ПроДанные

28.01.2020 СТАТЬИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

Пролог

Пока ФРИИ мечтает подарить гражданам возможность продавать «деперсонализированные» данные большим корпорациям, а ФАС рассчитывает получить полную государственную монополию на персональные данные, кажется, все уже продано...

Рынок украденных данных

Новости об утечках данных в последнее время стали такой же неотъемлемой частью информационного пейзажа, как рассказы о запусках баллистических ракет. Причем масштабность происшествий только растет. В части случаев огласка инцидентов даже стала элементом конкурентной борьбы.

Как утверждают профессионалы, если по примеру Данте спуститься в ад (то есть в даркнет), можно по бросовым ценам купить данные клиентов банков, сотовых операторов, ритейлеров и любых иных «ловцов цифровых душ», включая бюро кредитных историй. Причем цены на данные за год только росли: по абоненту сотовой сети — на 25 %, по клиенту банка — на 50 %. Приходится признать, что для платежеспособного спроса нет банковской, врачебной тайны, нет тайны переписки. И ответное предложение формируется галопирующими темпами. Сложилась целая экосистема похитителей, посредников, покупателей, где сбыт идет по каналам любых уровней.

Круговорот данных в упомянутой экосистеме совершается настолько быстро, что сотовые операторы, порой допускающие утечку (и нередко торгующие базами в маркетинговых целях самостоятельно), бодро рекомендуют своим клиентам купить у них услугу блокирования спам-звонков. Цифровой профиль человека становится товаром на черном рынке, а сам он — источником дополнительного дохода на официальном.

Риски и предпосылки утечек информации

В результате утечек персональных данных страдают и компании, и люди. Однако ключевые риски возникают именно у последних, поскольку с выходом информации за периметр для оператора история завершается, а для человека — только начинается. Даже если компания отрапортует о раскрытии преступления в «считанные часы» (Сбербанк), или патетично извинится за «случайное» раскрытие (Твиттер), это никак не отразится на дальнейшей судьбе данных, уже ушедших к получателю. Теперь упомянутые «считанные часы» останутся

у потенциальной жертвы до начала атаки. На базе полученных сведений социальная инженерия будет применена мошенниками во всех возможных вариациях: от попытки что-то продать до попытки просто украсть деньги.

На первый взгляд, при современном уровне хакерского искусства нет неприступных бастионов.

Однако практика показывает, что самые распространенные утечки — дело лиц, имеющих прямой доступ к информации и остро желающих его монетизировать (см. Табл. 1).

Как обстоят дела с превенцией («у них», «у нас»)

Универсального способа решения проблемы нет. Не в последнюю очередь потому, что нет прямой заинтересованности у игроков рынка персональных данных. Они максимизируют прибыль и минимизируют репутационные потери. Не приходит на помощь и государство, занимающееся проблемой очень избирательно.

Как известно, в современном обществе для законопослушного поведения нет стимула лучше, чем существенность и неотвратимость наказания. Если сравнивать подход законодателей и правоприменителей в разных странах, то стоит отметить более ответственное отношение к проблеме на Западе.

Так, согласно статье 83 Регламента (ЕС) 2016/679 (GDPR) Регламент (ЕС) 2016/679 Европейского Парламента и Совета «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46 / ЕС».), если речь идет об умышленном или неосторожном нарушении положений Регламента, могут применяться административные штрафы до 10 млн евро, а в случае с предприятием — до 2 % его общего годового оборота по всему миру (выбирается наибольшая сумма). Если же речь идет о несоблюдении распоряжения надзорного органа — административные штрафы вырастают до 20 млн евро, а в случае с предприятием — до 4 % его общего годового оборота во всем мире (выбирается наибольшая сумма). В статье 58

GDPR предусмотрен довольно широкий круг полномочий контролирующих органов, включая право глубоких проверок и раздачи указаний. С 20 июля 2018 года GDPR регулирует защиту персональных данных не только в ЕС, но и в странах, которые осуществили имплементацию его норм (Норвегия, Лихтенштейн, Исландия и прочие). На сегодняшний день наиболее выдающимися с точки зрения штрафных сумм примерами применения GDPR являются случаи British Airways (204 млн евро), Marriott International, Inc (110 390 200 евро) и Google Inc. (50 млн евро).

В США борьба с паразитированием на данных финансового характера ведется посредством Закона Грэма — Лича — Блили, согласно разделу 521 которого Федеральная комиссия по торговле (и другие официальные лица) вправе инициировать уголовное преследование, в результате которого могут налагаться уголовные штрафы до 200 тыс. долларов США (с возможностью тюремного заключения на срок до 5 или до 10 лет). Причем проблема считается настолько серьезной, что введена особая процедура ежегодных докладов Конгрессу — в соответствии с положением об отчетности в разделе 526 (b) Закона. В рамках этой процедуры Федеральная торговая комиссия и Прокурор докладывают обо всех случившихся за год эпизодах, о характере нарушений и примененных мерах воздействия, включая такие мелкие случаи, как рассылка спама с санкцией в 3500 долларов США. ФБР также принимает активное участие в раскрытии данных дел.

В России на сегодняшний день существуют следующие виды ответственности за утечки данных.

Административная ответственность

В данном разделе будет приведена часть наказаний, которые непосредственно касаются анализируемых случаев.
Согласно ч. ч. 6, 7 ст. 13.11 КоАП РФ невыполнение обязанности по соблюдению условий, обеспечивающих сохранность персональных данных, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование,

копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных — влечет наложение административного штрафа на граждан в размере от 700 до 2 000 рублей; на должностных лиц — от 4 000 до 10 000 рублей; на индивидуальных предпринимателей — от 10 000 до 20 000 рублей; на юридических лиц — от 25 000 до 50 000 рублей.
По данным Роскомнадзора, в 2018 году было составлено всего 30 административных протоколов (без указания конкретных сумм). Пока размер отдельных штрафов сопоставим со стоимостью нескольких чашек кофе, а количество случаев привлечения к ответственности — с количеством дней в ноябре, этот вид ответственности не будет способствовать более дисциплинированному подходу собирателей и хранителей информации к вопросу ее сохранности.

Уголовная ответственность

В соответствии со статьей 272 УК РФ неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, — наказывается «штрафом в размере до 200 000 рублей..., либо исправительными работами до 1 года, либо ограничением свободы до 2 лет, либо принудительными работами до 2 лет, либо лишением свободы на тот же срок. При крупном ущербе — штрафом от 100 000 до 300 000 рублей..., либо исправительными работами от 1 года до 2 лет, либо ограничением свободы до 4 лет, либо принудительными работами до 4 лет, либо лишением свободы на тот же срок». Группа лиц по предварительному сговору или организованная группа либо лицо, использующее служебное положение, наказываются «штрафом в размере до 500 000 рублей... с лишением права занимать определенные должности или заниматься определенной деятельностью до 3 лет, либо ограничением свободы до 4 лет, либо принудительными работами до 5 лет, либо лишением свободы на тот же срок». Если же деяния повлекли тяжкие последствия — они наказываются лишением свободы на срок до 7 лет.

Для того чтобы понять, насколько непримирима государственная система к преступлениям

данного рода, можно проанализировать статистику по статье 272 УК РФ за предыдущие два года (см. табл. 2).

Цифры довольно скромные при истинных масштабах преступлений подобного рода.

* Любые несовпадения в статье неслучайны и точно цитируются по данным АПИ.

Кроме того, анализ судебной практики показывает, что порой нужно очень настойчиво и методично заниматься ламповым хакерством, чтобы получить реальный срок (пример: Апелляционное постановление Свердловского областного суда от 18.12.2017 по делу № 22–9487/2017). Существует еще статья 137 УК РФ (незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия), ситуация с применением которой выглядит не лучше.
Потому угроза привлечения к уголовной ответственности на сегодняшний день не помогает предотвратить преступления.

Гражданско-правовая ответственность

Здесь можно найти только печально известную юристам статью 15 ГК РФ, а также статью 24 Закона о персональных данных (Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.) вместе со статьей 151 ГК РФ, по которой нашему правоприменению сложно гордиться размером присуждаемых сумм.

Этот вид ответственности также не гарантирует эквивалентной компенсации и общей превенции.

Дисциплинарная ответственность

Согласно подпункту «в» пункта 6 части 1 статьи 81 ТК РФ сотрудник может быть уволен за разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в

том числе — за разглашение персональных данных другого работника.

Как показывает практика, перспектива увольнения является менее пугающей, чем перспектива незаконного обогащения. И «волчьих» билетов по таким основаниям увольнения не существует, разве что «сарафанное радио» по службам безопасности. Потому и этот вид ответственности не дает эффекта общей превенции.

Вот, собственно, весь инструментарий, предназначенный для формирования добросовестного отношения граждан и организаций к вверенным им данным. Если для первых он хоть сколько-нибудь грозен, то для последних — «соломенная стена». И это положение необходимо исправлять, ведь впереди у все нас — сияющая биометрия в потенциально «свободном полете».

«Что делать?»

Как верно писал Брюс Шнайер (Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. — ISBN5–318–00193–9. — Спб. Издательский дом «Питер». — 2003.), «люди часто оказываются самым слабым звеном в системе мер безопасности, и именно они постоянно являются причиной неэффективности последних». Поэтому ключевым направлением совершенствования мер безопасности на локальном уровне является работа с людьми, включая формирование автоматизма в соблюдении правил информационной безопасности. Любой сотрудник, пойманный на хищении информации, должен в 100 % случаев привлекаться к ответственности с запретом на последующий доступ к данным. Обязателен максимальный отказ от сокрытия фактов утечек данных (репутационные риски не могут считаться превалирующими).

На государственном уровне стоит более системно заниматься частной и общей превенцией. Законодателем должен формироваться комплекс мер, позволяющих эффективно наказать, а главное — максимально восстановить нарушенные права жертвы информационной утечки. Стоило бы ввести ряд презумпций для упрощения доказывания убытков, а также

минимальные суммы возмещения — для ориентира судебному правоприменителю и снятия у него «суммовой скромности». Наказание компаний должно стать более ощутимым, чтобы дополнительно стимулировать уважительное отношение к чужим данным. И, безусловно, необходимо работать над повышением общественной значимости проблемы, без осознания которой любая борьба будет напоминать бой тощего Алонсо Кехана с известным строением, применяемым для помола зерна.

Диана Полетаева
советник управляющего партнера адвокатского бюро «Казаков и Партнеры»

СТАТЬИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ