

Защита персональных данных в сегменте интернета Darknet.

Научный руководитель – Новикова Рамиля Галимовна

Борисова Екатерина Дмитриевна

Студент (бакалавр)

Академия труда и социальных отношений, Москва, Россия

E-mail: Katerina16.01.01@icloud.com

В последнее время особого внимания не только юристов, но и специалистов широкого профиля заслуживают вопросы правового регулирования защиты персональных данных в интернет-пространстве, которое на современном этапе представлено не только в легализованном виде, но и имеется «теневой» вариант интернет-пространства или же Darknet, в частности, отсутствует законодательное закрепление мер защиты персональных данных, которые возможно окажутся выведенными в Darknet. Стоит признать тот факт, что продажа личной информации в Darknet стала обыденным явлением, к примеру, невозможно установить источник откуда фейк-компании берут номера телефонов с полными данными граждан.

Вся наша личная информация хранится, как минимум, в десятке разных организаций, начиная с базы "Госуслуг" и заканчивая компанией, доставляющей пиццу.

Украсть личные данные человека сейчас может не только сотрудник, имеющий доступ в рамках служебных полномочий, но и любой желающий — нужны лишь деньги и интернет.

Персональные данные - это любая информация, относящаяся к определенному физическому лицу, в частности, это может быть имя, фамилия, место работы, семейное положение, номер телефона и многое другое.

Длительное время общественные отношения в сфере безопасности личных данных были урегулированы Федеральным законом "О персональных данных" от 27.07.2006 N 152-ФЗ, однако, 23 декабря 2020 г. Госдума РФ приняла законопроект о внесении изменений в вышеназванный нормативный и правовой акт. Причем, указанный законопроект прошел слушания в двух чтениях за два дня, и уже 30 декабря 2020 г. Федеральный закон № 519-ФЗ "О внесении изменений в Федеральный закон "О персональных данных" уже был подписан Президентом РФ. Правовая реализация норм данного ФЗ осуществляется в два этапа: основная часть с 1 марта 2021г., вторая — с 1 июля 2021 г. Стоит обратить особое внимание на то, что в законодательных изменениях нет ни одного упоминания про Darknet, хотя большинство незаконных продаж личных данных происходит именно в этом сегменте интернета. В свою очередь, согласно сайту международной компании, работающей в сфере информационной безопасности, а именно АО «Лаборатория Касперского», Darknet «это скрытая группа веб-сайтов, доступная только через специализированные браузеры» [3], которые устанавливаются только между доверенными пользователями darknet, воспринимаемых в качестве «друзей». Даркнет отличается от зарегистрированного интернет-пространства тем, что https://ru.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB%D0%BE%D0%BE%D0%B1%D0%BC%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C происходит анонимно, т.к. <https://ru.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81> публично недоступны, и, следовательно, пользователи могут общаться без особых опасений и <https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%86%D0%B5%D0%BD%D0%B7%D1%83%D1%80%D0%B0>.

В Российской Федерации нет ни одного закона, где бы упоминался термин «Darknet», хотя в этом и есть одна из глобальных проблем утечки персональных данных граждан страны и не представляется возможным бороться с проблемой посредством устранения ее результатов.

Существует несколько способов борьбы с Darknet, в частности, самыми действенными являются:

- ужесточение наказания; • объединение усилий правоохранительных органов разных стран. Причем, особая эффективность достигается при их совокупности.

Статья 137 УК РФ устанавливает уголовную ответственность за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, в частности, мера ответственности в виде штрафа до 200 тыс. руб., либо обязательные работы на срок до 360 часов, либо исправительные работы на срок до одного года, либо принудительные работы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет или без такового), либо арест на срок до четырех месяцев, либо лишение свободы на срок до двух лет (с лишением права занимать определенные должности на срок до трех лет). Не смотря на данные меры ответственности это не является препятствием для преступников работающих в Darknet, так как на платформе они зарабатывают в разы больше.[2]

Стоит заметить, что полный список услуг, предоставляемых Darknet не имеет каких-либо границ, в особенности правовых, однако успешные операции по поимке преступников и уничтожению материалов существуют, хоть и в не так много. Министерством юстиции США 16 октября 2019 года был опубликован обзор [4] о закрытии правоохранительными органами США, Германии, Великобритании и Южной Кореи крупнейшего в мире Darknet-рынка детской порнографии. С марта 2018 года в ходе международной операции удалось задержать 337 пользователей сайта из Великобритании, США, Саудовской Аравии, Германии, Бразилии и ОАЭ. Транзакции для оплаты доступа к сайту оплачивался посредством криптовалюты Bitcoin. При содействии налоговой службы США, транзакции были отслежены. Данная новость показывает, что объединив усилия правоохранительных органов стран с преступностью в Darknet можно бороться и бороться успешно.

Источники и литература

- 1) Дейнеко А.Г. Цифровые права в Гражданском кодексе: ближайшие последствия и отдаленные перспективы // Труды Института государства и права РАН. 2020. № 15 (2). С.175-198.
- 2) "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 24.02.2021), УК РФ Статья 137. Нарушение неприкосновенности частной жизни
- 3) Что такое глубокий и теневой интернет?: <https://www.kaspersky.ru/resource-center/threats/deep-web>
- 4) Правоохранители США закрыли крупнейший даркнет-рынок: <https://news.myseldon.com/ru/news/index/217671672>