ЗАЩИТА ЛИЧНЫХ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ В СЕТИ «ИНТЕРНЕТ»

Бояхчян Д.В.

Научный руководитель: Инюшкин А.А.

Россия, г. Самара,
Самарский национальный исследовательский университет
имени академика С.П. Королева

Аннотация. *В данной статье рассматриваются вопросы защиты личных данных пользователей сети «Интернет». Личные данные – это информация, относящаяся к определенному субъекту, то есть его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, др. информация.*

Ключевые слова: *сеть; изображение; данные; личной; гражданин; интернет; использование.*

С развитием информационных технологий доступ в глобальную сеть «Интернет» стал доступен почти каждому человеку по всему миру, он дал доступ к миллионам книг по всему земному шару, к большому количеству информации, дает возможность развиваться в любой сфере жизнедеятельности: учеба, работа и развлечения, которые уже давно совмещены в черном экране монитора, планшета или смартфона. Мы получили возможность осуществлять коммуникацию с человеком независимо от его местонахождения, не выходя из дома. Однако за терабайтами информации скрывается не очень приятная сторона интернета, а именно тысячи слитых баз данных, содержащих в себе личные фотографии пользователей, паспортные данные, и иные, которые делают уязвимыми каждого из нас.

Рассматривая вопрос безопасности своих личных данных, необходимо убедится на конкретном примере, обратим внимание на такую социальную сеть, как «Facebook». Впервые вопрос о безопасности данной социальной сети в 2011 году поднял Джулиан Ассанж, основатель «WikiLeaks», который рассказал о продаже личных данных пользователей со стороны администраторов и основателей данной социальной сети, которые продавали заинтересованным лицам полную базу данных о людях, их отношениях друг с другом, их именах, адресах проживания, их личных связях.

Сущность защиты паспортных и иных данных в сети «Интернет». Переходя непосредственно к личным данным, а именно к паспорту, который, согласно указу Президента от 13.03.1997 г. N 232 «Об основном документе, удостоверяющем личность гражданина Российской Федерации на территории Российской Федерации», является удостоверением личности гражданина Российской Федерации. Фотографии паспортов, которые мы оставляем в сети «Интернет», могут легко попасть на специализированные площадки по продаже лич-

ных данных пользователей, цены на которые варьируется от 30 до 10 000 рублей, в зависимости от данных, которые продаются (фотография паспорта/гражданина на фоне с паспортом).

Как же попадают эти данные в «Интернет»? Например, желая завести аккаунт в каршеринге, чтобы пользоваться услугами, вы проходите стандартную верификацию своего профиля и идентификацию личности, для этого вам необходимо прислать фотографию паспорта в руках. Все эти документы попадают в базу данных каршеринговой компании, которую через какое-то время злоумышленникам удается частично взломать, происходит утечка данных, и все эти данные постепенно распространяются по глобальной сети.

Злоумышленники используют эти данные в различных целях, например, для мошеннических операций на торговых площадках, создания виртуальной банковской карты с реквизитами, для создания которой требуется всего лишь фотография паспорта, никакой проверки через камеру, и посещение какой-либо физической точки.

Большинство интернет-неприятностей случается именно с продвинутыми пользователями, причем по чистой случайности, лишь однажды утратившими бдительность. А ведь так немного их, этих простых правил, соблюдение которых если не полностью защитит от всех интернет-угроз, то существенно снизит вероятность их возникновения [2; с. 3].

В связи с развитием интернет-технологий все сервисы перешли на цифровой режим работы, и полностью отказаться от их использования не получится, поэтому нужно обращать внимание на важные моменты.

Первое, на что нужно обратить внимание, это на то, где мы оставляем свои личные данные. Необходимо понимать, на каких ресурсах их можно оставлять, а на каких не нужно, если это крупная социальная сеть/сервис, которые не были замечены в сливах данных своих пользователей, которые вы давно знаете и активно пользуетесь, которые используют защищенный протокол передачи данных HTTPS.

Второй момент, это минимизация количества личной информации на ресурсах, чем меньше мы оставляем на них своих данных, тем меньше вероятности использования этой информации против нас в дальнейшем, в случае кибератак на ресурс.

В-третьих, необходимо ставить сложные пароли на всех аккаунтах с использованием различных символов, включать двойную аутентификацию с использованием смс подтверждения для входа в аккаунт.

Большей опасности в данной сфере подвержены несовершеннолетние лица, которые в силу своего возраста, неопытности, отсутствия навыков пользования в глобальной сети «Интернет», не осознают опасности своих действий. Злоумышленники, имея данные этой категории лиц, осуществляют психологические манипуляции, шантаж, что очень сильно влияет на их психическую составляющую.

С целью защиты этой категории лиц необходимо отметить ряд моментов:

- необходим контроль за их действиями со стороны близких лиц и родителей;

- установление ряда программного обеспечения с целью ограничения определенной категории веб-сайтов для посещения, ограничить время пребывания в глобальной сети;

- постоянная коммуникация, общение на тему безопасности в сети «Интернет».

Одним из важных моментов является размещение своих фотографий в глобальной сети. Поскольку, с точки зрения систематики Гражданского кодекса Российской Федерации, изображение рассматривается как неимущественное благо, указаний относительно оборота права на него Кодекс, разумеется, не содержит. Статья 152.1 ГК РФ, как известно, подчиняет возможность обнародования и использования изображения принципу согласия и содержит три исключения из него:

1) использование изображения в государственных, общественных или иных публичных интересах;

2) съемка в местах, открытых для свободного посещения, или на публичных мероприятиях, если изображение не является основным объектом использования;

3) гражданин позировал за плату [3].

Публикуя простые изображения в социальной сети или отправляя друзьям в личные сообщения, мы не задумываемся о том, что, если данные изображения попадут в руки злоумышленников, безобидное изображение с вашим лицом может быть использоно против вас самих. Что же может быть, если ваше изображение попало в руки злоумышленников?

Неизвестные вам ранее лица будут знать, какие места вы посещаете, где обычно бываете, во сколько приходите домой, во сколько уходите, эта информация активно продается на специализированных площадках и пользуется таким же спросом, как и личные данные (паспортные, иные). Эти данные подвергают большой опасности тех, кто их публикует, в дальнейшем эти фотографии будут использованы в целях шантажа, кибербуллинга, и будут информацией, которая учитывается при расследовании реальных преступлений.

Полностью отказаться от размещения своих изображений в условиях развития информационных технологий не получится, так как все общение, деловая коммуникация, ушли именно в сеть «Интернет», но необходимо соблюдать ряд простых правил конфиденциальности:

1) использовать режимы закрытых аккаунтов в социальных сетях;

2) добавлять в круг лиц, которые будут иметь доступ к вашим фотографиям лишь тех, кого вы знаете и с кем вы поддерживаете коммуникацию;

3) не использовать систему геолокации, и не прикреплять данные к своим изображениям.

Переходя к спорным вопросам по праву распоряжения чужим изображением, можно сказать, что больше вопросов вызывает исключение «гражданин позировал за плату». Неясно, как разграничивать его с возмездно данным согласием, что можно продемонстрировать на реальных примерах из судебной практики.

К примеру, в одном из дел Санкт-Петербургский городской суд пришел к выводу, что согласие гражданина содержится в трудовом договоре (точнее, в должностной инструкции, к которой тот отсылал), но в конце добавил, что «судебная коллегия считает возможным также согласиться с выводом суда первой инстанции о том, что фактически Л. позировал за плату» (очевидно, имелась в виду заработная плата истца) [1].

Но в чем тогда смысл проверять содержание договора и инструкции на предмет наличия или отсутствия согласия, если в конце определения указано, что согласия не требуется вообще? Если «гражданин позировал за плату» и возмездное согласие – это одно и то же, то в таком случае исключение избыточно.

Во многих научно-исследовательских работах обращалось внимание на данный вопрос. Как в широком смысле понимать понятие «позировал», и касается ли оно тех моментов, когда гражданин не позировал, а лишь за плату разрешил использование ранее сделанного изображения [4].

В.А. Микрюков считает, если согласие было сделано на возмездной основе (в случаях, когда гражданин именно позировал), то это подпадает под исключение о позировании за плату. Поэтому, согласно подп. 3 п. 1 ст. 152.1 ГК РФ согласие вовсе не нужно, а это говорит о том, что отозвать ранее данное согласие даже при условии возмещения убытков (п. 49 Постановления Пленума ВС РФ от 23 июня 2015 г. N 25) невозможно [5].

Такой отзыв не будет иметь юридических последствий, потому что, опираясь на подп. 3 п. 1 ст. 152.1, обладатель исключительных прав сможет продолжать использовать, допустим, фотоснимок вне зависимости от мнения изображенного на нем лица.

Таким образом, развитие информационных технологий дало большой толчок обществу, но необходимо развивать не только возможности доступа к глобальной сети «Интернет», но и, самое главное, способы защиты своих личных данных, своих изображений, так как именно эти направления являются ведущими в сфере информационной безопасности.

Библиографический список

1. Апелляционное определение Санкт-Петербургского городского суда от 21 января 2016 г. N 33726/2016 по делу N 2-2141/2015 // СПС «КонсультантПлюс».

2. Библиотечка «Российской газеты». М.: Издательство «Российская газета». 2017. №2. А.Н. Тарасенкова. Интернет: правовые аспекты безопасного использования. 161 с. [Электронный ресурс]. URL: https://lib.rucont.ru/efd/552035 (дата обращения 01.11.2020).

3. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 г. N 51-ФЗ (ред. от 31.07.2020) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_5142/14c6c3902cffa17ab26d330b2fd4fae28e5cd059/ (дата обращения: 19.11.2020).

4. Беляева К.К. Распоряжение правом на изображение в Российской Федерации // Вестник гражданского права. 2019. Т.19. №2. С. 27-60.

5. Микрюков В.А. О возможности отмены согласия гражданина на использование его изображения // Юрист. 2013. № 13. С. 36-39.

PROTECTING YOUR PERSONAL DATA ON THE INTERNET

Boyakhchyan D.V.

Scientific adviser: Inyushkin A.A.

Samara National Research University, Samara, Russia

Abstract. *This article discusses the protection of personal data of Internet users. Personal data is information related to a specific subject, that is, his last name, first name, patronymic, year, month, date and place of birth, address, family, social, property status, education, profession, income, etc. information.*

Keywords: *network; picture; data; personal; citizen; the Internet; using.*