УДК 342.721

12.00.00 Юридические науки

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В РОССИИ И ЗА РУБЕЖОМ

Параскевов Александр Владимирович
РИНЦ SPIN-код = 2792-3483

Левченко Александра Владимировна
Студентка факультета прикладной информатики

Кухоль Юрий Алексеевич
Студент юридического факультета
ФГБОУ ВПО Кубанский государственный аграрный университет, г.Краснодар, Россия

В современном демократическом обществе права человека и, в частности, право на неприкосновенность частной жизни имеют первостепенное значение. Сведения о гражданах собираются и аккумулируются различными государственными (органы внутренних дел, бюро технической инвентаризации, органы актов гражданского состояния, медицинские учреждения, органы регистрации прав на недвижимое имущество и сделок с ним, органы регистрации юридических лиц и др.) и частными структурами (сотовые компании, частные образовательные, медицинские, юридические организации и т.д.) при рождении и получении документов, удостоверяющих личность, при поступлении на работу, при обращении в медицинские учреждения, при покупке недвижимого имущества (квартир, машин), при создании частных предприятий, в иных случаях. Совершая покупки в интернет - магазинах, потребитель вынужден сообщать свои персональные данные. Однако владельцы таких магазинов не всегда обеспечивают охрану персональных данных (в том числе банковских карт), а отсутствие соответствующего закона создает пробел в правовом регулировании. К самим же персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие

Ключевые слова: ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ЗАЩИТА ДАННЫХ, ЮРИДИЧЕСКАЯ СИСТЕМА, МОДЕЛЬ ПРАВОВОГО РЕГУЛИРОВАНИЯ, КАТЕГОРИИ ПЕРСОНАЛЬНЫХ ДАННЫХ,

UDC 342.721

Legal science

COMPARATIVE ANALYSIS OF LEGAL REGULATION OF PERSONAL DATA PROTECTION IN RUSSIA AND ABROAD

Paraskevov Alexander Vladimirovich
SPIN code = 2792-3483

Levchenko Alexandra Vladimirovna
Student of the Applied informatics department

Kuhol' Jurij Alekseevich
Student of the Law department
Kuban State Agrarian University, Krasnodar, Russia

In modern democratic society human rights and, in particular, the right to privacy is of paramount importance. Information about citizens is collected and accumulates various government (the Ministry of internal Affairs, Bureau of technical inventory authorities of acts of civil status, medical institutions, agencies of registration of rights to immovable property and transactions with it, the bodies of registration of legal entities, etc.) and private entities (cell companies, private educational, medical, legal organizations, etc.) at birth and receiving documents, identity when applying for a job, when applying to a medical institution, for the purchase of immovable property (apartments, cars), for the establishment of private enterprises in other cases. When making purchases in online stores, a consumer is forced to disclose their personal data. However, the owners of these shops do not always ensure the protection of personal data (including credit cards), and the absence of law creates a gap in legal regulation. To the very same personal data includes biographical and identifying data, personal characteristics, information about family, social status, education, profession, career and financial situation, health condition and other

Keywords: PERSONAL DATA, DATA PROTECTION, LEGAL SYSTEM, MODEL OF LEGAL REGULATION, CATEGORIES OF PERSONAL DATA, INTERNATIONAL PRACTICE

МЕЖДУНАРОДНАЯ ПРАКТИКА

Определение персональных данных.

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

В современном демократическом обществе права человека и, в частности, право на неприкосновенность частной жизни имеют первостепенное значение. Изменения, связанные с регулированием персональных данных (информации о личной жизни человека), происходят сейчас во многих государствах.

Причин этому достаточно много: глобализация бизнеса (передача персональных данных между странами), активное использование цифровых, в том числе, мобильных, технологий, рост сетевого пиратства и борьбы с ним, быстрое расширение социальных сетей и иных медиа, увеличивающееся стремление государств контролировать сетевые, массовые коммуникации, заинтересованность бизнеса в реализации интернет-рекламы, повышении ее эффективности, и так далее.

Существует множество подходов, которых придерживаются государства, устанавливающие правоотношения в сфере персональных данных: от максимальной защиты неприкосновенности таких данных, до почти полного отрицания права на анонимность в сетевых коммуникациях.

Но, если подумать, иногда именно раскрытие персональных данных в интересах правообладателей зачастую становится самым распространенным и самым надежным инструментом защиты интеллектуальных прав. Такое раскрытие требуется при сборе сведений о тех лицах, которые скачивают или распространяют контрафактные произведения, и при установлении глобальных систем контроля и

фильтрации потребляемого трафика, и при введении запретов на доступ к определенным сайтам пользователям из определенных стран, и при внедрении прав доступа к контенту в отношении различных групп пользователей, и в ряде иных случаев.

Получается, что любой стране выгодно максимальное использование персональных данных, которое позволяет настраивать глобальные, технологически эффективные, экономичные системы защиты прав на объекты интеллектуальной собственности. Но именно они чаще всего граничат с нарушением основополагающих прав человека.

Поэтому представляется весьма важным и интересным изучение тенденций изменения правового регулирования персональных данных.

А тот факт, что подобные изменения сейчас активно обсуждаются и внедряются во многих странах, причём сразу в обеих сферах, не вызывает никаких сомнений.

Углубимся в суть. Сведения о гражданах собираются и аккумулируются различными государственными (органы внутренних дел, бюро технической инвентаризации, органы актов гражданского состояния, медицинские учреждения, органы регистрации прав на недвижимое имущество и сделок с ним, органы регистрации юридических лиц и др.) и частными структурами (сотовые компании, частные образовательные, медицинские, юридические организации и т.д.) при рождении и получении документов, удостоверяющих личность, при поступлении на работу, при обращении в медицинские учреждения, при покупке недвижимого имущества (квартир, машин), при создании частных предприятий, в иных случаях. Совершая покупки в интернет - магазинах, потребитель вынужден сообщать свои персональные данные. Однако владельцы таких магазинов не всегда обеспечивают охрану персональных данных (в том числе

банковских карт), а отсутствие соответствующего закона создает пробел в правовом регулировании.

К самим же персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном, социальном положении, образовании, профессии, служебном и финансовом положении, состоянии здоровья и прочие.

Первоначально на проблему защиты персональных данных на международном уровне обратила внимание Организация по экономическому сотрудничеству и развитию (ОЭСР), принявшая в 1980 г. Директиву о защите неприкосновенности частной жизни и международных обменов персональными данными. В дальнейшем эти принципы были детализированы в Конвенции Совета Европы «Об охране личности в отношении автоматизированной обработки персональных данных» (1981 г.), в Директиве Европейского сообщества о защите граждан в плане обработки информации личного характера от 27 июля 1990г., в Директиве Европейского Союза и Парламента 95/46/ЕС от 24 октября 1995 г. о защите прав частных лиц применительно к обработке персональных данных и свободном движении таких данных и Директиве 97/66/ЕС от 15.12.97 по обработке персональных данных защите, конфиденциальности в телекоммуникационном секторе. В данных актах были определены основные принципы организации обработки данных личного характера и обеспечения права граждан на защиту персональных данных. Такие как:

- данные персонального характера должны быть собраны только для определенных целей и в строгом соответствии с законом;
- данные должны соответствовать требованиям, быть точными, полными и вовремя обновленными;

- цели, для достижения которых собираются и обрабатываются персональные данные, должны быть определены и утверждены до начала деятельности и использоваться только в этих целях;

- в системах учета персональных данных должны быть внедрены механизмы, предотвращающие потери или неправильное (или злоумышленное) использование персональных данных;

- деятельность организаций (как государственных, так и частных), имеющих базы данных, содержащих персональные данные, должна быть открытой;

- держатели данных должны быть подконтрольными для обеспечения соблюдения настоящих принципов, для этих целей должно быть предусмотрено создание независимого контролируемого органа как важного элемента защиты личности при автоматизированной обработке информации личного характера.

Исходя из всего вышесказанного, можно смело говорить о важности практики иностранных государств по правовой защите информации о неприкосновенности частной жизни и, более конкретно, вопросы защиты компьютерных баз данных и свободы информации. Такая практика, в большей степени, разработана в странах континентальной Европы (особенно в Германии) и в меньшей - в Канаде и Соединенных Штатах.

Особенности правового регулирования защиты персональных данных в России и за рубежом.

Модели правового регулирования защиты персональных данных.

Рассмотрим регулирование правил защиты персональных данных на федеральном и региональном уровне в различных странах и наличие

органа власти по контролю за соблюдением требований по защите персональных данных. Существует два типа систем правого регулирования: децентрализованная и централизованная.

Децентрализованная система.

Признаки:

- отсутствие единого подхода к защите персональных данных в рамках отраслевого законодательства;

- регламентация защиты персональных данных осуществляется посредством профильных нормативных актов комплексных отраслей законодательства (здравоохранение, финансовый сектор) и/или на разных уровнях власти (например, в США Health Insurance Portability and Accountability Act (HIPAA 1996) и Gramm-Leach-Bliley Act (GLB 1999));

- акты рекомендательного характера играют значительную роль (методики, + индустриальные стандарты);

- отсутствие единого надзорного органа.

Примеры: США, Канада и Австралия.

Централизованная система.

Признаки:

-прямое действие международных норм, гармонизирующих национальные законодательства государств (Конвенция о защите физических лиц при автоматизированной обработке персональных данных, Директива 95/46/ЕС, Директива 2002/58/ЕС);

-наличие национальных отраслевых законов, содержащих общеобязательные нормы в отношении защиты персональных данных (например, в Германии Bundesdatenschutzgesetz (BDSG));

-регулирование обработки персональных данных посредством учреждения единого надзорного ведомства («мегарегулятора»).

Страны ЕС, Израиль, Мексика, Гонконг, Швейцария, Сингапур

Также можно выделить **смешанную систему** правового регулирования.

Признаки:

Наличие одного или нескольких признаков, позволяющих отнести систему правого регулирования защиты персональных данных государства к централизованной или децентрализованной системе.

В Японии и на Тайване действуют единые законы о защите персональных данных, отсутствуют единые надзорные ведомства, применяются акты рекомендательного характера.

В Бразилии правовое регулирование осуществляется на основании общих норм, конституционных принципов и непрофильных законов, при этом присутствует единый надзорный орган. В Гражданском кодексе предусмотрено также, что физическое лицо может просить помощи в связи с любой угрозой его личным правам и что частная жизнь физического лица является неприкосновенной. Широкую защиту предоставляет также Кодекс защиты прав потребителей. Он, в частности, предусматривает права потребителей на доступ к любым зарегистрированным персональным данным и на внесение в них исправлений.

Также хочется сказать, что Бразилия вместе с Германией продвинула в ООН первую резолюцию, посвящённую защите персональных данных в интернете. В ней говорилось, что право на неприкосновенность частной жизни должно обеспечиваться как в реальной жизни, так и в Сети. Для страны, где электронную переписку защищают по тем же правилам, что и обычную, это совсем не удивительный подход.

Южная Америка также переживает настоящий бум интернет - законотворчества. Проекты рассматриваются месяцами, а то и годами. В авангарде находится Аргентина, признанная Еврокомиссией единственной

страной, в полной мере выполняющей требования по защите персональных данных в интернете.

В Южной Африке нет специальных законов о защите данных, однако в ее Конституции закреплено право на конфиденциальность. Положения, касающиеся личной информации, содержатся также в Законе о защите прав потребителей 2008 года и в Законе об электронных коммуникациях и сделках 2002 года. Соблюдение норм последнего закона носит добровольный характер и должно быть отражено в соглашении с субъектом данных.

Что касается скандинавских стран, то у них в той или иной форме принято законодательство по защите компьютерных банков данных. И в этом плане Швеция является примером для подражания - она первая приняла закон о свободе информации («О свободе изданий», 1776 г., который в 1949г. был модифицирован в закон о свободе печати, а в настоящее время является составной частью Конституции Швеции и гарантирует всем гражданам страны свободу получения информации в государственных органах на безвозмездной основе) и первая ввела законодательство по защите информации частного характера (в редакции Закона о конфиденциальности 1998 г. (Personuppgiftslagen)), хранящейся в компьютерных банках данных. Законодательство по защите компьютерных баз данных Швеции и Дании (Закон о защите данных 1979 года в редакции Закона об обработке персональных данных 2000 г. (Lov om behandling af personoplysninger)) главным образом ориентировано на компьютерную информацию в частном секторе.

В Китае принято множество релевантных актов иной отраслевой принадлежности, а также развито подзаконное регулирование, высока роль документов рекомендательного характера.

В Саудовской Аравии нет специальных законов о защите данных, хотя право на конфиденциальность закреплено в ряде ее законов. В частности, в Основном низаме правления Саудовской Аравии закреплён основной принцип, согласно которому вся переписка и все виды связи между сторонами строго конфиденциальны и раскрывать их не следует.

В отсутствие применимого законодательства суды руководствуются нормами шариата (исламского права). На основании норм шариата может быть предъявлен иск за ущерб, причинённый в связи с незаконным раскрытием личной информации физического лица, если раскрытие информации принесло убытки физическому лицу или нанесло ему вред.

В Объединённых Арабских Эмиратах нет специальных законов о защите данных, однако право на конфиденциальность закреплено в Конституции и в различных законах. В Конституции ОАЭ указано, что физическому лицу «гарантируется свобода и конфиденциальность переписки, передачи телеграфных сообщений и других средств связи в соответствии с законом». Кроме того, в Уголовном кодексе закреплены некоторые права на конфиденциальность и на защиту персональных данных.

В Индии отсутствует конституционное право на конфиденциальность, хотя Верховный суд постановил, что принцип конфиденциальности следует считать составляющей права на жизнь и личную свободу. Сбор и обработка персональных данных регламентируются Законом об информационных технологиях 2000 года, в котором указано, что компании должны принимать адекватные меры безопасности при обработке персональных данных и что при получении таких данных в соответствии с договором их нельзя раскрывать без согласия субъекта данных в нарушение договора.

Япония является членом Азиатско-Тихоокеанского экономического сотрудничества (АТЭС) и поддерживает его политику конфиденциальности. Сбор и использование персональных данных в Японии регламентируются Законом о защите личной информации. Он касается всех видов обработки данных, однако применяется лишь тогда, когда речь идет об информации, принадлежащей 5000 и более физических лиц. Этот закон устанавливает общие требования к разрешениям, безопасности и предоставлению информации, а также дополнительные требования по контролю за работниками и третьими лицами, занимающимися обработкой персональных данных.

Австралия - есть регулирование как на федеральном, так и на региональном уровнях. Федеральный документ:

• The Federal Privacy Act 1988.

• The Privacy Amendment (Enhancing Privacy Protection) Act 2012.

Региональные документы:

• Information Act 2002 (Northern Territory).

• Privacy and Personal Information Protection Act 1998 (New South Wales).

• Information Privacy Act 2009 (Queensland).

• Personal Information and Protection Act 2004 (Tasmania).

• Information Privacy Act 2000 (Victoria).

Орган по контролю за защитой ПДн -The Office of the Australian Information Commissioner.

Страны, которые сильнее выделяются на уровне других, отметим отдельно:

Канада - с практической точки зрения большой интерес вызывает Канадский Закон об охране персональной информации, который

предусматривает реальные механизмы защиты персональных данных и реализации права на доступ к сведениям о себе.

В соответствии с этим актом под персональной понимается информация о конкретном индивиде, записанная в любой форме, в том числе данные о национальности, расе, цвете кожи, религии, возрасте, образовании, состоянии здоровья, финансах, личных взглядах и т.п. Под действие акта не попадает информация об индивиде, который был или является сотрудником государственного учреждения, его должности, служебном адресе и телефоне, уровне зарплаты и служебных обязанностях. Персональная информация не может быть использована без согласия индивида и помимо целей, ради которых она собиралась. В ряде случаев персональная информация может быть раскрыта, например, по решению суда, для члена парламента, который помогает этому индивиду, в целях передачи в архив, сбора статистических данных.

Каждый гражданин или постоянно проживающий в Канаде человек может получить доступ к информации о себе, содержащейся в учреждениях, и исправить ее, если считает неверной.

В случае возникновения спорных ситуаций граждане могут опротестовать действия властей в офисе Комиссара по защите персональной информации, который является специальным чиновником, назначаемым и ответственным перед парламентом. Он наблюдает за исполнением данного закона, т.е. за сбором, использованием и распространением государством персональной информации о клиентах и работниках, а также рассматривает жалобы.

В итоге: есть регулирование как на федеральном, так и не региональном уровнях.

Основные документы:

• Personal Information Protection and Electronic Documents Act (“PIPEDA”);

• Personal Information Protection Act (“PIPA Alberta”);

• Personal Information Protection Act (“PIPA BC”);

• An Act Respecting the Protection of Personal Information in the Private Sector («Quebec Privacy Act»).

В каждом регионе присутствует свой орган по контролю:

• Office of the Privacy Commissioner of Canada (PIPEDA);

• Office of the Information and Privacy Commissioner of Alberta (PIPA Alberta);

• Office of the Information and Privacy Commissioner for British Columbia (PIPA BC);

• Commission d’accès à l’information du Québec (Quebec Privacy Act).

Так же организации должны сообщить о произошедших утечках ПДн только в провинции Альберте. Для других областей планируется введение подобных требований.

Германия. В Европе лидером в сфере правового регулирования персональных данных является Германия. Первый закон о защите персональных данных был принят в Германии в земле Гессен в 1970 году. До этого подобных законов нигде в мире не было. За ним последовало принятие в 1977 году Федерального закона о защите персональных данных, который в 1990 году был пересмотрен.

Все 16 земель Германии имеют собственные законы о защите персональных данных, распространяющиеся на государственный сектор административного управления землями. Контроль за исполнением закона осуществляет Федеральная комиссия по защите персональных данных. Соответствующие комиссии, обеспечивающие исполнение местных законов о защите персональных данных, есть в каждой земле Германии. В

частном секторе, однако, надзор осуществляется органом, указанным в законе, действующим в каждой из земель (обычно назначается комиссар по защите персональных данных). Кроме того, почти все германские законы, которые прямо или через поправки затрагивают проблему обращения с персональными данными физических лиц, содержат либо ссылки на соответствующий закон о защите персональных данных, либо специальные положения о правилах обращения с персональными данными, отражающие право на неприкосновенность частной жизни.

Персональные данные полагается получать непосредственно от субъекта данных, кроме тех случаев, когда данные требуются по закону в действительных коммерческих целях, либо когда для получения данных непосредственно от субъекта требуются неоправданно большие усилия и нет указаний на то, что интересы субъекта данных будут этим затронуты. Кроме того, в Федеральном законе о защите данных уделяется особое внимание разработке систем защиты данных, направленных на минимизацию объемов обрабатываемых персональных данных, например путем предоставления субъекту данных анонимного статуса или использования псевдонимов.

В итоге: Закон о защите данных: Федеральный акт о защите данных (Bundesdatenschutzgesetz – BDSG 2001).

Надзорный орган: Уполномоченное лицо Федеральной комиссии по защите данных.

Основные полномочия надзорного органа: обеспечить выполнение положений Акта:

- уполномоченное лицо обязано контролировать исполнение положений Акта, что дает ему право доступа к информации, а также возможность проверять все документы и право доступа на территорию любых официальных учреждений в любое время (ст.24);

- уполномоченное лицо может подавать жалобы в высшие инстанции (например, в компетентный высший федеральный орган), в случае нарушений законодательства о защите данных (ст.25);

- федеративное правительство может подавать запрос к Уполномоченному лицу, с целью получения рекомендаций по вопросам, связанным с законодательством о защите данных (ст.26).

Право уведомлять надзорный орган о нарушениях: имеет любое лицо.

Санкции, которые может наложить надзорный орган, в случае нарушения законодательства о защите данных: штрафы и заключение.

Необходимость получения разрешения на осуществление деятельности по обработке данных. Альтернатива, при которой получение разрешения является невозможным или нецелесообразным: Достаточно использовать альтернативные методы даже в тех случаях, когда это возможно или целесообразно.

Регулирование на федеральном уровне: Европейская директива 95/46/EC реализована в Federal Data Protection Act (Bundesdatenschutzgesetz in German) “BDSG”. Организации должны предпринимать необходимые шаги для защиты данных, от несанкционированного доступа и нарушений политик обработки.

Соединенные Штаты Америки. В отличие от большинства ведущих европейских стран, в Соединенных Штатах Америки до сих пор отсутствует общее (федеральное) законодательство о персональных данных. В случае же нарушения прав субъектов персональных данных применяются положения Конституции и практика прецедентного права, преобладающего в США.

Отказ от общего закона связывают с особой экономической и политической культурой, где власти способствуют саморегуляции бизнеса.

Так, свободу слова в конституции США гарантирует первая поправка, а право на неприкосновенность частной жизни напрямую в ней не прописана и только подразумевается. Но эти принципы не мешают инициативам на уровнях штатов. Известно, что общее законодательство в Соединенных Штатах, в большинстве своем, направлено на регулирование деятельности государственных органов, входящих в структуру исполнительной власти, с целью создания прозрачного механизма управления и подотчетности обществу.

Это в полной мере относится к сфере обработки персональных данных, где основными действующими документами являются Privacy Act of 1974 и Privacy Protection Act of 1980, регулирующие деятельность органов государственной власти при обработке персональных данных граждан. Однако, упомянутые нормативные акты, не всегда отвечают стремительно меняющимся условиям современного мира, характеризующегося международной интеграцией и колоссальным прогрессом в области информационных технологий.

Ещё одной из отличительных черт защиты данных в США является, так называемый зонтичный подход, обеспечивающий адекватную защиту данных в отдельных областях (отраслях; при исполнении отдельных договоров), который основан на использовании общего законодательства, отраслевых подзаконных актов и рекомендаций по защите информации, выраженных в т.ч. в примерах договоров. Примером такого зонтичного соглашения служит US Department of Commerce's Safe Harbor Privacy Principles (Принципы защиты информации Министерства торговли США) и Transfer of Air Passenger Name Record (PNR) Data (передача данных таможне и пограничной службе США) где, по заключению Еврокомиссии, обеспечивается адекватная защита данных.

В качестве рекомендаций по обеспечению защиты данных широко применяются документы «Дирекции управления и бюджета» (OMB — Office of Management and Budget) и «Национального института стандартов и технологий» (NIST - National Institute of Standards and Technology). Указанные нормативные акты регулируют деятельность по защите персональных данных в государственных структурах, для коммерческих же организаций они носят рекомендательный характер. В качестве борьбы с утечками конфиденциальной информации был задействован следующий механизм: каждый штат принимает закон, обязывающий компании сообщать о любых утечках информации. К 2008 году такие законы были приняты практически во всех штатах США, однако реально снизить количество нарушений такими мерами не удалось, о чем свидетельствует статистика утечек конфиденциальной информации за 2008 год.

Очередным шагом к централизованному регулированию отношений, связанных с обработкой персональных данных граждан, является документ NIST Special Publication 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Draft), проект которого вышел в свет в январе 2009 года. Цель документа - помощь государственным организациям и федеральным агентствам в защите персональных данных граждан.

NIST Special Publication 800-122 содержит общие рекомендации по защите персональных данных и ссылается на многочисленные нормативно-правовые акты внутреннего законодательства США, в которых отражены различные организационные, технические, юридические аспекты защиты ПДн.

Дополнительные меры защиты: уменьшение объемов обрабатываемых и хранимых ПДн (удаление ПДн по достижению целей их обработки), обезличивание ПДн (деление ПДн на части; добавление

«шума» (посторонней информации) в ПДн для усложнения идентификации ПДн; группирование общих характеристик ПДн; скрытие части данных и др.).

Обеспечение безопасности ПДн: управление доступом к ПДн; разделение прав доступа (все пользователи работают с обезличенной информацией, к кодам имеют доступ ограниченный круг пользователей); уменьшение количества привилегированных пользователей; запрет или ограничение на удаленный доступ; запрет или ограничение на хранение и обработку ПДн на мобильных устройствах; контроль попыток несанкционированного доступа к ПДн; мониторинг, анализ, уведомление (анализ активности пользователей в отношении ПДн); авторизация пользователей для доступа к ПДн; ограничение возможности копирования ПДн на внешние носители; шифрование ПДн, передаваемых за пределы организации и др.

Возможно, после вступления в силу документа NIST Special Publication 800-122 порядок защиты ПДн в США будет более понятен, тем не менее, остается много вопросов по практическому применению данного механизма.

С 2014 года в штате Калифорния действует закон, который обязывает сайты сообщать пользователям, отслеживают ли их поведение. Начиная с 2015 года жителям штата младше 18 лет также предоставят право быть забытыми, аналогичное европейскому.

В итоге: нет централизованного законодательства по защите персональных данных на федеральном уровне. Существуют разные законодательные акты в разных штатах, и в разных ведомствах. Организации должны предпринимать необходимые шаги для защиты данных, от несанкционированного доступа и нарушений политик обработки. В некоторых штатах также на законодательном уровне

закреплены минимальные требования по защите информации. Нет единого органа по защите ПДн. Но для многих случаев Federal Trade Commission (FTC) является контролирующим органом.

Таким образом, их положения практически аналогичны принципам, лежащим в основе европейской системы защиты персональных данных. Тем не менее, практика защиты персональных данных в США не является безупречной, чем, видимо, и объясняется включение США в список стран, не обеспечивающих адекватную защиту персональных данных, соответствующий порядок предусмотрен п.4 ст.25 Директивы ЕС 95/46/ЕС.

Россия.

Принято несколько категорий персональных данных. К ним могут относиться общедоступные ПДн, специальные категории ПДн, категории ПДн, обрабатываемые в информационных системах персональных данных (ИСПДн), биометрические ПДн и другие.

Общедоступные ПДн- общедоступными являются данные, доступ к которым предоставлен неограниченному кругу лиц с согласия субъекта ПДн или на которые, в соответствии с федеральными законами, не распространяются требования соблюдения конфиденциальности (фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные ПДн). Источниками такой информации являются, к примеру, справочники, адресные книги и т.п. Сведения о субъекте ПДн могут быть в любое время исключены из общедоступных источников по требованию субъекта либо по решению суда или уполномоченных государственных органов.

Специальные категории ПДн - касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских

убеждений, состояния здоровья, интимной жизни. Их обработка допускается только в следующих случаях: субъект ПДн **дал согласие** в письменной форме на обработку своих персональных данных; персональные данные являются общедоступными; персональные данные относятся к состоянию здоровья субъекта ПДн и получение его согласия невозможно, либо обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну; обработка персональных данных осуществляется в соответствии с законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, а также в соответствии с уголовно-исполнительным законодательством Российской Федерации или необходима в связи с осуществлением правосудия.

Категории персональных данных, обрабатываемых в ИСПДн:

Совместный приказ ФСТЭК, ФСБ и Министерства информационных технологий и связи РФ от 13 февраля 2008 года N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» определяет:

Категория 1 – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.

Категория 2 – персональные данные, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1.

Категория 3 – персональные данные, позволяющие идентифицировать субъекта ПДн.

Категория 4 – обезличенные и (или) общедоступные персональные данные.

Биометрические персональные данные – это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность. Биометрические персональные данные обрабатываются в соответствии со статьей 11 Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных». Они могут обрабатываться только при наличии согласия в письменной форме субъекта ПДн. Обработка биометрических персональных данных без согласия субъекта ПДн может осуществляться в связи с осуществлением правосудия, а также в случаях, предусмотренных законодательством Российской Федерации о безопасности, об оперативно-розыскной деятельности, о государственной службе, о порядке выезда из РФ и въезда в Российскую Федерацию, уголовно-исполнительным законодательством.

Оператор персональных данных – согласно федеральному закону от 27.07.2006 N 152-ФЗ операторами персональных данных являются государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Под обработкой ПДн понимаются действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе, передачу), обезличивание, блокирование, уничтожение ПДн.

Обеспечение безопасности (в данном случае конфиденциальности) в соответствии с российским законодательством не требуется лишь для обезличенных и общедоступных персональных данных.

Персональные данные могут быть общедоступными только с письменного согласия субъекта ПДн. Они могут включать фамилию, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом ПДн.

Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование и распространение персональных данных. Обязанность по обеспечению безопасности ПДн при их обработке в ИСПДн полностью возлагается на оператора персональных данных.

Безопасность ПДн при их обработке в ИСПДн обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (уполномоченное лицо). При этом оператор должен заключать договор с уполномоченным лицом. Существенным условием этого договора является обязанность уполномоченного лица обеспечить конфиденциальность и безопасность ПДн при их обработке в ИСПДн.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах оператором может назначаться структурное подразделение или должностное лицо (работник), ответственное за обеспечение безопасности персональных данных.

В соответствии со статьей 23 Федерального Закона «О персональных данных» для обеспечения контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона назначается Уполномоченный орган по защите прав субъектов персональных данных (далее, регулятор). Такие функции возложены на три организации:

1. Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) в части, касающейся соблюдения норм и требований по обработке персональных данных;

2. Федеральную службу безопасности РФ в части, касающейся соблюдения требований по организации и обеспечению функционирования шифровальных (криптографических) средств в случае их использования для обеспечения безопасности персональных данных при их обработке в ИСПДн;

3. Федеральную службу по техническому и экспортному контролю в части, касающейся контроля и выполнения требований по организации и техническому обеспечению безопасности ПДн (не криптографическими методами) при их обработке в ИСПН.

В итоге:

Государство создало необходимые условия для выполнения требований по безопасности персональных данных. Оно определило понятия ПДн и операторов, которые эти данные обрабатывают. Регулирование на федеральном уровне:

• Федеральный закон от 19 декабря 2005 г. N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».

• Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» (27 июля 2006 г.).

• Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

• Несколько подзаконных актов, включая: Постановления Правительства РФ, Указы Президента, и нормативные акты отдельных ведомств.

Организации должны предпринимать необходимые шаги для защиты данных, от несанкционированного доступа и нарушений политик обработки. Также на законодательном уровне закреплены минимальные требования по защите информации.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Защита ПДн при трансграничной передаче.

Модели трансграничной передачи персональных данных.

Нормативно-правовые акты:

Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.) с изменениями от 15 июня 1999 г.

Дополнительный протокол к Конвенции о защите частных лиц в отношении автоматизированной обработки данных личного характера, о наблюдательных органах и трансграничной передаче информации» ETS N 181 (Страсбург, 08 ноября 2001 г.).

Статья 2. Трансграничная передача персональных данных получателю, не являющемуся субъектом права Стороны Конвенции. Она гласит:

1. Каждая Сторона предусматривает передачу персональных данных получателю – субъекту права Государства или организации, не являющейся Стороной Конвенции, только если это Государство или организация обеспечат адекватный уровень защиты данных, предназначенных для передачи.

2. Каждая Сторона может разрешить передачу персональных данных:

a. если национальное право предусматривает это ввиду: определенной заинтересованности в отношении субъекта данных или законных интересов, наиболее важных государственных интересов;

b. если гарантии, которые могут быть, в частности, результатом условий договора, предусмотренные ответственным за передачу контролером, признаются адекватными.

В законодательстве РФ особое внимание уделено безопасности ПДн при их передаче за пределы Российской Федерации. До начала осуществления трансграничной передачи персональных данных оператор ПДн обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов ПДн. Министерство связи и массовых коммуникаций РФ (Минкомсвязи) в своем письме РФ от 13.05.2009 N ДС-П11-2502 «Об осуществлении трансграничной передачи персональных данных» (13 мая 2009 г.) определило «адекватную защиту» как защиту, при которой «обеспечивается уровень защищенности прав субъектов персональных данных не ниже, чем в Российской Федерации».

Одним из критериев оценки государства в данном аспекте может выступать факт ратификации им «Конвенции о защите прав физических лиц при автоматизированной обработке персональных данных» от 28 января 1981 г., ETS № 108. На сегодняшний день в число стран,

подписавших и ратифицировавших указанную Конвенцию, входят: Австрия, Андорра, Бельгия, Болгария, Дания, Великобритания, Венгрия, Германия, Греция, Израиль, Ирландия, Исландия, Испания, Италия, Латвия, Литва, Лихтенштейн, Люксембург, Мальта, Нидерланды, Норвегия, Польша, Португалия, Румыния, Сербия, Словакия, Словения, Финляндия, Франция, Хорватия, Черногория, Чехия, Швейцария, Швеция, Эстония.

В США отсутствуют нормативные положения, которые бы ограничивали трансграничную передачу данных. Норма Конституции США о регулировании торговли (*«commerce clause» - п. 3 разд. 8 ст. 1 Конституции США*) также не позволяет установить подобные ограничения на уровне штатов.

Особенности: США не рассматривается в качестве страны, обеспечивающей надлежащий уровень защиты персональных данных, с точки зрения европейского законодательства.

Последствия: В целях гармонизации был создан механизм утверждения международными корпорациями специальных, единых корпоративных правил обработки данных (*Binding Corporate Rules – ст. 26 (2) Директивы 95/46/ЕС*), а также выработаны специальные принципы (*Safe Harbor – Решение Комиссии ЕС от 26 июля 2000 г. N 2000/520/Е)*.

В ЕС Европейская комиссия утверждает список таких стран. Передача данных внутри интеграционного образования данному ограничению не подлежит. В некоторых случаях для третьих стран предусмотрены исключения *(ст. 26 Директивы 95/46/ЕС).*

Особенности: Несмотря на то, что данные ограничения являются дополнительной нагрузкой на бизнес, в ЕС пытаются не столько урегулировать рынок методом запретов, сколько «настроить» организационный механизм трансграничной передачи данных, например,

посредством разработки модельных контрактов, консультаций с операторами и т.п. *(Решения Комиссии ЕС от 15 июня 2001 года № 2001/497/ЕС, от 27 декабря 2014 № 2004/915/ЕС).*

В общем, устанавливается, что оператор - единственный субъект, подлежащий привлечению к ответственности.

Обработчик не несёт обязанностей непосредственно перед субъектом персональных данных. Ответственность за его действия несёт оператор.

Такой порядок в данный момент предусмотрен в Директиве 95/46/ЕС *(ст. 16, 17 и 23).* Обработчик несет ответственность перед оператором в рамках договорных отношений.

Ответственность за нарушение законодательства о защите персональных данных.

В РФ законом предусмотрена гражданская, уголовная, административная, дисциплинарная и иная ответственность за нарушение его требований. Так, Кодекс об административных правонарушениях предусматривает максимальный штраф в 500000 рублей за невыполнение законного предписания Роскомнадзора (ст. 19.5 КоАП). Тот же Кодекс предусматривает приостановку деятельности организации на срок до 90 суток при осуществлении деятельности по защите персональных данных без лицензии (ст. 19.20 КоАП).

В уголовном кодексе говорится о штрафе в 300000 руб., обязательных работах на срок до 1-го года, аресте до 6-ти месяцев и лишении права занимать должность на срок до 5-ти лет в случае осуществления защиты персональных данных без лицензии в случаях, если это деяние причинило крупный ущерб гражданам (ст. 171 УК).

При систематических и грубых нарушениях Роскомнадзор имеет право ходатайствовать об отзыве лицензий на основной вид деятельности.

Таблица. Сумма штрафов в некоторых странах.

Государство	Сумма (прибл.), USD
Австралия	1 500 000
Великобритания	800 000
Индия	700 000
Германия	400 000
Канада	100 000

Выводы.

Таким образом, после изучения российского законодательства и рассмотрения нормативно-правовой базы различных зарубежных стран в сфере защиты персональных данных, регулирующих так же сбор и обработку персональных данных, можно сделать вывод, что наиболее перспективным и эффективным механизмом охраны и защиты персональных данных является законодательство Германии, а именно, ФЗ «О защите данных» от 2001 года. Несмотря на то, что Германия относится к континентальной правовой системе, государственно-территориальное устройство федеративного типа, как и в нашей стране, всё же служит отличным примером надежной и «адекватной» системы защиты персональных данных.

Проанализировав современную международную практику, а так же законодательство и опыт отдельных стран в сфере правового обеспечения защиты персональных данных, мы можем констатировать наличие

устойчивой и весьма заметной тенденции к развитию универсализма в этой области, что ярко выражается в формировании общих подходов к правовому регулированию общественных отношений, связанных с защитой персональных данных и международных стандартов государственно-правовой защиты этих данных. Последние выступают правовым ориентиром в развитии российского законодательства, устанавливающего правовые механизмы защиты персональных данных, а так же для соответствующей правоприменительной практики.

И всё же, в заключение хочется сказать о том, что как бы не трудились «светлейшие умы» любой страны, данный вопрос всегда будет оставаться открытым. Прогресс не стоит на месте, и в соответствии с ярко выраженной тенденцией роста значения информационных технологий и их «просачивания» в каждую сферу жизнедеятельности, законодательство просто не сможет «поспеть» за ними, и всегда найдутся как плюсы, так и минусы в любом нормативно-правовом акте и любой правовой системы касательно данного вопроса.

Литература:

1. Развитие человеческого капитала и рост национального богатства / Н.Б. Читанава, А.Н. Мейтова, О.Б. Шилович, А.В. Параскевов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2014. – №01(095). С. 1192 – 1203. – IDA [article ID]: 0951401069. – Режим доступа: http://ej.kubagro.ru/2014/01/pdf/69.pdf, 0,75 п.л.
2. Федеральный закон Российской Федерации от 25 ноября 2009 г. N 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» по вопросам реализации международных договоров Российской Федерации о реадмиссии"
3. Кузнецова, Т.В. Организация работы с персональными данными / Т.В. Кузнецова // Трудовое право. – 2011. – № 5. – С. 75 – 80.
4. Трудовой кодекс Российской Федерации от 30.12.2001, в ред. от 19.07.2011 № 197-ФЗ // Парламентская газета – 2002. – № 2 – 5.
5. Малеина, М.Н. Право на тайну и неприкосновенность персональных данных / М.Н. Малеина // Журнал российского права. – 2010. – № 11. – С. 19 – 24.
6. Кодекс Российской Федерации об административных правонарушениях, в ред. от 04.11.2014 № 195-ФЗ // Российская газета. – 2001 г. – № 256.

7. О персональных данных: Федеральный закон от 27 июля 2006 в ред. от 04 июня 2014 № 152-ФЗ // Российская газета. – 2006 г. – № 165.

References

1. Razvitie chelovecheskogo kapitala i rost nacional'nogo bogatstva / N.B. Chitanava, A.N. Mejtova, O.B. Shilovich, A.V. Paraskevov // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2014. – №01(095). S. 1192 – 1203. – IDA [article ID]: 0951401069. – Rezhim dostupa: http://ej.kubagro.ru/2014/01/pdf/69.pdf, 0,75 p.l.

2. Federal'nyj zakon Rossijskoj Federacii ot 25 nojabrja 2009 g. N 266-FZ «O vnesenii izmenenij v Federal'nyj zakon «O personal'nyh dannyh» po voprosam realizacii mezhdunarodnyh dogovorov Rossijskoj Federacii o readmissii"

3. Kuznecova, T.V. Organizacija raboty s personal'nymi dannymi / T.V. Kuznecova // Trudovoe pravo. – 2011. – № 5. – S. 75 – 80.

4. Trudovoj kodeks Rossijskoj Federacii ot 30.12.2001, v red. ot 19.07.2011 № 197-FZ // Parlamentskaja gazeta – 2002. – № 2 – 5.

5. Maleina, M.N. Pravo na tajnu i neprikosnovennost' personal'nyh dannyh / M.N. Maleina // Zhurnal rossijskogo prava. – 2010. – № 11. – S. 19 – 24.

6. Kodeks Rossijskoj Federacii ob administrativnyh pravonarushenijah, v red. ot 04.11.2014 № 195-FZ // Rossijskaja gazeta. – 2001 g. – № 256.

7. O personal'nyh dannyh: Federal'nyj zakon ot 27 ijulja 2006 v red. ot 04 ijunja 2014 № 152-FZ // Rossijskaja gazeta. – 2006 g. – № 165.