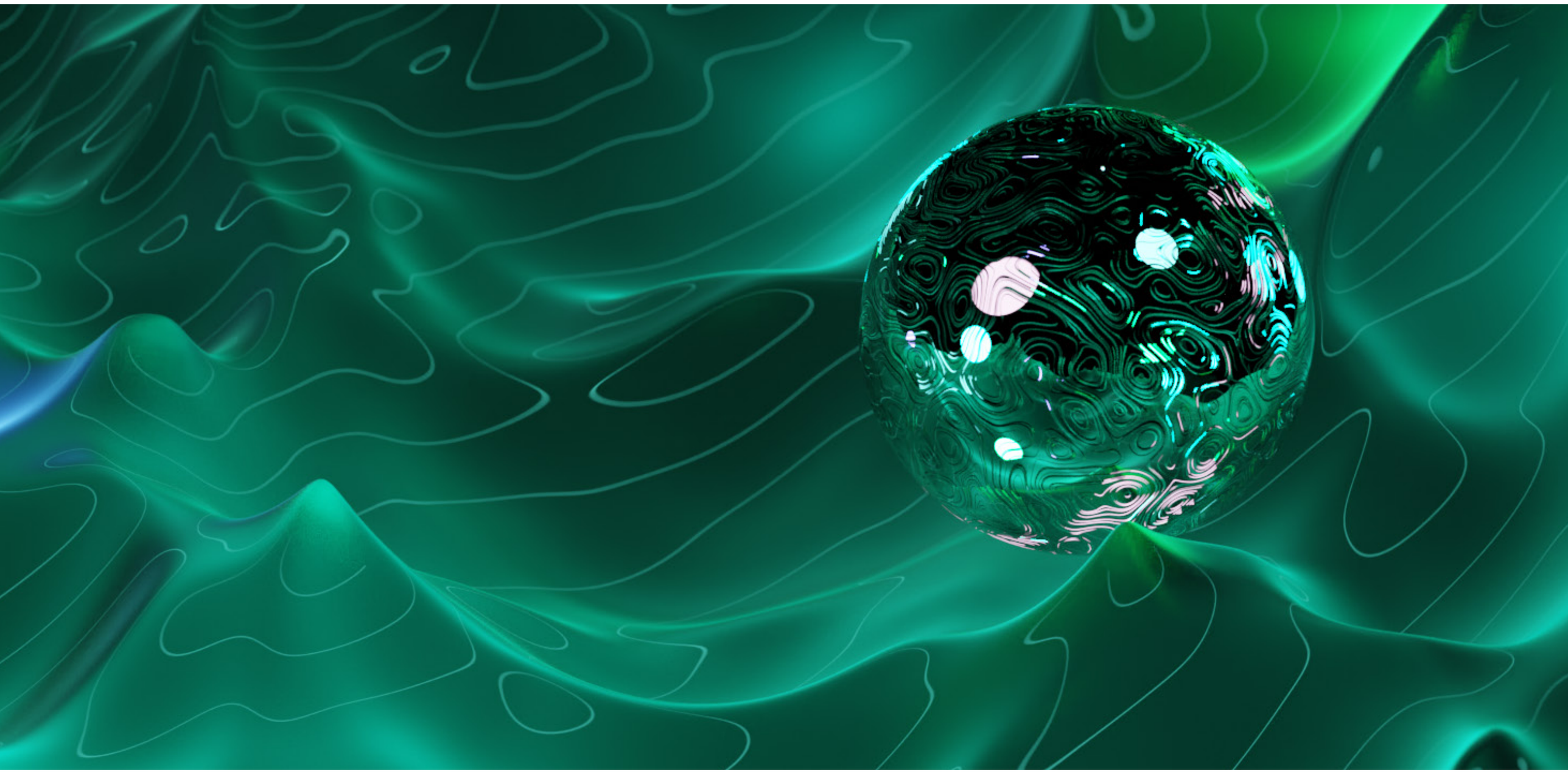
SCS SBER CYBER SECURITY

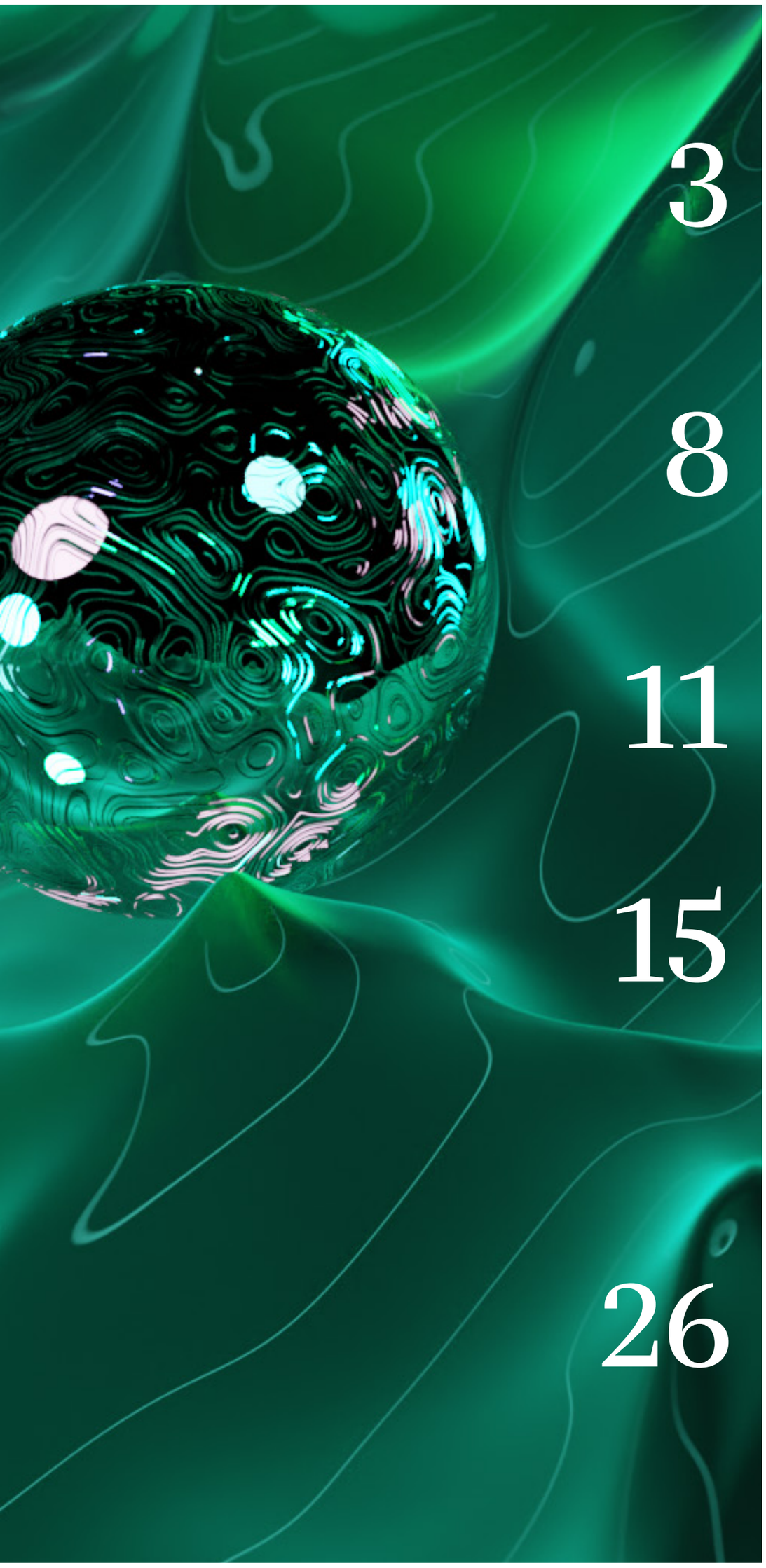
SBER PRIVACY JOURNAL

Журнал DPO о персональных данных и приватности



ВЫПУСК №2 | СЕНТЯБРЬ 2022

СОДЕРЖАНИЕ



Retrospectare[1]: как защищались персональные данные в Российской Империи и СССР?

В первом номере Sber Privacy Journal[2] мы рассказали об открытии концепции приватности (*англ. privacy*) в 1890 году известными американскими юристами Сэмюэлем Уорреном и Луисом Брандисом, которые определили приватность как право быть оставленным в покое или право быть предоставленным самому себе (*англ. the right to be let alone*), отмечая при этом всевозрастающую угрозу, исходящую со стороны новых изобретений и методов ведения бизнеса.

Сформированная в США концепция приватности оказала большое влияние на становление современной системы прав и свобод человека. В 1948 году на Генеральной Ассамблее ООН была утверждена Всеобщая декларация прав человека, провозгласившая, что никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, посягательству на неприкосновенность жилища, тайну его корреспонденции или на его честь и репутацию; а также право каждого человека на защиту от такого вмешательства и таких посягательств[3]. В 1950 году аналогичная норма была закреплена в Европейской конвенции о защите прав человека и основных свобод, согласно которой «каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции»[4]. И если Всеобщая декларация прав человека носила сугубо декларативный характер, то Европейская конвенция впервые на международном уровне закрепила юридически обязывающую норму по защите права человека на неприкосновенность его частной и семейной жизни. Благодаря данным документам право на неприкосновенность частной жизни получило признание в качестве неотъемлемого права каждого человека. А как же обстояло дело с приватностью в России? Постараемся ответить на этот вопрос.

В России концепция права на неприкосновенность частной жизни также имеет давнюю историю. До середины XIX века законодательство в той или иной степени охраняло жизнь человека, но предоставленные права собственности и иные блага, и интересы не обеспечивали необходимой защиты частной жизни человека и информации о ней. Начало защиты частной жизни в российском правовом поле было положено только во второй половине XIX века. При этом право на охрану частной жизни в России отличалось от концепции приватности, заложенной в США и Европе, предусматривая только отдельные элементы, направленные на защиту личных данных от разглашения «непосвященным» лицам.

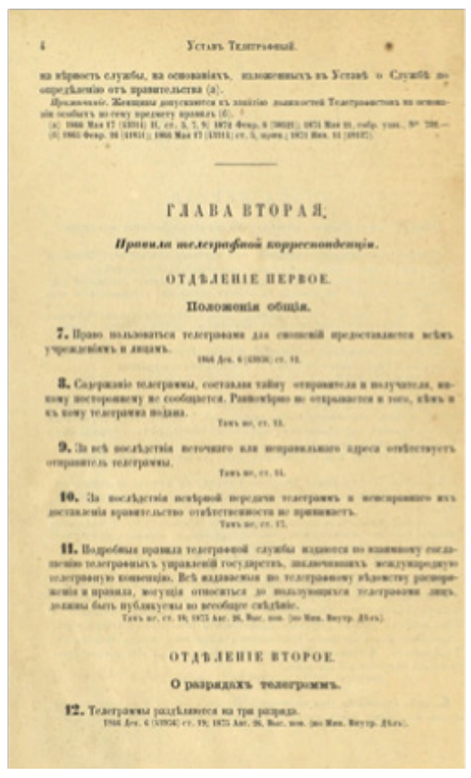
Изначально такие элементы права на неприкосновенность частной жизни были законодательно закреплены Почтовым уставом 1857 года, устанавливающим порядок получения корреспонденции только лицами, которым она предназначена,


УСТАВЪ

ТЕЛЕГРАФНЫЙ.

Изданіе 1876 года.

САНКТПЕТЕРБУРГЪ. 1876


Уставъ Телеграфный.

ГЛАВА ВТОРАЯ.

Правила телеграфной корреспонденціи.

ОТДѢЛЕНІЕ ПЕРВОЕ.

Положенія общія.

ОТДѢЛЕНІЕ ВТОРОЕ.

О разрядахъ телеграммъ.

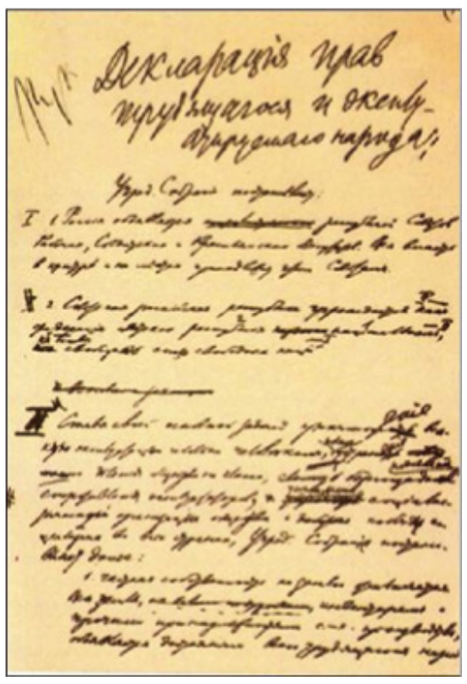
Телеграфный устав 1876 года.

1 Retrospectare (лат.) – смотреть назад, взгляд в прошлое.
2 Sber Privacy Journal vol.1// Пульс [Электронный ресурс]. URL: https://hr.sberbank.ru/platform/catalog/a5958b9e-a01b-47ec-8eae-ca0f790e1572 (дата обращения: 06.09.2022).
3 Всеобщая декларация прав человека от 10.12.1948, ст. 12 // СПС КонсультантПлюс.
4 Конвенция о защите прав человека и основных свобод от 04. 11.1950, ст.8 // СПС КонсультантПлюс.
5 Устав Телеграфный, 1876г., ст.8// Президентская библиотека имени Б.Н. Ельцина [Электронный ресурс]. URL: https://www.prlib.ru/item/460093 (дата обращения: 06.09.2022).
6 Первый уголовный кодекс в истории России.

и Телеграфным уставом 1876 года, устанавливающим следующие правила: *«содержание телеграммы, составляя тайну отправителя и получателя, никому постороннему не сообщается. Равномерно не открывается и тот, кем и к кому телеграмма подана.»*[5]

Также в дореволюционное время получила свое развитие уголовно-правовая охрана тайны корреспонденции, осуществляемая на основании нормативных актов, содержавших как нормы, регулирующие общие вопросы, так и устанавливающие ответственность за совершение конкретных преступных посягательств, в их числе:

- Уложение о наказаниях уголовных и исправительных 1845 года6, которое предусматривало, что почтовый чиновник, который не по неосторожности, а с какой-либо целью, в том числе из любопытства, распечатывал отданное для отправления письмо, адресованное на имя другого, наказывался «удалением с должности». В случае, если вскрытие чужой корреспонденции осуществлялось с целью передачи содержащейся в ней информации третьему лицу, почтовый чиновник подлежал наказанию тюремным заключением от 4 до 8 месяцев[7];
- Устав о наказаниях, налагаемых мировыми судьями 1864 года, предусматривающий ответственность за разглашение с намерением оскорбить чью-либо честь сведений, сообщенных втайне, или же узнанных вскрытием чужого письма или другим противозаконным образом, в виде ареста до 15 дней или денежного взыскания до 50 рублей[8];
- Уголовное Уложение 1903 года, которое устанавливало запрет на вмешательство должностных лиц при отправлении ими правосудия в личную и семейную жизнь человека[9].



Конституция СССР от 1924 года

По истечении некоторого времени после Октябрьской революции 1917 года произошла отмена предшествующего законодательства. Существенным образом «изменился» и подход к проблеме прав человека. Несмотря на то, что Конституция РСФСР 1918 года содержала раздел о правах человека под названием «Декларация прав трудящегося и эксплуатируемого народа» (далее — Декларация)[10], она не закрепляла прав человека на личную тайну. В Декларацию вошли лишь запрет эксплуатации, право уравнительного землепользования, освобождение трудящихся масс из-под ига капитала, право трудящихся в управлении.

В 1924 году была принята новая конституция — Конституция СССР, в которой вовсе не содержалось декларации прав. Из прав человека в ней были провозглашены лишь национальная свобода, равенство, единое союзное гражданство. Вместе с этим в конституции отдельная глава была посвящена учреждению Объединенного государственного политического управления с целью борьбы с политической и экономической контрреволюцией, шпионажем и бандитизмом и которое руководило репрессиями, попирающими все человеческие права. *«У людей не должно было быть никаких тайн от власти, всё должно решаться на открытых собраниях и дискуссиях, в том числе и вопросы об интимных отношениях, о наличии внутренних, скрытых от других глаз сведений о жизни человека»*[11].

Первые советские уголовные кодексы 1922 и 1926 годов также соответствовали духу времени и не содержали норм о преступлениях против личной и семейной тайны в плане уголовноправовой защиты личных прав человека.

Впервые глава о правах и обязанностях граждан появилась в Конституции СССР 1936 года («Сталинская»). Конституция закрепляла широкий перечень личных прав и свобод, а также право на неприкос-

7 Уложение о наказаниях уголовных и исправительных 1845г., ст.1104 // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?doc_itself=&empire=1&nd=142964&page=1&rdk=0&link_id=4#I0 (дата обращения: 06.09.2022).
8 Российское законодательство X-XX веков. Т.8.М., 1991. С.412.
9 Уголовное Уложение 1903г. СПб., 1903.С. 144-145.
10 Написана В.И.Лениным и принята 3 (16) января 1918 г. Всероссийским Центральным Исполнительным Комитет (ВЦИК), являет собой конституционный акт Советской республики, законодательно закрепивший завоевания Октябрьской революции и провозгласивший основные принципы и задачи социалистического государства. 18 (31) января 1918 г. Декларация была утверждена III Всероссийским съездом рабочих, солдатских и крестьянских депутатов.
11 Трофимова В. Е., Уголовное законодательство России об охране личной и семейной тайны: становление, этапы развития / В. Е. Трофимова. — Текст: непосредственный // Молодой ученый. — 2013. — № 3 (50). — С. 375-377. — URL: https://moluch.ru/archive/50/6303/ (дата обращения: 06.09.2022).

новенность жилища и тайну переписки, но с практической стороны закрепление данных прав было всего лишь формальностью, так как Кон- ституция была принята накануне массовых репрессий 1937-1938 годов, а приказом НКВД СССР было предписано стенографировать все без исключения международные телефонные разговоры, была введена цензура всей входящей и исходящей международной корреспонденции, а также установлен контроль над человеком и обществом с использованием осведомителей. Несмотря на очевидное нарушение такой практикой права на неприкосновенность частной жизни, подобные действия оправ- дывались как необходимые меры обеспечения безопасности государственного строя. А в 1940-е годы, с расширением репрессивно-карательной политики по отношению к инакомыслящим и ужесточением тоталитарного режима, проблема прав человека фактически была «закрыта».

Улучшаться ситуация стала только в период политической «оттепели» конца 1950-х — начала 1960-х годов, когда в стране была провозглашена полная победа социализма, что породило, в свою очередь, ответственность за нарушение прав и свобод человека. В 1960 году был принят Уголовный Кодекс РСФСР, в который была включена глава «Преступления против политических и трудовых граждан», где была предусмотрена уголовная ответственность за нарушение личной и семейной тайны, а также тайны усыновления и врачебной тайны. Тайна исповеди формально существовала, но государство в период «развитого социализма» относилось к ней безразлично, так как отношения с церковью были весьма натянуты.

В связи с ратификацией СССР в 1977 году Международного пакта о гражданских и политических правах[12] (от 16 декабря 1966 года) в СССР была принята новая Конституция СССР («Брежневская»), которая стала первой и единственной за весь советский период конституцией, включавшей стандартный для развитых европейских стран комплекс гражданских, политических, экономических, социальных и культурных прав. Гражданам были гарантированы неприкосновенность личности, жилища, а также охрана личной жизни, тайны переписки, телефон- ных переговоров и телеграфных сообщений, кроме того, было установлено, что уважение личности, охрана прав и свобод граждан являлись обязанностью всех государственных органов, общественных организаций и должностных лиц. Вместе с этим были также предприняты меры по защите «банковской тайны» (в современном ее понимании) — Уставом Государственных трудовых сберегательных касс СССР 1977 года на работников государственных трудовых сберкасс была возложена обязанность хранить в тайне сведения о вкладчиках и других клиентах, о совершенных ими операциях и состояниях счетов по вкладам.

Право на неприкосновенность частной жизни как самостоятельное право было впервые введено в России Декларацией прав и свобод человека и гражданина, принятой в 1991 году накануне распада союзного государства Верховным Советом РСФСР. В ней предусматривался запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согла- сия. Впоследствии данная норма была закреплена в Конституции РФ 1993 года.

Эпоха персональных данных началась в России в 1995 году с принятием Федерального закона «Об информации, информатизации и защите информации» № 24-ФЗ, где было впервые законодательно закреплено понятие персональных данных[13]. Кроме того, указанным законом предусматривались общие принципы сбора и использования информации о гражданах. Согласно этому закону, персональные данные были отнесены к информации конфиденциального характера.

Штаб-квартира ВТО в Женеве.

С 1993 года по 2011 год Россия вела переговоры о вступлении во Всемирную торговую организацию[14], одним из условий которой было принятие Конвенции Совета Европы о защите персональных данных[15]. 7 ноября 2001 года Россия подписала вышеуказанную конвенцию, что стало основой разработки российского законодательства, регулирующего вопросы обработки персональных данных. Впоследствии были приняты Федеральный закон от

12 Международный пакт о гражданских и политических правах принят резолюцией 2200 A (XXI) Генеральной Ассамблеи 16 декабря 1966 года.
13 Согласно статье 2 Федерального закона, персональные данные — сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.
14 Всемирная торговая организация (ВТО) — глобальная международная организация, регулирующая правила торговли между своими членами.
15 Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Заключена в г. Страсбурге 28.01.1981).

27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[16], Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», а также специализированные законы, содержащие требо- вания к обработке информации о человеке и защите личных данных: «О связи», «О банках и банковской деятельности», «Об основах охраны здоровья граждан РФ», «Об оперативно-розыскной деятельности» и соответствующие им подзаконные акты.

Федеральным законом № 152-ФЗ «О персональных данных» были определены органы, осуществляющие контроль и надзор за обработкой и защитой персональных данных в России:

- Уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) — осуществляет контроль (надзор) за обработкой персональных данных и соблюдением прав субъектов персональных данных;
- Федеральная служба по техническому и экспортному контролю (ФСТЭК России) — осуществляет контроль за выполнением организационных и технических мер по обеспечению безопасности персональных данных, обрабатываемых в информационных системах;
- Федеральная служба безопасности (ФСБ России) — осуществляет контроль за выполнением организационных и технических мер по обеспечению безопасности персональных данных с использованием средств криптографической защиты информации.

КоАП РФ введена административная ответственность за нарушение правил обработки персональных данных и обеспечения их конфиденциальности, УК РФ предусмотрены меры ответственности в сфере охраны личной, семейной и банковской тайны, а в ГК РФ установлена ответственность за причинение гражданину вреда в результате нарушения правил обработки персональных данных с возмещением убытков и / или компенсацией вреда, кроме того, закреплено право на защиту чести, достоинства и деловой репутации с возможностью опровержения и удаления порочащих сведений.

В заключение можно сделать вывод о непростом пути развития российского законодательства в сфере охраны частной жизни, который делится на четыре основных периода:

Первый период 1857 — 1917 гг
заложил основы развития отечественного законодательства, направленного на защиту сведений, составляющих тайну переписки и ответственности за посягательства на оную;

Второй период 1917 — 1960 гг
характеризуется исчезновением правовых норм по защите личной тайны;

Третий период 1960 — 1993 гг
отмечается возрождением норм, направленных на охрану отдельных видов тайн, при этом следует отметить, что защита частной жизни человека не предоставлялась иностранным гражданам;

Четвертый период 1993 г. — н.в.
отличается формированием норм с учетом международного права,[17] выделением сведений, составляющих личную, семейную тайну и персональные данные, а также совершенствованием федерального законодательства с учетом глобальных интеграционных процессов и интенсивного развития цифровых технологий.

Стоит также отметить, что на развитие законодательства России в послереволюционный период коренным образом влияла политическая ситуация в стране. Такая ситуация не обошла стороной и наше время, когда потребовалось принятие мер по защите личных данных граждан страны от посягательств на их неправомерное использование со стороны зарубежных технологических компаний, а также иностранных разведок и недобросовестных СМИ, в результате чего, в частности, были установлены требования по локализации баз персональных данных, ужесточены условия для трансграничной передачи и др.

Вместе с этим государство также обеспокоено ростом нарушений, связанных с неправомерной обработкой персональных данных и участившимися случаями утечек персональных данных, в связи с чем были внесены изменения в закон «О персональных данных» в части информирования операторами о фактах неправомерной передачи (предоставлении, распространении доступе) персональных данных третьим лицам, в том числе об утечках персональных

16 Отменяет Федеральный закон «Об информации, информатизации и защите информации» № 24-ФЗ.
17 Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных (в н.вр. отменена Общим регламентом защиты персональных данных (ст. 94 General Data Protection Regulation, GDPR, Пост. ЕС 2016/679).

данных. Государственной Думой, Правительством и Минцифры ведется работа по многократному усилению административной (финансовой) ответственности операторов персональных данных, допустивших утечку или неправомерную передачу персональных данных, и введению уголовной ответственности за неправомерное использование персональных данных, в том числе их продажу. В случае принятия соответствующих норм, возможное наказание станет серьезной мотивацией операторов персональных данных не нарушать закон и ответственно относиться к обработке и защите персональных данных.

автор
Алексей Савичев

AB OVO[1]: отнесение информации к персональным данным и их классификация

Введение

«Какие данные относятся к персональным?», «почему одни данные относятся к персональным, а другие – нет?» – вопросы, которые регулярно возникают в Банке как среди бизнес-подразделений, так и среди экспертов в области кибербезопасности и ИТ. Российское сообщество специалистов в области приватности тоже не пришло к единому мнению: на профильных конференциях («Защита персональных данных», Privacy Day) и на семинарах Роскомнадзора раз за разом обсуждение возвращается к этим онтологическим, фундаментальным вопросам. Несмотря на то, что законодательство о персональных данных с нами уже довольно давно, всё еще нет конкретных критериев и методик для однозначного ответа на эти вопросы. В практической деятельности противоречивые позиции регуляторов, судебных органов и экспертного сообщества приводят к тому, что бизнес в итоге принимает решение ориентироваться на «узкий» подход к определению персональных данных (ПДн). Такой подход, как правило, определяет ПДн только как информацию, однозначно идентифицирующую конкретного человека. Следствием такого подхода является нарушение прав субъектов компаниями, которые защищают данные по остаточному принципу, не считая их «персональными», выражающееся в бесконтрольном обороте и, в конечном счете, утечках данных. В подобной ситуации неопределенности разумной необходимостью выглядит разработка и принятие в компании собственной методики определения персональных данных среди прочей обрабатываемой информации. Далее мы расскажем о методике, принятой у нас в Сбербанке.

1 Ab ovo (лат.) – устойчивый фразеологический оборот, обозначающий «с самого начала».

Определение персональных данных

Для начала разберем подробнее действующее определение ПДн:

Статья 3. Основные понятия, используемые в настоящем Федеральном законе.

В целях настоящего Федерального законе используются следующие основные понятия:

1) персональные данные – *часть 1* любая информация, *часть 2* относящаяся к *часть 3* прямо или косвенно определенному *часть 4* физическому лицу (субъекту персональных данных);

Часть 1 *«любая информация...».* Согласно Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», информация — это сведения (сообщения, данные) независимо от формы их представления.

Часть 2 *«относящаяся к...».* Признак «относимости» — предмет регулярных дискуссий среди экспертов в области приватности. В Банке принята следующая трактовка: информация должна относиться к физическому лицу по одному или нескольким признакам: по «содержанию», «цели» или «результату».

a. По признаку «Содержание» информация относится к персональным данным, если она по своей природе является информацией о:

- физическом лице, например: имя, данные документа, удостоверяющего личность, данные местожительства и т.д.;
- других объектах, характеризующих физическое лицо, например: адрес места работы, техническая информация об устройствах, кото-

рые использует физическое лицо, информация о юридических лицах, представителем которого является физическое лицо;

b. По признаку «Цель» информация относится к персональным данным, если она используется для характеристики физического лица или его поступков (деятельности), влияния на статус или поведение физического лица, принятия решений в отношении физического лица;
c. По признаку «Результат» информация относится к персональным данным, если обработка данных влияет или может повлиять на права и интересы физического лица, выделит его среди остальных членов общества и позволит применить к нему определенную модель поведения.

Часть 3 *«прямо или косвенно определённому или определяемому...»*. На основании информации должно быть возможно либо установить физическое лицо с достаточной степенью точности («прямо определенное»), либо сделать это с использованием некоторых других данных («косвенно определяемое» лицо). Еще раз проговорим этот важный момент:

a. Прямое определение — это возможность однозначного определения конкретного физического лица, в частности путем соотнесения информации с:

- фамилией, именем и отчеством (при наличии), как с идентификатором гражданина в гражданском обороте, под которым он приобретает и осуществляет права и обязанности (п. 1 ст. 19 Гражданского кодекса РФ);
- идентификаторами субъектов персональных данных, использующимися в государственных системах, например, ИНН, СНИЛС, номер паспорта.

b. Косвенное определение — это возможность определения конкретного физического лица путем соотнесения нескольких его характеристик, которые хотя и не позволяют однозначно определить данное физическое лицо, но в конечном счете позволяют выделить его среди прочих.

Часть 4 *«...физическому лицу»*. Очевидно, субъектами персональных данных могут выступать только физические лица. Здесь важно сделать замечание. У юридических лиц нет персональных данных, однако Банк в рамках отношений с ними обрабатывает персональные данные физических лиц, уполномоченных совершать сделки от имени юридического лица или представлять его интересы, а также персональные данные физических лиц, имеющих те или иные отношения с юридическими лицами — их акционеров, бенефициаров, работников и т.д. («связанных физических лиц», СФЛ). Также заметим, что у ИП также нет каких-то «собственных» персональных данных — это персональные данные физического лица, зарегистрированного в качестве индивидуального предпринимателя.

In medias res[2]: Классификация персональных данных

Защита прав и свобод человека и гражданина при обработке его персональных данных, в том числе защита прав на неприкосновенность частной жизни, личную и семейную тайну — приоритет законодательства о ПДн. При оценке потенциального вреда, который может быть причинен физическим лицам в случае неправомерной обработки их персональных данных (напомним, что такая обязанность присутствует у оператора в силу п.5 ч.1 ст.18.1 152-ФЗ), важным фактором является возможность прямого или косвенного определения физического лица. Интуитивно понятно, что в случае нарушения конфиденциальности персональных данных ущерб, причиненный физическому лицу, будет разный в зависимости от вида данных (утечка номера телефона и полных данных паспорта очевидно приведет к бóльшим последствиям для конкретного физического лица, нежели утечка каких-либо обезличенных данных). Единые принципы управления персональными данными должны быть имплементированы на всех этапах их жизненного цикла, включая вопросы доступа, передачи и выгрузки данных из автоматизированных систем.

С учетом большого объема систем и видов информации, в Банке утверждена единая методология определения информации в качестве персональных данных.[3] Согласно утвержденной методике, все атрибуты персональных данных, обрабатываемые в Банке, делятся на два вида в зависимости от возможности определения физического лица — «прямые» и «косвенные» идентификаторы:

2 In medias res (лат.) - устойчивый фразеологический оборот, обозначающий «к самому важному», «к делу».
3 В Банке разработана единая методика, отвечающая на вопрос о классификации информации в качестве персональных – Памятка П-375.

Из приведенной выше схемы видим, что если у атрибута данных отсутствует принадлежность к физическому лицу или связь с ним, а также не удается определить конкретное физическое лицо или выделить некоторое их множество, то такой атрибут не является персональными данными. К примеру, абстрактное сочетание цифр, взятое вне какого-либо контекста, не будет являться персональными данными до того момента, пока мы не узнаем, что перед нами ИНН или СНИЛС (обратите внимание – не важно, знаем ли мы при этом, кому конкретно они принадлежат, достаточно того, что они относятся к некоторому физическому лицу). Также яркими примерами являются VIN-номер, государственный регистрационный номер или реквизиты ПТС автомобиля: все они не будут являться персональными данными до того, как появится «персона» — человек, купивший автомобиль и поставивший его на учёт.

Распределение атрибутов, таким образом, позволяет упорядочить работу с массивами данных, представляющими собой наборы из двух и более атрибутов. Помимо самых простых правил, например, «при наличии прямого идентификатора весь набор данных прямо определяет физическое лицо» (например, дата рождения, место рождения, имя, фамилия, СНИЛС / ИНН), в Банке с применением технологий машинного обучения реализуются и более сложные правила, например, «определенная комбинация косвенных идентификаторов позволяет прямо определить физическое лицо» (например, имя, отчество, гос. номер автомобиля, реквизиты ПТС для продуктов автокредитования).

Заключение

Итак, какова ценность указанного подхода? При увеличении атрибутного состава данных, их количества, а также количества автоматизированных систем, главным вопросом является обеспечение защиты данных, а также их точности, актуальности и своевременной доступности. Функционирование крупной компании предполагает наличие очень больших объемов потоков данных, как между внутренними подразделениями, так и с внешними партнерами. Количество автоматизированных систем, обрабатывающих персональные данные, как правило исчисляется десятками или даже сотнями. Построение системы управления жизненным циклом ПДн без решения, принятого централизованно о том, что считать «персональными данными» — нереализуемая задача. Отсутствие единого подхода к определению ПДн влечет риски нарушения прав субъектов, признания передачи данных неправомерной. Имплементация же описанного подхода позволяет не допустить в компании разночтения в определении персональных данных среди всего множества данных что, в свою очередь, позволяет выстроить централизованную систему управления данных и повысить защиту наиболее критичных для ПДн клиентов прямых идентификаторов.


авторы

Евгений Сердечнюк

Олег Беляев

Современные DLP-системы
как способ предотвращения утечек ПДн

С древних времен, когда люди впервые осознали ценность информации, они начали применять средства, направленные на ограничение доступа посторонних лиц к важной информации, а также от её утечки за периметр контролируемой зоны. С течением времени изобретались все новые и новые средства защиты информации — от использования хищных птиц для перехвата шпионских почтовых голубей до DLP-систем.

Исторический путь развития средств защиты информации — от натренированных хищных птиц до DLP-систем.

Исторический путь развития средств защиты информации — от натренированных хищных птиц до DLP-систем.

Голубиная почта — древнейший способ доставки письменных сообщений. Основным толчком развития голубиной почты служила война, а именно ценность оперативного и безопасного обмена информацией между войсками, при этом важным условием являлось недопущение получения её вражескими войсками. Натренированных голубей использовали лазутчики с целью передачи полученной ими секретной информации, например, о состоянии армии оборонительных и наступательных сооружениях, что могло кардинально повлиять на ход боевых действий. Для борьбы с этим использовались натренированные хищные птицы, которые перехватывали почтовых голубей, не позволяя противникам получить ценную информацию. При осаде Парижа в 1870 — 1871 годах прусскими войсками использовались специально обученные соколы и ястребы, которые перехватывали почтовых голубей, вылетевших из Парижа и доставляющих информацию о ходе обороны города для остальных частей французской армии, планирующих снятие блокады с Парижа, что в свою очередь способствовало взятию Парижа прусской армией. С приходом информационной эпохи и развитием цифровизации общества появились новые цифровые активы, которые необходимо было защищать, развивались и технологии хранения, передачи информации, появлялись все новые более сложные средства защиты данных. Современные средства защиты информации очень разнообразны и включают в себя различные аппаратные, программные и комбинированные комплексы.

> «Информация — это могущество. А иногда, если времени в обрез, еще и скорость»
>
> *Стивен Кинг*

21 век — век информационных технологий, которые очень глубоко интегрированы в жизнь каждого человека, посредством которых обрабатываются огромные объемы информации, относящейся к определенному человеку — персональные данные. Ввиду ценности, которую представляют собой персональные данные, в последние годы неумолимо растет количество случаев, связанных с их утечками. Наряду с применяемыми средствами защиты от несанкционированного доступа, межсетевыми экранами, системами антивирусной защиты информации, средствами криптографической защиты важным также является использование средств по недопущению несанкционированной передачи защищаемой информации за периметр компании.

Согласно Отчету об исследовании утечек информации ограниченного доступа в 2021 году, подготовленному компанией Infowatch[1] (далее — Отчет Infowatch), доля умышленных нарушений среди утечек внутреннего характера (по вине персонала в 2020 и 2021 годах составила более 51%, что говорит о наличии серьезного уровня угрозы безопасности персональных данных, обрабатываемых в компаниях, со стороны персонала самих компаний.

В отчете Infowatch приведена диаграмма распределения утечек по категориям внутренних нарушителей. Основная доля внутренних нарушителей приходится на непривилегированных работников — в среднем доля нарушений, допущенных непривилегированными работниками в период с 2018 года по 2021 год, составляла 83,7% от числа всех внутренних нарушителей.

1 Отчёт об исследовании утечек информации ограниченного доступа в 2021 году // Экспертно-аналитическим центром InfoWatch, [Электронный ресурс]. URL: https://www.infowatch.ru/sites/default/files/analytics/files/v-2021-stalo-bolshe-umyshlennykh-utechek.pdf (дата обращения: 06.09.2022).

В качестве одного из средств, обеспечивающим нейтрализацию действий внутренних нарушителей, направленных на нарушение конфиденциальности персональных данных, используются специальные системы предотвращения утечек информации — DLP-системы.

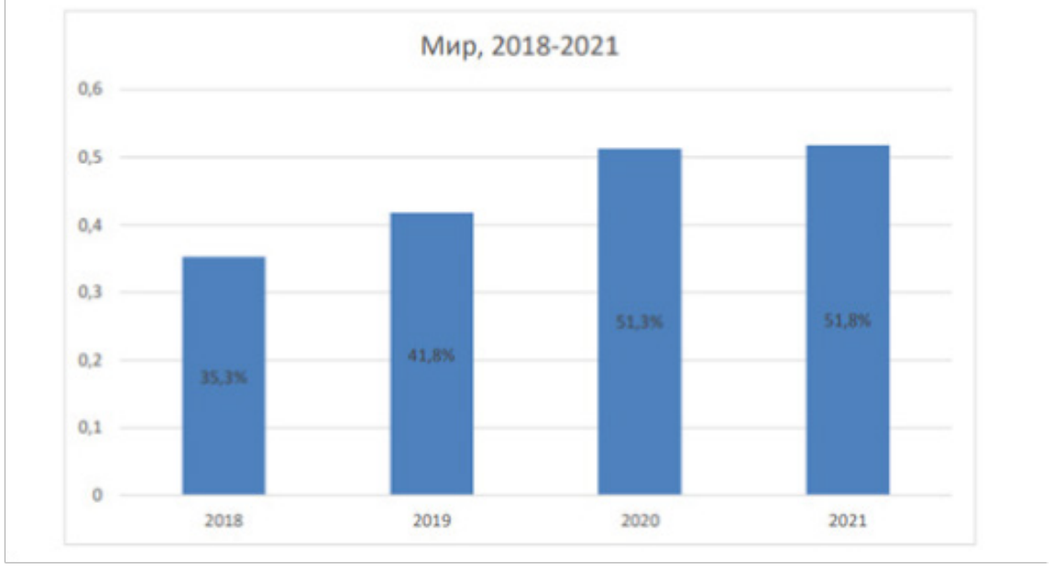


Рисунок 1. Динамика доли умышленных нарушений внутреннего характера: Мир, 2018-2021 гг.[2]

Распределение по категориям:

- 83,7% непривелигированные работники
- 6,2% подрядчики
- 5,9% руководители
- 2,6% бывшие сотрудники
- 0,8% системные администраторы

Просто о сложном

Что такое DLP-системы?

DLP-система (англ. *Data Leak Prevention*) — это программное обеспечение, посредством которого осуществляется мониторинг перемещения данных, в том числе персональных данных, в периметре или за периметр компании.

Как работает DLP-система?

DLP-система осуществляет анализ / мониторинг информационных потоков компании с целью выявления перемещения (передачи) конфиденциальной информации, в том числе персональных данных, и анализ таких потоков на соответствие политикам безопасности компании.

Анализ потоков осуществляется путем:

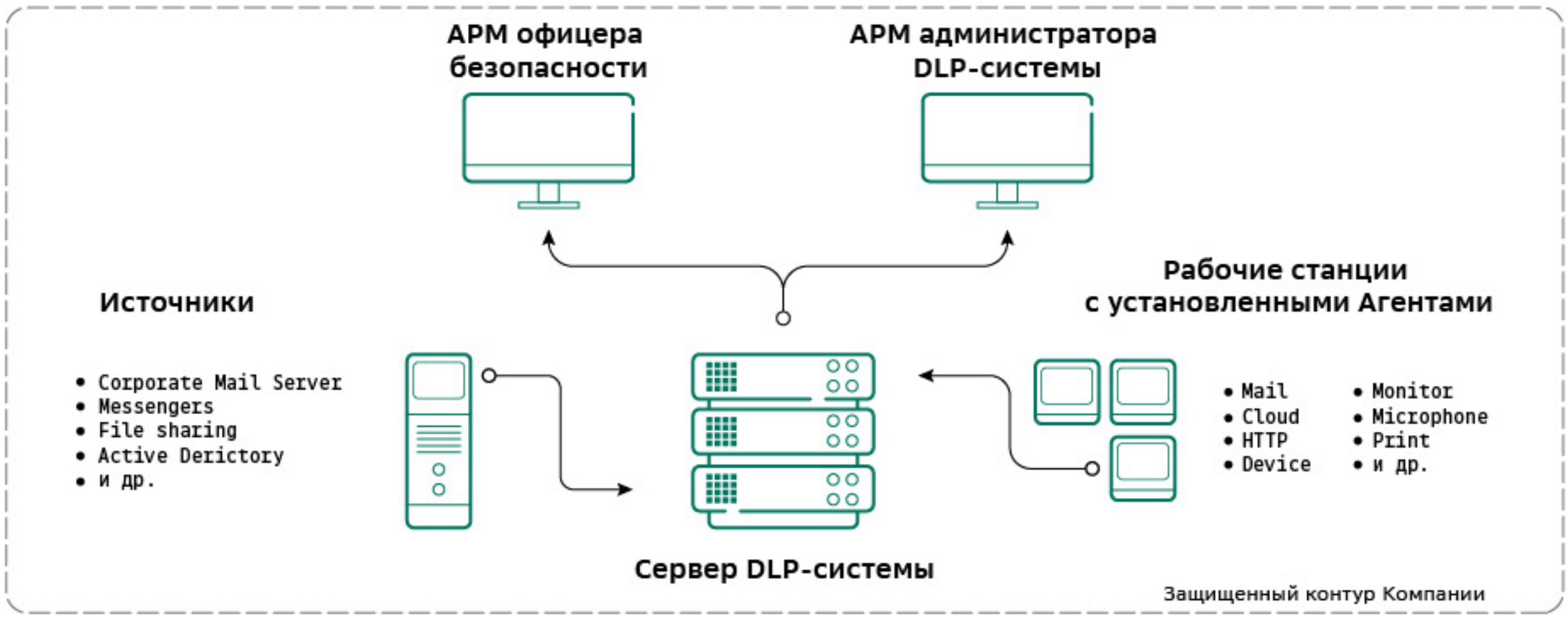
- анализа маркеров файла (название, специальные метки и т.д.);
- анализа содержимого самого файла.

В случае выявления DLP-системой инцидента, осуществляется его регистрация в соответствующем журнале. Реагирование на инцидент осуществляется уже по факту, при этом влияние на бизнес-процесс отсутствует, дальнейшая работа по разбору инцидента осуществляется со стороны работника службы безопасности.

DLP-система позволяет блокировать несанкционированную передачу конфиденциальной информации, что с одной стороны имеет большую эффективность в защите данной информации от передачи ее за периметр компании. С другой стороны, при неверной настройке политик DLP-систем, данный способ может заблокировать целый бизнес-процесс в самый неподходящий момент, в связи с чем должен осуществляться непрерывный анализ отчетов результатов мониторинга DLP — систем в целях своевременного обновления политик для обеспечения блокирования передачи запрещенного контента, но без негативного влияния на непрерывность бизнеса. Таким образом, основная задача DLP-системы — это анализ контента, отправляемого за периметр компании.

Принцип работы DLP-системы продемонстрирован на схеме ниже.

2 Там же.



В зависимости от критериев классификации существуют несколько типов DLP-систем. По сетевой архитектуре DLP-системы делятся на:

- **Шлюзовые DLP-системы** — осуществляют анализ направляемого на выделенный сервер всего исходящего трафика компании;
- **Хостовые DLP-системы** — осуществляют анализ действий работников на рабочих станциях, не позволяя работникам выходить за ограничения, установленные политиками безопасности.

Большое применение получили универсальные DLP-системы, сочетающие в себе одновременно и шлюзовые, и хостовые системы.

Практика применения DLP-систем и реагирования на инциденты

Внедрение и использование DLP-системы затрагивает важные аспекты работы компании. Легитимность DLP-системы должна основываться на внутренних нормативных документах компании, а также на сведениях об использовании DLP-системы, внесенных в трудовые договоры и правила внутреннего трудового распорядка.

Для внедрения DLP-системы и правомерного использования результатов анализа / мониторинга (отчетов), сформированных системой, при проведении с работниками разбирательства по выявленным инцидентам необходимо:

1. Прописать в трудовых договорах с работниками и правилах внутреннего трудового распорядка положения о том, что:
   - компания использует DLP-систему, необходимо также закрепить порядок осуществления анализа действий работника на оборудовании, принадлежащем компании;
   - все ресурсы и оборудование, которые используются в работе, принадлежат компании, и использование их в личных целях запрещено.
2. Внутренними нормативными документами утвердить:
   - перечень конфиденциальной информации, обрабатываемой в компании;
   - порядок работы с конфиденциальной информацией (в том числе политики информационной безопасности);
   - перечень лиц, допущенных к обработке конфиденциальной информации;
   - ответственность за нарушение правил работы с конфиденциальной информацией.
3. Ознакомить работников с вышеуказанными документами.

Важно при привлечении работника к дисциплинарной ответственности на основании данных, собранных DLP-системой, выполнить все процедуры, предусмотренные ст. 193 Трудового кодекса Российской Федерации от 30.12.2001 № 197-ФЗ:

1. Создать комиссию, которая делает вывод по результатам расследования инцидента и фиксирует его приказом. В комиссию целесообразно включать работника юридического подразделения, работника кадровой службы и работника службы безопасности, которая инициировала расследование выявленного инцидента;

2. Довести до работника обстоятельства инцидента;
3. Затребовать от работника письменное объяснение, которое он должен представить в течение двух рабочих дней;
4. Если объяснения не были представлены в установленный срок, то данный факт необходимо зафиксировать актом;
5. Сформировать и утвердить результаты расследования инцидента и зафиксировать их приказом;
6. Ознакомить работника с результатами расследования.

Работодатель вправе применять к работникам следующие дисциплинарные взыскания:

- замечание;
- выговор;
- увольнение по соответствующим основания.

Важно понимать, что при обработке конфиденциальной информации, в том числе персональных данных, в корпоративной сети благодаря DLP-системе риски утечки конфиденциальной информации сокращаются, а сознательность персонала компании при работе с данным видом информации пропорционально возрастает.

DLP-система — это действительно эффективное средство защиты информации, которое должно рассматриваться компаниями как «маст-хэв»[7] при выстраивании надежной системы защиты информации, которое способно с высокой степенью надежности исключить утечку конфиденциальной информации за пределы компании, но требующее больших ресурсов для развертывания: вычислительных ресурсов и высококвалифицированных работников, которые смогут эффективно выстроить работу DLP-системы.

При создании системы защиты информации необходимо учитывать, что за последнее время было выявлено большое количество утечек персональных данных, в связи с чем внимание государства к данному вопросу растет. Минцифры ведет работу по разработке законопроекта, согласно которому на компании, допустившие утечку персональных данных, будут налагаться оборотные штрафы, что может повлиять на экономическую стабильность компании. В свою очередь, использование DLP-систем позволит минимизировать риск утечек персональных данных, избежать многомилионных штрафов и репутационных потерь.

7 «Маст-хэв» – молодежный сленг, транслитерация с английского *«must have»*, используется для обозначения вещи, которая обязательно должна быть.

Опыт Сбера

Один из самых масштабных проектов по внедрению DLP-системы реализован специалистами Сбербанка при поддержке компании «РТК-Солар» на сетевой инфраструктуре Банка. Для защиты от утечек конфиденциальной информации Сбербанк использует широкую функциональность Solar Dozor, включающую фильтрацию и хранение данных в архиве, поиск и управление событиями и инцидентами информационной безопасности. Solar Dozor использует специализированные модули — модули перехватчики. Они собирают и передают на анализ все сообщения работников, контролируют действия работников на рабочих станциях, а также проверяют локальные и облачные файловые ресурсы[3].

Использование перехватчиков дает возможность контролировать корпоративную электронную почту, USB-носители, веб-сервисы, файловые хранилища, социальные сети и мессенджеры, блокируя передачу конфиденциальной информации за периметр компании.

С использованием модуля MultiDozor офицеры безопасности в режиме реального времени централизованно контролируют процессы передачи конфиденциальной информации и получают аналитику по всей филиальной сети[4].

Система Solar Dozor осуществляет мониторинг более 250 тыс. рабочих станций Банка, все подразделения Банка от Камчатки до Калининграда охвачены системой, обеспечивающей тотальный контроль передаваемой информации.

Solar Dozor формирует наглядные отчеты, содержащие исчерпы-вающие сведения об инциденте, нарушителях, потоках данных. Благодаря сформированным отчетам можно увидеть состояние защищаемой информации[5].

Система интегрирована с одним из крупнейших SOC (Security Operations Center) в мире[6]. Проекты подобного масштаба на территории страны ранее не реализовывались, что под-тверждает лидерские позиции Сбербанка в области кибербезопасности и делает «законодателем» и ориентиром для других компаний при выстраивании ими систем защиты информации.

3 Solar Dozor. Общая брошюра Ростелеком-Солар [Электронный ресурс]. URL: https://rt-solar.ru/upload/iblock/6cc/solar_dozor_obshchaya_broshyura.pdf (дата обращения: 02.09.2022).
4 Там же.
5 «Сбербанк и «РТК-Солар» реализовали крупнейший в России проект по защите от утечек информации»// SberPress [Электронный ресурс]. URL: https://press.sber.ru/publications/sberbank-i-rtk-solar-realizovali-krupneishii-v-rossii-proekt-po-zashchite-ot-utechek-informatsii (дата обращения: 01.09.2022).
6 Там же.

автор
Михаил Воробьёв

Privacy and Data Protection Regime in India: a Curtain Raiser!

Режим регулирования неприкосновенности частной жизни и защиты данных в Индии: приоткрывая завесу.

В рамках развития международного бизнеса в сентябре 2010 года Сбербанк открыл свой филиал в Индии, в г. Нью-Дели (далее - Филиал). На этапе становления Филиала его основной задачей стало формирование на индийском рынке стратегического плацдарма, который позволил бы Банку поддерживать высокие темпы развития бизнеса Группы. В следующем году Сбербанк планирует открыть еще один офис в Индии в г. Мумбаи и уже отправил соответствующий запрос местному регулятору[1]. В связи с тем, что Филиал осуществляет свою деятельность на территории Индии, он обязан соблюдать требования местных нормативных правовых актов в области персональных данных, поэтому мы попросили нашу коллегу, DPO Филиала ПАО Сбербанк в Индии, поделиться с нами знаниями о законодательных и регуляторных требованиях, предъявляемых к обработке персональных данных в Индии.

Редакция Sber Privacy Journal

1 «Сбербанк в 2023 году намерен открыть еще один офис в Индии» (6.09.2022)// РИА Новости [Электронный ресурс]. URL: https://ria.ru/20220906/ofis-1814701663.html (дата обращения 6.09.2022).

INTRODUCTION

The threat of breach of confidential / personal data has become a major concern globally leading to countries strengthening their Data Protection laws. The multifold growth of information and technology globally, has almost blurred the boundaries of privacy. Imagine a situation wherein the most private moments of our lives are published or revealed to the world at large? Hence, a greater need has been felt for data protection and the measures taken by different countries have not been adequate to ensure a comprehensive protection against such breaches of privacy.

Privacy is considered as a human right, as is enumerated under Article 12 of the Universal Declaration of Human Rights and Article 17 of International Covenant on Civil and Political Rights and India being a signatory to these international covenants, is under an obligation to protect privacy of its citizens. In India, the Right to Privacy[1] has been recognised as a Constitutional right which implies that a breach of

1 Article 21 of the Constitution of India//Legislative department, Ministry of Law and Justice, Government of India [Web-site] https://legislative.gov.in/sites/default/files/COI_English.pdf (accessed 1.09.2022).

ВВЕДЕНИЕ

В последнее время нарушение конфиденциальности информации вызывает всё более серьезное беспокойство во всем мире, в силу чего многие страны начинают ужесточать свои законы о защите данных. Происходящий в общемировом масштабе разносторонний информационный и технологический рост практически размыл границы приватности. Представьте себе ситуацию, в которой самые сокровенные моменты нашей жизни могут стать доступными широкой общественности по всему миру. Как следствие, мы ощущаем всё большую потребность в защите данных, но меры, принимаемые в разных странах, порой оказываются недостаточными для того, чтобы обеспечить всестороннюю защиту от подобных вторжений в частную жизнь.

В соответствии со Статьей 12 Всеобщей декларации прав человека[2] и Статьей 17 Международного пакта о гражданских и политических правах,[3] не-

2 Всеобщая декларация прав человека от 10.12.1948, ст. 12 // СПС КонсультантПлюс.
3 Международный пакт о гражданских и политических правах от 16.12.1966// Организация Объединенных Наций [Электронный ресурс]. URL: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (дата обращения 1.09.2022).

one's private information / personal data shall directly clash with one's constitutional / fundamental right.[2] Therefore, if privacy of any kind is breached for a person / citizen in India, they have the remedy to approach appropriate courts and initiate legal proceedings and the Government shall be bound to protect the same.

The Constitution of India also does not patently grant the fundamental right to privacy. However, the courts in India have held the right to privacy to be within the ambit of other recognised fundamental rights, i.e., freedom of speech and expression under Article 19(1)(a) and right to life and personal liberty under Article 21 of the Constitution of India. Nevertheless, these Fundamental Rights recognised under the Constitution of India are not absolute and are subject to reasonable restrictions provided under Article 19(2) of the Constitution that may be imposed by the Government. Recently, in the landmark case of Justice K S Puttaswamy (Retired) and Mr. Parvesh Sharma vs. Union of India and Others[3], the Constitution bench of the Hon'ble Supreme Court of India has held Right to Privacy to be a fundamental right, subject to certain reasonable restrictions.

LAWS AND REGULATIONS IN INDIA FOR DATA PROTECTION

Information Technology Act

In the ever-evolving global scenario, India still does not have any overarching national law regulating the collection and use of personal data. The most important piece of legislation with respect to data protection in India is the Information Technology Act, 2000 ("IT Act") read with the rules and regulations laid down thereunder. The said IT Act can be called as the only legal cornerstone to ensure the protection of personal information in India. Certain prescribed rules such as Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules") further implement the IT Act.

Section 43A of the IT Act imposes civil liability on the body corporate who deals with sensitive personal data in case of an instance of a breach. It states that a body corporate who is processing, dealing or handling any sensitive personal data or information of an individual, and is negligent in implementing and

2 2017 SCC Vol. 10 November 28, 2017 Part 1// Supreme Court Cases Online Blog [Web-site] https://www.scconline.com/blog/post/2017/12/13/2017-scc-vol-10-november-28-2017-part-1/ (accessed 1.09.2022).
3 Writ Petition (Civil) No. 494/ 2012.// Supreme Court of India [Web-site] https://main.sci.gov.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf

прикосновенность частной жизни считается одним из основных прав человека, а Индия в свое время подписала эти международные пакты и обязана защищать неприкосновенность частной жизни своих граждан. В Индии право на неприкосновенность частной жизни[4] признано одним из конституционных прав, в силу чего нарушение конфиденциальности личной информации / персональных данных по своей сути является и нарушением конституционного / основополагающего права.[5] Соответственно, граждане Индии располагают надлежащими средствами юридической защиты и, в случае вторжения в их частную жизнь, могут обратиться в суд и возбудить соответствующее дело, а правительство будет обязано их защищать.

При этом в Конституции Индии основополагающее право на неприкосновенность частной жизни открытым текстом не прописано. Тем не менее, индийские суды рассматривают это право как входящее в сферу действия иных признанных основополагающих прав, а именно права на свободу слова и мнений в соответствии со Статьей 19(1)(a) и права на жизнь и личную свободу в соответствии со Статьей 21 Конституции Индии. Тем не менее, эти основополагающие права, признанные в Конституции Индии, не являются абсолютными, а их действие может быть ограничено правительством в соответствии со Статьей 19(2). Не так давно, в ходе рассмотре-ния прецедентного дела «Судья К.С. Путтасвами (в отставке) и г-н Парвеш Шарма против Индийского Союза и других»,[6] Конституционная палата Верховного суда Индии признала право на неприкосновенность частной жизни основополагающим правом, действие которого может подвергаться определенным разумно обоснованным ограничениям.

НОРМАТИВНЫЕ АКТЫ В ОБЛАСТИ ЗАЩИТЫ ДАННЫХ В ИНДИИ

Закон об информационных технологиях

В постоянно меняющейся мировой ситуации, в Индии до сих пор нет всеобъемлющего национального закона, регулирующего сбор и использование персональных данных. Самым важным законодательным актом, касающимся защиты данных в Индии, является Закон об информационных технологиях от 2000 года (далее — Закон об ИТ) совместно с правилами и положениями, установленными им. Вышеупомянутый Закон об ИТ можно назвать единственным фундаментальным законом в сфере защи-

4 См. в сноске 3 выше.
5 См. в сноске 4 выше.
6 См. в сноске 5 выше.

maintaining reasonable security practices in protecting the data and results in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages to the person so affected. No maximum limit of what the compensation / penalty would be has been stated under the IT Act and may be claimed by the affected party based on the underlying circumstances.

It is to be noted that the aforementioned SPDI Rules and Section 43A of the IT Act apply only to a body corporates and individuals acting on behalf of body corporate. The provisions of the IT Act are necessary to be complied with by entities in or outside of India that process personal data either:

(i) in India, or
(ii) have a computer, computer system, or computer network located in India, as provided in the IT Act.

Further, Section 72A of the IT Act imposes a liability on any person for disclosing personal information of an individual to a third party without the explicit consent of such person. Such liability can be extended to imprisonment for a term extending to three years and fine extending up to INR 5,00,000/-. The said provision primarily imposes criminal liability. Further, Section 69 of the IT Act is a provision that deals with exception as to what will not be considered as private and secret information. This shall mean that the information that the government deems necessary for the interest of sovereignty or integrity of India, defence, security of state, friendly relation with foreign states, public order etc. shall be excluded from the ambit of personal data.

Information Technology Rules (SPDI Rules)

The collection, storage and disclosure of sensitive personal data or information are further laid out under the SPDI Rules. It is notable that the SPDI Rules issued under the IT Act applies only to electronic records and excludes manual records from its purview. “Personal Information” has been defined under the said SPDI Rules as any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

Sensitive Personal Data or Information (“SDPI”) also includes any details relation to the above if the person provides the data to a body corporate for service or under lawful contract for processing or storage.[4] Rule 3 of the SPDI Rules further stipulates

4 Rule 3 of the SPDI Rules.

ты персональной информации в Индии. Дальнейшую реализацию Закона об ИТ обеспечивает ряд принятых на законодательном уровне правил — например, принятые в 2011 году Правила информационных технологий (Разумно обоснованные практики и процедуры защиты чувствительных персональных данных или информации) (далее — Правила ИТ).

Разделом 43A Закона об ИТ предусматривается гражданская ответственность юридических лиц, работающих с чувствительными персональными данными, в случае нарушения их конфиденциальности. В данном разделе прописано, что юридическое лицо, которое обрабатывает чувствительные персональные данные или иную информацию о физическом лице и при этом халатно относится к внедрению практик обеспечения безопасности в сфере защиты данных, что приводит к вреду или неправомерной прибыли физического лица, может быть привлечено к ответственности в виде возмещения соответствующего ущерба. В то же время, в Законе об ИТ не устанавливается никакого максимального предела для подобных компенсаций / штрафов, которые могут быть заявлены потерпевшей стороной на основании конкретных обстоятельств.

Следует отметить, что вышеупомянутые Правила ИТ и Раздел 43A Закона об ИТ используются только в отношении юридических лиц и физических лиц, действующих от имени юридических лиц. Положения Закона об ИТ должны соблюдаться организациями, расположенными на территории Индии или за ее пределами, которые обрабатывают персональные данные:

(i) на территории Индии, или
(ii) располагают компьютерами, компьютерными системами или компьютерными сетями, расположенными на территории Индии, как указано в Законе об ИТ.

Далее, Разделом 72A Закона об ИТ предусматривается ответственность любого лица за раскрытие персональной информации физического лица третьей стороне без получения явно выраженного согласия такого физического лица. Подобная ответственность может принимать форму тюремного заключения на срок до трех лет и штрафа до 500 000 индийских рупий. Вышеупомянутое положение в первую очередь предусматривает уголовную ответственность. Кроме того, в Разделе 69 Закона об ИТ говорится о том, какая информация не считается конфиденциальной и секретной. Это означает, что информация, которую правительство сочтёт необходимой для обеспечения государственного суверенитета или территориальной целостности Индии, обороны, государственной безопасности, друже-

that sensitive personal data or information of a person means personal information that consists of information relating to passwords, financial information such as bank account or credit card or debit card or other payment instrument details, biometric information and any of the information received by body corporate for processing, stored or processed under lawful contract or otherwise, among others. It is however important to note that any information that is available in public domain, freely available, accessible or available under Right to Information Act, 2005 are excluded from the scope of sensitive personal data.

A body corporate must implement reasonable security practices, procedures and standards to handle sensitive personal data or information and have a comprehensive documented information security program and policy that contain technical, operational, managerial and physical security control measures for such information. Processing should always be limited to what are required and should be retained for a specific period only.[5] SDPI rules are not exhaustive but require companies / body corporates to have a privacy policy in place, to obtain consent when collecting or transferring sensitive personal data or information, and to inform data subjects of such collected data.

To be precise, consent is the essence of processing data. The nature of consent are not clearly defined under any act but if the consent is obtained freely and without undue influence, then there are a few limitations on the process and methods of obtaining consent. Under the SDPI Rules, the provider of data should have an option to opt out of providing the data or information that are being sought by body corporates. Information provider shall at all times have the option to withdraw their consent for processing and storing the data.

The IT Act has an extra territorial operation and applies to any offence or contravention committed outside India by any person irrespective of his nationality: as long as the act constituting the offence or contravention involves a “computer” or “computer system” in India. Even the SDPI rules cast obligations on body corporates that process sensitive personal data and such body corporates may or may not be incorporated within India only.

5 Rules 5(4) and 5(5) of the SDPI Rules.

ственных отношений с другими государствами, общественного порядка и т.д., может быть исключена из сферы действия положений о персональных данных.

Правила информационных технологий (Правила ИТ)

Более детально сбор, хранение и раскрытие чувствительных персональных данных регулируется Правилами ИТ. При этом следует отметить, что Правила ИТ, разработанные на основе Закона об ИТ, применяются только к электронным записям, а записи, сделанные без использования средств автоматизации, в сферу их действия не входят. «Персональная информация» в вышеупомянутых Правилах ИТ определяется как любая информация, относящаяся к физическому лицу, которая прямо или косвенно, в сочетании с иной информацией, доступной или потенциально доступной юридическому лицу, может идентифицировать соответствующее физическое лицо.

В состав чувствительных персональных данных или информации также входят любые подробные данные, относящиеся к физическому лицу, если оно предоставляет информацию юридическому лицу для получения каких-либо услуг или на основании правомерно заключенного договора об обработке или хранении данных.[7] Положение 3 Правил ИТ также предусматривает, что чувствительные персональные данные или информация физического лица - это персональная информация, в состав которой в числе прочего входит информация, относящаяся к паролям, финансовая информация, например, реквизиты банковского счета, кредитной или дебетовой карты или иного платежного инструмента, биометрическая информация и любая информация, получаемая юридическим лицом для обработки и хранения или обрабатываемая на основании правомерно заключенного договора. При этом, однако, следует отметить, что информация, являющаяся общедоступной или находящаяся в открытом доступе на основании Закона о праве на информацию от 2005 года, исключается из числа чувствительных персональных данных.

При работе с чувствительными персональными данными или информацией юридические лица должны использовать разумно обоснованные практики, процедуры и стандарты обеспечения безопасности, а также собственные всесторонние программы и политики обеспечения безопасности информации, предусматривающие надлежащие меры технического, операционного, управленческого характера, а также меры по контролю физической безопасности.

7 Правило 3, Правила ИТ.

Rules for transferring personal data to other jurisdictions

According to the SDPI Rules, sensitive personal data may be transferred by the collecting entity/ body corporate to another entity/person in another jurisdiction provided that the transferee ensures the same level of data protection that is adhered by the transferor under the SDPI Rules. Further, the transfer is allowed only if it is necessary for the performance of a lawful contract and / or the owner/provider of the sensitive personal data has consented for such transfer of data.

Nevertheless, sectoral regulators have their own set of regulations for transfer of the personal data and the same must be followed for those specific sectors. For instance, all the data of banks must be stored only in India and data processed (in case the processing is done abroad) will have to be brought back to India within 24 hours.[6] Further, the regulator for Banks, i.e.The Reserve Bank of India ("RBI") has come up with mandatory compliances for the deletion of card data by entities in the transaction chain and a transition to tokenisation of card details. "Tokenisation" involves replacing actual card details with a token i.e., a number that is the combination of elements involved in tokenisation (e.g. device ID, token requestor ID and merchant). The RBI's intent is to protect card data; this can be traced back to the guidelines laid down by RBI on Regulation of Payment Aggregators (PAs) and Payment Gateways dated 17th March 2020. An increasing number of transaction frauds and data breaches were linked to data stored with merchants and PAs. These guidelines required PAs and merchants to cease storage of end users' card data, which the author believes to be a step in the right direction.

Regulator for data protection in India

The IT Act does not establish a regulator to oversee the implementation of data protection (similar to a data protection authority under the GDPR). Ministry of Electronics and IT ("MeitY"), meanwhilet is empowered to provide guidance on matters in the realm of information and technology. This organisation has constituted the Indian Computer Emergency Response Team ("CERT") which acts as the nodal agency that receives and responds to all breach notifications. Otherwise, there are no data protection authority in India as such neither organizations like MeitY have any formal process for seeking clarifications. Cybersecurity

6 RBI/2017-18/153 DPSS.CO.OD NO. 2785/06.08.005/2017-2018 dated 6th April, 2018.

Обрабатывать данные всегда следует только в необходимых пределах, а обрабатываемая информация должна храниться только в течение конкретного периода времени.[8] Правила ИТ не являются исчерпывающими, но требуют от компаний / юридических лиц издания политик конфиденциальности, получения согласий при сборе или передаче чувствительных персональных данных или информации, а также уведомления субъектов персональных данных о собираемой информации.

Если говорить точнее, то основное значение для обработки данных имеет получение согласия. Характер согласия четко не определяется ни в одном нормативном правовом акте, но если оно получено по доброй воле и без ненадлежащего влияния, то в отношении процесса и способов получения такого согласия не будет использоваться практически никаких ограничений. В соответствии с Правилами ИТ, физическое лицо, предоставляющее персональные данные, должно иметь возможность отказаться от предоставления данных или информации, которую от него требуют юридические лица. Такое физическое лицо должно иметь возможность отозвать свое согласие на обработку и хранение данных в любое время.

Закон об ИТ имеет экстерриториальное действие и применяется к любым правонарушениям, совершаемым за пределами Индии любыми лицами вне зависимости от гражданства, если эти правонарушения совершаются с использованием «компьютеров» или «компьютерных систем», расположенных на территории Индии. Правила ИТ также накладывают определенные обязательства на юридические лица, обрабатывающие чувствительные персональные данные, которые могут быть зарегистрированы как на территории Индии, так и за её пределами.

Порядок передачи персональных данных в другие юрисдикции

ССогласно Правилам ИТ, чувствительные персональные данные могут передаваться от собирающего их юридического лица другому лицу, находящемуся в иной юрисдикции, при условии, что получающая сторона обеспечит такой же уровень защиты данных, который обеспечивается передающей стороной в соответствии с Правилами ИТ. Кроме того, рассматриваемая передача допускается только тогда, когда это необходимо для исполнения правомерно заключенного договора и / или когда физическое лицо — субъект чувствительных персональных данных дает свое согласие на подобную передачу.

8 Правила 5(4) и 5(5), Правила ИТ.

incidents such as unauthorized access to IT systems / data and the comprising of information must be reported by entities, i.e. service providers, intermediaries, data centers and body corporates to CERT-IN. Such incidents are required to be reported along with the details of the matter within a reasonable time for timely action to be taken in this regard. However, CERT-IN has issued a direction according to which certain specified types of cyber incidents (such as targeted scanning / probing of critical networks / systems, comprise of critical systems / information, unauthorised access of IT systems / data etc.) are required to be mandatorily reported by service providers, data centers, body corporates etc within six hours of noticing such incidents or being brought to notice of such incidents.[7] Important to note that India has no mandatory requirement to report data breaches to affected data subjects as per IT act and related rules. However, organizations like CERT-IN may report such data breaches to general public and other stakeholders for promoting awareness.

KEY RIGHTS OF INDIVIDUALS FOR PROCESSING OF THEIR PERSONAL DATA

Administrative sanction or criminal penalties for breach of data protection

A data breach can definitely lead to an administrative order or criminal penalties. As per section 43A of the IT Act, negligence in implementing the security standards can lead to compensation claims from affected users. Additionally, any data breach as already stated above needs to be reported to CERT-In which may investigate to determine the security practices in place. Failure to report this information may result in financial penalties amounting to INR 25,000[8]. Further, if the CERT-In specifically asks for information, failure to provide the same may invoke both civil and criminal penalties. Under section 70B (7) of the IT Act, failure to provide information to the CERT-In, when requested by the CERT-In is punishable with imprisonment of one year or with monetary fine of a maximum of INR 100,000 or both.

I. Right of access to data / copies of data

The owner of the sensitive data has the right at any time to request a review of their SPDI provided by them to the collecting entity under the SPDI Rules.

7 Directions dated 28th April, 2022
8 Section 45 of IT Act, 2000.

При этом, однако, отраслевыми регуляторами приняты собственные правила передачи персональных данных, которым необходимо следовать в соответствующих конкретных отраслях. Например, все данные банков должны храниться только на территории Индии, а обрабатываемые данные (если обработка осуществляется за рубежом) должны быть возвращены в Индию в течение 24 часов.[9] Кроме того, банковский регулятор — Резервный банк Ин- дии (далее — RBI) выдвинул обязательное требова- ние по удалению реквизитов карт юридическими лицами, участвующими в операциях, и переходу на токенизацию этих данных. «Токенизация» предполагает замену реальных реквизитов карты токеном, т.е. номером, представляющим собой комбинацию элементов, используемых при токенизации (например, идентификационный номер устройства, идентификатор стороны, запрашивающей токен, и мерчанта). Таким образом RBI намеревается защитить реквизиты карт, причем данное намерение можно заметить в рекомендациях, которые RBI дал в Положении об использовании платежных агрегаторов и платежных шлюзов от 17 марта 2020 года. Рост числа мошеннических операций и нарушений безопасности данных связывался именно с данными, которые хранились мерчантами и платежными агрегаторами. Рассматриваемые рекомендации потребовали от платежных агрегаторов и мерчантов прекратить использование реквизитов карт конечных пользователей, что, по убеждению автора, является шагом в правильном направлении.

Регулятор в сфере защиты данных в Индии

Закон об ИТ не определяет уполномоченный орган для надзора за защитой данных (как, например, уполномоченный орган по защите данных, предусмотренный в GDPR). Тем временем право давать указания по вопросам в сфере информации и технологий предоставлено Министерству электроники и ИТ (далее - MeitY). Эта организация учредила Индийский центр реагирования на компьютерные инциденты (далее - CERT), которая выступает в качестве основного органа для получения информации о нарушениях и реагирования на них. Помимо этого, в Индии нет никаких органов по надзору за соблюдением законодательства о защите данных, а организации вроде MeitY не предусматривают официальной процедуры получения разъяснений. Об инцидентах в сфере кибербезопасности, таких как несанкционированный доступ к ИТ-системам / данным и компрометация информации, юридические лица, т.е. поставщики услуг, посредники, ЦОД и ком-

9 Там же.

II. Right to rectification of errors

Owner of the sensitive data have the right to seek corrections to amendments to their SDPI in respect of inaccuracies or deficiencies under the SDPI Rules.

III. Right to erasure

The idea of being forgotten is not an alien concept. For all the good we want to be remembered but for anything bad, we also like to be forgotten. While physically we may change places in order to be forgotten, it is not so easy to be forgotten on social media, online platforms etc. Your data remains forever in public unless you request to be forgotten. The General Data Protection Regulation has greatly strengthened the right to be forgotten in Europe. Article 17 of the GDPR explicitly speaks about “Right to Erasure”. This also means right to be forgotten. This allows an individual to request their respective regulator to ensure that their personal data on them available on technology platform or elsewhere be erased.

In August 2021, in a matter, the Madras High Court dismissed a petitioner’s right to be forgotten, seeking to have his criminal and court records expunged following his acquittal from the said matter. The court dismissed the matter stating that the fulfilment of a task which is in interest of public shall trump the individual’s right to privacy. It is said that the Right to be Forgotten in India has been included in the Personal Data Protection Bill, 2019 (PDP Bill). Nonetheless, the Supreme Court ruled in the matter of Justice K.S.Puttaswamy(Retd) and Another v. Union of India, 2018 that the right to security is a fundamental right.

The Supreme Court of India held that the right to privacy is a fundamental right in a landmark judgment in 2017. “The right to security is maintained as an intrinsic element of the right to life and individual freedom under Article 21 and as a portion of the opportunities guaranteed by Part III of the Constitution..” the Court stated at the time. The case changed the contours of Indian privacy laws, the interpretation of existing privacy laws and raised the specter of a robust law for data protection. Other landmark judgment of the Supreme Court of India in the matter of data protection is R. Rajagopal and Ors vs. State of Tamil Nadu[9] which recognizes tortious remedies for breach of privacy and the ability to seek damages for invasion of privacy. Interestingly, post the Puttuswamy judgment, different High Courts in India grappled with the exercise of various dimension of privacy rights and right to erasure.

9 Writ Petition (Civil) No. 422 of 1994.

пании, должны сообщать в CERT-IN. При этом вместе с информацией о подобных инцидентах необходимо представить детальную информацию о соответствующей проблеме в сроки, достаточные для принятия своевременных мер в ее отношении. В то же время, однако, CERT-IN издала директиву, в соответствии с которой об определенных типах кибер-инцидентов (таких как целевое сканирование / зондирование критически важных сетей / систем, компрометация критически важных систем / информации, несанкционированный доступ к ИТ-системам / данным и т.д.) поставщики данных, ЦОД и др. обязаны сообщать в течение шести часов после их обнаружения.[10] При этом следует отметить, что в Индии нет никаких обязательных требований в отношении сообщения о нарушении безопасности данных субъектам персональных данных, ни в Законе об ИТ, ни в связанных с ним правилах. Вместе с тем, такие организации, как CERT-IN, могут сообщать о подобных нарушени- ях широкой общественности и прочим заинтересованным лицам для повышения уровня их осведомленности.

Административные санкции или уголовные наказания за нарушение безопасности данных

Нарушение безопасности данных может повлечь за собой административное или уголовное наказание. В соответствии с Разделом 43A Закона об ИТ, халатное отношение к соблюдению стандартов безопасности может привести к возбуждению исков о возмещении ущерба по инициативе потерпевших пользователей. Кроме того, как было сказано выше, о любом нарушении безопасности данных необходимо сообщать в CERT-IN, которая может провести расследование в отношении того, какие меры безопасности используются соответствующей организацией. Непредставление данной информации организацией может привести к штрафу в размере до 25 000 индийских рупий[11]. Кроме того, если CERT-IN запрашивает информацию, ее непредставление может стать основанием как для гражданских, так и для уголовных наказаний. В соответствии с Разделом 70B (7) Закона об ИТ, непредставление информации, запрашиваемой CERT-IN, наказывается тюремным заключением сроком на один год, или штрафом в размере до 100 000 индийских рупий, или и тем, и другим.

10 Там же.
11 Раздел 45 Закона об ИТ, 2000.

IV. Right to object processing

No such right has been explicitly provided under the IT Act and/or SDPI Rules but as per the privacy policy that each body corporate may have, one may object to processing of their sensitive personal data.

V. Right to restrict processing

No such right has been explicitly provided under the IT Act and/or SDPI Rules but as per the privacy policy that each body corporate may have, one may restrict to processing of their sensitive personal data.

VI. Right to withdraw consent

Information provider may withdraw consent given to the body corporate at any time while availing themselves of its services by giving notice in writing under the SDPI Rules. In such cases, the body corporate has the option of not providing the goods or services for which such information was sought.

VII. Right to object to marketing

The owner of the information, may choose not to be marketed without their written consent given to the body corporate. Having said that, body corporate may also choose not to provide service or goods for which such information was sought.

VIII. Right to complain to the relevant data protection authority(ies)

No such right has been explicitly provided under the IT Act and/or SDPI Rules.

DATA PROTECTION BILL AND UNDERLYING ISSUES

In 2018, the Srikrishna Committee released a 176 page report and proposed the first draft of the Personal Data Protection Bill. The draft went through several rounds of consultation processes and revision after which it was introduced in parliament in 2019 along with the Committee's recommendations. In December 2019, the Bill was sent to the Joint Parliamentary Committee for review from both Houses, which came out with its report in December, 2021[10]. The said Joint Parliamentary Commission's report paved way for India's privacy and protection of data regime. The bill was primarily modelled on GDPR and seeks to protect the personal data of individuals and establish a

10 Article "the Withdrawal of the PDP Bill and the road ahead" dated August 8, 2022 by Ayushi Kar- Business Line.

ЗАЩИТА ПРАВ ФИЗИЧЕСКИХ ЛИЦ В СФЕРЕ ОБРАБОТКИ ИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

I. Право на доступ к данным / копиям данных

В соответствии с Правилами ИТ субъект чувствительных данных имеет право в любой момент запросить возможность ознакомления с чувствительными данными, предоставленными собирающей их организации.

II. Право на исправление ошибок

В соответствии с Правилами ИТ субъект чувствительных данных имеет право запросить исправление или дополнение информации о себе в связи с неточностями или отсутствием каких-либо сведений.

III. Право на удаление данных

Идея «быть забытым» не является чуждой нам концепцией. Мы хотим, чтобы другие люди запомнили о нас все хорошее, но забыли все плохое. Физически, чтобы нас забыли, мы можем сменить место жительства, но не так-то просто быть забытым в социальных сетях, на онлайн платформах и т.д. Ваши данные навсегда останутся выставленными на всеобщее обозрение, если только вы специально не потребуете, чтобы вас «забыли». В Европе соответствующее право было весьма сильно укреплено регламентом GDPR. В Статье 17 данного документа прямо говорится о «праве на удаление данных». Это одновременно означает и «право быть забытым». Данное право позволяет физическим лицам требовать от соответствующего регулятора гарантий удаления их данных, доступных на технологических платформах или где-либо еще.

В августе 2021 года Высокий суд Мадраса отклонил ходатайство истца о «праве быть забытым», так как тот требовал удаления сведений об уголовном деле и судебных слушаниях после его оправдания по соответствующему делу. При этом суд отметил, что выполнение задачи в интересах общества в целом является более важным, чем право физического лица на неприкосновенность частной жизни. «Право быть забытым» в Индии было включено в Законопроект о защите персональных данных от 2019 года (далее - PDPB). При этом уже в ходе рассмотрения дела «Судья K.C. Путтасвами (в отставке) и другие против Индийского Союза» 2018 года Верховный суд постановил, что право на неприкосновенность личности является основополагающим.

В 2017 году Верховный суд Индии в своем прецедентном постановлении признал основополагающим и право на неприкосновенность частной жизни.

Data Protection authority to regulate all personal data related activities within India.

However, the said bill has been withdrawn in the parliament due to immense pressure and facing pushback from a range of stakeholders including big tech companies such as Facebook and Google etc and shall be brought for stakeholder's consultation once again so as to build stakeholder confidence and clear doubts on contentious provisions.

The tech companies had, in particular questioned a provision related to data localisation according to which it would have been mandatory for companies to store a copy of certain sensitive personal data within India and the export of undefined "critical" personal data from the country would be prohibited.

ENDNOTE

Despite the constant efforts of government to make data protection law as a separate discipline in India, the Indian legislature has not done enough in bringing out a comprehensive legislation pertaining to data protection. Any piecemeal legislation is insufficient to oversee the data breach of a country as vast as India. With the evolution of Information Technology ("IT"), data is the main asset and if the same is not vehemently protected, it may lead to massive repercussions in the future. The IT Act of India is a generic legislation which does not explicitly and exclusively covers personal data protection in India. There is no actual legal framework for personal data protection, data quality, transparency etc. There is a need for single statute legislation. Lack of awareness on the importance and impact of personal data may be called into question but only after introduction of a comprehensive legislation. Considering India's growth in the global digital economy, government of India will have to introduce a framework that brings stringent data protection laws at par with the other leading jurisdictions. Further, a growing international consensus also suggests that next-generation innovation in technology needs regulations pertaining data protection in place.

В этом постановлении говорится: «Право на неприкосновенность личности является неотъемлемым элементом права на жизнь и свободу личности в соответствии со Статьей 21 и входит в состав возможностей, гарантируемых Частью III индийской Конституции». Это изменило контуры действия индийских законов о неприкосновенности частной жизни и их толкование, а также расширило спектр эффективных законов для защиты данных. Еще одним прецедентным постановлением Верховного суда Индии по вопросу о защите данных является постановление по делу «Р. Раджагопал и другие против Штата Тамилнад»[12], в котором признаются деликтные меры юридической защиты, применяемые в случае нарушения неприкосновенности частной жизни, и возможность требования возмещения ущерба за вторжение в частную жизнь. Что интересно, после вынесения решения по делу «Путтасвами», разные Высокие суды Индии стали обращать внимание на различные аспекты права на неприкосновенность частной жизни и права на удаление данных.

IV. Право на возражение против обработки

Ни Законом об ИТ, ни Правилами ИТ подобное право явным образом не предусматривается, но в соответствии с политиками обеспечения конфиденциальности, которые могут приниматься отдельными организациями, физические лица могут возражать против обработки своих конфиденциальных персональных данных.

V. Право на ограничение обработки

Ни Законом об ИТ, ни Правилами ИТ подобное право явным образом не предусматривается, но в соответствии с политиками обеспечения конфиденциальности, которые могут приниматься отдельными организациями, физические лица могут требовать ограничения обработки своих конфиденциальных персональных данных.

VI. Право на отзыв согласия

Субъект данных может в любой момент отозвать свое согласие, данное юридическому лицу при использовании его услуг, путем направления ему соответствующего письменного уведомления в соответствии с Правилами ИТ. В подобных случаях юридическое лицо может отказаться от предоставления товаров или услуг, для которых требуется соответствующая информация.

12 См. выше.

Secretariat Building, New Delhi

VII. Право на возражение против использования данных в целях маркетинга

Субъект данных имеет право на то, чтобы его персональные данные не использовались в целях маркетинга без его письменного согласия, данного организации. При этом такая организация может отказаться от предоставления товаров или услуг, для которых требуется соответствующая информация.

VIII. Право на направление жалоб в соответствующие органы по надзору за соблюдением законодательства о защите персональных данных

Ни Законом об ИТ, ни Правилами ИТ подобное право явным образом не предусматривается.

ЗАКОНОПРОЕКТ О ЗАЩИТЕ ДАННЫХ И ЕГО ОСНОВНЫЕ МОМЕНТЫ

В 2018 году Комитет Шрикришны выпустил 176-страничный доклад и предложил первый проект Закона о защите персональных данных (далее — PDPB). Этот проект прошел несколько раундов обсуждений и рассмотрений, после чего был представлен в парламенте в 2019 году вместе с рекомендациями Комитета. В декабре 2019 года PDPB был направлен обеими палатами на рассмотрение в Объединенный парламентский комитет, который опубликовал соответствующий доклад в декабре 2021 года[13]. Этот доклад создал условия для формирования в Индии режима обеспечения неприкосновенности частной жизни и защиты данных. Законопроект преимущественно был составлен по образу регламента GDPR и был направлен на защиту персональных данных физических лиц, а также на учреждение органа по надзору за соблюдением законодательства о защите персональных данных, который мог бы регулировать всю деятельность в сфере персональных данных на территории Индии.

Однако рассматриваемый законопроект был отозван по причине очень серьезного давления и противодействия со стороны весьма широкого круга заинтересованных сторон, включая такие крупные технологические компании, как Facebook и Google, и будет направлен на новый тур консультаций с заинтересованными сторонами, с целью, чтобы повысить их уверенность и устранить сомнения по поводу спорных положений.

13 Там же.

В частности, технологические компании ставили под сомнение положения о локализации данных, в соответствии с которыми компании были бы обязаны хранить копию определенных чувствительных персональных данных на территории Индии, а экспорт неких «критически важных» персональных данных из страны был бы запрещен.

ЗАКЛЮЧЕНИЕ

Несмотря на постоянные усилия правительства Индии, направленные на превращение защиты данных в отдельную отрасль права, индийские законодательные органы пока не создали всестороннего законодательства в данной сфере. Отдельных законодательных актов для контроля за нарушением безопасности данных в такой огромной стране, как Индия, конечно, недостаточно. С развитием информационных технологий (далее — ИТ) данные становятся главным активом и, если их не защищать должным образом, это может привести к весьма серьезным последствиям в будущем. Индийский Закон об ИТ представляет собой нормативный правовой акт самого общего характера, в котором прямо не говорится именно о защите персональных данных в Индии. На данный момент в стране по сути нет никакой нормативно-правовой базы для защиты персональных данных, обеспечения их качества, прозрачности и т.д. Как следствие, существует потребность в едином законодательном акте в данной сфере. При этом, конечно, можно поднять вопрос и о недостаточной осведомленности о важности и влиянии персональных данных, но только после принятия всестороннего законодательства. Учитывая развитие Индии в рамках мировой цифровой экономики, правительству Индии будет необходимо создать нормативно-правовую базу, состоящую из строгих законов о защите данных, ничем не уступающих законам, принятым в других ведущих юрисдикциях. Кроме того, укрепление международного консенсуса в рассматриваемой сфере также указывает на то, что для технологических инноваций нового поколения необходимы нормативные правовые акты, касающиеся защиты данных.

автор
Shilpa Thakur

Законный интерес
как основание обработки персональных данных

«Нельзя обрабатывать персональные данные без согласия» — Вы наверняка слышали этот широко распространённый тезис. Для многих может оказаться неожиданным, что это всего лишь очередное широко распространенное заблуждение. Федеральный закон от 27.07.2006 года №152-ФЗ «О персональных данных» (далее — Закон №152-ФЗ) предусматривает 12 различных оснований для обработки персональных данных, и согласие субъекта — лишь одно из них. В частности, закон допускает обработку персональных данных без согласия физического лица, если это необходимо для исполнения требований законодательства, заключения или исполнения договора с физическим лицом и в целом ряде других случаев.

В настоящей статье мы детальней остановимся на таком основании для обработки персональных данных, как осуществление прав и законных интересов оператора. Рассмотрим наглядный пример, где согласия будут являться избыточными.

Например, при организации пропускного режима в бизнес-центре, чтобы исключить несанкционированный доступ, обеспечить сохранность имущества, часто осуществляется запись тех лиц, которые проходят на территорию такого бизнес-центра. Сбор согласий в таком случае будет являться избыточным, поскольку в данном случае обработка персональных данных осуществляется для сохранности имущества бизнес-центра и взыскания убытков, которые могут причинить посетители.

Если предположить, что в данном случае бизнес-центр организует обработку персональных данных на основании согласий, то он должен будет, следуя букве закона, прекратить обработку персональных данных после отзыва согласия. Кроме того, а что если субъект не захочет давать согласие на обработку персональных данных? Его нельзя будет пропустить в бизнес-центр?

В соответствии с п.1 ст.9 Закона № 152-ФЗ) каждый субъект принимает решение о предоставлении его персональных данных и даёт согласие на их обработку свободно, своей волей и в своём интересе. Учитывая, что посетитель бизнес-центра вынужден давать согласие на обработку своих персональных данных не в своём интересе, а под принуждением (поставлен перед выбором, дать согласие и пройти в бизнес-центр или не давать согласие и не попасть в бизнес-центр, где, например, у него назначена важная встреча), возникают сомнения в добровольности такого согласия. Кроме того, согласие не будет соответствовать принципам Закона № 152-ФЗ (обработка персональных данных должна осуществляться на законной и справедливой основе), и возникнет риск неправомерной обработки персональных данных.

Анализ других правовых оснований, предусмотренных 152-ФЗ (кроме п. 7 ч. 1 ст. 6 152-ФЗ), также указывает на их неприменимость. В частности, пункт 2 части 1 статьи 6 152-ФЗ допускает обработку персональных данных для достижения целей, предусмотренных законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей. Однако закона, который обязывал бы все бизнес-центры организовывать пропускной режим не существует. Рассматривая другие правовые основания обработки, необходимо также рассмотреть пункт 5 части 1 статьи 6 152-ФЗ, который допускает обработку персональных данных для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных. Однако доступ в бизнес-центр не предполагает заключение подобного рода договоров. Подобные вопросы возникают и в целом ряде других случаев, в которых осуществляется обработка персональных данных: в рамках обеспечения безопасности банковских операций, при обработке данных в доверенности, при оценке деловой репутации партнеров и так далее.

Представляется, что правильным решением для таких и иных подобных случаев будет применение нормы пункта 7 части 1 статьи 6 152-ФЗ, а именно исходить из того, что обработка персональных данных является допустимой без отдельного согласия, как необходимая для осуществления прав и законных интересов оператора.

Российский закон текстуально близок к европейскому закону — Общему Регламенту по защите данных (*General Data Protection Regulation*), где применение законного интереса оператора в качестве правового основания для обработки персональных данных широко распространено. Однако практика применения этого основания в Европе и в России кардинально отличается: если в Европе такое основание широко применяется, то в России Роскомнадзор не издал никаких официальных разъяснений по применению этого основания, что многими российскими компаниями толкуется как невозможность применения указанного основания. Таким образом, сложилась интересная ситуация — норма в законе есть, но из-за её абстрактности никто не понимает, как её применять и можно ли ее применять вообще. Однако в отличие от Роскомнадзора, суды применяют законный интерес как основание для обработки персональных данных при рассмотрении конкретных споров. Опираясь на судебную практику, можно сделать вывод о допустимости применения указанного правового основания, например, при предоставлении акционеру документов о деятельности общества, при предоставлении реестров собственников помещений многоквартирного дома инициативным группам граждан для проведения общих собраний собственников и в ряде других случаев. Таким образом отдельные судебные решения допускают применение указанного законного основания в отдельно взятых ситуациях, тем не менее общей проблемы они не решают.

Учитывая вышесказанное, представляется, что применение законного интереса как основания обработки персональных данных является допустимым, однако к его применению необходимо подходить максимально аккуратно, проводя в каждом случае оценку допустимости применения законного интереса. Лучшей практикой в данном случае можно считать подход, разработанный в Сбере и одобренный для включения в «Белую книгу» лучших практик Ассоциации Больших Данных.[1] Данный подход закреплен во внутреннем нормативном документе Банка[2] и предполагает проведение отдельной оценки и фиксацию её результатов в наиболее нетипичных ситуациях. В типовых же случаях, если состав данных и цели обработки совпадают с перечнем зафиксированных заранее типовых случаев — оценка может не проводиться. Такой подход позволяет не только более тщательно проверить применимость данной нормы для конкретной ситуации, но и заранее подготовить позицию для проверяющих или суда.

Подход Сбера состоит в следующем:

При проведении оценки применимости законного интереса в качестве основания обработки персональных данных следует рассматривать следующие критерии:

A. Идентификация цели и определение соответствия цели правам и законным интересам оператора или третьего лица.

B. Необходимость обработки персональных данных для достижения цели.

C. Отсутствие нарушения прав и свобод субъекта персональных данных.

Указанные критерии следуют из прямого толкования нормы пункта 7 части 1 статьи 6 152-ФЗ и систематического толкования 152-ФЗ. Оценка должна считаться пройденной успешно только при одновременном соответствии всем трём критериям.

1. Идентификация цели и определение соответствия цели правам и законным интересам оператора или третьего лица.

В соответствии с пунктом 7 части 1 статьи 6 152-ФЗ обработка персональных данных допускается если такая обработка «необходима для осуществления прав и законных интересов оператора или третьих лиц, … либо для достижения общественно значимых целей…». Оценка на соответствие данному критерию подразумевает формулирование конкретной цели обработки персональных данных и проверку соответствия её достижения осуществлению прав и законных интересов оператора или третьего лица. При этом преследуемый в рамках обработки интерес не должен нарушать запретов и противоречить требованиям, установленным законодательством РФ.

1 «Белая книга: Свод лучших практик в сфере добросовестного использования данных// Центр стратегических разработок [Электронный ресурс] URL: https://www.csr.ru/upload/iblock/8d0/pztil1xd1v6ae91lmhby30qyah3ee7ds.pdf (дата обращения 09.09.2022).
2 Памятка по проведению оценки применимости законного интереса в качестве основания обработки персональных данных от 08.07.2021 N П-382// SCS- методология [Электронный ресурс] URL: https://confluence.sberbank.ru/pages/viewpage.action?pageId=5187472119 (дата обращения 09.09.2022).

2. Необходимость обработки персональных данных для достижения заявленной цели.

Данный критерий вытекает из ч.2 ст.5 152-ФЗ: *«2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определённых и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных».*

Оценка данного критерия предполагает анализ альтернативных способов достижения цели обработки персональных данных, возможности отказа от обработки избыточных атрибутов, возможность применения других оснований обработки персональных данных. Наряду с этим, необходимость обработки персональных данных для осуществления прав и законных интересов оператора или третьего лица должна прямо или косвенно следовать из действующего законодательства, а также сложившейся на рынке практики (при условии отсутствия предписаний со стороны регулятора в отношении операторов, применяющих такие практики).

3. Отсутствие нарушений прав и свобод субъекта персональных данных.

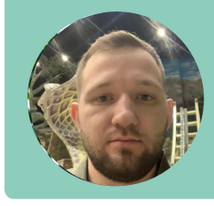
Данный критерий вытекает из самой нормы, которая завершается оговоркой, что основание применимо «…при условии, что при этом не нарушаются права и свободы субъекта персональных данных».

При оценке данного критерия необходимо помнить, что цель 152-ФЗ — это обеспечение защиты прав и свобод гражданина при обработке его персональных данных. Российское законодательство не предусматривает право субъекта отказаться от обработки персональных данных, если обработка осуществляется с целью защиты прав и законных интересов оператора, поэтому крайне важно определить, имеет ли место нарушение прав и свобод гражданина при обработке его персональных данных.

Заключение

Несмотря на то, что закон не устанавливает четких критериев к применению законного интереса как основания для обработки персональных данных, необходимо понимать, что при отсутствии официальных разъяснений от регулятора и недостаточно наработанной судебной практики, применение данного основания все-таки возможно. Однако применение данного основания (применения законного интереса) не должно подменять собой другие основания обработки персональных данных и должно опираться на принципы и требования, заложенные в законодательстве о персональных данных, а также на лучшие практики применения законного интереса как в России, так и за её пределами.

авторы
Константин Малофеев



Антон Фишер

SCS SBER CYBER SECURITY

РЕДАКЦИЯ

Амина Замулина
редактор

Евгений Щербатов
дизайн, вёрстка, обложка

АВТОРЫ

Алексей Савичев

Константин Малофеев

Евгений Сердечнюк

Олег Беляев

Михаил Воробьёв

Shilpa Thakur
Филиал ПАО Сбербанк в Индии

Антон Фишер

SBER PRIVACY
JOURNAL
ВЫПУСК №2 | СЕНТЯБРЬ 2022

SCS SBER CYBER SECURITY