Proceedings of IYSC, (2021), vol. 10

Journal homepage: http://journals.sdu.edu.kz/index.php/iysw

2021 International Young Scholars' Conference

Защита персональных данных как проблема обеспечения международной информационной безопасности

Селеубаева А.С.

магистрант 1-курса специальности Право ИТ

Университет имени Сулеймана Демиреля

Абстракт

Қазіргі әлемде компьютерлер санының өсуі және ақпараттық жүйелерді пайдалану жылдамдығы - жалпы алғанда барлық техникалық прогресс қоғамдық өмірдің барлық салаларына әсер етті және нәтижесінде ақпараттық қоғам пайда болды. Қазіргі әлемде дербес деректерді өңдеу көлемінің өсіп келе жатқандығын ескере отырып, дербес деректер үшінші тараптардың шабуылына осал болып келеді. Заманауи ақпараттық технологиялар үнемі кеңею және даму барысында болғандықтан, дербес деректерді өңдеу қызметіне тәуелділік тек артуда. Тиісінше, деректер субъектісінің өзінің жеке деректерін заңсыз өңдеуден қорғау туралы алаңдаушылығы барған сайын тереңдей түседі. Осылайша, дербес деректерді үшінші тұлғалардың теріс пайдалануынан қорғау қазіргі таңда жеке мемлекеттер үшін де, халықаралық қауымдастық үшін де аса маңызды және өзекті мәселеге айналды. Бұл мақалада мемлекеттер мен халықаралық қауымдастықтың осы мәселені неғұрлым оңтайлы шешу жолдары және халықаралық құқыққа сәйкес дербес деректерді өңдеу мен қорғаудың заңнамалық базасы ұсынылған.

Ключевые слова:

персональные данные, защита персональных данных, конфиденциальность, неприкосновенность частной жизни, информатизация, информационно – коммуникационные технологии, права человека

Любая информация, которая может быть связана с физическим лицом, подпадает под содержание термина “персональные данные”. С помощью личных данных можно узнать многое о человеке. Поскольку персональные данные представляют собой информацию о физическом лице, касающуюся его личной жизни и даже профессиональной деятельности, они имеют огромную ценность для субъекта данных. Данные собирались, хранились, использовались и распространялись на протяжении всей истории. Древнеримская перепись, например, показала, что администраторы ходят от двери к двери, чтобы собрать информацию о гражданах, начиная от размера их домашнего хозяйства и заканчивая количеством земли в собственности. Однако развитие компьютеров в 1950-х годах и все более широкое их использование в 1960-х годах изменили характер обработки персональных данных и степень необходимости их защиты.

Технический прогресс и развитие информационно - коммуникационных технологий повлияло почти на все сферы общественной жизни: на политику, культуру, экономику, на социум и все это в совокупности создало информационное общество. [1] Растут масштабы информатизации, возрастает роль информационного сектора экономики, стремительно развиваются сети и средства информационной коммуникации, меняется образ жизни людей в новой информационной среде, происходит информатизация профессиональной деятельности [2]. На международном уровне это называется глобальное информационное общество.

Сегодня многие важнейшие интересы человека, общества и государства во многом определяются состоянием окружающей их информационной сферы. Расширение сферы применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно создает новые информационные угрозы.[3] Принимая во внимание растущий объем обработки данных в современном мире, личные данные становятся более уязвимыми для атак со стороны третьих лиц. В результате постоянно расширяющегося влияния современных информационных технологий зависимость от деятельности по обработке данных постоянно растет. Соответственно, беспокойство субъекта данных о защите своих персональных данных от несанкционированной обработки данных все больше углубляется.

Однако на сегодняшний день уровень развития информационных технологий достиг того уровня, когда самостоятельная защита информационных прав и Персональных данных уже не является эффективным средством против посягательств на чью-то жизнь.

Широкое использование Интернета во всем мире является еще одним существенным фактором, способствующим увеличению объема обработки данных. Постоянное распространение информации физических лиц через Интернет облегчает несанкционированный доступ к персональным данным, и поэтому постоянно возникают обоснованные опасения по поводу недобросовестной обработки. То есть, как только мы появляемся в Интернете, все наши действия или посещаемые веб-сайты записываются и впоследствии вся информация становится нашими цифровыми следами личной жизни.

Возможности трансграничного распространения информации все чаще используются для достижения геополитических, военно-политических, противоречащих международному праву, а также террористических, экстремистских, преступных и иных противоправных целей, противоречащих международному праву, в ущерб международной безопасности и стратегической стабильности [4].

Таким образом, защита данных от злоупотреблений со стороны третьих лиц становится действительно трудоемким вопросом. Упомянутые выше события побудили государства и международные институты проработать эту проблему и разработать правовую базу для обработки и защиты данных.

Право человека на защиту его личных данных

С зарождением Интернета - в цифровую эпоху количество прав человека значительно увеличилось. В современном цифровом и информационном мире право человека на защиту его личных данных является одним из главных и важных его прав. В век цифровизации появилось понятие “информационные или цифровые права человека”, которое объединяет в себе право человека на свободу мысли, свободу слова, право на получение и распространение информации и они нужны человеку для реализации своих информационных свобод. Сейчас право на информацию реализуется по большей части посредством Интернета,

как и многие другие права человека и право на доступ к Интернету является ключевым для защиты других информационных прав человека [5].

Право на неприкосновенность частной жизни все чаще закрепляется в конституционных документах и документах по правам человека, а в некоторых случаях также включается конкретное право на защиту персональных данных. Защита частной жизни не может быть отделена от технологического развития: в настоящее время, в связи с развитием науки и техники, возросла возможность вторжения в чью-либо частную жизнь[6]. В то же время конфиденциальность и защита персональных данных находятся под угрозой в цифровую эпоху, в частности, из-за глобального распространения интернет-коммуникаций, которые, как известно, трудно контролировать.

В последнее десятилетие появилась международная тенденция: конфиденциальность данных. Защита данных всегда была связана с конфиденциальностью таким образом, что очень трудно оценить само ее понятие, цель и ценность, не возвращаясь к конфиденциальности. Неприкосновенность частной жизни является одним из основных прав человека, признанных в Декларации прав человека ООН, Международной конвенции о гражданских и политических правах и во многих других международных и региональных договорах. Неприкосновенность частной жизни лежит в основе человеческого достоинства и других ключевых ценностей, таких как свобода ассоциаций и свобода слова. Это стало одним из самых важных вопросов прав человека в современную эпоху.

В ЕС человеческое достоинство признается абсолютным фундаментальным правом. В этом понятии достоинства, неприкосновенности частной жизни или права на частную жизнь, быть автономным, контролировать информацию о себе играет ключевую роль.[7] Неприкосновенность частной жизни - это не только индивидуальное право, но и социальная ценность. Вступление в силу Лиссабонского договора 1 декабря 2009 года ознаменовало исторический момент для защиты данных: это право было возведено в статус фундаментального права в рамках правового порядка ЕС наряду с правом на неприкосновенность частной жизни.

Когда речь заходит о защите данных, существование различных правовых систем и

культур означает, что существуют различные термины, используемые для обозначения или определения одних и тех же или связанных между собой вещей. Возьмем, к примеру, саму защиту данных. В некоторых местах это называется “конфиденциальность данных”. Здесь мы используем термин "защита данных", но его следует рассматривать как взаимозаменяемый с термином "конфиденциальность данных".

Быстрое распространение Интернета создало новые проблемы в области применения защиты данных. В частности, это затруднило осуществление прав пользователей. Это происходит по двум причинам:

- Растущий объем потоков данных:

  В соответствии с принципами защиты данных собственники базы данных должны быть подотчетны и прозрачны в отношении своей обработки персональных данных. Например, пользователи имеют право знать, какие данные хранятся о них, и иметь возможность изменять или удалять эти данные при соблюдении определенных условий. Однако растущий поток данных затрудняет выполнение этого обязательства. Все чаще персональные данные перемещаются через несколько юрисдикций, которые могут иметь различные обязательства. Например, кто-то может использовать службу такси, работающую через онлайн-платформу в России, но персональные данные, относящиеся к его поездкам, могут обрабатываться компанией, штаб-квартира которой находится в Америке, которая, в свою очередь, использует компанию, предоставляющую глобальные услуги хранения данных. Это может означать, что их данные в конечном итоге будут храниться где угодно.

- Сложность получения осмысленного согласия:

  В цифровую эпоху значительно возросла автоматическая генерация персональных данных, а автоматизированный сбор и обработка персональных данных стали намного дешевле и легче. Это означает, что обеспечение того, чтобы пользователи могли осуществлять свои права на свои данные, является гораздо более сложной задачей. Одна из причин заключается в том, что сам

масштаб сбора данных привел к тому, что контролеры данных традиционно полагались на “галочки” условий соглашений об обслуживании (TSAS) для получения согласия на сбор и обработку персональных данных. Соглашение TSA обычно показывают субъектам данных коробку с изложением условий предоставления услуг контролера данных и запросом разрешения не только собирать данные, но и делиться ими с другими субъектами или “третьими лицами”. Это часто упоминается в краткой форме как “уведомление и согласие”. Но эти уведомления не предоставляют никакого реального агентства субъекту данных, у которого нет другого выбора, кроме как принять соглашение, если он хочет воспользоваться услугой. На практике эта ситуация дает пользователям очень мало власти над обработкой их данных.

Международно-правовое регулирования защиты персональных данных

Проблема международной информационной безопасности осознается международным сообществом как составная часть всеобъемлющей международной безопасности. В настоящее время распространение и использование ИКТ затрагивает интересы всего международного сообщества; эти технологии потенциально могут быть использованы в целях, несовместимых с целями международной стабильности и безопасности, и могут оказать негативное воздействие на целостность инфраструктуры государств, нарушая их безопасность во многих сферах.

Информационное право человека на защиту его личных данных и в целом его личной жизни берет свое начало с середины XX века, с появлением на свет Рекомендованной для всех стран-членов ООН Всеобщей декларации прав человека. Согласно данному международному документу, все люди имеют право на охрану от вмешательства в личную жизнь и на тайну переписки(статья 12). А также согласно статье 3 Каждый человек имеет право на личную неприкосновенность.[8] При расширенном толковании становится ясно, что персональные данные в рамках этой концепции являются частью личной жизни, и посягательство на них без воли человека не разрешается никаким третьим лицам. Более того, информация о себе является своеобразным активом, имеющим определенную ценность и

соответственно она также подлежит охране.

Наиболее сложной проблемой является влияние ИКТ на сложившиеся отрасли и институты международного права. Механизм развития норм международного права таков, что правовые нормы, как правило, “отстают” от уровня развития ИКТ. [1] Современная международная практика является ярким доказательством этого. Есть довольно много случаев, подтверждающих неэффективность и слабость правовой базы по защите персональных данных отдельных государств и всего международного сообщества в целом.

- В кейсе **Wisse v. France** Оба заявителя были арестованы по подозрению в совершении вооруженных ограблений и помещены под стражу до суда. В соответствии с ордером, выданным следственным судьей, были записаны телефонные разговоры между ними и их родственниками в комнатах для свиданий в тюрьме. Заявители подали безуспешное ходатайство о признании недействительными и незаконными действия в ходе разбирательства, связанных с записью их разговоров. Они утверждали, что запись их разговоров в комнатах для свиданий в тюрьме представляла собой вмешательство в их право на уважение их частной и семейной жизни.

  Суд ЕСПЧ постановил, что имело место нарушение статьи 8 Конвенции, установив, что французское законодательство не указывает с достаточной ясностью, каким образом и в какой степени власти могут вмешиваться в частную жизнь задержанных, а также объем и порядок осуществления их полномочий по усмотрению в этой сфере.[9]

- В кейсе **R.E. v. the United Kingdom** заявитель, который был трижды арестован и содержался под стражей в Северной Ирландии в связи с убийством сотрудника полиции, жаловался на режим скрытого наблюдения за консультациями между задержанным и их адвокатом.

  Это дело рассматривалось с точки зрения принципов, разработанных Судом в области перехвата телефонных разговоров адвоката и клиента, которые требуют строгих гарантий. Суд постановил, что эти принципы должны применяться к

скрытому наблюдению за консультациями адвоката и клиента в полицейском участке. В настоящем деле Суд постановил, что имело место нарушение статьи 8 Конвенции в отношении скрытого наблюдения за юридическими консультациями. Она, в частности, отметила, что с 22 июня 2010 года были введены в действие руководящие принципы, предусматривающие безопасное обращение, хранение и удаление материалов, полученных в результате такого скрытого наблюдения.[9]

- Дело **Bărbulescu v. Romania** касалось решения частной компании уволить сотрудника – заявителя – после мониторинга его электронных сообщений и доступа к их содержанию. Заявитель жаловался, что решение его работодателя было основано на нарушении его частной жизни и что национальные суды не смогли защитить его право на уважение его частной жизни и переписки.[9]

Подобные кейсы имеют место каждый день. Открыв новостную ленту мы обязательно можем увидеть и прочитать, что у кого-то были украдены деньги со счетов, чьи-то персональные данные оказались незаконным путем у третьих лиц, у определенной организации, хранящей персональные данные миллионов людей - своих клиентов случилась протечка данных. Закон должен реагировать на эти изменения, обеспечивая правовую защиту частной жизни. То есть о чем нам говорит всё это? Подобная ситуация на сегодняшний день показывает, что институт международного права по защите персональных данных неэффективен в достаточной мере, что требуется проработка действующих механизмов по защите данных.

Совет Европы, созданный в 1949 году, является межправительственным учреждением, занимающимся вопросами прав человека, демократии и верховенства права. В этом контексте Совет принял Конвенцию о защите прав человека и основных свобод (Европейская конвенция о правах человека (ЕСПЧ)) в 1950 году. Преследуя цель сохранения и применения норм, закрепленных во Всеобщей декларации прав человека, Конвенция, в частности, предусматривает право на уважение частной и семейной жизни в статье 8[9]. Как видно из содержания этой статьи, право на защиту данных прямо не упоминается. Однако особый акцент следует сделать на применении этой статьи, разработанной Европейским Судом по

правам человека. В результате беспрецедентного технического прогресса Суд расширил практику применения статьи 8, с тем чтобы рассматривать жалобы в связи с неправомерным использованием персональных данных. Статья 10 Конвенции предусматривает право на свободу выражения мнения (включает свободу придерживаться своего мнения и свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ)[10], что трактуется в том числе как право на информацию.

В 1981 году была издана Конвенция о защите физических лиц в связи с автоматической обработкой персональных данных , которая до сих пор считается единственным обязательным международно-правовым документом с общемировой сферой применения в этой области, поскольку она открыта для государств-членов и государств, не являющихся членами данной Конвенции. В то время как Совет устанавливал принципы, изложенные в Конвенции №108, одной из целей Совета было материализовать основные положения, выдвинутые статьей 8 ЕСПЧ, и определить более конкретные гарантии защиты данных.

Среди международных документов важно упомянуть также Руководящие принципы ОЭСР по защите неприкосновенности частной жизни и международных обменов персональными данными, опубликованные в 1980 году[11]. Даже если документ ОЭСР не имеет обязательной силы, его основополагающие принципы рассматриваются как руководящие правила для стран, в которых сфера защиты данных специально не регулировалась. Новые технологии и современные сети связи привели к необходимости обновления ее правил с целью повышения уровня защиты. Соответственно, ОЭСР выпустила обновленные Руководящие принципы в 2013 году. Поскольку руководящие принципы ОЭСР все еще принимаются в качестве свода специальных правил, касающихся защиты данных, они оказывают значительное воздействие как на государства-члены ОЭСР, так и за ее пределами.

Отдельно следует подчеркнуть усилия Организации Объединенных Наций (ООН). В 1990 году Руководящие принципы ООН, касающиеся компьютеризированных картотек,

содержащих данные личного характера, принятые Генеральной Ассамблеей, охватывают девять основных принципов, все из которых носят рекомендательный характер.

В целях гармонизации свободного потока персональных данных между государствами-членами ЕС и обеспечения общего уровня защиты по всему Европейскому Союзу была введена Директива 95/46/ЕС от 24 октября 1995 года о защите данных (Общая директива ЕС), и государствам-членам был предоставлен трехлетний период для ее реализации. На сегодняшний день все государства-члены ЕС выполнили Общую Директиву и приняли законы о защите данных на национальном уровне. Благодаря высокоразвитому механизму трансграничной передачи данных Общая директива ЕС оказывает все большее влияние на сферу защиты данных во всем мире. С 2012 года была разработана новая законодательная база (так называемое Общее положение о защите данных (GDPR)), направленная на укрепление стандартов защиты данных в ЕС и обновление положений Общей директивы ЕС. В конце декабря 2015 года между Европейским парламентом, Советом и Комиссией ЕС было достигнуто соглашение об этих новых рамках. В апреле 2016 года последняя версия GDPR была соответственно одобрена Советом Европейского Союза и Европейским Парламентом. В конечном счете, официальный текст GDPR был опубликован в Официальном журнале ЕС 4 мая 2016 года. В соответствии со статьей 99 GDPR государствам-членам предоставляется двухлетний переходный период, начинающийся с даты его вступления в силу (24 мая 2016 года), и таким образом Постановление становится непосредственно применимым во всех государствах-членах с 25 мая 2018 года.

Кроме того, важность права на защиту данных была еще раз подтверждена статьей 8 Хартии основных прав Европейского Союза, в которой на государства-члены возлагается обязанность в полной мере уважать это право. Поскольку Хартия стала юридически обязательной с 2009 года, было установлено признание защиты данных в качестве основного права граждан в Европе.

Заключение

Приведенный выше анализ основных особенностей новой информационной реальности показывает, что изменения, происходящие сегодня в информационной сфере

общества, влекут за собой не только радикальные изменения в социально-экономической структуре общества и организации общественного производства, но и изменяют процессы формирования личности и жизни.

Вопросы информационной безопасности, актуальные с развитием информационно-коммуникационных технологий, выходят за рамки традиционных вопросов информационной безопасности и затрагивают абсолютно все сферы жизни. Для решения глобальных проблем обеспечения информационной безопасности человечеству потребуется сформировать новую систему правовых отношений в информационной сфере общества, новую информационную культуру и информационную этику. Однако самое главное-осознать суть и актуальность этих проблем, необходимость их скорейшего решения цивилизованными методами.

Список использованной литературы

1. Valentina Petrovna Talimonchik - Legal Aspects of International Information Security. Published: April 24th 2019

2. Tsvyk V.A. Professional ethics: the foundations of a general theory. Вестник Российского Университета дружбы народов. - 2012:32 – стр. 133.

3. Vladimir A. Tsvyk1, Irina V. Tsvyk1 - Personal Information Security as a Global Problem.

4. Tsvyk A.V. Ethics of Political Responsibility in International Relations // Bulletin of the Peoples' Friendship University of Russia. Series: International Relations. - 2017. - T. 17. No. 2. - P. 257-264.

5. Талапина Э.В. Права человека в Интернете. Журнал Российского права №2. стр 41-54

6. Adrienn Lukács - What is privacy? The history and definition of privacy. URL: https://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf

7. Data protection. URL: https://edps.europa.eu/data-protection/data-protection_en#:~:text=In%20the%20EU%2C%20human%20dignity,but%20also%20a%20social%20value.

8. Всеобщая декларация прав человека. URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml

9. Практика ЕСПЧ https://www.echr.coe.int/documents/fs_data_eng.pdf

10. Европейская конвенция по правам человека. URL: https://www.echr.coe.int/documents/convention_rus.pdf

11. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. URL: https://www.oecd.org/digital/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm