СРАВНЕНИЕ НОРМАТИВНО – ПРАВОВОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЗАРУБЕЖНЫХ СТРАНАХ И В УЗБЕКИСТАН

Ходжанова Мафират Абдумаликовна
магистр Ташкентский государственный Юридический Университет
Научные руководитель: **Топилдиев Бахром Рахимжанович**
доктор юридических наук,
профессор кафедры «Гражданского права»
Ташкентский Государственный Юридический Университет

АННОТАЦИЯ

В данной статье было проанализировано законодательство нескольких зарубежных стран и Республики Узбекистан. Был проведен сравнительных анализ схожих и отличительных сторон.

Ключевые слова: *Персональные данные, законодательство, закон, технологический прогресс, информация, обработка, защита, меры, сравнительных анализ.*

COMPARISON OF REGULATORY AND LEGAL PROTECTION OF PERSONAL DATA PROTECTION IN FOREIGN COUNTRIES AND IN UZBEKISTAN

ABSTRACT

This article analyzed the legislation of several foreign countries and the Republic of Uzbekistan. A comparative analysis of similar and distinctive aspects was carried out.

Key words: *Personal data, legislation, law, technological progress, information, processing, protection, measures, comparative analysis.*

ВВЕДЕНИЕ

В нынешнее время информация играет огромную и ключевую роль как в обычном мире, так и цифровом пространстве и поэтому защита персональных данных оставалось и остаётся наиболее Темой для развития. Законодательство многих стран выбирает свой собственный путь в данной сфере правовых отношений. Разные законодательства устанавливают определённые требования критерия принципы при обработке передачи хранению и сбору персональных данных.

В мире существует огромное количество стран чье законодательство хотелось бы проанализировать, изучите и сравнить с законодательством Республики Узбекистан. В данной диссертации были изучены законодательство Европейского союза GDPR, федеральные законы о защите данных США, законодательства отдельных стран, таких как Япония, Китай, Сингапур и Россия и проведён сравнительный анализ с законодательством Республики Узбекистан.

Европа. Определение персональных данных по законодательству Республики Узбекистан по закону о персональных данных от 21 июня 2019 года, [1] Персональные данные — зафиксированная на электронном, бумажном и (или) ином материальном носителе информация, относящаяся к определенному физическому лицу или дающая возможность его идентификации.(статья 4) Сравнение хотелось бы начать с Европейского союза. По определению, [2] Федеральным акта по защите персональных данных (Datenschutzgesetz 2000 – DSG 2000), принятого в 2000 году, статья номер два параграфа номер четыре это информация, которая имеет отношение к идентифицированному (“identified”) или же имеющему высокую вероятность идентификации (“identifiable”) лицу, являющемуся ее [т.е. такой информации] субъектом.

ОБСУЖДЕНИЕ И РЕЗУЛЬТАТЫ

Другая дефиниция персональных данных, которая обращает на себя интерес, это дефиниция Великобритании, которая также определяет персональные данные как информацию, которая связана с каким-либо индивидом, информация, с помощью которой можно его идентифицировать и эта информация также включает в себя и выражение мнений о данном субъекте, но без указания намерения в отношении него.

Британское законодательство дает определение персональным данным, в соответствии с Законом от 1998 г. О защите данных — Data Protection Act, статьей 1, [3]что не только как информация, но и как мнение и намерение, в местном законодательстве чего нет. Кроме вышеуказанного в Британии есть еще и акт под названием Закон о свободе информации от 2000 года, в части 2, статье 40, [4]определяют персональные данные, как и запрос, представляющий собой информацию о субъекте персональных данных.

[1] Закон Республики Узбекистан «О персональных данных» от 2019 года
[2] Федеральным акт «По защите персональных данных» (Datenschutzgesetz 2000 – DSG 2000), 2000 г
[3] Закон от 1998 г. «О защите данных» — Data Protection Act
[4] «Закон о свободе информации» от 2000 года

Самым главным все-таки можно выделить для Европейского союза присущий общий законодательный регламент по защите данных, то есть [5]GDPR (General Data protection regulation - Общие правила защиты данных), который вступил в силу в Европейском Союзе 25 мая 2018 года. Хотелось бы ещё отметить очень важный аспект, что в соответствии со статьей 3, под названием Территориальная сфера действия, что данный регламент применяется не только к странам участникам Евросоюза, но также и к юридическим лицам и даже к иностранным гражданам, которые обрабатывают персональные данные граждан Евросоюза.

Статья четыре данного закона даёт определение персональным данным. Как и во многих законодательствах, тут говорится, что это опять-таки информация, которая относится к физическому лицу, даёт определение физическому лицу. Но уже в данной статье указано, что информация может быть не только такими как ими местонахождение, но также и онлайн идентификаторы суда могут отнести как компьютеры, так и смартфоны. То есть данный закон идёт со временем современных технологий. Отличиями можно выделить использование в законе таких понятий как идентификатор, индивид и контролёр. В сравнение, в законодательстве Республики Узбекистан используется определение оператор, субъект. По законодательству Евросоюза контролёр собирает персональные данные. То есть он их используют, обрабатывает до тех пор, пока он не нарушает закона.

В законодательстве Евросоюза касательно персональных данных чётко отмеченные правила использования и также говорится о том, что каждый субъект, который не будет выполнять правила данного законодательства будет оплачивать штрафы вплоть до 20 млн евро или до 4% от выручки.

Глава вторая регламента, а в основном Статья 5. [6]Принципы обработки персональных данных указывает на все принципы данного регламента. Самый первый, принцип законности, прозрачности и справедливости, то есть любая информация, которая идентифицируют гражданина должна быть получена законными так и справедливыми способами и средствами и только согласия субъекта данных.

Принципом является ограничение цели, это значит, что цель, ради, которой обрабатываются и собирается информация должна быть законная и не должно иметь иных целей за исключением одной определённой.

[5] General Data Protection Regulation, GDPR; Постановление 2016/679 от 25 мая 2018 года.
[6] General Data Protection Regulation, GDPR; Постановление 2016/679 от 25 мая 2018 года

Следующим пунктом является минимизация данных. Контролёр или иной, который имеет право собирают персональных данные, должен собирать столько, сколько нужно для цели.

Четвёртым пунктом является точность, это слово определяет собой что информация, которая обрабатывается или, которая получается должна быть точной, актуальной и полной. Точнее говоря любые ошибки и неточности должны быть исправлены. Данные должны храниться только для выполнения определённой цели, для которой эти данные были собраны, но не дольше.

Основным я считаю, является целостность и конфиденциальность, то есть персональные данные сборы и хранение обеспечиваться определёнными гарантиями безопасности от потери от несанкционированного доступа и конечно же от уничтожения.

Последним седьмым пунктом является Подотчетность. Это значит, что любые компании любые юридические лица несут ответственность за все свои действия касательно персональных данных личности из-за нарушения требований регламента предусмотрены огромные штрафы, которые были выше указаны.

США. В Соединённых Штатах Америки Федеральное законодательство обязывает только государственные органы в сфере защиты персональных данных. Что же касается юридических лиц которые обрабатывают персональные данные, то их права и обязанности определяет нормы на уровне штатов. Так примером может послужить штат Калифорния которая приняла в 2020 году закон (California Consumer PrivacyAct (CCPA), который [7]регулирует правила сбора данных и работа и работы с этими данными, что любое физическое лицо которые используют интернет и пользуются услугами различных интернет-компании имеет право знать, какую именно информацию собирает данные компании которые он пользуется также определить цель они собирают эту информацию. И последнее он может узнать каким образом будут использованы данные персональные данных. Уточняет права физических лиц на требование уничтожить свои персональные данные, а также запрещать передачу собранных данных третьим лицам. В данном аспекте есть схожесть законодательством Республики Узбекистан, так как в законе данных субъект персональных данных такие схожие права.

В Америке проблема с киберпреступностью которая включает в себя и несанкционированный доступ к личным субъектов правовой точки зрения имеет двоякую природу. свод законов США а точнее раздел 18 глоссит о

[7] California Consumer PrivacyAct (CCPA), 2020

существующей ответственность если была совершена кража персональных данных а также Взлом системы компьютеров которая налагает на ответчика от100.000 долларов до 250.000 долларов. Сумма штрафа зависит от меры преступления. (§ 3571 разд. 18 СЗ США) [8] А с другой стороны после случившихся терактов сентября был разрешён сбор данных об гражданах Соединённых Штатах на государственном уровне что и было включено в Закон о патриотизме (USA PATRIOT).

Но с 2015 года новая появилась тенденция к либерализации, так как начал действовать и был введен в действие [9] Акт о свободе (USA FREEDOM). Агентство национальной безопасности (АНБ США), раньше основываясь на Закон о патриотизме мог собирать массовую информацию, это включало в себя и перехват данных, теперь может осуществлять сбор данных только после получения судебного ордера. Важным аспектом является, что собирать данные могут только уполномоченные лица, которые по закону называются провайдерами. Если же эти провайдеры будут перехватывать данные незаконным способом, то могут попасть в тюрьму сроком от 6 месяцев до 5 лет в зависимости от тяжести преступления.

Интересным является понятие экстерриториальности в соответствии со статьей 15 [10] Конвенции ООН против транснациональной организованной преступности от 15 ноября 2000 года, которая гласит, что расследовать могут и правонарушения в сфере цифровой информации, то есть компьютерной, даже если оно не направлено прямо против граждан США, но было зафиксировано касательно серверов находящихся территориально США. То есть законом не ограничено территориальность национального законодательства стран участников ООН.

Китай. В ноябре 2016 года Постоянный Комитет Всекитайского собрания народных представителей (ПК ВСНП) принял закон, [11]запрещающий Интернет-провайдера сбор информации о пользователях без их согласия. Это стало отправной точкой для развития законодательства в сфере защиты ПД в стране. Закон вступил в силу 1 июня 2017 года.

Несмотря на то, что государство и Компартия Китая оказывают влияние на все сферы жизни, включая информационную, КНР стремится к созданию системы защиты персональных данных, схожей с GDPR. Так, например, в марте 2018 года Национальный технический комитет по стандартизации

[8] Закон о патриотизме (USA PATRIOT), 2011
[9] «Акт о свободе» (USA FREEDOM), 2015
[10] Конвенции ООН «Против транснациональной организованной преступности» от 15 ноября 2000
[11] Закон «О кибербезопастности» от 1 июня 2017 года

информационной безопасности Китая (ТС260) выпускает государственный стандарт [12] Спецификация безопасности личной информации, регламентирующий сбор, хранение, использование, обмен, передачу и раскрытие информации о пользователях интернета. Считается, что Китай может перенять из европейского опыта такие аспекты, как условия получения согласия пользователей, право на забвение, формулирование политики конфиденциальности бизнеса и так далее.

Следует отметить, что законодательство КНР о защите ПД находится на стадии развития. Приоритетом в стране по-прежнему является государственный контроль, однако КНР постепенно двигается к более совершенной системе защиты персональных данных.

В целом, можно сказать, что Китай заимствует опыт Европы в области защиты персональных данных, но делает это с учетом своих особенностей.

Япония и Сингапур. 2005 год стал знаменательным для защиты персональных данных в Японии, ознаменовавшись вступлением в силу Закона О защите персональной информации.[13] Этот закон закрепил право на защиту ПД как неотъемлемую часть права на неприкосновенность частной жизни, гарантированного японской Конституцией 1947 года.

С этого момента любой интернет-сайт любой японской компании, работающей с персональными данными своих граждан, обязан иметь специальный раздел Политика по защите персональной информации. В этом разделе компания обязана подробно изложить, как она реализует нормы Закона, какие меры она принимает для обеспечения безопасности ПД и как эти меры будут корректироваться в будущем.

Таким образом, Япония продемонстрировала свою приверженность защите персональных данных своих граждан, создав комплексную правовую и информационную систему, призванную гарантировать конфиденциальность их информации.

В 2012 году Сингапур сделал важный шаг в сфере защиты персональных данных, приняв Закон «О защите персональных данных». Этот закон устанавливает чёткие правила сбора, использования, раскрытия и хранения ПД, обеспечивая тем самым конфиденциальность информации граждан.

Одной из интересных особенностей закона является создание национального реестра DonotCall (DNC). Включение своего номера в этот

[12] Спецификация безопасности личной информации" от 24 июня 2022 года
[13] Закон "О защите персональной информации" от 2005года

реестр позволяет сингапурцам оградить себя от навязчивых маркетинговых звонков, СМС-сообщений и факсов от различных организаций.

Важно отметить, что сингапурские компании могут собирать, использовать или раскрывать ПД только с явного согласия человека. При этом цели обработки должны быть обоснованными и соответствовать законодательству.

Таким образом, Закон «О защите персональных данных» демонстрирует стремление Сингапура к созданию общества, где право на конфиденциальность информации является одним из ключевых прав граждан.

Россия. Статья 19 [14] Федерального закона № 152-ФЗ «О персональных данных» гласит**,** что Российское законодательство о персональных данных обязывает юридические лица предпринимать меры по защите данных физических лиц. Эти меры должны быть достаточными, чтобы предотвратить неправомерный или случайный доступ к данным, их уничтожение, изменение, распространение и другие незаконные действия.

Меры защиты можно разделить на правовые, примерами можно отнести создание комплекта документов, регламентирующих защиту персональных данных и технически – организационные, которым относиться действия, направленные на обеспечение безопасности данных, например, шифрование, обучение сотрудников.

Для некоторых категорий юридических лиц законодательством предусмотрены специальные требования защиты персональных данных. Так, госорганы должны следовать Перечню мер (утвержден Постановлением Правительства РФ от 17 ноября 2007 г. № 808)., а компании, работающие с гражданами ЕС, обязаны соблюдать GDPR.

За нарушение законодательства о персональных данных предусмотрена административная и уголовная ответственность. Административная ответственность: штраф для юридических лиц может составлять от 30 000 до 18 000 000 рублей, в зависимости от характера нарушения (статья 13.11 КоАП РФ). Уголовная ответственность: незаконное собирание или распространение информации о частной жизни может привести к штрафу до 200 000 рублей или лишению свободы на срок до 2 лет (статья 137 УК РФ).

Важно отметить, что перечисленные меры защиты являются минимумом, необходимым для соблюдения законодательства.Компании должны самостоятельно оценивать риски, связанные с обработкой персональных данных, и принимать дополнительные меры защиты, если это необходимо.

[14] **Федерального закона № 152-ФЗ "О персональных данных» от 2006 года**

Несоблюдение требований законодательства о персональных данных может привести к серьезным последствиям для юридических лиц.

Принятие Федерального закона № 152-ФЗ в России и GDPR в Европе ознаменовало собой важный шаг в деле защиты персональных данных. Однако, несмотря на наличие законодательной базы, российская система защиты ПД все еще имеет ряд существенных недостатков.

Первый пробел заключается в ограниченном применении закона. Закон № 152-ФЗ фокусируется на операторах, зарегистрированных в РФ, оставляя без защиты персональные данные россиян, обрабатываемые зарубежными компаниями. GDPR же, напротив, защищает данные всех граждан ЕС, независимо от юрисдикции компании-оператора.

Второй недостаток – это слабые санкции. Максимальный штраф за сбор и обработку ПД без согласия в России составляет всего 75 000 рублей, что значительно ниже, чем в ЕС или Канаде, где штрафы исчисляются миллионами или процентами от выручки. Отсутствует и специализированная уголовная статья за хищение ПД, что приводит к несоразмерно мягким наказаниям даже в серьезных случаях.

Несмотря на эти проблемы, власти РФ предпринимают шаги к ужесточению санкций. Первый зампред комитета Госдумы по информационной политике Сергей Боярский пообещал последовательно увеличивать штрафы за хищение и использование чужих ПД.

В целом, Россия, как и Китай, пытается найти баланс между невмешательством государства и защитой ПД. С одной стороны, власти стремятся сохранять контроль над информацией о гражданах, с другой – не препятствовать сбору и использованию ПД в собственных интересах.

Узбекистан. В современном мире, где информация играет все более важную роль, защита персональных данных (ПД) становится одной из ключевых задач государства. В Узбекистане данная сфера регулируется комплексной системой нормативно-правовых актов, призванных обеспечить конфиденциальность и безопасность ПД граждан.

Основные законы и нормативные акты Узбекистана в отрасли персональных данных:

[15]Конституция Республики Узбекистан: Статья 24 гарантирует право на неприкосновенность частной жизни, что является основополагающим принципом защиты ПД.

[15] Конституция Республики Узбекистан от 30 апреля 2023 года.

[16]Закон Республики Узбекистан О персональных данных (от 02.07.2019 г. № ЗРУ-547): это основополагающий закон, который определяет основные понятия, принципы, права и обязанности в сфере защиты ПД.

Постановление Кабинета Министров Республики Узбекистан «Об утверждении некоторых нормативно-правовых актов в области обработки персональных данных» (от 05.10.2022 г. № 570): Этот документ детализирует требования к обработке ПД, включая уровни защиты, порядок хранения, меры по обеспечению безопасности и другие аспекты.

Другие законы и подзаконные акты: в различных отраслях законодательства также могут содержаться нормы, касающиеся защиты ПД, например, в Гражданском кодексе, Трудовом кодексе, законе «Об электронных документах и электронной цифровой подписи».

Основные принципы защиты, очень схожи с другими вышеуказанными странами. То есть так же присуще законность, то есть сбор, обработка и хранение ПД должны осуществляться только в соответствии с законом. Целесообразность, которая диктует, что ПД должны обрабатываться только для целей, заранее определенных и согласованных с субъектом ПД. Соответствие цели, когда Обработка ПД должна соответствовать заявленным целям. Необходимость и достаточность, когда объем обрабатываемых ПД должен быть не более того, который необходим для достижения целей обработки. Точность, которая означает, что ПД должны быть точными и, при необходимости, обновляться. Конфиденциальность, когда доступ к ПД должен быть ограничен только теми лицами, которым он необходим для достижения целей обработки. Безопасность, когда должны быть приняты меры по защите ПД от несанкционированного доступа, изменения, уничтожения, распространения или иных неправомерных действий.

Права субъекта персональных данных так же имеют схожесть с другими странами. Например, пункты на получение информации о своих данных, то есть субъект ПД имеет право знать, кто обрабатывает его ПД, для каких целей, какие ПД обрабатываются. Право на доступ к своим, когда субъект ПД имеет право ознакомиться со своими ПД, получить их копии и потребовать их исправления или удаления. Право на возражение против обработки своих ПД, когда субъект ПД имеет право в ряде случаев возразить против обработки своих ПД. Право на отзыв согласия на обработку своих ПД, когда субъект ПД имеет право в любой момент отозвать свое согласие на обработку своих ПД. Субъект ПД также имеет право на защиту своих ПД от неправомерного

[16] Закон Республики Узбекистан "О персональных данных" (от 02.07.2019 г. № ЗРУ-547

использования, право на блокирование своих ПД, право на подачу жалобы в уполномоченный орган по защите ПД.

За нарушение законодательства о защите ПД предусмотрена административная и уголовная ответственность в Республике Узбекистан. Административная ответственность выражается в виде штрафов, а уголовная ответственность – в виде штрафов, лишения свободы и других видов наказания. В Узбекистане создана комплексная система нормативно-правового обеспечения защиты ПД, которая соответствует международным стандартам.

Нет, наверное, в мире ни одного человека, который бы не делился какого-либо с другим человеком о себе: например, дату рождения имя фамилия отчество какие-нибудь документов сведения, может быть о своём здоровье и так далее. А ведь информация, которая была перечислено выше, это не просто информация это персональные данные. В современном мире люди научились использовать всякого рода информацию в своих корыстных целях и против человека и поэтому многие люди учёные который озабочены глобальными проблемами нынешнего века предсказывает, что XXI век это век когда человек информации будет владеть и самим миром. Если сравнить законодательство защиты персональных данных в различных странах можно найти много общего и конечно же какие-то и отличительные стороны.