DOI: 10.17805/trudy.2023.5.10 *ЮРИСПРУДЕНЦИЯ*

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОСТИ И БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

А.М. Поваляев
Московский гуманитарный университет

Аннотация: *В статье проведен анализ возможностей государственного регулирования приватности и обеспечения безопасности персональных данных в интернете. Что следует сделать, чтобы защитить приватность в интернете.*

Ключевые слова: *защита конфиденциальности; приватность в интернете; кибербезопасность*

LEGAL REGULATION OF THE PROTECTION OF PRIVACY AND SECURITY ON THE INTERNET

A.M. Povalyaev
Moscow University for the Humanities

Abstract: *The article analyzes the possibilities of state regulation of privacy and ensuring the security of personal data on the Internet. What should be done to protect privacy on the internet?*

Keywords: *privacy protection; Internet privacy; cybersecurity*

Конфиденциальность индивидов в интернете зависит от способности контролировать объем предоставляемых личных сведений и доступ разных лиц к этим сведениям. Выполняя повседневные операции в интернете, можно непреднамеренно раскрыть личные сведения, которые злоумышленники могут использовать в противоправных целях. К таким сведениям относится конфиденциальная информация, в частности, IP-адрес, адрес эл. почты, текущее физическое расположение, домашний или рабочий адрес пользователя. Так, для совершения транзакций в интернет-магазинах часто требуются сведения о кредитной карте и ваш домашний адрес.

Интернет является сравнительно новым пространством, где возникают, изменяются и прекращаются общественные отношения. Он продолжает стремительно развиваться, в связи с чем имеют место ситуации, при которых законодатель не успевает своевременно реагировать на новые явления в цифровом пространстве.

Конституция Российской Федерации гарантирует гражданину право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (далее – Закон об информации)

является ядром нормативно-правового регулирования информационных отношений в России, определяя ключевые для данной сферы термины. Так, согласно п.1 ст.2 названного закона, информация – это любые данные, сведения и сообщения, представляемые в любой форме. Также в данном акте приведены определения понятий «сайт», «электронное сообщение» и «поисковая система». Соответственно, при составлении документов по информационной безопасности, необходимо руководствоваться в первую очередь Законом об информации.

Данный закон проясняет, какая информация считается конфиденциальной, а какая – общедоступной, когда и каким образом доступ к информации может быть ограничен; описывает процесс обмена данными. Также нормы Закона об информации содержат основные требования к защите информации и определяют ответственность за нарушения в рассматриваемой сфере правового регулирования.

На наш взгляд необходимо отметить ключевые аспекты информационной безопасности, предусмотренной в Законе об информации:

1. Закон запрещает собирать и распространять информацию о жизни человека без его согласия.

2. Все информационные технологии равнозначны – нельзя обязать компанию использовать какие-то конкретные технологии для создания информационной системы.

3. Запрещает ограничивать доступ к некоторым видам информации, например, сведения о состоянии окружающей среды.

4. Запрещает распространять информацию, например, ту, которая пропагандирует насилие или нетерпимость.

5. Лицо, которое хранит информацию, обязан ее защищать, например, предотвращать доступ к ней третьих лиц.

6. Государство ведет реестр запрещенных сайтов. Роскомнадзор может вносить туда сайты, на которых хранится информация, запрещенная к распространению на территории РФ.

7. Владелец заблокированного сайта может удалить незаконную информацию и сообщить об этом в Роскомнадзор – в таком случае его сайт разблокируют.

Также стоить упомянуть ФЗ-152 «О персональных данных».

Этот закон регулирует работу с персональными данными – личными данными конкретных людей. Его обязаны соблюдать те, кто собирает и хранит эти данные. Например, компании, которые ведут базу клиентов или сотрудников.

Одной их наиболее актуальных проблем в области обеспечения кибербезопасности можно отнести торговлю базами данных в интернете: их беспрепятственно можно найти в поисковиках, соцсетях и мессенджерах. Поисковые системы выдают результаты по множеству сайтов, где продаются сведения о людях, которые обладают достаточно большим капиталом, пенсионерах, мигрантах, должниках, автовладельцах и так далее в зависимости от целей злоумышленников (Персональные сданные…, Электр. ресурс).

Подобные базы данных (формат MS Excel) по всем регионам России содер-

жат: ФИО, пол, телефон, полные паспортные данные (серия, номер, кем и когда выдан), СНИЛС, адрес регистрации и проживания, иные персональные документы и данные в финансово-кредитным учреждениям граждан Российской Федерации,

Зачастую базы данных продаются сотрудниками банков, сервисов доставки и иных цифровых площадок нелегально, однако, привлечь к уголовной ответственности удается лишь единицы от общего процента таких сотрудников. Как показывает судебная практика, правонарушители получают либо штраф, либо условный срок (Как наказывают… Электр. ресурс).

По мнению автора, необходимо усилить контроль и наказание за продажу и обнародование персональных личных данных сотрудниками банка, других организаций и цифровых сервисов.

Также не стоит забывать, что существуют различные боты в мессенджере «Телеграм», которые позволяют найти все данные человека за определенную плату: все социальные сети, объявления, которые были зарегистрированы на определенный номер телефона. Роскомнадзор заявил, что добился в суде запрета Telegram-бота «Глаз бога». Деятельность этого ресурса нарушает «права граждан на неприкосновенность частной жизни, личную и семейную тайну», а конкретно статью 23 Конституции Российской Федерации. Также информация, распространяемая «Глазом Бога», признана «обрабатываемой с нарушением законодательства России в области персональных данных». В свою очередь, основатель «Глаза бога» сообщил, что решение касается не созданного им продукта, а его копии. Следовательно, необходимо запретить любые аналоги таких Telegram-ботов.

В некоторых социальных сетях запрещено указывать не настоящие ФИО, необходимо сделать это правом человека, а доступ к настоящим ФИО должен находится у администраторов социальной сети.

Необходимо ввести контроль за бесплатным интернетом в общественных местах. Бесплатный интернет предоставляется во многих кафе, гостиницах и других общественных местах. Если в открытой сети используется простая аутентификация, к ней легко подключиться. Однако так же легко человек может стать жертвой киберпреступника. Не стоит использовать общественный Wi-Fi для оплаты покупок и перевода средств или обмена конфиденциальными данными.

По мнению руководителя направления «Разрешение IT & IP споров» юрфимы «Рустам Курмаев и партнеры» Ярослава Шицле, на данный момент охране персональных данных не уделяется так много внимания, как этого требуется для защиты общественных интересов. Очевидно, что для решения проблемы нужно одновременно усилить контроль за расследованием подобного рода преступлений и применять системный подход к выявлению утечек и реализации персональных данных.

Если учитывать, что в большинстве случаев информация уходит через работников, то особое внимание нужно уделить работе с персоналом. Можно выделить несколько методов профилактики в данной сфере.

Необходимо проводить аудиты бизнес-процессов, в которых используются персональные данные клиентов. Например, программ лояльности. С помощью внутренних и внешних аудитов, то есть периодических обзоров всех процессов приватности, в компании или у ИП легче выявить риски утечек данных и риски несоблюдения законодательства (Как сливают данные…, Электр. ресурс).

Обеспечение приватности – не одноразовая мера. Необходимо не только внедрить все предусмотренные законом документы, необходимо работать и отслеживать нарушения в данной сфере.

Если во время аудита выяснится, что данные клиентов передаются третьим лицам – контрагентам – без соглашения о защите данных или без положений в договоре о соблюдении конфиденциальности, то оператор данных незаконно разглашает персональные данные.

Если у фирмы много клиентов – физических лиц, она обрабатывает их данные и совершает массовые рассылки, то необходимо инспектировать работников на предмет того, как они работают с персональными данными. Для этой цели видится целесообразным составить опросник и попросить работников, которые имеют доступ в информационные системы, заполнять его каждые два-три месяца.

В опроснике должны быть вопросы, которые позволяют выяснить, в какой сфере необходимо усилить контроль чтобы предотвратить утечку данных.

Если есть подозрения, что произошла утечка корпоративных паролей или персональных данных, то клиентам необходимо разослать уведомление о том, что конфиденциальность их данных, возможно, была нарушена.

В соответствии со статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», субъект персональных данных имеет право получать информацию, которая касается обработки его данных. Раз есть право субъекта, значит, есть и обязанность оператора передавать такие данные.

В заключение можно отметить, что наше государство предпринимает попытки регулировать вопрос приватности, но из-за быстрого развития интернета это нередко происходит с опозданием. Так же можно заключить, что для полного соблюдением приватности необходимо провести большую работу в сфере кибербезопасности и принятие новых законопроектов, которые помогут сражу же пресекать любые действия, направленные на продажу и получение личных данных.

СПИСОК ЛИТЕРАТУРЫ

Как наказывают за незаконную торговлю персональными данными? // habr.com [Электронный ресурс] URL: https://habr.com/ru/post/442506/ (дата обращения: 23.11.2022)

Как сливают данные компаний. Исследование // secretmag.ru [Электронный ресурс] URL: https://secretmag.ru/practice/informacionnaya-bezopasnost-prevyshe-vsego-kak-slivayut-dannye-kompanii.htm (дата обращения: 23.11.2022)

Персональные сданные: как будут отслеживать продавцов незаконных баз //

Известия. iz.ru [Электронный ресурс] URL: https://iz.ru/1262783/valerii-kodachigov/personalnye-sdannye-kak-budut-otslezhivat-prodavtcov-nezakonnykh-baz (дата обращения: 23.11.2022)

Поваляев Андрей Михайлович – студент юридического факультета Московского гуманитарного университета. Научный руководитель: Рогова А.А. – доцент кафедры государственно-правовых дисциплин Московского гуманитарного университета. Адрес: 111395, Россия, г. Москва, ул. Юности, д. 5. Тел.: +7 (917) 519-13-33. Эл. адрес: andreiaistrup@icloud.com

Povalyaev Andrey Mikhailovich is a student of the Faculty of Law of the Moscow University for the Humanities. Scientific supervisor: Rogova A.A. – Associate Professor of the Department of State and Legal Disciplines of the Moscow University of the Humanities. Address: 5 Yunosti str., Moscow, 111395, Russia. Tel.: +7 (917) 519-13-33. Email: andreiaistrup@icloud.com

Для цитирования:

Поваляев А.М. Правовое регулирование защиты конфиденциальности и безопасности в интернете. 2023. № 5. С. 49–53. DOI: https://www.doi.org/10.17805/trudy.2023.5.10