

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

имени М.В.Ломоносова

ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра предпринимательского права

Курсовая работа по теме:

«Правовой режим сетевых идентификаторов гражданина как персональных данных»

Выполнил студент 215 группы

Купцов Даниэль Эдуардович

Научный руководитель

д.ю.н.

профессор

Харитоновна Юлия Сергеевна

Дата представления курсовой работы в учебный отдел:

«__» _____ 20__

Дата сдачи научному руководителю: «__» _____ 20__ г.

Дата защиты курсовой работы: «__» _____ 20__ г.

Оценка: _____

Москва

2023 г.

Оглавление

| | |
|---|-------|
| Введение | 3-5 |
| Глава 1 Основы правового режима персональных данных гражданина | 5-15 |
| §1 Зарождение института персональных данных на законодательном уровне: переход от приватности к детализации предмета исследования | 5-8 |
| § 2 Конкретизация понятия персональных данных: современный опыт зарубежного регулирования частной сферы жизни гражданина | 9-12 |
| § 3 Регулирование персональных данных в Российской Федерации: история отечественного подхода и основные проблемы | 12-15 |
| Глава 2 Сетевые идентификаторы гражданина как элемент института персональных данных | 15-24 |
| §1 Структура института персональных данных: пользовательские данные как элемент персональных данных | 15-18 |
| § 2 Правовое регулирование сетевых идентификаторов как пользовательских данных в зарубежных правовых порядках | 18-21 |
| §3 Правовое регулирование пользовательских данных и сетевых идентификаторов в РФ | 21-24 |
| Заключение | 24-25 |
| Список использованной литературы | 25-29 |

Введение

Текущий информационный век объявляет новые вызовы, ставя ряд современных проблем, требующих такого же современного решения. Получение данных, обеспеченное развитием технологий, безусловно, создает новые возможности для пользователя, так как позволяет получать информацию своевременно, быстро и качественно. Однако важным фактором получения данных является факт возможности содержания определенного вида информации о конкретном лице, что создает в перспективе проблему доступности их третьим лицам. Определенно, приведенный выше факт вопрос о защите положения данного лица, чьи данные могут перейти к иному лицу, нарушив интересы лица.

Рассуждая о трагичных последствиях перехода личных данных лица, стоит поговорить о самих последствиях подобных утечек данных и привести реальные примеры таких процессов. Подобные утечки могут сопровождаться продажей самих массивов данных, которые были предметом незаконного приобретения на

чёрном рынке¹. Доступом к данным могут обладать не только государственные органы, но и частные компании, которые могут участвовать в товарообмене подобной информации. Иллюстрирующим примером можно рассмотреть дело *S. and Marper v. the United Kingdom* (4 декабря 2008 г.), которое было рассмотрено Европейским судом по правам человека: Данным о ДНК и отпечатках пальцев 25 миллионов британцев владели десятки предприятий наряду с правоохранительными органами². Другим примером служит случай 11 января 2021 года, когда в сеть попали огромные массивы информации, включающие личные переписки пользователей, изображения и видео. Размер утечки оценивался в 70 терабайт данных. В тот же день в сеть попали данные о 214 миллионов пользователей социальных сетей Facebook и Instagram³.

Исходя из вышеперечисленных фактов, можно заявить, что отсутствие правильного и эффективного подхода к защите данных граждан может привести к информационным катастрофам, так как данные, являясь неотъемлемым ресурсом в современной среде, представляют ценность как для самих пользователей, так и для сторонних потенциальных владельцев информации. Конечно, не стоит говорить об отсутствии намерений законодателя в регулировании данной проблемы. Так, например, не позднее 1 июля 2023 года правительство предложит внести изменения в штрафы за увольнение для юридических лиц, разглашающих персональные данные. То же касается и правил о повышенной ответственности за неправомерное распространение персональных данных и иные нарушения в данной сфере. Правительство и ЦБ РФ рассмотрят вопрос о том, следует ли обязать финансовые учреждения

¹ Статья: Гражданско-правовые аспекты регулирования оборота персональных данных (Савельев А.И.) ("Вестник гражданского права", 2021, N 4)

² Статья: Антропология прав человека в цифровую эпоху (опыт сравнительного анализа) (Ковлер А.И.) ("Журнал российского права", 2022, N 12)

³ Eugene Bekker. Data Breach & Technology. IdentityForce. January 11, 2021. URL: <https://www.identityforce.com/blog/2021-data-breaches>

выплачивать компенсацию клиентам, чьи деньги были похищены мошенниками.

4

Однако в данной работе я бы хотел сфокусироваться на конкретном элементе общего информационного поля- сетевых идентификаторах. Сетевые идентификаторы имеют огромную важность в вопросе защиты данных пользователей, так как они выполняют задачу обмена данными и используются для идентификации конкретного физического лица. Также они могут быть собраны и обрабатываться различными организациями, включая интернет-провайдеров, социальные сети, онлайн-магазины.

В своей работе я хотел бы выяснить правовую природу сетевых идентификаторов и соотношение их с персональными данными; проанализировать развитие национального и европейского права в регулировании вышеперечисленных вопросов, а также привести возможные варианты регулирования сетевых идентификаторов гражданина.

Глава 1 Основы правового режима персональных данных гражданина

§1 Зарождение института персональных данных на законодательном уровне: переход от приватности к детализации предмета исследования.

Развитие человечества и технологический прогресс с каждым веком преподносят совершенно явления и конструкции для исследования и использования человечеством. Институт персональных данных является относительно новым явлением, так как появление компьютерных технологий и распространение сети Интернет пришли к нам совсем недавно. Однако сама проблема, безусловно, не нова. Развитие конституционализма, рост требований граждан в защите их прав привел к вопросу о защите информации о самих гражданах. Первой страной, которая проложила вектор в исследовании неприкосновенности частной сферы

⁴ Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека (утв. Президентом РФ 12.01.2023) (<http://www.kremlin.ru/acts/assignments/orders/70349>)

жизни человека, является США, введя термин «privacy»⁵ Категория «privacy» определяет обширный круг понятий, представляя собой всю совокупность всех сторон частной жизни личности. Данная категория раскрывается через право человека «быть оставленным наедине с самим собой» (right to be bet alone)⁶. Авторы данного определения, Сэмюэль Уоррен и Луис Брандейс, утверждали, что право на приватность с развитием технических устройств и использования их в сфере бизнеса всё больше находится под угрозой его нарушения. Формулирование проблемы американскими юристами предопределило будущую деятельность учёных в попытке защитить данное право, так как с распространением всё большего количества способов, методов и средств получения информации о гражданах, использования и манипулирования ею проблема становилась серьезнее и серьезнее.

Однако проблема, поставленная американскими учеными в конце девятнадцатого века, стала решаться не сразу. Лишь к середине двадцатого века отчётливо сформировался вектор в решении проблемы о защите приватности американскими судами. Так, в 1965 году Верховный суд США в ходе дела *Griswold v. Connecticut*⁷ закрепил право на неприкосновенность частной жизни индивида (основываясь на толковании первой, третьей, четвертой, пятой и девятой поправок к Конституции)⁸. Результатом судебной практики США выступил первый законодательный акт о защите данных - Fair Credit Reporting Act (FCRA)- закон "О добросовестном предоставлении кредитной информации"⁹. Целью FCRA было установить ограничения на обмен данными в сфере потребительской кредитной. FCRA создал трехстороннюю модель для последующего законодательства о защите данных, которая (1) обеспечивала уведомление потребителей о конкретном типе записи данных, (2) устанавливала

⁵ Вajorова М.А. «История возникновения и становления института персональных данных»

⁶ Warren S., Brandeis L. The Right to Privacy // Harvard Law Review. 1890. Vol. 4. No. 5. P. 193 - 220.

⁷ U.S. Supreme Court, *Griswold v. Connecticut* 381 U.S. 479 (1965).

⁸ Статья: Особенности формирования межсистемных правовых образований для регулирования защиты персональных данных при их трансграничной передаче (Нефедов Б.И., Истомин Н.А.) ("Российский юридический журнал", 2021, N 2)

⁹ Dário Moura Vicente Sofiade Vasconcelos Casimiro Editors «Data Protection in the Internet» P 410

административную процедуру возмещения ущерба, управляемую правительственным агентством, и (3) определяла условия, при которых правоохранительные органы могли получить доступ к данным, соблюдая различные стандарты доказательств.

Опыт американской доктрины в защите приватной жизни индивида всеобъемлюще повлиял мировую концепцию рассмотрения персональных данных гражданина. Конкретным актом можно рассмотреть Всеобщую Декларацию прав человека, принятой Генеральной Ассамблеей ООН 10.12.1948, а именно статью двенадцатую: «Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек имеет право на защиту закона от такого вмешательства или таких посягательств.»¹⁰. Данное положение лишь заложило основу в мировом направлении защиты частной жизни лица, став фундаментом для создания будущих норм в данной сфере права. Оно не могло предоставить будущую защиту данных лица из-за постоянных прогрессивных скачков в развитии технологий, из-за чего пришлось создавать более детальные и узкие нормы ради обеспечения приватности граждан. Так, огромный вклад в развитие и создание подобных норм внёс Европейский континент. основополагающими документами здесь являются Закон Земли Гессен 1970 года, изданный в ФРГ- «О защите личных данных»¹¹ и Федеральный закон о персональных данных 1977 года. Закон Земли Гессен обеспечивал запрет об уведомлении 3 лиц о полученных персональных данных, однако он не проводил обязанность согласия субъекта персональных данных на обработку этих данных. Закон 1977 года в свою очередь закрепил определение для такого понятия как персональные данные: «Персональные данные – это данные о личных или фактических обстоятельствах, относящихся к определенному или определяемому

¹⁰ "Всеобщая декларация прав человека" (принята Генеральной Ассамблеей ООН 10.12.1948)

¹¹ http://www.datenschutz.rlp.de/downloads/hist/ldsg_hessen_1970.pdf

(идентифицируемому) физическому лицу»¹². Данное определение углубляет сформированные принципы и наработки в сфере защиты персональных данных граждан. Принципы защиты неприкосновенности частной жизни индивида, определенно, уже были закреплены, как в вышеупомянутой Декларации прав человека, так и в Основном законе ФРГ. Так что немецкий опыт в данной отрасли лишь показывает нам, что уже ко второй двадцатого века регулирование вопроса приватности перешло от конституционного уровня к конкретным нормативным актам. Но не менее важно само определение немецким законодателем цели и направления стремления защиты граждан в данной сфере. Конституционный суд ФРГ объяснял данное стремление с позиции необходимого условия для развития личности в рамках демократической системы общества. Защита граждан от незаконного хранения, сбора, обработки их данных является условием свободы личности и её равенства с остальными субъектами правоотношений. Закон должен гарантировать право личности на предоставление своих данных и использование их обратной стороной¹³.

Проанализировав ранний этап формирования института, можно сделать ряд выводов. Как уже было сказано, проблема защиты приватности является относительно новой для правового сегмента. Конституционная защита прав послужила фундаментом для дальнейшей деятельности законодателя в сфере защиты персональных данных граждан. США внесли значительный вклад в определении вектора для ученых. Однако на исторически первых этапах в решении данной проблемы тяжело заметить фокус внимания исследователей на охране именно технической стороны обработки, сбора и использования данных гражданина. Поэтому в следующей части своей работы я бы хотел отделить этапы внимания законодателя от формулировки общей неприкосновенности частной жизни гражданина к защите именно персональных данных в

¹² §2(1) Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG), 1977. S. 202.

¹³https://web.archive.org/web/20101116085553/http://zensus2011.de/fileadmin/material/pdf/gesetze/volkszaehlungsurte_1_1983.pdf

соответствии с новой технологической плоскостью и условием современной эпохи.

§ 2 Конкретизация понятия персональных данных: современный опыт зарубежного регулирования частной сферы жизни гражданина.

В прошлой части работы мною был рассмотрен процесс формирования института персональных данных. Определенно, он внес огромное значение в будущую исследовательскую работу, но его изучение даёт нам крайне мало информации о понимании текущего регулирования данной сферы. Чтобы определить вопрос регулирования персональных данных, статус сетевых идентификаторов, нам необходимо проанализировать переход от ранней стадии с всё более новому и современному взгляду на защиту персональных данных гражданина.

Фокус внимания стоит перевести на совершенно качественно новый документ, который сильно продвинул правовую науку и практику в исследуемом вопросе- Директива N 95/46/ЕС Европейского парламента и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных", которая нынче утратила свою силу в связи с выходом новой Директивы в 2018 году, к которой я обращусь позже. В директиве сохранились цели защиты персональных данных, закрепленные в первой статье. Однако уже во второй статье мы можем ознакомиться с определениями, которые нам предоставляет Директива. Под «персональными данными» теперь же понимается: «любая информация, относящаяся к определенному или определяемому физическому лицу ("субъекту данных"); определяемым является лицо, которое может быть определено, прямо или косвенно, в частности, через идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической,

культурной или социальной идентичности»¹⁴. Также документ закрепил собственную сферу применения. Директива охватывает полную или частичную обработку персональных данных автоматизированными средствами и к обработке неавтоматизированными средствами персональных данных, составляющих часть файловой системы или предназначенных составлять часть файловой системы. Из данной посылки можно сделать ряд выводов. Первое, закреплена обширная сфера защиты данных-формулировка «любая информация», а также необходимость принадлежности её к субъекту защиты. Второе, закреплено то, что европейский законодатель стремится защитить любую возможность обработки автоматизированным или же неавтоматизированным средством данных субъекта. Многие страны перенесли определение персональных данных в свое национальное законодательство, но поскольку определение имеет широкое содержание, оно привело к будущему различному толкованию со стороны этих государств¹⁵. Важной, особенно в рамках производимого исследования, проблемой определения персональных данных в Директиве 1995 года выступило отсутствие включения в определение персональных данных сетевых идентификаторов гражданина. Также не были включены в определение биометрические данные гражданина, генетические данные, которые напрямую связаны с данными о физическом лице. Вышеперечисленные недостатки европейского регулирования сферы защиты персональных данных найдут своё решение в новой Директиве, выпущенной в 2018 году, речь о которой пойдет далее.

Начиная с мая 2018 года, в Европе начал действовать новый акт о защите персональных данных, который отменил действие Директивы N 95/46/ЕС Европейского парламента и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных"- Регламент ЕС 2016/679 от 27.04.2016, GDPR - General Data Protection

¹⁴ Директива N 95/46/ЕС Европейского парламента и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных"

¹⁵ Handbook of Research on Cyber Law, Data Protection, and Privacy, 2022

Regulation. Регламент имеет силу на территории 28 государств ЕС. Данный акт имеет ряд особенностей: был введен экстерриториальный принцип юридической сил акта об обработке данных, а также была глобально усилена ответственность за нарушение этих правил¹⁶. Стоит отметить, что GDPR является наиболее обширным и полным актом в сфере защиты персональных данных в орбите международных и наднациональных правовых актов о персональных данных. Акт создает серьезные обязательства для государств-участников, поэтому государствам срок для подготовки к началу соблюдения данных правил в 2 года¹⁷. Под персональными данными в GDPR стала пониматься любая информация, которая имеет отношение к идентифицированному или идентифицируемому физическому лицу (субъекту персональных данных). Идентифицируемое лицо – это лицо, которое может быть идентифицировано, прямо либо косвенно, посредством ссылки на идентификационный номер, данные о местоположении, онлайн-идентификатор или один либо несколько специфичных факторов, касающихся его физической, психологической, генетической, ментальной, экономической, культурной либо социальной идентичности¹⁸. Также GDPR закрепил важный принцип в условии хранения персональных данных. Акт выдвинул ограничительное условия хранения и обработки данных, заключающееся в том, что данные должны храниться в форме, позволяющей идентифицировать субъекта данных, не более срока, чем это необходимо для целей, для которых обрабатываются персональные данные¹⁹. Также обработчик данных обязан применять технические и организационные меры, такие как шифрование для обеспечения уровня безопасности²⁰. В поле

¹⁶ Статья: Защита персональных данных в условиях применения цифровых технологий (Солдатова В.И.) ("Lex russica", 2020, N 2)

¹⁷ Castro, D., & Chivo, E. (2019). Want Europe to have the best AI? Reform the GDPR. International Association of Privacy Professionals. <https://iapp.org/news/a/want-europe-to-have-the-best-ai-reform-the-gdpr/>

¹⁸ Статья 4 Регламент N 2016/679 Европейского парламента и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)".

¹⁹ GDPR Статья 5.1.е.

²⁰ GDPR Статья 32

понятие персональных данных были включены выше упомянутые сетевые идентификаторы и биометрические данные физического лица²¹.

“Data protection by design”:

Принцип “Data protection by design”, заложенный в GDPR, четко даёт понять взгляд европейского юридического сообщества на формирование будущей законодательной системы в области защиты персональных данных, так как в своем ядре он предназначен для борьбы с злоупотреблением использованием новых появляющихся средств обработки данных²². Данный принцип гласит, что сторона, обрабатывающая данные субъекта, обязана учитывать риски при осуществлении своей деятельности, а также предоставлять необходимые гарантии защиты данных субъектов²³.

Введение новых принципов, расширение ключевых понятий, совершенствование инструментов регулирования- всё это является заслугой европейского законодателя, который повлиял на продвижение науки правовом поле конфиденциальности. Отношение к данной проблеме отличает европейского законодателя особым моральным и нравственным характером его деятельности: расширение требований в процессе работы с данными; опора на добросовестность стороны, обрабатывающей данные и повышение роли конфиденциальности на примере роста ответственности за нарушение введенных правил. Так, анализ европейского законодателя на примере двух основополагающих актов, упомянутых ранее, предоставляет нам образ текущего уровня подхода общепринятого законодательства в общих чертах. Далее же можно перейти к рассмотрению отечественного опыта в регулировании персональных данных, а также вектора, который российская доктрина принимает как превалирующий.

²¹ GDPR Статья 9

²² The Future of Privacy. Article 29 Data Protection Working Party. Working Party on Police and Justice. 02356/09/EN WP 168. 2009.

²³ Klitou D. Privacy-Invasive Technologies and Privacy by Design // Information Technology and Law. 2014. Vol.

§ 3 Регулирование персональных данных в Российской Федерации: история отечественного подхода и основные проблемы

Российская доктрина, как и американская, взяла старт в анализе вопроса о неприкосновенности частной жизни еще в 19 веке. Устав о Телеграфах 1876 года и Почтовый устав 1857 уже содержали в себе нормы, направленные на защиту частной жизни²⁴. Так, дореволюционные акты содержали в себе нормы о неприкосновенности корреспонденции. Определенно, можно заявить, что данная норма относится к сфере неприкосновенности частной жизни. С приходом советской власти работа в данном направлении была приостановлена на определенный срок, однако уже в 1936 году получила своё законодательное отображение норма о неприкосновенности личности, а также о неприкосновенности жилища и переписки. Указанные нормы были закреплены в Конституции 1936 года, однако на практике они, к сожалению, были лишь формальностью²⁵. Но не стоит отрицать, что на теоретическом уровне это было крупным достижением советского законодателя, так как, прежде всего, эти нормы были закреплены на конституционном уровне. Спустя несколько лет проблема прав человека снова осталась без внимания из-за изменения политики в сторону более радикального подхода по отношению к инакомыслящим. С наступлением политической «оттепели» в 50-60 годах в СССР вопрос защиты неприкосновенности жизни граждан снова пошел в обсуждаемую законодательно повестку. Выход в свет новой Конституции 1977 года вывел на новый уровень советский подход к неприкосновенности частной жизни, закрепив достижения советской доктрины последних лет. Конституция закрепляла, что личная жизнь граждан, тайна переписки, телефонных переговоров и телеграфных сообщений охраняются законом;²⁶ст. 55

²⁴ "Модернизация информационных отношений и информационного законодательства: Монография" (Терещенко Л.К.) ("ИЗиСП", "ИНФРА-М", 2013)

²⁵ Указ Соч. (Терещенко Л.К.)

²⁶ "Конституция (Основной Закон) Союза Советских Социалистических Республик" (принята ВС СССР 07.10.1977) (ред. от 14.03.1990)

гарантировала неприкосновенность жилища граждан СССР²⁷. Все эти элементы были объединены и привели к окончательному формированию права на неприкосновенность частной жизни в Декларации прав и свобод человека и гражданина 22 ноября 1991 года²⁸ в ст. 9: «Каждый имеет право на неприкосновенность его частной жизни, на тайну переписки, телефонных переговоров, телеграфных и иных сообщений.»²⁹. Статья была помещена в Конституцию РФ 1993 года.

Предыдущим этапом в создании отечественного акта о защите персональных данных является Федеральный закон 1995 "Об информации, информатизации и защите информации». Важно устремить фокус внимания на данный акт из-за его новаторских качеств в формировании понятия персональных данных. Из второй статьи закона можно вывести определение персональных данных- «информация о гражданах (персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность»³⁰. Да, проводя сравнительный анализ с ранее рассмотренным европейским подходом можно выявить некоторые отличия во взгляде отечественного законодателя на понятие персональных данных. Отечественный законодатель решил пойти сформировать свое собственное определение персональных данных, введя слово «косвенно» в определение Данная особенность даёт понять, что в российском правовом поле граница охвата регулирования персональных данных намного шире по сравнению с европейским правопорядком из-за того для определения информации как персональных данных вовсе не обязателен факт её необходимости для определения или же идентификации личности³¹.

²⁷ Статья: История, смысл и перспективы института персональных данных (Дмитрик Н.А.) ("Вестник гражданского права", 2020, N 3)

²⁸ Статья: Актуальные проблемы реформирования законодательства о суррогатном материнстве (Богданова Е.Е., Белова Д.А.) ("Актуальные проблемы российского права", 2021, N 4)

²⁹ Постановление ВС РСФСР от 22.11.1991 N 1920-1 "О Декларации прав и свобод человека и гражданина"

³⁰ Федеральный закон от 20.02.1995 N 24-ФЗ (ред. от 10.01.2003) "Об информации, информатизации и защите информации"

³¹ Статья: К вопросу о правовом режиме Больших данных (Романова А.Ю.) ("Конституционное и муниципальное право", 2019, N 8)

Но и финальным основным документом в регулировании конфиденциальности граждан выступил Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных". Я хотел бы кратко рассмотреть причину небольшого отхода от европейской концепции определения персональных данных. Стоит упомянуть, что разработка федерального закона началась еще до выхода описанной ранее европейской Директивы 1995 года. Исходной концепцией закона был проект с названием «Об информации персонального характера» 1998 года. Однако данный проект не получил своего развития и позже был подготовлен новый проект, разработанный рабочей группой в Совете Безопасности РФ. Данный проект вышел в свет в 2006 году в форме ФЗ «О персональных данных» от 27.07.2006 г. №152-ФЗ.

Именно по этим причинам Российский подход имеет свой уникальный взгляд на концепцию защиты персональных данных, не отождествляя себя ни с американским подходом, ни с европейским. Так, проделанный анализ данной главы предоставляет нам достаточное понимание для последующего рассуждения на тему элементов персональных данных и сравнения мировых порядков. Безусловно, дальнейший труд невозможен без отсылок на первую главу и добавления новых структурных компонентов, необходимых для исследования. Этими замечаниями можно завершить первую главу моей работы, перейдя к следующей части исследования.

Глава 2 Сетевые идентификаторы гражданина как элемент института персональных данных

§ 1 Структура института персональных данных: пользовательские данные как элемент персональных данных

Персональные данные, как уже говорилось ранее, с течением времени и развитием технологического прогресса охватывают всё больший и больший массив информации, которая позволяет идентифицировать индивида. Вопрос об определении общей совокупности элементов, подходящих к сфере

персональных данных, воспринимается по-разному в зависимости от правопорядка. Так, можно снова обратиться к упомянутому GDPR, который воспроизводит общую систему компонентов персональных данных. К ним можно отнести: имя лица; физические характеристики; информацию о здоровье; данные о местоположении; экономическое, культурное, социальное положение лица; идентификационный номер и сетевые идентификаторы (включая IP – адреса) ³². В российском правопорядке структура системы будет схожа с европейской; она включается в себя: ФИО; пол и возраст; биографические факты; семейное положение; ³³данные об образовании; финансовое положение³⁴ и фотография личности³⁵.

Структура персональных данных охватывает в себя элемент «пользовательских данных», компоненту которых посвящена данная часть работы. Теперь же нужно разобраться в соотношении этих двух понятий и определить особенность «пользовательских данных». Пользовательские данные – это данные, которые обычно являются уникальными для каждого пользователя и используются им для выполнения конкретных задач³⁶. Причиной перехода фокуса внимания к пользовательским данным является их область применения. Так, пользовательские данные находятся в активной фазе, когда субъект персональных данных взаимодействует с какими-либо объектами в сети Интернет. Почему же важна категория пользовательских данных. Дело в том, что с развитием технологий и средств массовой информации люди делают пользовательские данные доступными для всех видов электронных носителей. Многие разработанные и широко используемые технологические системы при встрече с пользователем записывают его номер телефона и дату подключения к этой системе. Электронные средства массовой информации часто имеют

³² Регламент N 2016/679 Европейского парламента и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)"

³³ Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) "О персональных данных" (с изм. и доп., вступ. в силу с 01.03.2023)

³⁴ Письмо Роскомнадзора от 07.02.2014 N 08КМ-3681

³⁵ Письма Роскомнадзора от 10.02.2020 N 08АП-6782, Минцифры России от 17.07.2020 N ОП-П24-070-19433

³⁶ IBM Documentation. URL: <https://www.ibm.com/docs/en/aix/7.2?topic=strategy-system-data-versus-user-data>

тенденцию получать доступ к большему, чем желаемые частные данные. Например, если мы посмотрим на широко используемые сегодня приложения, у владельца данных запрашивается разрешение на доступ к частным данным, таким как телефонные номера, сообщения и детали разговоров человека, который хочет установить приложение на свое мобильное устройство, а владельцы данных предоставляют доступ для установки и использования приложения. Методы получения пользовательских данных меняются с каждым днем. Широко используемым методом доступа к данным является доступ с согласия лица в связи с положениями о предотвращении использования пользовательских данных, регулируемые законодательством³⁷.

К пользовательским данным относятся cookies, IP-адреса, геолокационные данные, данные о посещенных веб-страницах, поисковых запросах и т.п. Так, эти компоненты пользовательских данных позволяют их владельцу анализировать время, действия, которые осуществляет пользователь онлайн-ресурса, что позволяет делать выводы о конкретных интересующих вещах на портале.

Стоит отметить, что пользовательские данные имеют ряд отличающих их от персональных данных характеристик. Да, являясь категорией персональных данных, пользовательские данные характеризуются наличием специальной цели их обработки. В рамках данной категории данных их владельцу не так важно будет информацию, например, о его реальном имени или физические особенности. Сейчас же владельцу сервиса необходима информация о поведении пользователя на данный ресурс. Так, он может выработать взаимодействие с клиентом, получить информацию о представляемом продукте, узнать предпочтения пользователей.

Переходя от пользовательских данных к идентификаторам, стоит также разобраться и с данным институтом. Онлайн-идентификатор используется для

³⁷ Data Privacy Notice on the duties of disclosure upon the collection and processing of personal data in accordance with the Swiss Data Protection Act and the EU General Data Protection Regulation (GDPR)

доступа к различным интернет-сервисам, включая социальные сети, электронную почту, онлайн-банкинг³⁸. Идентификатор также используется для идентификации пользователя в системах электронной подписи и для подтверждения личности во время онлайн-платежей. Да, частота использования данной технология достаточно высокая, особенно, в рамках работы пользовательских данных.

Онлайн-идентификаторы гражданина помогают предотвращать мошенничество и кражу личных данных, поскольку они обеспечивают проверку подлинности и личности пользователя. Кроме того, использование онлайн-идентификаторов гражданина может ускорить процесс регистрации на сайтах и в онлайн-сервисах, так как пользователь может использовать один и тот же идентификатор для доступа к различным сервисам.

Однако, использование онлайн-идентификаторов гражданина также может вызывать опасения в отношении безопасности персональных данных, особенно если идентификатор становится известен злоумышленникам. Поэтому важно соблюдать правила безопасности и сохранять конфиденциальность своих онлайн-идентификаторов³⁹.

Я считаю, что для более подробного и понятного ответа на вопрос о регулировании сетевых идентификаторов, можно рассмотреть на конкретном примере работу идентификатора

Cookie- файлы- это специальные файлы, находящиеся на диске компьютера пользователя и содержащие текстовую информацию, которая нужна серверу для функционирования какого-либо сайта⁴⁰. Куки применяются с целью аутентификации пользователя и отслеживания его запросов, предпочтений на

³⁸ Markus S., Matthias E., Martin S. Web-Tracking Report 2014 // SIT Technical Reports. 2014.

³⁹ Charlotte R. Like or Dislike – Web Tracking // Big Data in Context (eds.: Thomas H., Barbara K.-R.). 2018.

⁴⁰ Статья: Информация об интересах и поведении потребителя как объект правоотношений в период цифровизации (Белов В.А.) ("Журнал российского права", 2023, N 2)

сервисе. Они позволяют пользователю однократно ввести интересующую сервис информацию, не прибегая к многократному повторению процесса ввода данных.

§ 2 Правовое регулирование сетевых идентификаторов как пользовательских данных в зарубежных правовых порядках

США:

В США правовое регулирование пользовательских данных осуществляется на федеральном и штатном уровнях. Эта тема остается крайне актуальной в свете роста количества онлайн-сервисов и социальных сетей, которые собирают и хранят большие объемы личной информации пользователей. В большинстве законов, регулирующих защиту пользовательских данных в США, упоминается роль онлайн-идентификаторов (например, cookies, IP-адресов и т.д.) в сборе и использовании личной информации пользователей. Некоторые законы конкретно прямо регулируют использование онлайн-идентификаторов, в то время как другие относятся к этому вопросу более косвенно. Далее я бы хотел систематично рассмотреть структуру основных актов, которые касаются регулирования пользовательских данных и онлайн идентификаторов гражданина:

1. «Закон о защите конфиденциальности детей в интернете» (COPPA) запрещает сбор личной информации детей младше 13 лет без явного согласия их родителей или опекунов. Это включает сбор информации с помощью cookies и других онлайн-идентификаторов.⁴¹
2. «Закон о защите потребителей Калифорнии» (CCPA) требует, чтобы компании, которые продолжают личную информацию пользователей третьим сторонам, предоставляли пользователям возможность отказаться от такой

⁴¹ Federal Trade Commission. (2019). Complying with COPPA: Frequently Asked Questions. <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>

продажи. Это относится и к онлайн-идентификаторам, которые могут быть использованы для определения личности пользователя.⁴²

3. GDPR, хотя и не является законодательством США, но имеет применение к многим компаниям, работающим в США. GDPR устанавливает требования для сбора, использования и хранения личной информации пользователей, включая информацию, собранную с помощью cookies и других онлайн-идентификаторов.

Также следует отметить, что Федеральная комиссия по торговле США (FTC) рекомендует бизнесам соблюдать общие принципы защиты данных, включая сбор и использование сетевых идентификаторов только с согласия пользователя и обеспечение безопасности их хранения⁴³. Согласно законодательству США, сетевые идентификаторы могут рассматриваться как личная информация, если они могут быть использованы для идентификации конкретного пользователя. В этом случае, использование сетевых идентификаторов подпадает под регулирование в соответствии с соответствующим законодательством.

ЕС:

Одним из основных законодательных актов, регулирующих пользовательские данные в ЕС, является уже не раз упомянутый GDPR. GDPR устанавливает общие правила по обработке и защите персональных данных всех физических лиц в ЕС, независимо от их гражданства или места жительства. Кроме того, GDPR устанавливает обязательства для всех организаций, обрабатывающих персональные данные, включая требования к получению согласия на обработку данных, право на доступ к данным и право на удаление данных. Еще одним важным законодательным актом, регулирующим пользовательские данные в ЕС, является Директива по электронной коммерции (eCommerce Directive), которая была принята в 2000 году. Директива регулирует коммерческие сайты и услуги, предлагаемые в Интернете, и устанавливает правила по предоставлению

⁴² California Attorney General. (2021). California Consumer Privacy Act (CCPA). <https://oag.ca.gov/privacy/ccpa>

⁴³ Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business; (FTC): <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>

информации о компании, а также требования к обработке персональных данных пользователей⁴⁴.

Европейский подход к регулированию пользовательских данных также включает в себя защиту персональных данных в рамках бизнес-отношений. Пример: контракты на обработку персональных данных по требованию законодательства обязаны иметь определенные стандарты безопасности и конфиденциальности, а также предусматривать возможность регулярной проверки соответствия.

Таким образом, регулирование пользовательских данных и сетевых идентификаторов в ЕС основано на принципах конфиденциальности, согласия и прозрачности. Оно предусматривает права пользователей на доступ, исправление, удаление и передачу своих данных, а также требует от организаций обеспечивать безопасность и конфиденциальность данных. Регулирование сетевых идентификаторов также включает в себя защиту данных в рамках бизнес-отношений и уведомление пользователей о любых нарушениях безопасности⁴⁵.

Далее стоит объединить перечисленные факты, исходя из проведенного исследования:

ЕС охватывает весь объем использования пользовательских данных, с момента получения ее элементов из различных источников, включая обработку этих данных и заканчивая решением с проведением права на их оспаривание. США же в свою очередь регулирует пользовательские данные методом установления фрагментарных ограничений на сбор и эксплуатацию перечисленных видов данных .

§3 Правовое регулирование пользовательских данных и сетевых идентификаторов в РФ

⁴⁴ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic

⁴⁵ Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. 3 October 2017.

Подходя к финальной части работы, стоит сказать, что мною был проанализирован в первой главе институт персональных данных сначала на зарубежном уровне, потом на национальном, а во второй главе переход к пользовательским данным, в частности, онлайн-идентификаторам лица. В прошлом параграфе я рассмотрел общую концепцию регулирования данных объектов права на примере США и ЕС. Так что логично было бы перейти к национальному уровню РФ, проведя сравнительную характеристику с рассмотренными выше правовыми порядками.

Рассмотреть регулирование стоит, основываясь на уже охарактеризованных в первой главе работы, законодательных актах, таких как: Федеральный закон "О персональных данных"; Федеральный закон "Об информации, информационных технологиях и о защите информации" и Федеральный закон "О связи".

Вышеперечисленные законы устанавливают правила обработки данных, требования к их защите, а также права и обязанности субъектов персональных данных.

Отличительными характеристиками российского подхода к регулированию пользовательских данных заключаются в усилении контроля государства за их обработкой. Например, Федеральный закон "О персональных данных" предусматривает обязательную регистрацию баз данных, в которых содержатся персональные данные. Также законодательство обязывает операторов обеспечивать защиту персональных данных на высоком уровне, что может создавать дополнительные затраты для бизнеса ⁴⁶.

Российское законодательство устанавливает обязательность использования определенных сетевых идентификаторов при оказании услуг связи, например, уникального идентификатора абонента (MSISDN) для мобильной связи и стационарного номера телефона (NAT) для фиксированной связи. Кроме того, закон устанавливает требования к обеспечению безопасности передачи

⁴⁶ "Цифровая экономика: актуальные направления правового регулирования: научно-практическое пособие" (под ред. И.И. Кучерова, С.А. Синицына) ("ИЗиСП", "НОРМА", 2022)

информации через сеть связи, в том числе защите от несанкционированного доступа к сетевым идентификаторам и защите от перехвата информации⁴⁷.

В целом, регулирование пользовательских данных и сетевых идентификаторов в России направлено на защиту прав граждан на конфиденциальность пользователей и безопасность информации, которую они предоставляют во взаимодействии, а также на обеспечение безопасности функционирования систем связи. Однако, некоторые положения законодательства могут создавать дополнительные затраты и ограничения для бизнеса, что может затруднять развитие инновационных технологий и услуг в данной области.

Ширина определения категории персональных данных создает определенные проблемы в типичных ситуациях обработки данных. Получение данных о работе устройства технически не должно подходить под категорию получения персональных данных⁴⁸. Однако владельцы данных сервисов обязаны соблюдать конституционные права⁴⁹ граждан - что доказывает судебная практика⁵⁰. Так, онлайн-сервисы, получая данные о пользователе при создании им своей учётной записи, аккаунта или профиля, могут обработать данные, которые будут подпадать под категорию персональных данных (данные банковских карт, идентификаторы).

Следующей особенностью является обязанность стороны, обрабатывающей данные, осуществлять свою деятельность, используя базы данных исключительно на территории РФ. Локальный характер обработки влечет проблему сопоставления данных и гражданина⁵¹.

⁴⁷ Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 18.03.2023) "О связи"

⁴⁸ Харитонов Ю.С. Контекстная (поведенческая) реклама и право: точки пересечения // Право в сфере интернета (ред.: Рожкова М.А.). 2018.

⁴⁹ "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)

⁵⁰ Апелляционное определение Московского городского суда от 16.09.2015 по делу N 33-30344/2015
Требование: О защите нематериального блага - права на личную тайну, тайну переписки, взыскании компенсации морального вреда. Обстоятельства: Истец указал, что является пользователем электронного почтового ящика, при прочтении своей личной переписки обнаружил, что рекламные объявления, встроенные в текст письма, соответствуют содержанию текста электронной переписки истца, что нарушает его конституционное право на личную тайну, тайну переписки. Решение: В удовлетворении требования отказано, поскольку истец не представил доказательств, подтверждающих, что ответчик занимается обеспечением функционирования почтового сервиса, а также просматривает личную переписку.

⁵¹ Савельев А.И. Законодательство о локализации данных и его влияние на рынок электронной коммерции в России // Закон. 2014. N 9.

На этом стоит подвести характеристику отечественного правового положения пользовательских данных в сравнении с рассмотренным опытом США и ЕС. Первой отличительной характеристикой является прозрачность: Европейский и американский подходы уделяют большое внимание прозрачности в отношении сбора и использования данных. В России требования к прозрачности не так жестки, и иногда пользователи не имеют достаточной информации о том, как их данные собираются и используются, а также о границах обработки их данных. Локальный характер: в Европе и США регулирование пользовательских данных имеет более интернациональный характер, распространяя свое действие на зарубежные базы данных и компании. В РФ строго локального характера, описанный в законе, сильно снижает эффективность работы с данными и достоверность информации о лице в сравнении с информацией, находящейся в базе данных.

Заключение

Подводя итоги, хочу сказать, что в данной работе я попытался достаточно систематично проанализировать положение и роль в различных правовых порядках защиты данных лица, перейдя от института персональных данных к пользовательским.

В первой главе работы я попытался рассмотреть институт персональных данных, который имеет прямое отношение к пользовательским. От зарождения института, я перешел к его развитию и состоянию в современных правовых порядках ЕС и США. Далее я повернул свой курс на отечественный правовой порядок, проанализировав дореволюционный, советский и текущий период времени.

Во второй главе я рассмотрел пользовательские данные в системе персональных данных, перейдя к онлайн-идентификаторам. От этого уже возможно было перейти к анализу отечественного и зарубежного законодательства, проведя определенные рассуждения по данному вопросу.

Правовое регулирование сетевых идентификаторов гражданина, безусловно, должно сопровождаться грамотным и разумным соблюдением прав и свобод человека. Однако слишком жесткое регулирование может привести бизнес к

неэффективности и остановить его развитие. Государство должно наоборот предоставлять все меры ради сбалансированного прогресса данной экономической области, предостерегая её от нарушений, дисфункций и всевозможных скандалов.

Да, отечественный законодатель избрал собственный путь в решении данного вопроса, хоть и опираясь на зарубежный опыт. В работе были приведены особенности и недостатки российского регулирования в сравнении с зарубежным. Однако стоит следить за информационным прогрессом и быть готовыми работать над законодательством ради эффективности отечественного правопорядка, не забывая о нравственных началах подобного регулирования.

Список правовых актов

1. "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)
2. "Конституция (Основной Закон) Союза Советских Социалистических Республик" (принята ВС СССР 07.10.1977) (ред. от 14.03.1990)
3. "Всеобщая декларация прав человека" (принята Генеральной Ассамблеей ООН 10.12.1948)
4. Директива N 95/46/ЕС Европейского парламента и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных"
5. Регламент N 2016/679 Европейского парламента и Совета Европейского Союза "О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)".
6. California Attorney General. (2021). California Consumer Privacy Act (CCPA).// <https://oag.ca.gov/privacy/ccpa>
7. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

8. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. 3 October 2017.
9. Федеральный закон от 20.02.1995 N 24-ФЗ (ред. от 10.01.2003) "Об информации, информатизации и защите информации"
10. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 14.07.2022) "О персональных данных" (с изм. и доп., вступ. в силу с 01.03.2023)
11. Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 18.03.2023) "О связи"

12. Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека (утв. Президентом РФ 12.01.2023) // <http://www.kremlin.ru/acts/assignments/orders/70349>
13. Письмо Роскомнадзора от 07.02.2014 N 08КМ-3681
14. Письма Роскомнадзора от 10.02.2020 N 08АП-6782, Минцифры России от 17.07.2020 N ОП-П24-070-19433
15. Постановление ВС РСФСР от 22.11.1991 N 1920-1 "О Декларации прав и свобод человека и гражданина"
16. IBM Documentation. URL// <https://www.ibm.com/docs/en/aix/7.2?topic=strategy-system-data-versus-user-data>
17. Federal Trade Commission. (2019). Complying with COPPA: Frequently Asked Questions// <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>
18. §2(1) Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG), 1977. S. 202.
19. Data Privacy Notice on the duties of disclosure upon the collection and processing of personal data in accordance with the Swiss Data Protection Act and the EU General Data Protection Regulation (GDPR)
20. Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business; (FTC): <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance>

Список использованной литературы:

1. Статья: Гражданско-правовые аспекты регулирования оборота персональных данных (Савельев А.И.) ("Вестник гражданского права", 2021, N 4)
2. Статья: Антропология прав человека в цифровую эпоху (опыт сравнительного анализа) (Ковлер А.И.) ("Журнал российского права", 2022, N 12)
3. Eugene Bekker. Data Breach & Technology. IdentityForce. January 11, 2021.
URL: <https://www.identityforce.com/blog/2021-data-breaches>
4. Важорова М.А. «История возникновения и становления института персональных данных»
5. Warren S., Brandeis L. The Right to Privacy // Harvard Law Review. 1890. Vol. 4. No. 5. P. 193 - 220.
6. Статья: Особенности формирования межсистемных правовых образований для регулирования защиты персональных данных при их трансграничной передаче (Нефедов Б.И., Истомин Н.А.) ("Российский юридический журнал", 2021, N 2)
7. Dário Moura Vicente Sofiade Vasconcelos Casimiro Editors «Data Protection in the Internet» P 410
8. Handbook of Research on Cyber Law, Data Protection, and Privacy, 2022
9. Статья: Защита персональных данных в условиях применения цифровых технологий (Солдатова В.И.) ("Lex russica", 2020, N 2)
10. Castro, D., & Chivo, E. (2019). Want Europe to have the best AI? Reform the GDPR. International Association of Privacy Professionals. // <https://iapp.org/news/a/want-europe-to-have-the-best-ai-reform-the-gdpr/>
11. The Future of Privacy. Article 29 Data Protection Working Party. Working Party on Police and Justice. 02356/09/EN WP 168. 2009.
12. Klitou D. Privacy-Invasive Technologies and Privacy by Design // Information Technology and Law. 2014. Vol.

13. "Модернизация информационных отношений и информационного законодательства: Монография" (Терещенко Л.К.) ("ИЗиСП", "ИНФРА-М", 2013)
14. Статья: История, смысл и перспективы института персональных данных (Дмитрик Н.А.) ("Вестник гражданского права", 2020, N 3)
15. Статья: Актуальные проблемы реформирования законодательства о суррогатном материнстве (Богданова Е.Е., Белова Д.А.) ("Актуальные проблемы российского права", 2021, N 4)
16. Статья: К вопросу о правовом режиме Больших данных (Романова А.Ю.) ("Конституционное и муниципальное право", 2019, N 8)
17. Markus S., Matthias E., Martin S. Web-Tracking Report 2014 // SIT Technical Reports. 2014.
18. Charlotte R. Like or Dislike – Web Tracking // Big Data in Context (reds.: Thomas H., Barbara K.-R.). 2018.
19. Статья: Информация об интересах и поведении потребителя как объект правоотношений в период цифровизации (Белов В.А.) ("Журнал российского права", 2023, N 2)
20. "Цифровая экономика: актуальные направления правового регулирования: научно-практическое пособие" (под ред. И.И. Кучерова, С.А. Сеницына) ("ИЗиСП", "НОРМА", 2022)
21. Харитонов Ю.С. Контекстная (поведенческая) реклама и право: точки пересечения // Право в сфере интернета (ред.: Рожкова М.А.). 2018.
22. Савельев А.И. Законодательство о локализации данных и его влияние на рынок электронной коммерции в России // Закон. 2014. N 9.

Судебная практика:

1. U.S. Supreme Court, *Griswold v. Connecticut* 381 U.S. 479 (1965).
2. Апелляционное определение Московского городского суда от 16.09.2015 по делу N 33-30344/2015

Онлайн-ресурсы:

1. http://www.datenschutz.rlp.de/downloads/hist/ldsg_hessen_1970.pdf

2.https://web.archive.org/web/20101116085553/http://zensus2011.de/fileadmin/material/pdf/gesetze/volkszaehlungsurteil_1983.pdf

UPD: работа подготовлена с использованием СПС «Консультант Плюс»

