирование играет решающую роль в защите личной информации и обеспечении того, чтобы организации следовали лучшим практикам при сборе, хранении и использовании персональных данных. Однако существует несколько проблем, связанных с правовым регулированием безопасности личной информации, которые необходимо решить. В этой статье мы рассмотрим проблемы правового регулирования безопасности личной информации и предложим возможные решения.

Защита личной информации регулируется различными правовыми системами по всему миру. В Европейском союзе Общее положение о защите данных (GDPR) обеспечивает всеобъемлющую правовую основу для защиты персональных данных. GDPR устанавливает строгие правила обработки персональных данных и налагает суровые наказания за несоблюдение. Аналогичным образом в Соединенных Штатах Закон о неприкосновенности частной жизни 1974 года и Закон о переносимости и подотчетности медицинского страхования (HIPAA) обеспечивают правовую основу для защиты персональных данных.

Кроме того, различные международные организации, такие как Международная организация по стандартизации (ISO) и Целевая группа по разработке Интернета (IETF), разработали стандарты и руководящие принципы для защиты личной информации. Эти рамки предоставляют организациям набор наилучших практик, которым следует следовать при обработке персональных данных, и могут помочь им соблюдать требования законодательства.

Утечки данных происходят, когда доступ к личной информации осуществляется или раскрывается без разрешения. Эти нарушения могут произойти по различным причинам, включая кибератаки, человеческую ошибку или системные сбои. Правовые рамки, как правило, требуют от организаций незамедлительно сообщать о нарушениях данных регулирующим органам и пострадавшим лицам. Непредставление сообщения об утечке данных может привести к суровым наказаниям, включая штрафы и юридическую ответственность.

В большинстве правовых систем обработка персональных данных требует согласия субъекта данных. Организации должны получить явное согласие от физических лиц на сбор, хранение и использование их персональных данных. Согласие должно быть дано свободно, конкретным, информированным и недвусмысленным. Организации также должны предоставить отдельным лицам право отозвать свое согласие в любое время.

Правовые рамки, как правило, предоставляют отдельным лицам право на доступ к своим персональным данным и требовать их удаления. Организации должны предоставлять частным лицам копию их персональных данных по запросу и удалять их, если в них больше нет необходимости для цели, для которой они были собраны. Правовые рамки требуют от организаций принятия соответствующих мер безопасности для защиты персональных данных от несанкционированного доступа, раскрытия или уничтожения. Эти меры безопасности могут включать шифрование, контроль доступа и регулярные проверки безопасности.

Безопасность личной информации – важнейший вопрос, требующий надежного правового регулирования для защиты физических лиц от утечек данных и киберпреступлений. Правовая база предоставляет организациям набор наилучших практик, которым следует следовать при обработке персональных данных, включая получение явного согласия, сообщение о нарушениях

данных, предоставление отдельным лицам права на доступ и удаление их персональных данных и внедрение соответствующих мер безопасности. Соблюдение этих правовых рамок имеет важное значение для поддержания доверия клиентов, защиты персональных данных и избежания юридической ответственности.

Одной из основных проблем правового регулирования безопасности личной информации является отсутствие международной согласованности. В разных странах действуют разные правовые рамки защиты персональных данных, что может создать путаницу для глобальных организаций. Например, Общий регламент Европейского союза по защите данных (GDPR) является одной из наиболее всеобъемлющих правовых рамок для защиты персональных данных, но он существенно отличается от других рамок, используемых в Соединенных Штатах и Азии. Такое отсутствие согласованности может затруднить организациям соблюдение требований законодательства и защиту персональных данных.

Многосторонние международные правовые акты в сфере обеспечения информационной безопасности относятся к различным и нередко разрозненным институтам информационного права, таким как преступность в сфере компьютерной информации [1; 2], обработка персональных данных [3] и т. д. В настоящее время, несмотря на предпринятые попытки создания, не существует единого международного соглашения в сфере информационной безопасности [4]. Законодательство отдельных стран показывает скачкообразный рост числа актов, принимаемых в рамках обеспечения информационной безопасности и безопасности данных [5]. Отдельно стоит отметить Директиву Европейского союза о безопасности сетей и информационных систем [6], подчеркивающую особую роль информационных технологий для развития общества и защиты пользователей, закон Сингапура о кибербезопасности [7], проект закона Китайской Народной Республики [8]. Кроме отдельных отраслевых законов, зарубежные страны разрабатывают и принимают стратегические документы в сфере обеспечения информационной безопасности, например, Стратегию национальной кибербезопасности Словении [9], регулирующую технические и внетехнические меры обеспечения безопасности государства, общества и личности. Необходимо отметить, что большая часть положений зарубежного законодательства обращена как раз к технической составляющей информационной безопасности личности.

Правовые рамки обеспечения безопасности личной информации могут быть сложными, и ориентироваться в них непросто. Например, GDPR представляет собой сложную правовую базу, которая требует от организаций соблюдения конкретных требований по защите данных. Эта сложность может затруднить организациям понимание своих юридических обязательств и их соблюдение. Кроме того, сложность правовой базы может затруднить эффективное применение нормативных актов регулирующими органами.

Еще одной проблемой правового регулирования безопасности личной информации является «неадекватное» правоприменение. Даже при наличии строгих правовых рамок организации все равно могут не соблюдать требования законодательства. Без эффективных механизмов обеспечения соблюдения организации могут не столкнуться с последствиями несоблюдения, что может привести к отсутствию подотчетности и повышенному риску утечки данных [10].

Быстро меняющийся технологический ландшафт является еще одной проблемой правового регулирования безопасности личной информации. По мере развития новых технологий организациям может потребоваться собирать и обрабатывать персональные данные новыми способами. Правовая база не всегда может соответствовать этим изменениям, оставляя пробелы в регулировании защиты персональных данных. Кроме того, новые технологии могут создавать новые риски для безопасности персональных данных, которые правовые рамки могут не учитывать.

Чтобы решить проблему отсутствия международной согласованности, организации могут работать над внедрением лучших мировых практик защиты персональных данных. Международные организации, такие как Международная организация по стандартизации (ISO) и Целевая группа по разработке Интернета (IETF),

способны предоставить рекомендации и стандарты, которые могут принять во всем мире.

Правовые рамки обеспечения безопасности личной информации могут быть упрощены путем предоставления четких руководящих принципов и стандартизации юридических формулировок. Регулирующие органы могут работать над разработкой простых, удобных для пользователя руководящих принципов, которые могут быть легко поняты организациями и которым они должны следовать.

Чтобы усилить правоприменение, регулирующие органы могут увеличить штрафы за несоблюдение правовых рамок. Кроме того, регулирующие органы могут проводить регулярные аудиты, чтобы убедиться, что организации соблюдают требования законодательства.

Чтобы адаптироваться к технологическим изменениям, регулирующие органы могут работать над разработкой гибкой правовой базы, способной идти в ногу с быстро меняющимся технологическим ландшафтом. Кроме того, регулирующие органы могут тесно сотрудничать с экспертами в области технологий для выявления новых рисков и разработки новых нормативных актов для их устранения.

Растущее значение персональных данных в современном мире привело к растущей потребности в эффективном правовом регулировании безопасности личной информации. Регулирование безопасности персональных данных имеет важное значение для обеспечения конфиденциальности и безопасности отдельных лиц и организаций. В этой статье мы рассмотрим перспективы правового регулирования безопасности личной информации, включая преимущества и проблемы, связанные с таким регулированием [11].

Правовое регулирование безопасности личной информации обеспечивает основу для защиты персональных данных от неправильного использования, несанкционированного доступа и других угроз. При наличии надлежащего регулирования организации обязаны соблюдать конкретные стандарты и процедуры обработки персональных данных, что снижает риск утечки данных и кражи личных данных. Когда потребители знают, что их персональные данные защищены законом, они с большей вероятностью будут доверять организациям, которые обрабатывают их данные. Это может привести к повышению лояльности и доверия потребителей, что крайне важно для успеха любой организации.

Правовое регулирование безопасности личной информации также может привести к улучшению практики управления данными. Организации, которые обязаны соблюдать определенные стандарты и процедуры, с большей вероятностью будут инвестировать в системы и процессы управления данными, которые могут помочь им соответствовать этим стандартам. Это может привести к более эффективным методам управления данными и снижению риска утечки данных. Правовое регулирование безопасности личной информации может помочь гармонизировать законы и нормативные акты, касающиеся конфиденциальности и безопасности данных, в разных странах и регионах. Это может привести к повышению согласованности и уменьшению путаницы для организаций, которые работают в нескольких юрисдикциях.

Одной из самых больших проблем правового регулирования безопасности личной информации является нахождение правильного баланса между безопасностью и конфиденциальностью. Хотя важно защищать персональные данные от несанкционированного доступа и неправильного использования, также важно сделать так, чтобы права отдельных лиц на неприкосновенность частной жизни не нарушались. Достижение правильного баланса между этими двумя факторами может оказаться непростой задачей.

Еще одна проблема правового регулирования безопасности личной информации заключается в том, чтобы идти в ногу с быстро меняющимся технологическим ландшафтом. По мере развития новых технологий организациям может потребоваться собирать и обрабатывать персональные данные новыми способами. Правовая база не всегда может соответствовать этим изменениям, оставляя пробелы в регулировании защиты персональных данных.

Эффективное соблюдение правовых норм, связанных с безопасностью личной

информации, имеет решающее значение для их успеха. Однако правоприменение может быть сложным, особенно в случаях, когда организации, обрабатывающие персональные данные, расположены в разных юрисдикциях. «Неадекватное» правоприменение может привести к отсутствию подотчетности и повышенному риску утечки данных. Соблюдение правовых норм, связанных с безопасностью личной информации, может быть дорогостоящим, особенно для малого и среднего бизнеса. У этих организаций может не хватить ресурсов для инвестирования в надежные системы управления данными и процессы, необходимые для соблюдения требований законодательства [12].

Для развития института информационной безопасности личности необходимо исходить из принципа баланса интересов, поиска эффективных механизмов защиты прав и свобод личности в информационной сфере. «Так как в сферу информационной безопасности личности входят также иные информационные права, такие как право на информацию, необходимо разрабатывать внетехнические меры обеспечения информационной безопасности личности. Так, при реализации права на информацию, граждане сталкиваются не только с угрозой недостаточной доступности информации, но и с проблемой качественного характера такой информации, отвечающей критериям безопасности, достоверности и т. д. Поэтому регулирование в данной сфере должно учитывать социальные реалии, национальные и культурные традиции, а также отвечать целям защиты личности от существующих информационных угроз» [13].

В заключение следует отметить, что перспективы правового регулирования безопасности персональной информации многообещающие. Преимущества такого регулирования включают защиту персональных данных, повышение доверия потребителей, усовершенствованные методы управления данными и глобальную гармонизацию. Однако существуют также проблемы, связанные с правовым регулированием, включая обеспечение баланса между безопасностью и конфиденциальностью, соответствие технологическим изменениям, правоприменение и затраты на соблюдение требований. Решение этих проблем потребует совместных усилий правительств, регулирующих органов и организаций, которые обрабатывают персональные данные. Работая сообща, мы можем гарантировать защиту персональных данных и соблюдение прав отдельных лиц на неприкосновенность частной жизни.

Можно также сделать вывод о том, что толкование информационной безопасности личности как состояние защищенности от внешних и внутренних угроз в текущих нормативных источниках неоднородно и поэтому используется преимущественно в технической сфере. Очевидно, что информационная безопасность личности предполагает также наличие определенной свободы личности в информационной среде, в том числе свободы на реализацию конституционных и информационных прав, однако обеспечение такой свободы должно гарантироваться правовыми и социальными методами.

По итогу, правовое регулирование безопасности личной информации имеет решающее значение для защиты персональных данных и поддержания доверия клиентов. Однако существует ряд проблем, связанных с правовым регулированием, включая отсутствие международной согласованности, сложность правовых рамок, неадекватное правоприменение и быстро меняющийся технологический ландшафт. Для решения этих проблем организации могут работать над внедрением лучших мировых практик, упрощением правовой базы, усилением правоприменения и адаптацией к технологическим изменениям. Поступая таким образом, организации могут защитить персональные данные и обеспечить соблюдение требований законодательства.

Поступила: 03.09.24; рецензирована: 17.06.24;
принята: 19.06.24.

Литература

1. *Марков А.С.* Руководящие указания по кибербезопасности в контексте / А.С. Марков, В.Л. Цирлов // Вопросы кибербезопасности. 2014. № 1 (2). URL: https://ru.scribd.com/document/456568043/rukovodyaschie-ukazaniya-po-kiberbezopasnosti-v-kontekste-iso-27032-pdf (дата обращения: 01.03.2023).

2. Конвенция о преступности в сфере компьютерной информации (ETS № 185). Заключена в г. Будапеште 23.11.2001 г. Документ опубликован не был.
3. Конвенция о защите физических лиц при автоматизированной обработке персональных данных. Заключена в г. Страсбурге 28.01.1981 г. // Бюллетень международных договоров. 2014. № 4.
4. Конвенция об обеспечении международной информационной безопасности (концепция). URL: http://www.mid.ru/en/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/191666?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=ru_RU (дата обращения: 20.02.2024).
5. *Tzanou M.* Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right / M. Tzanou // International Data Privacy Law. 2013. Vol. 3. № 2.
6. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union // OJ L 194, 19.7.2016. P. 1–30.
7. Cybersecurity Act. URL: https://www.csa.gov.sg/legislation/cybersecurity-act (дата обращения: 20.02.2024).
8. Ministry of Public Security of the People's Republic of China published the Draft Regulations on the Classifi ed Protection of Cybersecurity. URL: https://www.huntonprivacyblog.com/2018/07/17/china-publishes-draft-regulations-classified-protection-cybersecurity (дата обращения: 20.02.2024).
9. Slovenian National Cyber Security Strategy. URL: https://www.enisa.europa. eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-securitystrategy-in-slovenia (дата обращения: 20.02.2024).
10. Конвенция об обеспечении международной информационной безопасности (концепция). URL: http://www.mid.ru/en/foreign_policy/official_documents//asset_publisher/CptICkB6BZ29/content/id/191666?p_p_id=101_INSTANCE_CptICkB6BZ29&_101_INSTANCE_CptICkB6BZ29_languageId=ru_RU (дата обращения: 25.02.2024).
11. *Худойкина Т.В.* Информационные аспекты систематизации законодательства в сфере социальной защиты населения / Т.В. Худойкина, Н.А. Толкунова // Информационное право. 2010. № 3. URL: http://www.unn.ru/pages/disser/901.pdf (дата обращения: 03.03.2024).
12. *Журавлев М.С.* Правовое обеспечение электронного документооборота в телемедицине / М.С. Журавлев // Информационное право. 2017. № 4. URL: https://publications.hse.ru/articles/211102387 (дата обращения: 03.03.2024).
13. Отдельные аспекты правового регулирования информационной безопасности личности. URL: https://cyberleninka.ru/article/n/otdelnye-aspekty-pravovogo-regulirovaniya-informatsionnoy-bezopasnosti-lichnosti (дата обращения: 03.03.2024).