Федеральное государственное автономное образовательное учреждение
высшего образования «Белгородский государственный национальный
исследовательский университет»

На правах рукописи

Хохлова Елена Васильевна

НЕЗАКОННЫЕ ДЕЙСТВИЯ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ: УГОЛОВНО-ПРАВОВОЕ ИССЛЕДОВАНИЕ

5.1.4. Уголовно-правовые науки

Диссертация
на соискание ученой степени кандидата
юридических наук

Научный руководитель –
кандидат юридических наук, доцент
Урда Маргарита Николаевна

Белгород – 2023

ОГЛАВЛЕНИЕ

Введение 4
ГЛАВА I. СОЦИАЛЬНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НЕЗАКОННЫЕ ДЕЙСТВИЯ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ 19
§ 1. Социальная обусловленность уголовной ответственности за незаконные действия с персональными данными 19
§ 2. Ответственность за незаконные действия с персональными данными по уголовному законодательству зарубежных стран 37
§ 3. Состояние норм российского уголовного закона об ответственности за незаконные действия с персональными данными 62
ГЛАВА II. ПОНЯТИЕ И ПРИЗНАКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИМЕЮЩИЕ УГОЛОВНО-ПРАВОВОЕ ЗНАЧЕНИЕ 75
§ 1. Понятие персональных данных для целей уголовного закона 75
§ 2. Соотношение персональных данных со смежными категориями, имеющими уголовно-правовое значение 94
§ 3. Общедоступность персональных данных и ее значение для уголовно-правовой оценки содеянного 113
ГЛАВА III. ОПТИМИЗАЦИЯ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ ПЕРСОНАЛЬНЫХ ДАННЫХ 140
§ 1. Совершенствование уголовно-правовой оценки незаконных действий с персональными данными (de lege lata) 140
§ 2. Концептуальная модель уголовно-правовой охраны персональных данных (de lege ferenda) 163
Заключение 195
СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ 200
ПРИЛОЖЕНИЯ 245
Приложение 1. Проект постановления Пленума Верховного Суда РФ «О внесении дополнений в постановление Пленума Верховного Суда Российской Федерации от 25 октября 2018 года № 46 "О некоторых вопросах судебной

практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138^1, 139, 144^1, 145, 145^1 Уголовного кодекса Российской Федерации)"» 245

Приложение 2. Анкета для экспертов и результаты их опроса 250

Введение

Актуальность темы исследования. Персональные данные как высокодоходный «товар» стали первопричиной образования и тотального разрастания в Российской Федерации подпольного рынка торговли конфиденциальной информацией о человеке. О масштабной трансформации этого теневого сегмента свидетельствуют закрытые интернет-платформы, на которых размещены массовые объявления о сбыте информационных массивов – баз данных, содержащих миллионное количество строк-записей о гражданах.

За последние несколько лет в РФ имели место резонансные случаи утечки персональных данных в Глобальную сеть, которые были вызваны хакерскими атаками и иным неправомерным доступом к ним злоумышленников, приведшие не только к масштабной компрометации, но и многомиллионному материальному ущербу, связанному с устранением их последствий. Неслучайно в указе Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» в качестве целей государственной политики обозначены снижение до минимально возможного уровня количества утечек персональных данных и нарушений требований по их защите, а также обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий (п. 57).

В механизме правового обеспечения защиты персональных данных особое место должно занимать уголовное право. Однако в Уголовном кодексе Российской Федерации (далее – УК РФ) ответственность за незаконные действия, совершаемые в отношении персональных данных или с их использованием, не предусмотрена (исключение составляет ст. 173^2 о незаконном использовании документов для образования (создания, реорганизации) юридического лица).

Ввиду непризнания персональных данных самостоятельным предметом уголовно-правовой охраны, а следовательно и отсутствия сведений официальной статистики оценка количественно-качественных показателей общественно опасного поведения, связанного с персональными данными, не может быть

точной и объективной. Между тем они изменили облик преступности в разных сферах (частная жизнь, экономика, правоохранительная служба, банковский сектор и др.).

Следственно-судебная практика и сообщения средств массовой информации свидетельствуют о том, что основными причинами массовых утечек персональных данных являются так называемые «сливы», производимые сотрудниками кредитно-финансовых учреждений, телекоммуникационных компаний, маркетплейсов, сервисов доставки, транспортных компаний и др. Представители правоохранительных органов используют ведомственные информационно-поисковые системы для получения чужих личных данных и их передачи третьим лицам за денежное вознаграждение или по мотиву иной личной заинтересованности.

Новыми угрозами, порождаемыми незаконными действиями с персональными данными, становятся посягательства на национальную и государственную безопасность, террористические акты, в том числе в отношении общественных деятелей, сотрудников правоохранительных органов, военнослужащих, судей, журналистов и их близких[1]. Из недавних примеров – резонансные убийства политического обозревателя Дарьи Дугиной и военного корреспондента Владлена Татарского, персональные данные которых находились в открытом доступе на украинском сайте «Миротворец». После их убийства на странице сайта с их фотографиями появилась отметка «Ликвидирован». По заявлению постоянного представителя РФ при ООН Василия Небензя, в базу этого сайта внесены и личные данные 327 детей, которых националисты считают врагами Украины[2].

---

[1] См.: ФСБ разоблачила преступную группу, сливавшую персональные данные силовиков // РИА Новости. URL: https://ria.ru/20220620/dannye-1796661868.html (дата обращения: 16.03.2023).

[2] См.: Небензя показал в ООН распечатку скриншота с украинского сайта «Миротворец», на котором фото Дугиной перечеркнуто надписью «ликвидирована» // Российская газета. URL: https://rg.ru/2022/08/24/postpred-rossii-pri-oon-vasilij-nebenzia-ne-znaiu-pochemu-ssha-pri; Небензя задал вопрос о реакции ООН на внесение данных детей в «Миротворец» // РИА Новости. URL: https://ria.ru/20221206/deti-1836811096.html (дата обращения: 16.03.2023).

Рост умышленных преступлений для завладения персональными данными (хищение мобильных телефонов, неправомерный доступ к компьютерной информации, коррупционные, должностные и служебные преступления и др.) с целью совершения других общественно опасных деяний (получение кредитов, микрозаймов, мошенничество, вымогательство, сталкерство и др.), использование кибертехнологий, увеличивающих их гиперлатентность, – эти и другие криминальные риски обусловливают потребность активного поиска и внедрения оптимальных средств уголовно-правового противодействия рассматриваемым посягательствам.

Актуальность исследованию придает и неэффективность имеющихся в уголовном праве норм, опосредованно оберегающих персональные данные, их недостаточный предупредительный потенциал, что подтверждается несоответствием числа выявленных преступлений показателям криминальной деаномизации личной информации о россиянах в информационных ресурсах. Нуждается в рекомендациях по квалификации тех преступлений, которые закреплены в уголовном законе для охраны персональных данных, и правоприменитель, отмечающий недостаток знаний об их специфике. Изложенное подтверждает актуальность темы диссертационной работы для доктрины уголовного права, правоприменения и правотворчества.

Степень научной разработанности проблемы. Отмечая высокую потребность в проведении исследования проблем противодействия преступлениям, связанным с персональными данными, следует признать заметное отставание теоретического, прежде всего уголовно-правового, осмысления современных аспектов этого вида общественно опасных деяний и законодательного закрепления уголовно-правовых средств реагирования на них со значительным опережением практического развития права на защиту персональных данных.

Комплексный характер темы диссертационной работы явился основанием для использования нескольких групп научных источников. *Первую* из них составляют публикации, подготовленные по отдельным проблемам уголовно-

правовой охраны частной жизни и персональных данных. Это труды Э.И. Атагимовой, С.В. Баринова, И.Р. Бегишева, К.С. Беловой, Л.А. Букалеровой, М.А. Бучаковой, Е.С. Вологдиной, А.С. Горденко, В.Е. Дивольд, М.А. Дударевой, А.С. Журавлевой, Г.Г. Камаловой, О.С. Капинус, Д.В. Карелина, Д.В. Кирпичникова, Д.А. Конева, Ю.А. Кузьмина, Э.Ю. Латыповой, В.А. Мазурова, А.В. Макарова, Е.О. Машуковой, Т.Н. Нуркаевой, А.С. Озеровой, А.А. Павлинова, Н.И. Пикурова, А.Т. Потемкиной, М.А. Радовой, Е.А. Русскевича, Е.Н. Рязановой, В.С. Соловьева, С.А. Стяжкиной, А.Р. Сысенко, А.С. Унуковича, М.А. Филатовой, Э.Т. Халиулиной, И.Г. Цопановой, В.А. Чукреева, А.А. Шутовой, И.А. Юрченко и др.

Вторую группу составили научные работы по проблеме права на защиту персональных данных в контексте конституционного права на неприкосновенность частной жизни, личную или семейную тайну М.Ю. Авдеева, И.А. Вельдера, И.В. Винюковой, Ю.А. Говенко, С.П. Гришаева, В.М. Елина, А.А. Елисеевой, А.К. Жаровой, В.П. Иванского, Д.А. Ильютовича, Н.Е. Крыловой, С.Е. Кузахметовой, Б.М. Леонтьева, М.Н. Малеиной, Л.Г. Мачковского, Е.А. Миндровой, И.А. Михайловой, В.А. Новикова, С.Ю. Пашаева, И.Л. Петрухина, М.И. Проскуряковой, В.Д. Рузановой, Т.Ю. Сапранковой, О.В. Судаковой, Ю.С. Телиной, А.Х. Хуаде, Э.А. Цадыковой, И.А. Шевченко и др.

Третья группа источников включает научные труды представителей науки информационного права и общей теории права по вопросам защиты персональных данных: М.С. Абламейко, М.Н. Алексашиной, А.И. Алексеенцева, Е.В. Андреевой, В.В. Архипова, О.В. Афанасьевой, И.Л. Бачило, М.В. Бундина, М.А. Важоровой, А.В. Губаревой, А.Н. Гулемина, Е.К. Волчинской, В.В. Дятленко, И.С. Иванова, В.Н. Лопатина, А.В. Минбалеева, А.Г. Мираева, В.Б. Наумова, В.В. Павлюкова, В.Н. Петрова, Н.И. Петрыкиной, С.Г. Пилипенко, Н.И. Платоновой, О.Б. Просветовой, А.И. Савельева, В.И. Солдатовой, Л.К. Терещенко, А.С. Федосина, М.А. Федотова, Н.Е. Циулиной и др.

Интерес научной общественности к межотраслевой теме персональных данных и их охране уголовным правом нельзя признать значительным. Исключением в этом смысле стала единственная работа С.И. Гутника «Уголовно-правовая характеристика преступных посягательств в отношении персональных данных» на соискание ученой степени кандидата юридических наук (Владивосток, 2017).

Признавая высокую теоретическую ценность проведенных исследований, в целом как фрагментарные могут быть оценены имеющиеся в науке уголовного права разработки, посвященные изучаемой проблематике. Их эмпирическая основа в силу высокого динамизма и социальной подвижности проблемы персональных данных использоваться уже не может. В содержании многих публикаций на тему персональных данных нет системного исследования норм международного и зарубежного законодательства; цельно, во взаимосвязи друг с другом не освещались проблемы их охраны российским конституционным, гражданским и административным правом. Понятийно-категориальный аппарат не разработан – нет принятого научной общественностью определения персональных данных с выделением их признаков и дефиниции как предмета и средства преступления. Глубокому и обстоятельному исследованию не подвергались ошибки в уголовно-правовой оценке деяний, связанных с персональными данными, которые оказывают негативное влияние на качество правоприменения. Решение указанных проблем теоретического и прикладного характера определяет объективную необходимость проведения специального диссертационного исследования избранной темы.

Объектом исследования являются общественные отношения, связанные с установлением и реализацией уголовной ответственности за незаконные действия в отношении персональных данных или с их использованием.

Предмет исследования составили нормы Конституции РФ, международного и зарубежного уголовного права, отечественного уголовного, административного и гражданского законодательства, ведомственных и иных правовых актов, затрагивающие в своем содержании вопросы охраны

персональных данных; материалы следственно-судебной практики по изучаемой категории дел; сведения официальной статистики о преступности и правонарушениях в РФ; результаты проведенных социологических исследований.

Цель исследования определяется как формирование нового научного знания о теоретико-прикладных аспектах уголовно-правовой охраны персональных данных для противодействия незаконным действиям, совершаемым в отношении них или с их использованием.

Для достижения обозначенной цели были намечены следующие исследовательские **задачи**:

– определение социальной обусловленности уголовной ответственности за незаконные действия, совершаемые в отношении персональных данных или с их использованием, в России;

– выявление положительного зарубежного опыта уголовно-правовой охраны персональных данных;

– оценка состояния норм российского уголовного закона об ответственности за незаконные действия с персональными данными;

– раскрытие содержания нормативного и доктринальных подходов к определению персональных данных;

– разграничение персональных данных со смежными категориями, имеющими самостоятельное юридическое, в том числе уголовно-правовое, значение;

– выявление значения общедоступности персональных данных для целей уголовного права;

– установление проблем квалификации незаконных действий с персональными данными и выработка рекомендаций, направленных на их разрешение;

– формулирование научно обоснованных предложений нормотворческого характера по совершенствованию уголовно-правовой охраны персональных данных.

Методология диссертационной работы определяется характером и содержанием исследуемого круга вопросов. Основу научного исследования составил всеобщий диалектический метод познания преступлений, связанных с персональными данными. Активно применялись методы анализа и синтеза, аналогии, индукции и дедукции, сравнения и обобщения в целях вычленения и описания новых тенденций преступного поведения, связанного с персональными данными (для обоснования социально-правовой обусловленности уголовной ответственности за их незаконный оборот; выявления соотношения понятий «персональные данные», «частная жизнь», «личная тайна», «семейная тайна»; систематизации собранного материала; формулирования выводов и результатов проведенного исследования).

Статистический и документальный методы использовались для изучения документов, печатных и электронных изданий, содержащих сообщения об утечке персональных данных, официальной статистики о преступности и правонарушениях в РФ; структурно-функциональный и формально-юридический – при изучении международных нормативных актов, российского и зарубежного уголовного законодательства, постановлений Пленума Верховного Суда РФ, материалов правоприменительной практики; сравнительно-правовой – для выявления в зарубежных уголовных законах моделей ответственности за преступления с персональными данными; метод классификации – для выделения видов преступлений, связанных с персональными данными; анкетирование и логико-математический – при проведении экспертного опроса в целях выявления проблем квалификации рассматриваемых преступлений и обработки ответов экспертов.

Правовую основу исследования составили международные правовые акты, направленные на защиту персональных данных, Конституция РФ, уголовное, административное, гражданское, информационное законодательство, федеральные законы о персональных данных, подзаконные федеральные и ведомственные нормативно-правовые акты по вопросам защиты персональных

данных, соответствующие нормы уголовного законодательства ряда зарубежных стран.

Теоретическую основу диссертационного исследования составляют научные положения о криминализации деяний, квалификации преступлений и уголовной ответственности за преступления, связанные с персональными данными, а также относящиеся к объекту исследования труды по международному, конституционному, уголовному, гражданскому, информационному праву, криминологии и социологии.

На формулирование содержащихся в диссертации положений и выводов оказали влияние труды таких ученых, как М.Ю. Авдеев, С.В.Баринов, Н.Г. Белгородцева, И.В. Бондарь, Л.А. Букалерова, М.В. Бундин, В.В. Вабищевич, М.А. Важорова, И.А. Вельдер, Р.Р. Гайфутдинов, И.С. Гутник, Р.И. Дремлюга, М.А. Ершов, В.П. Иванский, В.П. Кузьмин, А.В. Кучеренко, Э.Ю. Латыпова, В.А. Мазуров, М.Н. Малеина, Н.И. Петрыкина, Н.И. Пикуров, О.Б. Просветова, Е.А. Русскевич, В.С. Соловьев, Ю.С. Телина, Л.К. Терещенко, А.С. Федосин, Э.А. Цадыкова, И.А. Шевченко, И.А. Юрченко, А.А. Шутова и др.

Эмпирическая база исследования включает:

– результаты изучения 120 приговоров, вынесенных судами по уголовным делам о преступлениях, совершенных в отношении персональных данных или с их использованием, 20 судебных постановлений о прекращении уголовного дела (уголовного преследования), 30 уголовных дел с обвинительными заключениями, 50 решений судов по гражданским делам о защите персональных данных, 70 постановлений по делам об административных правонарушениях, связанных с незаконным оборотом персональных данных, за период с 2020 по 2023 гг.;

– результаты анкетирования 250 практических работников (судей, прокуроров, следователей, оперативных сотрудников) по проблемам уголовно-правового противодействия преступлениям, связанным с незаконным оборотом персональных данных, проведённого в 2020–2023 гг. в г. Москве, г. Санкт-Петербурге, Курской, Московской, Нижегородской, Пензенской, Саратовской, Тамбовской областях и Краснодарском крае;

– статистические данные за 2020 – первое полугодие 2023 гг. о количестве нарушений законодательства о защите персональных данных и операторов персональных данных, опубликованные Генеральной прокуратурой РФ, Судебным департаментом при Верховном Суде РФ, ГИАЦ Министерства внутренних дел РФ, Следственным комитетом РФ, Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор);

– обзоры и обобщения опубликованной практики Европейского Суда по правам человека, Конституционного и Верховного судов РФ, федеральных судов общей юрисдикции уровня субъектов РФ, Генеральной прокуратуры РФ, Следственного комитета РФ, МВД России за 2020 – первое полугодие 2023 гг.;

– отчеты и экспертно-аналитические обзоры международных организаций, российских и зарубежных компаний, обеспечивающих защиту объектов информационно-коммуникационной инфраструктуры (Group-IB, Лаборатория Касперского и др.);

– результаты обобщения информации, опубликованной в печатных средствах массовой информации и интернет-изданиях.

Научная новизна диссертации обеспечивается оригинальностью подхода к исследованию персональных данных как самостоятельного социально-правового феномена, отличного от частной жизни и нуждающегося в самостоятельной уголовно-правовой охране от незаконных действий. На основе нового научного знания о теоретико-прикладных аспектах уголовно-правовой охраны персональных данных, полученного при проведении настоящего исследования, сформировано концептуальное системное представление о модели такой охраны.

На публичную защиту выносятся следующие научные положения:

1. Социальная обусловленность уголовной ответственности за незаконные действия с персональными данными определяется: 1) общественной опасностью, выраженной объективно существующими связями с самостоятельными объектами уголовно-правовой охраны: неприкосновенностью частной жизни,

собственностью, честью, достоинством, деловой репутацией, личной свободой и др.; 2) сверхспособностью к детерминации других преступлений, обусловленной интенсивной цифровизацией всех областей общественной жизни с глобальным ростом объемов вверяемой для идентификации конфиденциальной информации о человеке, обрабатываемой с использованием средств автоматизации, объективно вызвавших появление новых способов посягательств на персональные данные человека (DDOS-атаки на информационные ресурсы с помощью вредоносных программ, взлом аккаунтов, подмена личности и др.); 3) гипертаргетированностью указанных деяний – их нацеленностью на значительное число потерпевших - представителей разных социальных групп (военнослужащие, сотрудники правоохранительных органов, пациенты, клиенты банков, пользователи соцсетей, сайтов, приложений и др.); 4) существенностью вреда, причиняемого физическими и юридическим лица (материальный ущерб, моральный вред, деловая репутация), а также радикальным изменением социальной значимости вреда, причиняемого государству (национальная, общественная, информационная безопасность, обороноспособность, правосудие).

2. Уголовное законодательство зарубежных стран обнаруживает тенденцию к постановке персональных данных под непосредственную уголовно-правовую охрану путем придания им самостоятельного уголовно-правового значения: 1) *в составе охраны тайны частной жизни* (Дания, Испания, Лихтенштейн, Нидерланды, ФРГ); 2) *наряду с ней* (Беларусь, Грузия, Казахстан) или 3) *самостоятельно* (Великобритания, США, Латвия, Узбекистан, Франция, Швейцария, Швеция, Япония). *Первый подход* к формулированию уголовно-правовых запретов незаконных действий с персональными данными характеризуется поименованием их видов в качестве составляющих информации о частной жизни человека (видео или фотоизображение, аудиозапись голоса); *второй* – определением персональных данных как конструктивного признака уголовно наказуемого деяния, альтернативного сведениям о частной жизни; *третий* – выделением специального состава преступления, в котором персональные данные получают закрепление вне связи с частной жизнью.

3. В отличие от зарубежных правопорядков уголовно-правовая охрана персональных данных в России осуществляется (или может осуществляться) с привлечением уголовно-правовых средств, выполняющих иные уголовно-политические функции. Это охрана конституционных прав и свобод человека и гражданина, семьи и несовершеннолетних, экономических отношений, интересов в сфере компьютерной информации, государственной службы, правосудия и порядка управления. В механизме опосредованной уголовно-правовой охраны персональных данных условно можно выделить две группы составов преступлений, в которых персональные данные могут выступать в качестве: 1) *предмета преступления* (ст. 137, ст. 138, ст. 140, ст. 155, ст. 183, ст. 272, ст. 274^1, ст. 275, ст. 276, ст. 283, ст. 283^1, ст. 283^2, ст. 284, ст. 310, ст. 311, ст. 320, ст. 325, ст. 327, ст. 330^1, ст. 330^2 УК РФ), 2) *средства его совершения* (ст. 142, ст. 159^1, ст. 173^2 УК РФ). Учитывая низкий предупредительный потенциал имеющихся уголовно-правовых средств охраны персональных данных в силу их иного предназначения, появление новых трендов преступности и высокую степень общественной опасности самих по себе незаконных действий с персональными данными, требуется их специальная уголовно-правовая охрана.

4. Персональные данные как предмет или средство совершения преступления представляют собой зафиксированную с помощью материального носителя или в нематериальной (идеальной) форме информацию (сведения) о физическом лице (субъекте персональных данных), охраняемую в режиме конфиденциальности (ограниченного доступа), на основании которой может быть осуществлена его однозначная идентификация.

5. «Частная жизнь» и «персональные данные» – пересекающиеся понятия, исключающие полное содержательное совпадение. Они различаются режимами правовой охраны: в случае с персональными данными их конфиденциальность предполагает иную форму ограничения доступа к ним (обеспечение их неприкосновенности третьими лицами, согласие обладателя на их распространение), отличающуюся от режима тайны применительно к частной

жизни, личной или семейной тайне, что должно учитываться при конкретизации объекта уголовно-правовой охраны и предмета соответствующих преступлений.

6. Персональные данные не имеют одного правового режима. Они могут находиться в режиме конфиденциальности (ограниченного доступа) или доступной информации (общедоступность). Конфиденциальность – дискретный признак, влияющий на наличие состава преступления в случае сбора или распространения персональных данных, охраняемых в режиме конфиденциальности (ограниченного доступа), а общедоступность его исключает. Для целей уголовного права, исходя из разности правового режима открытой информации и информации ограниченного доступа, предлагается толковать понятия «общедоступность» и «конфиденциальность» применительно к персональным данным как кардинально противоположные и взаимоисключающие. С этих позиций уголовную ответственность за нарушение неприкосновенности персональных данных должны исключать согласие лица на предание огласке личных данных о себе и (или) их общедоступность. Право на неприкосновенность персональных данных является абсолютным личным правом, а потому от волеизъявления лица зависит юридически значимый факт: в случае, если обладатель этого права дает согласие на собирание или распространение персональных данных, состав преступления отсутствует.

7. В целях совершенствования механизма уголовно-правового обеспечения неприкосновенности персональных данных, с учетом положений международного права и соответствующего уголовно-правового опыта зарубежных законодателей, требуется специальная их охрана путем установления уголовной ответственности за собирание персональных данных или их распространение. Для концептуального единства уголовной ответственности проектируемый состав преступления предлагается ввести в главу 19 УК РФ по признаку общности его видового объекта со ст. 137 УК РФ (частная жизнь). Объектом здесь следует признать общественные отношения, обеспечивающие неприкосновенность персональных данных, а предметом – конкретные сведения, при наличии признаков, характеризующих их как персональные данные.

8. Для восполнения пробела, существующего в доктрине уголовного права, и размежевания понятий «частная жизнь» и «персональные данные» предлагается ввести в научный оборот определение неприкосновенности персональных данных для их непосредственной охраны уголовно-правовыми средствами. Под ней понимается самостоятельное право человека, представляющее собой гарантированные государством правомочия контролировать свои персональные данные, разрешать или ограничивать доступ к ним с определением порядка и условий такого доступа и требовать защиты в случае его нарушения.

На основании полученных теоретических результатов и выводов разработаны **предложения по совершенствованию действующего уголовного законодательства и практики его применения**:

1. Ввести специальную норму в УК РФ, устанавливающую ответственность за незаконные действия с персональными данными в следующей редакции:

«**Статья 137[1]. Нарушение неприкосновенности персональных данных**

1. Незаконные собирание и (или) распространение персональных данных в целях совершения преступления, либо повлекшие причинение существенного вреда правам и законным интересам граждан или организаций, либо охраняемым законом интересам общества или государства, –

наказываются …

2. Те же деяния, совершенные:

а) группой лиц по предварительному сговору или организованной группой;

б) с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

в) в отношении информационно-поисковых систем (баз данных), –

наказываются …».

2. Дополнить часть первую статьи 63 УК РФ пунктом «т», закрепляющим новое отягчающее наказание обстоятельство «совершение преступления с использованием персональных данных».

3. В целях обеспечения правильной и единообразной квалификации незаконных действий с персональными данными во взаимосвязи

с компьютерными, должностными, служебными преступлениями разработан проект постановления Пленума Верховного Суда РФ «О внесении дополнений в постановление Пленума Верховного Суда Российской Федерации от 25 октября 2018 года № 46 "О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138^1, 139, 144^1, 145, 145^1 Уголовного кодекса Российской Федерации)"» (*приложение 1 к диссертации*).

Теоретическая значимость диссертационного исследования выражается в том, что в диссертации обоснованы и доказаны положения, расширяющие научные представления о механизме уголовно-правовой охраны неприкосновенности персональных данных, его элементах, особенностях функционирования с учетом социальных и правовых реалий. Научно обоснована дефиниция «персональные данные» с выделением их признаков для целей уголовного закона; изучена связь персональных данных со смежными правовыми категориями частной жизни, личной и семейной тайны; проведено их разграничение; разработано понятие общедоступности персональных данных, исключающее использование средств уголовно-правовой охраны; разработано определение неприкосновенности персональных данных как самостоятельного объекта уголовно-правовой охраны. Полученные результаты и выводы могут служить концептуальной основой для дальнейшего изучения преступлений, связанных с персональными данными, и уголовного законодательства по избранию оптимальных инструментов, охраняющих соответствующие общественные отношения.

Практическая значимость диссертационного исследования. Разработанная автором модель криминализации незаконных действий с персональными данными может быть полезна в законотворческом процессе. Сформулированные по результатам исследования положения в части уточнения понятийного аппарата, а также разработанная специальная методика оценки незаконных действий с персональными данными в механизме совершения должностных, служебных преступлений, преступлений против конституционных

прав и свобод человека и гражданина, в сфере компьютерной информации будут способствовать их точному толкованию и правильной оценке, формированию единообразной следственно-судебной практики. Они могут учитываться при разработке соответствующего интерпретационного судебного акта. Итоговые выводы и результаты, изложенные в материалах диссертации, могут быть полезны при подготовке и проведении лекций и семинарских занятий по дисциплинам уголовно-правового цикла.

Достоверность результатов исследования обеспечена широким комплексом общенаучных и частнонаучных методов познания, изучением значительного количества фундаментальных и прикладных научных трудов, учебной литературы, опубликованных материалов конференций, круглых столов и семинаров, информационно-справочных и документальных источников, сообщений в средствах массовой информации, материалов, размещенных в информационно-телекоммуникационной сети Интернет, сведений уголовной статистики, обзоров опубликованной правоприменительной практики, материалов уголовных дел, результатов опроса экспертов.

Апробация результатов исследования. Диссертационная работа обсуждена на кафедре уголовного права и процесса Белгородского государственного национального исследовательского университета и рекомендована ею к защите. Отдельные положения и результаты диссертации нашли отражение в одиннадцати научных статьях, из которых шесть опубликованы в рецензируемых научных журналах, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования РФ. Основные теоретические положения, выводы и рекомендации по теме научного исследования докладывались соискателем на пяти международных (г. Краснодар, 2022; г. Москва, 2023; г. Санкт-Петербург, 2023) и всероссийских (г. Кострома, 2023, г. Владивосток, 2023) научно-практических конференциях.

Структура диссертации определяется логикой исследования, его целью и задачами и состоит из введения, трех глав, объединяющих восемь параграфов, заключения, списка используемых источников и приложений.

ГЛАВА I. СОЦИАЛЬНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НЕЗАКОННЫЕ ДЕЙСТВИЯ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

§ 1. Социальная обусловленность уголовной ответственности за незаконные действия с персональными данными

С развитием информационных технологий и их глобальным внедрением во все сферы жизни социума значительно увеличилось количество электронных баз, содержащих персональные данные о человеке, доступ к которым многократно увеличил риск вторжения в чужую частную жизнь, причинения вреда иным охраняемым благам и интересам. Так, в 2022 г. в России было зафиксировано рекордное число утечек персональных данных россиян. Как свидетельствуют эксперты «Лаборатории Касперского», количество «слитой» информации с персональными данными в нашей стране составило 1,5 млрд записей, что превышает численность всего российского населения[1]. В отчете экспертно-аналитического центра компании Group-IB говорится, что объём утечек и похищения конфиденциальной информации в 2022 г. вырос в 40 раз по отношению к 2021 г.[2]. По подсчету аналитиков InfoWatch, в 2022 г. самым продаваемым в Darkweb и закрытых Telegram-каналах типом данных стали персональные сведения о клиентах компаний и государственных органов (81 %)[3]. Ими отмечается и рост количества утекших записей персональных данных в финансовом секторе в 1,7 раза, а объема похищенных персональных данных – в 32 раза. Результатом 48 инцидентов стала компрометация 45 млн записей (имена и фамилии людей, их контакты, сведения о лежащих на счетах деньгах и др.)[4].

---

[1] Эксперт Новикова: Более 1,5 млрд записей с персональными данными попали в сеть в 2022 году // Российская газета. URL: https://rg.ru/2022/12/08/bolee-15-mlrd-zapisej-s-personalnymi-dannymi-popali-v-set-v-2022-godu.html (дата обращения: 09.12.2022).

[2] Group-IB: объём попавших в сеть персональных данных россиян в 2022 году вырос в 40 раз // Хабр. URL: https://habr.com/ru/news/t/712488/ (дата обращения: 17.03.2023).

[3] В России резко участились кражи персональных данных – число похищенных записей превысило население страны // Газета.ru. URL: https://www.infowatch.ru/analytics/analitika/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda (дата обращения: 09.01.2023).

[4] Как мошенники получают наши персональные данные из банков? Объяснил эксперт // Аргументы и факты. URL: ttps://aif.ru/money/mymoney/kak_moshenniki_poluchayut_nashi_personalnye_dannye_iz_bankov_obyasnil_ekspert (дата обращения: 17.03.2023).

Для понимания глобальности проблемы незаконного оборота персональных данных человека приведем статистику состояния защищенности неприкосновенности частной жизни в России. Она более показательна, если принимать в расчёт единицы (объем данных) расшифрованной личной информации, а не количество инцидентов с ней. В этих целях укажем в скобках количество пользователей различных приложений, плеймаркетов и прочих сервисов, чье право на анонимизацию частной жизни было нарушено. Среди допустивших попадание клиентской базы в открытые источники: Сбербанк (65 млн россиян)[1]; «Почта России» (10 млн данных отправителей и получателей)[2]; РЖД (700 тыс. сотрудников)[3]; авиакомпания «Победа» (2268 сотрудников)[4]; бизнес-школа «Сколково» (420 тыс. студентов)[5], телекоммуникационные компании «Ростелеком» (109 тыс. пользователей)[6] и «ВымпелКом» («Билайн») (2 млн абонентов)[7]; Служба доставки «Экспресс-курьер» (СДЭК) (25 млн пользователей)[8]; компания «Туту.ру» (2 млн 627 тыс. пассажиров)[9]; Delivery Club

---

[1] В разное время о компрометации учетных записей клиентов подтверждали представители Альфа-банка, МКБ, Газпромбанка, ВТБ, Почта Банка, Промсвязьбанка, «Хоум Кредита», ОТП-банка и др. См.: Сбербанк: с начала военной операции на Украине были украдены данные 65 млн россиян // Коммерсантъ. URL: https://www.kommersant.ru/doc/5413181 (дата обращения: 17.08.2022).

[2] Данные пользователей «Почты России» попали в интернет // Коммерсантъ. URL: https://www.kommersant.ru/doc/5490311 (дата обращения: 09.08.2022).

[3] Персональные данные 700 тыс. сотрудников РЖД утекли в Сеть // РБК. URL: https://www.rbc.ru/society/27/08/2019/5d65020c9a79473ae12bdea1? (дата обращения: 27.08.2022).

[4] Роскомнадзор направил запрос лоукостеру «Победа» из-за возможной утечки персональных данных сотрудников // Рамблер. URL: https://travel.rambler.ru/news/47996286/?utm_content=travel_media&utm_medium=read_more&utm_source=copylink (дата обращения: 23.08.2022).

[5] Сливы общества: IT-компании заявили об утечке данных бизнес-школы «Сколково» // Известия. URL: https://iz.ru/1336396/ivan-chernousov-natalia-ilina/slivy-obshchestva-it-kompanii-zaiavili-ob-utec (дата обращения: 25.08.2022).

[6] Роскомнадзор составил протокол на «Ростелеком» за утечки данных // РБК. URL: https://www.rbc.ru/technology_and_media/22/07/2022/62da01319a794734d858b656 (дата обращения: 17.08.2022).

[7] СМИ: «Вымпелком» допустил крупнейшую утечку данных за весь 2021 год – Daily Storm // News. URL: https://news.myseldon.com/ru/news/index/258751819 (дата обращения: 17.08.2022).

[8] Роскомнадзор запросил у СДЭК информацию об утечке данных клиентов // РИА Новости. URL: https://ria.ru/20220715/sdek-1802778865.html?utm_source=yxnews& (дата обращения: 17.08.2022).

[9] В Сети появились данные клиентов сервиса по заказу билетов Туту.ру // РБК. URL: https://www.rbc.ru/technology_and_media/02/07/2022/62c058429a7947e0e7f75aff (дата обращения: 27.08.2022).

(521 тыс. курьеров)[1]; ритейлер «Лента» (90 тыс. покупателей)[2]; алкомаркет «Красное&Белое» (17 млн покупателей)[3]; портал SuperJob (4,8 млн пользователей)[4]; интернет-магазин Ozon (450 тыс. пользователей)[5]; маркетплейс микрозаймов «Юником 24» (12 млн заемщиков)[6]. В апреле 2022 г. сервис «Яндекс.Еда», допустивший утечку персональных данных 58 тыс. клиентов и 700 тыс. курьеров[7], был оштрафован мировым судом на 60 тыс. руб., а в августе СМИ сообщили о возбуждении уголовного дела по ст. 137 УК РФ[8]. В зависимости от аккумулирующего анонимные данные оператора в открытый доступ попали ФИО, дата рождения, гражданство, номера СНИЛС, ИНН, адреса места жительства, телефоны, фото, серии и номера паспорта, суммы дохода, электронная почта, пароли от аккаунтов, данные кредитных карт, банковские счета, авиа- и железнодорожные перелеты, сведения о недвижимости, о членах семьи и др.

По оценке экспертов по незаконному обороту персональных данных, это самые большие и подробные базы с компрометацией учетных записей россиян, которые когда-либо были размещены на специализированных форумах. Активность злоумышленников в отношении именно этих данных объясняется их коммерциализацией и ликвидностью на «черном рынке», поскольку существует спрос на базы данных о российских гражданах. А потому периодически фиксируются утечки в Сеть огромного массива личной информации из баз

---

[1] Delivery Club оштрафовали на 80 тыс. руб. за утечку персональных данных // Коммерсантъ. URL: https://www.kommersant.ru/doc/5515445 (дата обращения: 17.08.2022).

[2] Роскомнадзор проверит «Ленту» после утечки личных данных россиян // РБК. URL: https://www.rbc.ru/business/03/02/2020/5e380bf19a794791dbe68722 (дата обращения: 17.08.2022).

[3] Клиенты алкомаркета «утекли» в Сеть // Коммерсантъ. URL: https://www.kommersant.ru/doc/4234529 (дата обращения: 17.08.2022).

[4] SuperJob отрицает утечку данных 5 млн пользователей // Коммерсантъ. URL: https://www.kommersant.ru/doc/4390414 (дата обращения: 17.08.2022).

[5] Почти полмиллиона логинов и паролей от аккаунтов на Ozon попали в открытый доступ // Коммерсантъ. URL: https://www.kommersant.ru/doc/4026663 (дата обращения: 17.08.2022).

[6] В Сеть утекли данные о 12 млн заемщиков микрокредитных организаций // Известия. URL: iz.ru/1005868/2020-04-29/v-set-utekli-dannye-o-12-mln-zaemshchikov-mikrokreditnykh-organizatcii (дата обращения: 17.08.2022).

[7] РКН составил протокол на «Яндекс.Еду» после утечки данных курьеров // Коммерсантъ. URL: https://www.kommersant.ru/doc/5458856 (дата обращения: 17.08.2022).

[8] СК возбудил уголовное дело после утечки данных пользователей «Яндекс.Еды» // РБК. URL: https://www.rbc.ru/society/06/08/2022/62ed82249a79476795ab9b0e (дата обращения: 17.08.2022).

данных ГИБДД, судов, полиции, турагентств, медицинских учреждений, коллекторских агентств, интернет- и офлайн магазинов, управляющих и страховых компаний, частных детективных агентств и др.

По утверждению специалистов, несанкционированный доступ к большим объёмам персональной информации в 90 % случаев допускается юридическими лицами[1]. По состоянию на 01.09.2022 реестр Роскомнадзора, уполномоченного органа по защите прав субъектов персональных данных, включает сведения о 453754 операторах персональных данных[2]. По оценке самого ведомства, это далеко не полная статистика. Свыше 6 млн организаций и индивидуальных предпринимателей занимаются обработкой персональных данных, а количество баз, откуда они получены, составляет более 3 млн В зависимости от активности в сети «Интернет» на каждого гражданина РФ имеется от 10 до 100 и более баз данных, что в среднем составляет около 13 млрд записей, содержащих личную информацию[3]. Иными словами, анализ случившихся только в последние годы инцидентов с массовой утечкой в открытые источники личных данных миллионов граждан подтверждает социальную обусловленность уголовной ответственности за посягательства в отношении персональных данных человека. Она определяется, прежде всего, объективной потребностью в защите права человека как субъекта таких данных на неприкосновенность частной жизни, которое гарантируется статьями 23 и 24 Конституции РФ, а также его информационными правами, в том числе правом на свободу информации. В решениях Конституционного Суда РФ нашла отражение позиция о том, что «использование мер уголовной ответственности оправдано необходимостью обеспечения указанных в статье 55 (часть 3) Конституции РФ целей защиты здоровья,

---

[1] Капинус О.С. Безопасность персональных данных как один из важнейших объектов конституционно-правовой охраны // Вестник Университета прокуратуры Российской Федерации. 2018. № 6 (68). С. 12.

[2] Реестр операторов, осуществляющих обработку персональных данных // Роскомнадзор. URL: https://pd.rkn.gov.ru/operators-regis (дата обращения: 17.08.2022).

[3] Подведены итоги работы Роскомнадзора в 2021 году по защите прав и интересов граждан в сфере персональных данных // Роскомнадзор. URL: https://rkn.gov.ru/news/rsoc/news74048.htm?print=1&utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 17.08.2022).

нравственности, прав и законных интересов других лиц. Устанавливая уголовную ответственность …. государство реализует *свою конституционную обязанность защищать достоинство человека, его права и свободы*» (курсив авт.)[1].

При сохранении дискуссии об основаниях уголовного запрета (или уголовной ответственности) учеными не опровергается тезис об отнесении законодателем того или иного деяния к категории преступных на основе оценки общественной опасности, раскрывающей его социальную природу. Норма уголовного закона должна предусматривать те деяния, которые действительно опасны для общества и с которыми вести борьбу можно только уголовно-правовыми средствами[2]. Учитывать в правотворчестве общественную опасность как свойство поведения людей рекомендует законотворцу и Конституционный Суд РФ в постановлении от 27.06.2005 № 7-П4[3]. В теории уголовного права доказано, что общественная опасность преступления обладает признаком причинения правоохраняемым благам неизбежного или максимально вероятного вреда, а в случае с персональными данными еще и множественного. В этой связи справедливым является мнение Э.А. Цадыковой, что «…само по себе распространение персональных данных не столько наносит ущерб личности, сколько создает возможность для причинения ущерба. Защита персональных данных подстраховывает от возможных нарушений неприкосновенности частной жизни»[4].

---

[1] По делу о проверке конституционности статьи 265 УК РФ в связи с жалобой гражданина А.А. Шевякова: постановление Конституционного Суда РФ от 25.04.2001 № 6-П // Рос. газета. 2001. 15 июня.

[2] Кудрявцев В.Н. Криминализация: оптимальные модели // Уголовное право в борьбе с преступностью. М.: Изд-во ИГиП АН СССР, 1981. С. 6.

[3] По делу о проверке конституционности положений частей 2 и 4 ст. 20, ч. 6 ст. 144, п. 3 ч. 1 ст. 145, ч. 3 ст. 318, частей 1 и 2 ст. 319 УПК РФ в связи с запросами Законодательного собрания Республики Карелия и Октябрьского районного суда города Мурманска: постановление Конституционного Суда РФ от 27.06.2005 № 7-П. Доступ из справ.-прав. системы «КонсультантПлюс».

[4] Цадыкова Э.А. Гарантии охраны и защиты персональных данных человека и гражданина // Конституционное и муниципальное право. 2007. № 14. С. 15; Конев Д.А. Цифровые технологии и биометрические данные: постановка проблемы // Пробелы в российском законодательстве. 2021. Т. 14, № 4. С. 291.

Высокая степень общественной опасности противоправных деяний с чужими персональными данными, *во-первых,* обусловлена последующим их использованием для совершения новых преступлений, а потому причиняемый от незаконного доступа и (или) распространения личной информации вред не может быть минимизирован административной ответственностью. По данным нашего опроса эксперты выделили две самые большие группы преступлений с персональными данными человека – против собственности (*44 %*) и против конституционных прав и свобод человека и гражданина (*24 %*). Как показывает следственно-судебная практика, после покупки в сети Интернет на нелегальных сервисах, занимающихся противоправным оборотом личной информации, конфиденциальные сведения о человеке (доходы, состояние здоровья, биометрия, генетика, собственность) используются для совершения правонарушений и иных преступлений как приготовление к ним[1].

Вред приобретает здесь иные качественно-количественные характеристики, что придает деяниям, связанным с персональными данными, свойство общественной опасности, отличающее его от административно-правовых нарушений. Он проявляется не только в самой «деаномизации», но и в увеличении риска наступления особой тяжести последствий для идентифицированного лица. В их числе дискредитация потерпевшего (опорочение чести и достоинства (в том числе т.н. порноместь[2]), деловой репутации, клевета), вымогательство денежных средств, а также мошеннические схемы с использованием личных данных о нем – получение микрозаймов по скан-копиям чужих паспортов, предъявление фальшивых требований по возврату налогов, перевод пенсий в различные НПФ без ведома владельца, транзакции под «легендой» хищения денег злоумышленниками, оформление кредитов и др.[3]. Для

---

[1] Хохлова Е.В. Социальная обусловленность уголовной ответственности за преступления, связанные с персональными данными // Вестник Тверского государственного университета. Серия: Право. 2022. № 3(71). С. 144.

[2] Соловьев В.С. Порноместь: сущность явления и проблемы его уголовно-правовой оценки // Уголовное право. 2017. № 6. С. 60.

[3] Кузьмин Ю.А. Кража персональных данных (криминологический аспект) // Oeconomia et Jus. 2020. № 3. С. 50; Рязанова Е.Н. Ответственность за распространение персональных данных как

получения хранящихся в мобильных телефонах персональных данных получила широкое распространение криминальная практика похищений смартфонов с целью их использования в доступе к банковским картам и счетам потерпевшего[1].

К примеру, у И. был похищен смартфон, в котором были установлены приложения «Госуслуги», мобильный банк, электронная почта и др. Злоумышленники онлайн переводом сняли деньги в мобильном банке, а получив доступ к учетной записи на «Госуслугах», изменили контактную информацию (email, моб. телефон) и пароль. После замены данных письма со ссылками и проверочные СМС-сообщения приходили им, что позволило оформить в нескольких банках на имя кредитную карту и микрозаймы на общую сумму более 1 млн руб., дебетовую карту и запросить кредит наличными. Кредит был оформлен посредством электронной цифровой подписи, полученной с использованием ИНН и СНИЛС с портала «Госуслуги». Отозвать сертификат на подпись не удалось, поскольку удостоверяющий центр, где он был выдан, не установили. Дебетовая карта была получена в другом городе по поддельному паспорту со всеми данными, которые идентифицируют личность потерпевшего (кроме фото и подписи)[2].

Увеличивается количество фактов использования методов социальной инженерии, т.е. психологического манипулирования людьми с использованием персональных данных для совершения ими определенных действий или разглашения конфиденциальной информации (52,5 % преступлений). Только в I квартале 2022 г. Банк России зафиксировал 258097 операций без согласия клиентов, объем которых составил 3 млн 294 тыс. руб. По этим фактам ЦБ РФ инициировал проверку 89554 номеров телефонов и 1886 доменных имен, используемых в противоправных целях, операторами связи и регистраторами

способ противодействия правонарушениям в сфере информационно-коммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. 2022. № 3 (95). С. 120.

[1] Бугера М.А. Борьба с хищениями сотовых телефонов и персональных данных, содержащихся в них: проблемы и пути решения // Вестник Санкт-Петербургского университета МВД России. 2022. № 2 (94). С. 109–111.

[2] Потерял телефон – отдавай миллион // Финансовая культура. URL: https://fincult.info/rake/poteryal-telefon-otdavay-million (дата обращения 02.02.2023).

доменных имен сети Интернет, а также направил в Генеральную прокуратуру РФ информацию о 1298 доменах сети Интернет для проведения проверочных мероприятий и последующего ограничения доступа к ним[1].

О других типичных способах использования расшифрованной личной информации свидетельствует обобщение следственно-судебной практики по делам, связанным с персональными данными человека. Среди них изготовление поддельных паспортов на чужое имя («кража личности»)[2]; создание «фирм-однодневок» для внесения в Единый государственный реестр юридических лиц сведений о подставном лице[3]; создание электронных цифровых подписей и совершение юридически значимых действий (например, продажа квартиры); иные посягательства против собственности (покупки в интернет-магазинах, кражи с банковских счетов и др.).

Незаконный оборот чужих персональных данных несет в себе потенциальную угрозу многим общественным отношениям при «подмене личности», когда преступник, противоправно обладая персональной информацией другого человека, выдает себя за него. Особую опасность представляют деяния, совершенные в электронных, информационно-телекоммуникационных сетях (включая сеть Интернет). Действуя от имени другого лица, злоумышленник совершает тяжкие преступления: доведение до самоубийства, вовлечение несовершеннолетних в совершение действий, представляющих опасность для их жизни; незаконный оборот наркотических средств, психотропных веществ или их аналогов, оружия или порнографических материалов или предметов (в том числе с порнографическими изображениями несовершеннолетних) и др.[4]

---

[1] Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств // ЦБ РФ. URL: https://cbr.ru/analytics/ib/review_4q_2022/ (дата обращения: 01.09.2022).

[2] См., напр.: Атагимова Э.И., Потемкина А.Т., Цопанова И.Г. «Кража личности» как самостоятельное преступление или разновидность мошенничества // Правовая информатика. 2017. № 3. С. 14–22.

[3] Шутова А.А. Социальная обусловленность существования норм об уголовной ответственности за посягательства на персональные данные // Вестник Нижегородской академии МВД России. 2015. № 4 (32). С. 333.

[4] Чукреев В.А. Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 3 (91). С. 111.

Используются персональные данные и для слежки за оппонентами в судебных спорах. При этом фигуранты уголовных дел зачастую прибегают к помощи сотрудников правоохранительных органов для получения личных сведений из служебных баз МВД, что позволяет говорить о высоком риске коррупционного поведения, способствующего нарушению неприкосновенности частной жизни человека.

Например, П-ев, совладелец федеральной сети кофеен Traveler's Coffee в г. Новосибирске, вел судебную тяжбу с бывшими партнерами за право использования кофейного бренда. Он обратился к сотруднику УЭБиПК УМВД г. Новосибирска П., который за денежное вознаграждение в размере 321 тыс. руб. предоставил бизнесмену фотографии, серии и номера паспортов, водительских прав, адреса регистрации, контактные телефоны ответчиков. П. был осужден по ст. 137 и ст. 285 УК РФ за нарушение неприкосновенности частной жизни и злоупотребление должностными полномочиями на полтора года лишения свободы условно с испытательным сроком один год, а по ч. 6 ст. 290 УК РФ за получение взятки – к 8 годам лишения свободы в колонии строгого режима со штрафом в 3,2 млн руб.[1]

Как утверждают криминологи, личные данные жертвы создают анонимность для преступников, экстремистов и террористов, лиц, призывающих к осуществлению террористической деятельности, публично оправдывающих терроризм или пропагандирующих его, что представляет угрозу как для национальной безопасности, так и для частных лиц[2]. Думается, что легализация под чужими данными членов ОПГ, киллеров, незаконных мигрантов, лиц, находящихся в международном и федеральном розыске, агентов спецслужб иностранных государств и других особо опасных преступников облегчает совершение убийств, в т.ч. государственных и общественных деятелей, посягательств на объекты обеспечения жизнедеятельности населения и др.

[1] Вынесен приговор по делу о подкупе сотрудника МВД для слежки за оппонентами в судебном споре // Legal. report. URL: https://legal.report/vynesen-prigovor-po-delu-o-podkupe-sotrudnika-mvd-dlya-slezhki-za-opponentami-v-sudebnom-spore/ (дата обращения: 07.12.2022).

[2] Криминология / под ред. В.Н. Кудрявцева и В.Е. Эминова. 5-е изд., перераб. и доп. М.: Норма-ИНФРА-М, 2022. С. 437.

Очевидно, что посягательства, связанные с персональными данными, могут быть отнесены к числу уголовно-правовых норм с двойной превенцией, т.е. «устанавливающих ответственность за общественно опасные деяния, которые обусловливают последующее совершение других преступлений»[1].

Во-вторых, социальный интерес в установлении уголовно-правового запрета на противоправный доступ к персональным данным человека и их незаконный оборот детерминирован не только массовостью преступлений, а их организованным и профессиональным характером, трансграничными связями организованных групп и использованием иностранного сегмента сети Интернет. Правоохранительные органы выявляют многочисленные случаи размещения баз с персональными данными российских граждан на территории иностранных государств. К примеру, интернет-сервис «Сердитый гражданин», оказывавший бесплатные услуги в подготовке и подаче обращений, собрал персональные данные 400 тыс. пользователей, от имени которых отправлял жалобы в различные государственные ведомства. Роскомнадзором были установлены факты передачи владельцами сервера личных данных россиян на территорию ФРГ. Поскольку портал без согласия пользователей обрабатывал их персональные данные, прокуратура г. Москвы по иску в суд добилась признания информации, размещенной на страницах сайта www.angrycitizen.ru запрещенной к распространению на территории РФ, однако данные пользователей на зарубежном хостинге удалены не были[2]. До состоявшегося решения суда НП «Гражданин», которому принадлежит сервис, неоднократно признавалось виновным в совершении административного правонарушения, предусмотренного ст. 13.11 «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)» КоАП РФ, с назначением штрафа в размере 5 тыс. руб., однако свою противоправную деятельность не прекратило. Другим примером является

---

[1] Ображиев К.В., Шуйский А.С. Уголовно-правовые нормы с двойной превенцией: понятие, сущность и виды // Законы России: опыт, анализ, практика. 2009. № 12. С. 119.

[2] Решение Гагаринского районного суда г. Москвы от 30.08.2017 по делу № 2-3908/2017 // Мосгорсуд. URL: https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/e42670fa-d3d3-4b0d-8e94-45ad1fe78753 (дата обращения: 17.08.2022).

кибератака на внутренние ресурсы РЖД жителя г. Краснодара, специалиста в it-сфере. Используя для авторизации незаконно добытые учетные записи работников ОАО «РЖД» и 96 уникальных ip-адресов, он скопировал несколько сотен тысяч фотографий и другие персональные данные 700 тыс. руководителей и сотрудников, включая имена, даты рождения, адреса, номера СНИЛС, должности, фотографии и номера телефонов. Впоследствии он опубликовал эту информацию на хостинге интернет-ресурса, расположенного в ФРГ[1].

О компрометации учетных данных российских абонентов Facebook, WhatsApp, Telegram и Google при участии зарубежных SMS-агрегаторов сообщали СМИ. Социальные сети и мессенджеры при отправке смс с кодом, подтверждающим регистрацию, получают номер телефона, коды, пароли, данные о мобильном устройстве и его местоположении. Сообщение от иностранного сервиса поступает на телефон абонента через иностранные компании-агрегаторы. Передача СМС не шифруется, что позволяет видеть содержание сообщений – контакты, фотографии и пр.[2]. В том числе и по этим основаниям борьбу с новым видом преступности в отношении персональных данных можно вести только посредством самого сурового вида ответственности – уголовной, поскольку административно-правовой запрет по степени своего воздействия в отношении нарушителя существенно ей уступает.

В-третьих, деяния, связанные с незаконным нарушением сохранности персональных данных человека, создают угрозу причинения ущерба и государственной безопасности в том случае, когда речь идет о лицах, ее обеспечивающих. Криминальная практика последних лет подтверждает факты незаконного сбора персональных данных сотрудников правоохранительных органов и военнослужащих, что создает угрозу не только их жизни, здоровью, а также личной безопасности их родных и близких. К примеру, в 2011 г. разгорелся

---

[1] Жителю Краснодарского края предъявлено обвинение в совершении киберпреступлений // Следственный комитет РФ. URL: https://zmsut.sledcom.ru/news/item/1417513 (дата обращения: 17.08.2022).

[2] Переписка и геоданные россиян могли утекать зарубежным мошенникам // Известия. URL:https://iz.ru/1385527/2022-08-26/perepiska-i-geodannye-rossiian-mogli-utekat-zarubezhnym-moshennikam (дата обращения: 17.08.2022).

скандал в связи с официальными запросами следователей Следственного управления СК РФ по Чеченской Республике в Министерство обороны РФ и другие силовые структуры с требованиями сообщить персональные данные, предоставить фотографии военнослужащих, принимавших участие в контртеррористической операции на Северном Кавказе. После обращения лидера ЛДПР В.В. Жириновского к тогдашнему министру обороны РФ Анатолию Сердюкову эти сведения были засекречены[1]. В 2022 г. по сообщениям Центра общественных связей ФСБ РФ спецслужба пресекла деятельность группы из четырех сотрудников частного сыска и налоговых органов, осуществлявших с 2019 г. в интересах третьих лиц, в том числе иностранных граждан, незаконный сбор персональной информации, позволяющей идентифицировать тридцать человек. Именно налоговики, имея доступ к базе данных «предоставляли через посредника информацию об источниках дохода физических лиц, счетах, открытых в кредитных организациях, адресах регистрации и имуществе, а также другие сведения, составляющие охраняемую законом тайну»[2].

О сохранении тенденции высокого риска физической расправы говорят подтвержденные факты убийства лиц, выполнявших свой профессиональный долг или служебные обязанности, персональные данные которых были похищены и размещены на печально известном украинском портале «Миротворец».

В-четвертых, общественная опасность деяний, посягающих на сохранность персональных данных, видится и в том, что они препятствуют нормальной деятельности правоохранительных органов и судов, затрудняют установление истины по делу, способствуют уходу виновных от уголовной ответственности, чем подрывают авторитет правосудия у граждан. К примеру, в г. Калининграде был вынесен оправдательный приговор двум убийцам местного предпринимателя. После оглашения вердикта было установлено, что личные данные трех членов коллегии присяжных заседателей использовались для оказания на них

---

[1] Чеченские следователи запрашивают данные на русских солдат // Комсомольская правда. URL: https://www.kp.ru/daily/25707/907381/ (дата обращения: 24.08.2022).

[2] ФСБ РФ разоблачила сливавших иностранцам данные о военнослужащих // Известия. URL: https://iz.ru/1352429/2022-06-20/fsb-rf-razoblachila-slivavshikh-inostrantcam-dannye-o-voennosluzhashchikh (дата обращения: 23.08.2022).

психологического давления, в том числе путем угроз расправой по мобильному телефону. Приговор был отменен, а уголовное дело рассматривалось иным составом суда присяжных, постановившим новый оправдательный вердикт. Как утверждают источники в правоохранительных органах, члены второй коллегии присяжных заседателей также получали угрозы перед каждым заседанием, о чем имеется оперативная информация[1].

Другим примером оказания психологического воздействия на суд стал процесс в Мосгорсуде по резонансному делу об убийстве в центре Москвы адвоката Станислава Маркелова и журналистки Анастасии Бабуровой. Председательствующему Александру Замашнюку при рассмотрении дела была предоставлена государственная охрана. Ее основанием послужила оперативная информация о размещении на форумах националистов в сети Интернет персональных данных судьи, что создавало вероятность их использования для совершения против него посягательств на жизнь или здоровье[2]. Сюда же относятся случаи необеспечения конфиденциальности персональных данных свидетелей по уголовному делу, получивших государственную защиту, что создает потенциальную угрозу и их личной безопасности, и отправлению справедливого правосудия. Согласимся с аргументацией С.И. Гутника, что «важность обеспечения конфиденциальности персональных данных свидетеля (фамилия, имя, отчество, место жительства, место работы и т.д.) гарантирует не только его личную безопасность, но и позволяет сохранить важный источник информации для эффективного и быстрого отправления правосудия»[3].

Как показывает судебная практика, персональные данные другого человека используются виновным с целью воспрепятствования отправлению правосудия или уклонения от отбывания назначенного судом наказания («кража личности»). В 2020 г. СМИ сообщили о резонансном уголовном деле в г. Саратове,

---

[1] «Придешь на суд – будет плохо». Как запугивают и подкупают присяжных в России // Lenta.ru. URL: https://lenta.ru/articles/2021/06/24/prisazhnie/ (дата обращения: 17.08.2022).

[2] Судье по делу об убийстве адвоката Маркелова предоставили охрану // РИА Новости. URL: https://ria.ru/20110304/342145271.html (дата обращения: 17.08.2022).

[3] Гутник С.И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: дис. … канд. юрид. наук. Красноярск, 2017. С. 107.

по которому невиновный Дмитрий Рубинштейн более полугода находился в колонии. Преступление фактически совершил сын его приемной матери – Студентов, который, обладая внешним сходством, представился Рубинштейном, а впоследствии предъявил его документы. Студентов, ранее судимый по ст. 228 УК РФ условно, был вновь задержан в 2019 г. по факту незаконного приобретения и хранения наркотиков. Опасаясь замены не отбытого наказания по первому приговору на реальное лишение свободы, он совершил подмену личности, назвав не свои данные. В связи с тем, что по второму приговору Студентову-«Рубинштейну» за нарушение режима отбывания условное наказание заменили лишением свободы, Дмитрий Рубинштейн был взят под стражу и отправлен в колонию. По данным следствия, сотрудники полиции не удостоверили надлежащим образом личность подозреваемого, в связи с чем было возбуждено уголовное дело по факту фальсификации доказательств по уголовному делу и привлечения заведомо невиновного к уголовной ответственности[1]. И подобные факты с подлогом личности преступника в правоохранительной системе нередки[2]. Иными словами, нарушение права на сохранность персональных данных одного человека детерминирует другие противоправные проявления с возрастанием степени их вредоносности по отношению к другому, более широкому спектру общественных отношений (личная свобода, авторитет правосудия, доброе имя, здоровье, жизнь).

В-пятых, общественно опасными последствиями несанкционированного доступа к персональным данным человека, хранящимися на специальных ресурсах операторов, является материальный ущерб, который может быть причинен от их похищения. Это основание коррелирует с таким социально-

---

[1] Брат за брата. В Саратове осудили и отправили в колонию невиновного // Аргументы и факты. URL: https://aif.ru/society/law/brat_za_brata_v_saratove_osudili_i_otpravili_v_koloniyu_nevinovnogo (дата обращения: 17.08.2022).

[2] Московский бизнесмен пришел получать паспорт и узнал, что давно сидит в тюрьме // Московский комсомолец. URL: https://www.mk.ru/social/2015/02/08/moskovskiy-biznesmen-prishel-poluchat-pasport-i-uznal-chto-davno-sidit-v-tyurme.html (дата обращения: 01.09.2022); Мужчина представился полиции чужим именем. Наказан невиновный // Четвертая власть. URL: https://www.4vsar.ru/news/82285.html (дата обращения: 01.09.2022); Наказали невиновного. В Смоленске нарушитель представился полицейским чужим именем // Смоленские новости. URL: https://smoldaily.ru/nakazali-nevino(дата обращения: 01.09.2022).

экономическим принципом криминализации, как причинение большого материального ущерба и морального вреда. И речь идет не только об использовании конфиденциальной информации персонального характера для совершения новых преступлений, но и о финансовых затратах, которые возникают при устранении последствий ее обнародования. Об этом на Петербургском международном экономическом форуме в 2022 г. заявил, в частности, зампред правления Сбербанка Станислав Кузнецов. В результате компрометации 13 млн банковских карт Сбербанк был вынужден осуществить перевыпуск 1 млн карт своих клиентов, ущерб от которого составил не менее 4,5 млрд руб. Другие 12 млн карт принадлежат владельцам иных кредитных организаций, что только подтверждает тяжесть последствий «большой утечки» для всей отрасли[1]. Материальный ущерб от преступлений, связанных с персональными данными, ежегодно увеличивался в геометрической прогрессии (в 2022 г. он составил 16,5 млрд руб.). По прогнозам специалистов международной компании CyberCube, глобальный ущерб, связанный с этим видом преступности, к 2025 г. достигнет 10,5 трлн долл.[2]

В-шестых, общественную опасность незаконных действий с персональными данными увеличивает их совершение с использованием информационных технологий (прежде всего, хакерские атаки на информационные ресурсы посредством вирусных программ)[3]. Существенный рост преступлений против неприкосновенности частной жизни при обработке персональных данных с использованием информационных технологий отмечается и в п. 14 Доктрины информационной безопасности Российской Федерации[4]. Правоприменительная

---

[1] Сбер оценивает ущерб от перевыпуска скомпрометированных в России карт в 4,5 млрд рублей // Газета.ru. URL: https://www.gazeta.ru/business/news/2022/06/16/17944346.shtml (дата обращения: 17.08.2022).

[2] CyberCube: глобальный ущерб, связанный с киберпреступностью, к 2025 году достигнет 10,5 трлн. долларов // Cisoclub. URL: https://cisoclub.ru/cybercube-globalnyj-ushherb-svyazannyj-s-kiberprestupnostyu-k-2025-godu-dostignet-105-trln-dollarov/ (дата обращения: 17.03.2023).

[3] Русскевич Е.А., Дмитренко А.П., Кадников Н.Г. Кризис и палингенезис (перерождение) уголовного права в условиях цифровизации // Вестник Санкт-Петербургского университета. Право. 2022. Т. 13, № 3. С. 586.

[4] Доктрина информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646 // Рос. газета. 2016. 6 дек.

практика объективно указывает на то, что именно признак использования информационно-коммуникационных технологий является новой «цифровой» формой посягательств на персональные данные, его способом (информационный)[1]. Именно он многократно повышает степень общественной опасности деяний, при совершении которых для неправомерного доступа к соответствующим объектам используются компьютерные системы или сети. Глобальная доступность к новым IT-технологиям, стремительно совершенствующимся и способствующим «перезагрузке» преступности, позволяет прогнозировать появление новых угроз их использования в ущерб конфиденциальности индивида[2].

В-седьмых, негативным следствием перехода общества в цифровую эпоху явилась все большая «миграция» преступлений, связанных с персональными данными, в киберпространство[3]. Виртуализацию этого вида преступности, как социально-криминологического фактора, обусловила масштабная цифровизация частной жизни человека. Новые информационные формы общения людей (мессенджеры, социальные сети, электронная почта, порталы госуслуг и т.п.) потребовали согласия на персональную идентификацию. Это способствовало массовому распространению в теневом сегменте Интернета анонимной информации о личности пользователей как своего рода «товара», кибер-сталкингу, или преследованию жертвы, данные которой было получены с помощью кражи онлайн-личности (в соцсетях, на веб-сайтах и через поисковые системы), кибербуллингу, диффамации и др.[4]. Все это подтверждает не только

---

[1] Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. ... д-ра юрид. наук. М., 2021. С. 364.

[2] Русскевич Е.А., Чернова К.Б. Цифровые аналоги официальных документов как предмет преступления: постановка проблемы // Вестник Московского университета МВД России. 2022. № 3. С. 231.

[3] Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. ... д-ра юрид. наук. С. 73.

[4] Соловьев В.С. Криминологическая типология механизмов совершения преступлений с использованием информационно-телекоммуникационных технологий // Вестник Краснодарского университета МВД России. 2021. № 4 (54). С. 51.

сохранение, а преумножение риска причинения вреда (ущерба) общественным отношениям, поставленным под охрану закона.

Традиционно в научных исследованиях в качестве другого из социально-криминологических оснований общественной опасности приводится показатель распространённости (массовости) того или иного посягательства, однако подобный анализ исключен ввиду объективных причин. В государственной системе учета преступлений деяния, предметом которых являются персональные данные человека либо они используются для совершения других преступлений, не выделяются специально. В юридической литературе в этой связи для противодействия их потере в общей массе иных преступлений обоснованно предлагается соответствующее изменение статистических карточек первичного учета преступлений и форм федерального статистического наблюдения[1]. Косвенно судить о состоянии с защитой персональных данных человека позволяет приведенная выше статистика, подтверждающая не только особую тяжесть последствий в виде причинения вреда (жизни, чести и достоинству, собственности, материального ущерба и др.), но и его множественность с огромным числом потерпевших[2]. К примеру, по информации Роскомнадзора, за 2021 г. граждане, чьи персональные данные оказались в свободном доступе, получили более 3,7 млн звонков от телефонных мошенников, а также с навязчивыми рекламными сообщениями, предложениями сделок по микрозаймам микрофинансовых организаций[3]. Беспрецедентное количество жертв позволяет говорить о гипертаргетированности этого вида преступности, то есть нацеленности на значительное число потерпевших – физических лиц как участников больших целевых групп (пользователи соцсетей, приложений),

---

[1] Капинус О.С. Указ. соч. С. 11.

[2] Унукович А.С. Меры предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных технологий в отношении граждан // Научный вестник Омской академии МВД России. 2023. Т. 29, № 2 (89). С. 99.

[3] Роскомнадзор пресек неправомерную обработку персональных данных 90 млн человек за два года // Рамблер. URL: https://news.rambler.ru/internet/37796282/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (дата обращения: 17.08.2022).

а также представителей отдельных социальных групп (военнослужащие, сотрудники правоохранительных органов).

О том, что количество преступлений данного вида ежегодно увеличивается, подтверждается экспертным мнением прокурорских работников. Так, по данным опроса 661 слушателя факультета профессиональной переподготовки и повышения квалификации Университета прокуратуры РФ и сотрудников прокуратуры в субъектах РФ 461 респондент (69,7 %) отметил значительный рост рассматриваемых деяний[1] (*по нашему опросу, 60 % экспертов разделяют это мнение*). При этом представители надзорного органа отнесли исследуемую группу преступлений к посягательствам с высоким индексом латентности. Процентное выражение латентности неучтенных деяний, по оценке опрошенных, выглядит следующим образом: она составляет от 26 % до 50 % (35,6 %); от 51 % до 75 % (26,6 %); от 76 % до 100 % (16,3 %). Как подсчитали эксперты, почти 2/3 уголовных дел, связанных с персональными данными, остаются нераскрытыми, что характеризует этот вид преступности как гиперлатентный.

Таким образом, социальная обусловленность уголовной ответственности за незаконные действия в отношении персональных данных определяется их общественной опасностью, выраженной объективно существующими связями с самостоятельными объектами уголовно-правовой охраны: неприкосновенностью частной жизни, здоровьем, собственностью, честью, достоинством, деловой репутацией, личной свободой и др. Эти деяния отличает гиперлатентность и сверхспособность к детерминации других преступлений (экономика, страхование, предпринимательство, банковский, финансовый сектор, налоговая, правоохранительная система и др.), что обусловлено интенсивной цифровизацией всех областей общественной жизни с глобальным ростом объемов вверяемой для идентификации конфиденциальной информации о человеке, обрабатываемой с использованием средств автоматизации, объективно вызвавших появление новых способов посягательств в отношении персональных данных человека (DDOS-

[1] Халиулина Э.Т., Журавлева А.С. Преступления, совершаемые с использованием персональных данных: характеристика состояния // Военное право. 2021. № 2 (66). С. 290.

атаки на информационные ресурсы с помощью вредоносных программ, взлом аккаунтов, подмена личности и др.). Следствием этих процессов стала гипертаргетированность незаконных действий с персональными данными – их нацеленность на значительное число потерпевших: представителей разных социальных групп (военнослужащие, сотрудники правоохранительных органов, пациенты, клиенты банков и др.) и участников больших целевых сообществ (пользователи соцсетей, приложений, сайтов). Социальная обусловленность уголовной ответственности за незаконные действия в отношении персональных данных определяется и радикальным изменением социальной значимости вреда, причиняемого государству (национальная, общественная, информационная безопасность, обороноспособность, правосудие) и юридическим лицам (материальный ущерб, деловая репутация).

§ 2. Ответственность за незаконные действия с персональными данными по уголовному законодательству зарубежных стран

Многие государства мира в последнее десятилетие реформировали национальное уголовное право в связи с высоким ростом распространенности способов совершения преступлений в отношении персональных данных человека или с их использованием. Концепция уголовно-правового противодействия преступлениям с персональными данными в европейских странах начала формироваться, *во-первых*, более трех десятилетий назад, когда с принятием специального национального законодательства был введен институт защиты персональных данных человека; *во-вторых*, под влиянием принятого Европейским союзом Общего регламента по защите персональных данных (General Data Protection Regulation, далее GDPR)[1]. Его нормы стали применяться

[1] О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных: регламент (EU) от 27.04.2016 № 2016/679. URL: https://ogdpr.eu/ru/gdpr-2016-679; О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования уголовных преступлений, ведения розыскных или судебных действий или исполнения уголовных наказаний, а также за свободное перемещение таких данных: директива (EU) от 27.04.2016 № 2016/680. URL: https://ogdpr.eu/ru/gdpr-2016-680 (дата обращения: 21.05.2022).

во всех государствах-членах ЕС с 25.05.2018. Положения GDPR были внесены в действующие либо в новые законы стран ЕС о защите персональных данных с отменой ранее принятых, а также учитывались и в государствах, не входящих в этот союз.

В-третьих, новеллы в некоторые уголовные кодексы стран дальнего зарубежья и бывшего Советского Союза последовали после принятия национальных законов о правовом регулировании защиты персональных данных. При этом в одних странах уголовно-правовые средства защиты персональных данных изложены только в кодифицированных законах, а в других – систематизируются в специальных законах, действующих вместе с кодексом или только самостоятельно.

В зависимости от технико-юридических особенностей отображения персональных данных в конструкциях уголовно-правовых норм можно выделить *три подхода* их закрепления.

Первый подход предусматривает систему норм об ответственности за нарушения неприкосновенности разного вида тайны (личной или семейной, переписки, врачебной, адвокатской, банковской, следствия и др.), в которых не упоминаются персональные данные человека, однако их охрана презюмируется ввиду расширительного их толкования как тайны; эта группа уголовно наказуемых деяний, как и в России, рассредоточена по разным разделам или главам. При этом ответственность в уголовном законе некоторых стран дальнего зарубежья предусмотрена за достаточно ограниченный круг деяний, признаваемых посягательствами на неприкосновенность персональных данных.

Одним из представителей такого подхода на сегодняшний день является Дания. Здесь действует Закон № 502 от 23.05.2018 о защите персональных данных[1], а в *Уголовном кодексе Королевства Дания*[2], в гл. 27 «Преступления против личной чести и определенных личных прав», содержатся составы

[1] Закон о защите данных (the Data Protection Act). URL: https://www.datatilsynet.dk/media/7753/danish-data-protection-act.pdf (дата обращения: 12.08.2022).

[2] Уголовный кодекс Королевства Дания (Danish Criminal Code) (с изм. и доп. от 11.08.2021). URL: http://www.unodc.org/tldb/pdf/Denmark_Criminal_Code_2016.pdf (дата обращения: 29.07.2022).

преступлений, которые по нашему УК оцениваются как посягательства на личную или семейную тайну или на тайну переписки (§263). Неизвестен уголовному закону России состав незаконного использования изображений человека как биометрических персональных данных (§264d). Виновным признается тот, «кто незаконно передает информацию или изображения, касающиеся частной жизни другого лица, или другие изображения лица при обстоятельствах, которые могут очевидно предполагаться в качестве удерживаемых от общества». Диспозиция содержит оговорку о том, что §264d применяется и в случае, если информация или изображение касаются умершего лица. В отечественной теории предлагается криминализация использования изображения человека без его согласия в СМИ, социальных сетях, по ТВ (фото, видео), когда такие материалы сопровождаются неприличными, порочащими подписями и комментариями в отношении изображенного лица[1].

В разделе V «Преступные деяния, посягающие на частную сферу и нарушающие служебную тайну» *Уголовного кодекса Лихтенштейна*[2], содержатся три состава, непосредственно связанные с незаконным получением и использованием персональных данных как информации о частной жизни лица. Это нарушение тайны переписки и сокрытие корреспонденции (§118); нарушение коммуникационной тайны (§119) и злоупотребления со звукозаписывающими и прослушивающими устройствами (§120). Иными словами, право на защиту конфиденциальных данных о человеке здесь состоит в запрете передачи информации от одних частных лиц к другим.

Говоря об особенностях уголовно-правовой охраны рассматриваемой категории информации в княжестве Лихтенштейн, А.В. Серебренникова и А.А. Трефилов указывают на то, что кодекс признает самостоятельным

---

[1] Букалерова Л.А., Остроушко А.В. Информация, содержащая фотографии (изображения) человека, нуждается в уголовно-правовой защите // Правовые вопросы связи. 2007. № 1. С. 44; Павлинов А.А. Уголовная ответственность за нарушение неприкосновенности частной жизни // Пробелы в российском законодательстве // Юридический журнал. 2013. № 6. С. 189; Латыпова Э.Ю. Некоторые аспекты уголовной ответственности за деяния, посягающие на неприкосновенность частной жизни // Oeconomia et Jus. 2019. № 2. С. 41.

[2] Уголовный кодекс Лихтенштейна / под ред. А.В. Серебренниковой. М.: МАКС Пресс, 2013. С. 69.

преступлением обнародование звукозаписи высказывания лица против его воли, когда виновный записал на диктофон голос собеседника и затем распространил его, не имея согласия на это[1]. По этому поводу теоретиками предложена имплементация аналога этой нормы в УК РФ для ее применения, прежде всего, к пранкерам, имитирующим голоса государственных деятелей и должностных лиц. Пранкер, оставаясь анонимом, в диалоге с жертвой получает, а затем публикует личную (конфиденциальную) информацию (видео-, аудиозапись), которая компрометирует собеседника[2]. Эта новелла может быть заимствована российским законодателем ввиду нарушения права на защиту персональной информации и причинения вреда репутации потерпевшего.

В *Кодексе о наказаниях Королевства Нидерланды*[3] Книги 2 Раздела V «Преступления против общественного порядка» (ст. ст. 138-139g) охрана права на неприкосновенность частной жизни связывается не с его конституционным статусом, а со способом его нарушения. Законодатель Нидерландов придает статус преступления сбору личных данных только если подслушивание, подсматривание или запись совершаются с использованием специальных технических средств[4]. Так, по ч. 1 ст. 139a специально конкретизируются способы сбора сведений: когда лицо «в жилом доме, изолированной комнате или в помещении с помощью технического приспособления» умышленно подслушивает (1) или (2) осуществляет запись разговора, не являясь его участником, без согласия собеседников. По ч. 2 наказывается лицо, использующее технические средства для перехвата и записи данных, которые передаются другим лицом в

---

[1] Серебренникова А.В., Трефилов А.А. Преступления против личности по уголовному кодексу княжества Лихтенштейна: общая характеристика // Lex Russica. 2016. № 12 (121). С. 118.
[2] Латыпова Э.Ю. Указ. соч. С. 43.
[3] Уголовный кодекс Королевства Нидерланды (Wetboek van Strafrecht van Nederland) (с изм. и доп. от 14.04.2021). URL: http://www.wetboek-online.nl/wet/Sr.html (дата обращения: 12.08.2022).
[4] Примечательно, что суд Гааги в Нидерландах еще в 2015 г. признал закон о сборе и хранении провайдерами и телефонными компаниями персональных данных пользователей интернета и телефонных сетей, аналогичный закону Яровой 2016 г., нарушающим право на частную жизнь. Согласно решению суда, запрет на хранение личных данных «может повлиять на расследование преступлений, однако это не оправдывает нарушения права клиентов компаний на частную жизнь». См.: В Нидерландах отменили закон о хранении данных пользователей телефона и интернета // Официальный сервер Международной Организации Труда. URL: https://www.kommersant.ru/doc/2685042 (дата обращения: 09.08.2022).

каком-то жилом помещении «с помощью компьютерного устройства или системы». В ст. 139b законодатель описывает аналогичные ст. 139a действия, совершенные умышленно тайно не в жилом помещении (доме, изолированной комнате), а «в любом другом месте».

Выделены в самостоятельный состав конкретные действия в отношении незаконно полученной информации о частной жизни человека, включая его персональные данные. Субъектом здесь признается тот, кому эти данные, добытые запрещенным способом, были переданы, и кто знает или предполагает преступный характер их происхождения. В п.1-3 ч. 1 ст.139e приводится описание трёх уголовно наказуемых деяний. По п. 1 предусматривается ответственность за наличие в распоряжении лица изображений и материалов, полученных в результате «незаконного подслушивания или записи разговора, телесвязи или другого типа передачи информации компьютерным устройством или системой», т.е. за их хранение; по п. 2 – за умышленное сообщение таких данных другому лицу; по п. 3 – за их умышленное распространение.

К двум составам из группы преступлений, связанных с незаконным получением персональных данных, относятся также ст. ст. 139f и 139g. Российского аналога этих составов преступлений, предусматривающих ответственность за незаконные создание, хранение или демонстрацию чужого изображения, нет. Диспозиция первого из них – ст. 139f – сформулирована по образцу усеченного состава преступления. В ее ч. 1 устанавливается наказание для того, кто «с помощью технического приспособления, обмана или хитрости умышленно создает изображение лица, присутствующего в жилом помещении и комнате, закрытых для публики, что может причинить вред законным интересам этого лица». По второй ее части виновным в хранении («имеет в своем распоряжении») изображения другого человека признается лицо, достоверно знающее или обоснованно предполагающее незаконность получения чужого видео- или фотоизображения. По второй, 139g статье, преступлением признается демонстрация изображения другого человека, полученного при обстоятельствах, изложенных в ст. 139f.

В Германии вопросам защиты персональных данных посвящены положения нового федерального закона (Bundesdatenschutzgesetz) (BDSG-neu), действующего с 25.05.2018 вместе с Положением об общей защите данных. В *Уголовном уложении Федеративной Республики Германия*[1] Раздел 15 «Нарушение неприкосновенности частной жизни и частных тайн» предусматривает защиту персональных данных как одного из видов тайн в рамках права на неприкосновенность частной жизни (переговоров, изображения, тайны частной жизни, тайны коммерческой), в том числе технически защищенных, законного доступа к которым у посягателя нет[2].

По мнению исследователей, немецкий опыт уголовно-правовой охраны личной информации о гражданах основан на детальном и достаточно жестком европейском регулировании порядка обращения персональных данных, что подчеркивает важность и значимость недопущения нарушений при сборе персональной информации, ее хранении, передаче, разглашении и использовании[3]. Другой особенностью уголовного закона ФРГ является максимально широкий подход к определению объема охраны персональных данных[4]. Так, в § 201а самостоятельно выделен запрет, выраженный в «нарушении неприкосновенности сугубо личной сферы частной жизни и прав личности посредством снимков с изображением другого лица». Подразумевается любая (обычная или цифровая) фото-, кино-, видеосъёмка, съёмка посредством инфракрасных или рентгеновских лучей и пр., кроме картин, рисунков или

---

[1] Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия (German criminal code) (с изм. и доп. от 19.06.2021). URL: http://www.gesetze-im-internet.de/englisch_stgb/ (дата обращения: 15.08.2022).

[2] Филатова М.А. Уголовно-правовая охрана персональных данных. URL: https://www.youtube.com/watch?v=mGyIkYEYn2Y&t=5714s (дата обращения 10.08.2022)

[3] Вабищевич В.В. Опыт уголовно-правовой охраны персональных данных Казахстана и Германии // Борьба с преступностью: теория и практика: тез. докл. VIII междунар. науч.-практ. конф. (23 апреля 2020 г.). Могилев: Изд-во Могил. ин-та МВД РБ, 2020. С. 24.

[4] Сапранкова Т.Ю. Особенности регламентации уголовной ответственности за нарушение неприкосновенности частной жизни в законодательстве зарубежных стран // Проблемы экономики и юридической практики. 2016. № 4. С. 124–127.

карикатур[1]. Наказывается тот, кто незаконно изготавливает, использует или публикует (распространяет) снимки, запечатлевшие другое лицо, находящееся в жилище или в ином непубличном помещении, а также его беспомощное состояние, и умершее лицо (абз.1-4). Снимки могут быть изготовлены и без нарушения закона, однако виновный без соответствующих полномочий обеспечивает третьим лицам доступ к ним, чем нарушает частную жизнь отображённого человека (абз.5).

В абз. 1 § 203а «Нарушение частных тайн» подробно описан род деятельности распространителя персональных данных человека, полученных при осуществлении им профессиональной деятельности (врач, ветеринар, аптекарь, психолог, адвокат, нотариус, аудитор, присяжный бухгалтер-ревизор, специалист по вопросам, связанным с беременностью, консультант вопросам брака, семьи, воспитания, по делам несовершеннолетних, налогам, социальный работник, педагог, сотрудник частной страховой компании). По абз. 2 § 203а за распространение чужой тайны наказываются должностные лица, лица, находящиеся на государственной службе, члены следственного комитета, эксперты, научные сотрудники при осуществлении научно-исследовательских работ и др., которым она была доверена или стала известной иным образом, и обязанные ее сохранять, и в том числе после смерти лица. Квалифицирующим признаком является цель деяния: получение вознаграждения, личной выгоды, обогащение другого лица или нанесение вреда другому лицу.

Наказуемо и сокрытие или предоставление ложных сведений о гражданском состоянии другого лица или родителях ребенка (§169 «Фальсификация актов гражданского состояния»). Объектом охраны являются только данные, подлежащие регистрации в государственном учреждении, ответственном за ведение книги записей гражданского состояния[2].

---

[1] Головненков П.В. Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия: Strafgesetzbuch (StGB): научно-практический комментарий и перевод текста закона. Постдам: Universitätsverlag Potsdam, 2021. С. 313.

[2] Павлинов А.А. Указ. соч. С. 189.

Преступлением по немецкому законодательству признается и несанкционированный доступ к персональным данным посредством преодоления их защиты (§ 202a. «Выведывание данных») или применения специальных технических средств (§ 202b. «Перехват данных») (аналог ст. 272 УК РФ). Изготовление, покупка, продажа, передача и иное распространение и обнародование кодовых слов или иных защитных кодов, компьютерных программ, открывающих доступ к данным, признаются «подготовкой выведывания и перехвата данных» (§ 202c.). В § 202d. «Скупка краденных данных» криминализированы приобретение в корыстных целях или для нанесения ущерба другому лицу закрытых данных, использование доступа к ним, распространение и иные способы придания им публичности (абз. 1 § 202d).

В Испании основным актом о защите конфиденциальных сведений о человеке является Органический закон 3/2018 «О защите персональных данных и обеспечении цифровых прав» от 05.12.2018[1]. Собирание или разглашение тайных сведений о человеке, а также публичное использование его образа без согласия *Уголовным кодексом Испании*[2] наказывается по ст. 202 раздела X «Преступления против неприкосновенности частной жизни, права на собственное изображение и неприкосновенности жилища» Книги II. Безопасность персональных данных обеспечивается и путем запрета их незаконного присвоения, использования или изменения, если они хранятся в государственных или частных электронных файлах, в электронных или телекоммуникационных сетях, на компьютере, открытых или частных записях, архивах или реестрах, что наносит ущерб субъекту данных или третьему лицу («any other kind of file or public or private record») (ч. 2 ст. 197).

По испанскому уголовному закону подвергаются наказанию и те, кто осуществляет незаконный сбор (перехват) электронных сообщений, файлов или других коммуникационных сигналов, содержащих закрытые персональные

---

[1] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales // BOE. Núm. 294. 06.12.2018. Pág. 119788-119857.

[2] Уголовный кодекс Испании (Codigo Penal de Espana) (с изм. и доп. от 13.03.2022). URL: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html (дата обращения: 13.08.2022).

данные; передачу данных, незаконно полученных обработчиком персональных данных. К «чувствительным» персональным данным относятся сведения об идеологии, религии, убеждениях, состояния здоровья, сексуальной ориентации. Их сбор и передача сами по себе образуют состав преступления (ч. 5 ст. 197), а отягчают наказание их совершение в отношении инвалидов и несовершеннолетних, лицами, управляющими или ответственными за информационные, электронные или телевизионные картотеки, архивы или регистры, а также цель получения выгоды[1].

При обращении к законодательству большинства государств постсоветского пространства обнаруживается, что система составов преступлений, посягающих на неприкосновенность тайны, подобна российской. В их диспозициях нет упоминания о персональных данных человека. Уголовно-правовые средства используются исключительно для защиты конкретного вида тайны (личной, семейной, корреспонденции, банковской, усыновления, предварительного следствия и др.). В этой связи утрачивает исследовательский интерес подробный анализ похожего оформления запретов в уголовном законе многих государств бывшего Союза (Азербайджан, Армения, Кыргызстан, Литва, Молдова, Таджикистан, Туркменистан, Узбекистан, Украина). При характеристике указанной группы преступлений следует отметить одно из ее отличий от УК РФ – установление ответственности за нарушение врачебной тайны, которая также может содержать и персональные данные. Ее разглашение наказуемо в Кыргызстане (ст. 153)[2], Таджикистане (ст. 145)[3], Армении (ст. 145)[4] и Украине (ст. 145)[5].

---

[1] Вабищевич В.В. Зарубежный опыт уголовно-правовой охраны персональных данных // Журнал Белорусского государственного университета. Право. 2019. № 1. С. 77.

[2] Уголовный кодекс Кыргызской Республики (с изм. и доп. от 09.08.2022) // Законодательство стран СНГ. URL: https://base.spinform.ru/show_doc.fwx?rgn=94723 (дата обращения: 14.08.2022).

[3] Уголовный кодекс Республики Таджикистан (с изм. и доп. от 19.07.2022) // Законодательство стран СНГ. URL: http://base.spinform.ru/show_doc.fwx?rgn=2324 (дата обращения: 27.07.2022).

[4] Уголовный кодекс Республики Армения (с изм. и доп. от 24.05.2022) // Законодательство стран СНГ. URL: https://base.spinform.ru/show_doc.fwx?rgn=7472 (дата обращения: 04.08.2022).

[5] Уголовный кодекс Украины (с изм. и доп. от 14.04.2022) // Законодательство стран СНГ. URL: https://online.zakon.kz/Document/?doc_id=30418109&pos (дата обращения: 04.08.2022).

Согласно *второму подходу,* охрана персональных данных осуществляется посредством их введения в качестве дополнительного конструктивного признака в уже имеющиеся уголовно-правовые запреты нарушения неприкосновенности различных видов тайны как объекта посягательства. Так, в *Уголовном кодексе Республики Беларусь*[1] содержатся две новые нормы об охране персональных данных – ст. ст. 203^1, 203^2, внесённые в УК Законом Республики Беларусь от 26.05.2021 № 112-З «Об изменении кодексов по вопросам уголовной ответственности»[2]. Причем их конституционность проверялась Конституционным Судом Беларуси в порядке обязательного предварительного контроля[3]. В доктрине уголовного права Беларуси активно дискутировалась состоятельность ст. 179 УК «Незаконное собирание либо распространение информации о частной жизни», которая не могла, по мнению ученых, обеспечить эффективную охрану персональных данных, в связи с чем предлагалась криминализация конкретных действий с персональными данными (обработка, сбор, трансграничная передача, хранение, обезличивание, разглашение и т.д.)[4].

В результате модернизации кодекса ст. 179 была из него исключена. Вместо нее УК был дополнен статьями 203^1, 203^2 с изменением местоположения (из главы 21 о преступлениях против уклада семейных отношений и интересов несовершеннолетних в главу 23 «Преступления против конституционных прав и свобод человека и гражданина»).

По ст. 203^1 «Незаконные действия в отношении информации о частной жизни и персональных данных» наказуемы умышленные незаконные сбор,

---

[1] Уголовный кодекс Республики Беларусь (с изм. и доп. от 13.05.2022) // Законодательство стран СНГ. URL: https://online.zakon.kz/Document/?doc_id=30414984&doc_id2=30414984#activate_doc=2&pos=6;-98&pos2=1840;-97 (дата обращения: 24.07.2022).

[2] Об изменении кодексов по вопросам уголовной ответственности: закон Республики Беларусь от 26.05.2021 № 112-З // Национальный правовой Интернет-портал Республики Беларусь, 08.06.2021. № 2/2832.

[3] О соответствии Конституции Республики Беларусь Закона Республики Беларусь «Об изменении кодексов по вопросам уголовной ответственности»: решение Конституционного Суда Республики Беларусь от 17.05.2021 № Р-1270/2021 // Вестник Конституционного Суда Республики Беларусь. 2021. № 2.

[4] Абламейко М.С. Правовое регулирование персональных данных с учетом введения ID-карт и биометрических паспортов // Журнал Белорусского государственного университета. 2018. № 1. С. 16.

предоставление информации о частной жизни и (или) персональных данных другого лица без его согласия (ч.1), умышленное незаконное распространение информации о частной жизни и (или) персональных данных другого лица без его согласия (ч. 2). По обеим частям эти деяния должны повлечь причинение существенного вреда правам, свободам и законным интересам гражданина, а в части 3 отягчающим обстоятельством признается их совершение в отношении лица или его близких в связи с осуществлением им служебной деятельности или выполнением общественного долга. Недостатком этой нормы ученые называют неоднозначно толкуемую «существенность» вреда, что формирует неединообразную правоприменительную практику с разной квалификацией одних и тех же деяний[1]. Диспозиция второго состава преступления – ст. 203[2] «Несоблюдение мер обеспечения защиты персональных данных» – наделена признаком специального субъекта, осуществляющего обработку персональных данных. Содеянное должно повлечь только неосторожное их распространение и причинение тяжких последствий.

Уголовный кодекс Грузии[2] в главе XXIII «Преступления против прав и свобод человека» с 2016 г. содержит обновленную норму об ответственности не только за посягательство на личную или семейную тайну, информацию, но и персональные данные (ст. 157). По первой ее части наказываются незаконные получение, хранение, использование, распространение информации, отражающей личную жизнь, или персональные данные либо иное обеспечение доступа к ним, повлекшие значительный вред. Вторым наказуемым действием в отношении персональных данных, помимо незаконного использования, грузинский законодатель в ч. 2 называет их распространение в произведении, через Интернет, социальные сети, массовое вещание или при ином публичном выступлении, повлекшее значительный вред.

---

[1] Вабищевич В.В. Зарубежный опыт уголовно-правовой охраны персональных данных // Журнал Белорусского государственного университета. Право. 2019. № 1. С. 75.

[2] Уголовный кодекс Грузии (Criminal Code of Georgia) (с изм. и доп. от 18.04.2022). URL: http:// https://www.legislationline.org/download/id/8847/file/Georgia_Criminal_Code_am2020_ru.pdf (дата обращения: 22.07.2022).

Особое внимание в кодексе уделено регламентации отягчающих обстоятельств. По ч. 3 ими признается совершение указанных в первых двух частях ст. 157 деяний из корыстных побуждений (а) или неоднократно (б), а по ч. 4 – специальным субъектом. Это лица, использовавшие служебное положение либо обязанные ввиду служебного положения, профессиональной деятельности или других обстоятельств хранить эту информацию или данные.

Из бывших республик СССР первой страной, установившей уголовную ответственность именно за нарушение Закона от 21.05.2013 № 94-V «О персональных данных и их защите»[1], стал Казахстан. После его принятия статья 147 «Нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите» главы 3 «Уголовные правонарушения против конституционных и иных прав и свобод человека и гражданина» Особенной части *Уголовного кодекса Республики Казахстан*[2] подверглась изменениям[3].

В качестве предмета преступления персональные данные указаны в ч ч. 1 и 2 ст. 147 УК РК, а ответственность дифференцирована в зависимости от характера совершаемых с ними противоправных действий[4]. В одной норме было объединено нарушение неприкосновенности частной жизни и несоблюдение мер по защите персональных данных, сопряжённые с общественно опасными последствиями в виде «существенного вреда правам и законным интересам лиц» (ч. 1).

В части 1 содержится прямое указание на субъект преступления, который обозначен как «лицо, на которое возложена обязанность принятия таких мер». По части 2 уголовно наказуемым деянием признается причинение существенного

---

[1] О персональных данных и их защите: закон Республики Казахстан от 21.05.2013 № 94-V (с изм. и доп. от 30.12.2021) // Казахстанская правда. 2013. 25 мая; 2021. 31 дек.

[2] Уголовный кодекс Республики Казахстан от 03.07.2014 № 226-V (с изм. и доп. от 27.06.2022) // Казахстанская правда. 2014. 09 июля. 2022. 28 июня.

[3] О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информатизации: закон Республики Казахстан от 24.11.2015 № 419-V // Казахстанская правда. 2015. 26 нояб.

[4] Новиков В.А. Уголовная ответственность за нарушение неприкосновенности частной жизни по законодательству Российской Федерации и Республики Казахстан // Вестник Института законодательства и правовой информации Республики Казахстан. 2015. № 3 (39). С. 147.

вреда правам и законным интересам лица в результате незаконных сбора и (или) обработки иных персональных данных (иных – кроме сведений, составляющих личную или семейную тайну).

В ряду квалифицирующих признаков посягательств на защиту персональных данных человека казахстанский УК выделяет:

– совершение указанных деяний с использованием служебного положения или специальных технических средств, предназначенных для негласного получения информации, либо путем незаконного доступа к электронным информационным ресурсам, информационной системе или незаконного перехвата информации, передаваемой по сети телекоммуникаций, либо в целях извлечения выгод и преимуществ для себя, других лиц или организаций (ч. 3);

– причинение существенного вреда правам и законным интересам лица в результате незаконного сбора и (или) обработки иных персональных данных (ч. 4);

– распространение сведений в публичном выступлении, публично демонстрирующемся произведении, в средствах массовой информации или с использованием сетей телекоммуникаций (ч. 5)[1].

Третьим является *подход*, в соответствии с которым ответственность за незаконные деяния с персональными данными человека устанавливается в специальной норме (нормах). Они могут содержаться не только в кодифицированных уголовных законах, но и в специальных нормативных актах. При этом в зарубежных национальных законодательствах действует и самостоятельный уголовно-правовой запрет нарушения неприкосновенности частной жизни. Другой особенностью абсолютного большинства национальных законодательств стран дальнего зарубежья является использование максимально широкого подхода при определении правовых средств охраны

[1] Хохлова Е.В. Об уголовной ответственности за нарушение неприкосновенности персональных данных человека в странах бывшего СССР // Вестник Российской правовой академии. 2022. № 3 (1). С. 93.

неприкосновенности персональных данных[1]. Примером здесь служит Великобритания[2]. Ввиду отсутствия кодифицированного уголовного закона нормы об уголовной ответственности за посягательства на персональные данные содержатся в специальном парламентском акте – Законе о защите данных 2018 г. (Data Protection Act 2018, далее DPA). Этот статут заменил закон Соединенного Королевства с аналогичным названием 1998 г. и имплементировал в национальную правовую систему положения GDPR. Действующим источником права являются и судебные решения в части их ratio decidendi (*нормы права, на основе которых было разрешено данное дело*), состоявшиеся до 2018 г. Учитывая особую уязвимость персональных данных, судебная практика Великобритании демонстрирует жесткий подход к наказанию виновных в посягательствах на персональные данные. Ответственности подлежат, к примеру, журналисты за публикацию сведений, полученных на законных основаниях[3].

В соответствии с DPA Великобритании каждый, кто несет ответственность за использование персональных данных, должен соблюдать строгие правила или «принципы защиты данных». Исходя из этого предписания, систематизируются составы преступлений, охраняющие персональные данные. Правоведы предлагают разную их классификацию[4], однако, на наш взгляд, все перечисленные в DPA посягательства делятся на две группы: связанные с их сохранностью или состоящие в нарушении установленного порядка обработки персональных данных:

Первая группа преступлений включает:

---

[1] Макаров А.В., Вологдина Е.С. Персональные данные как объект преступных посягательств на неприкосновенность частной жизни: законодательный опыт в России и зарубежных странах // Российский следователь. 2019. № 5. С. 73.

[2] Жарова А.К. Опыт правового обеспечения безопасности персональных данных в Великобритании // Государство и право. 2017. № 6. С. 74.

[3] Перова Н.А. Ограничения свободы слова в целях предотвращения разглашения личной и государственной тайны в праве США и Великобритании // Право и управление. XXI век. 2012. № 1. С. 96.

[4] Озерова А.С. Социальная обусловленность уголовно-правовой охраны персональных данных: опыт некоторых зарубежных стран // Правовое государство: теория и практика. 2022. Т. 205, № 1. С. 165.

– незаконное использование персональных данных, совершенное умышленно или по неосторожности: (a) получение или распространение персональных данных; (b) хранение персональных данных; (c) продажа персональных данных (ст.170 DPA) (эти действия наказуемы, если они причинили или могли причинить существенный вред правам и свободам человека);

– требование о предоставлении персональных данных: (a) при найме виновным сотрудника, (b) в трудовых отношениях, когда виновный является работодателем, (c) при заключении договора на оказание услуг, заказчиком по которому выступает виновный, (d) в связи с оказанием виновным услуг населению и, если это требование является условием оказания услуг (ст. 184 DPA).

Ко *второй группе преступлений* относятся:

– обработка персональных данных, которые были повторно идентифицированы: (a) без согласия оператора, ответственного за обезличивание персональных данных, и (b) в случае, если повторная идентификация являлась незаконной (ст. 171 DPA);

– изменение, уничтожение или сокрытие персональных данных с целью воспрепятствовать предоставлению информации, которую субъект персональных данных имел право получить (ст. 173 DPA).

Преступление, именуемое «присвоением личности», в *Своде законов Соединенных Штатов Америки* было введено в раздел 18 «Преступления и уголовный процесс» (§ 3571 разд. 18 СЗ США), а первыми штатами, уголовным законом которых впервые была криминализирована «кража (подмена) личности» (англ. Identity theft), стали Алабама и Калифорния[1]. Эти новеллы последовали после принятия в 1998 г. Конгрессом первого закона «О предотвращении кражи личных данных и предполагаемом сдерживании»[2]. Федеральным уголовным преступлением были признаны умышленные незаконные передача и

[1] Сабол Марта А. Закон о защите от кражи личных данных и предположений 1998 года – получают ли отдельные жертвы, наконец, свой день в суде? // 11 Loy. Потребитель Л. Rev. 165, 169 (1999).

[2] Закон о предотвращении кражи личных данных и предположений 1998 года, Pub. L. № 105-318, 112 Stat. 3007 (30 октября 1998 г.), кодифицированный в 18 U.S.C. §1028.

использование персональных данных другого человека «с намерением совершить или помочь или подстрекать любую незаконную деятельность, которая представляет собой нарушение федерального закона, или является преступлением в соответствии с любым применимым законодательством штата или местным законодательством» (§1028).

В 2004 г. второй закон «Об усилении наказания за кражу личных данных», критикуемый американскими учеными за «символическую криминализацию» (т.е. принятие новых популистских законов в угоду избирателям)[1], изменил понятие кражи чужих личных данных[2]. Наказанию теперь подлежало лицо, которое «сознательно передает, владеет или использует без законных полномочий средство идентификации другого лица» во время и в связи с совершением конкретных преступлений[3]. Их перечень дается в 18 U.S.C. §1028A «Кража личных данных при отягчающих обстоятельствах» (c): кража государственных денег, имущества или записей; кража, растрата или незаконное использование денег сотрудником банка; незаконное получение гражданства; незаконное приобретение огнестрельного оружия; мошенничество с почтовыми и банковскими переводами; нарушения, связанные с национальностью и гражданством, с паспортами и визами; нарушения, касающиеся умышленного отказа покинуть США после депортации и создания поддельной регистрационной карточки иностранца и др.

Следует отметить сходство в национальных подходах ряда государств к пониманию «кражи личности». В Канаде ею признаются умышленное владение и получение персональной информации с целью совершения нового преступления или для избегания уголовной ответственности. Преследуются уголовным законом и незаконные передача, распространение, раскрытие и продажа такой информации, и в том числе по неосторожности. Во Франции целью

---

[1] Martin J. Обвинения в неправомерной краже личных данных в делах белых воротничков // Law360. 7/14/14.

[2] Закон об усилении наказания за кражу личных данных от 15.07.2004, Pub. L. № 108-275, 118 Stat. 831 (15 июля 2004 г.), кодифицированный в 18 U.S.C. §§1028, 1028A.

[3] Кузьмин Ю.А. Кража персональных данных (криминологический аспект) // Oeconomia et Jus. 2020. № 3. С. 55.

использования идентифицирующих лицо данных называется нарушение его покоя, чести и достоинства, а в Финляндии – обман третьего лица с причинением ущерба или созданием значительных затруднений для потерпевших. В Австралии обязательной целью покупки, продажи и владения идентифицирующей информации является совершение новых преступлений.

Отличие же в аналогах норм разных стран о «краже личности» усматривается в содержании той информации о человеке, которая может быть предметом похищения[1]. Так, в США понятие «средство идентификации» определяется чрезмерно широко, а именно как «любое имя или номер, которые могут использоваться отдельно или в сочетании с любой другой информацией для идентификации конкретного лица» (§18 U.S.C. §1028 (a)). Идентифицирующей является любая информация, в том числе имя, номер социального страхования потребителя (SSN), номер водительских прав, дата рождения, регистрационный номер иностранца, номер государственного паспорта, идентификационный номер работодателя или налогоплательщика; уникальные биометрические данные, отпечаток пальца, отображение сетчатки или радужной оболочки глаза и другие физиологические характеристики человека (b), уникальный электронный идентификационный номер, адрес или код маршрута (c), номер учетной записи, пароль (IP-адрес компьютера и телефона) (d)[2]. Американской судебной практике известны уголовные дела и по факту присвоения подписи (подделка)[3], использования чужого паспорта[4], разрешения на ношение оружия с чужими данными[5]. Информацией конфиденциального характера в штате Нью-Йорк признаются сведения из карточки читателя в библиотеках.

---

[1] Рязанова Е.Н. Ответственность за распространение персональных данных как способ противодействия правонарушениям в сфере информационно-коммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. 2022. № 3 (95). С. 120.

[2] Филатова М.А. Уголовно-правовая охрана персональных данных. URL: https://www.youtube.com/watch?v=mGyIkYEYn2Y&t=5714s (дата обращения 10.08.2022); Кузьмин Ю.А. Указ. соч. С. 56.

[3] Соединенные Штаты против Портера, 745 F.3d 1035 (10-й Cir. 2014).

[4] Соединенные Штаты против Осуны-Альвареса, 788 F.3d 1183 (9-й Cir. 2015).

[5] Соединенные Штаты против Спирс, 729 F.3d 753 (7-й Cir. 2013).

Во Франции с учетом GDPR была изменена редакция Закона № 78-17 от 06.01.1978 «Об обработке данных, файлах и свободах», а в *Уголовном кодексе Франции*[1] изменилась система преступлений, предметом которых выступает и частная жизнь, и упоминаемая в диспозициях «именная информация» (персональные данные). Французская группа рассматриваемых преступных деяний характеризуется достаточно высоким уровнем детализации в зависимости от видовой принадлежности тайны[2]. В главе VI «О посягательствах на личность» Книги II, исходя из структурного ее деления, деяния, связанные с причинением вреда частной жизни человека, даны в отделах о посягательствах: на частную жизнь (Отдел I), на изображение лица (Отдел II) и на тайну (Отдел IV). Нарушения, связанные с персональными данными, находятся в разделах о посягательствах на права лица, возникающие в связи с ведением картотек и обработкой информации (Отдел V), на человека, связанных с исследованием его генетических свойств или идентификацией посредством его генетических признаков (Отдел VI)[3].

Преступления, направленные против персональных данных, условно представлены в следующей классификации:

1. *Посягательства, связанные с нарушением установленного режима персональных данных*:

1.1. Сбор персональных данных, касающихся здоровья, обманным, самоуправным или запрещенным законом способом при отсутствии персонального информирования человека о его праве определять содержание передаваемой информации и ее получателей, либо вопреки его возражениям о распространении этих данных (ст. 226-18); 1.2. Идентификация какого-либо человека посредством его генетических признаков в медицинских целях без его

---

[1] Уголовный кодекс Французской Республики (Code pénal France) (с изм. и доп. от 01.06.2022). URL: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 (дата обращения: 21.07.2022).

[2] Говенко Ю.А. Уголовно-правовая охрана тайны частного характера: автореф. дис... канд. юрид. наук. Краснодар, 2010. С. 15.

[3] Хохлова Е.В. Уголовно-правовая охрана персональных данных в зарубежных странах // Известия Юго-Западного государственного университета. Серия: История и право. 2022. Т. 12, № 4. С. 69.

согласия (ст. 226-27), либо при отсутствии медицинских, научных целей, а также вне рамок уголовного судопроизводства (ст. 226-28); 1.3. Распространение персональных данных другого лица без его согласия, выразившееся в ознакомлении с этими сведениями третьих лиц, не имеющих на это права (ст. 226-22); 1.4. Незаконное использование сведений, касающихся генетической характеристики человека, в том числе в медицинских целях или в рамках научного исследования (ст. 226-26).

2. *Посягательства, связанные с нарушениями правил обработки, хранения и передачи персональных данных*:

2.1. Нарушение, умышленное или по неосторожности, правил при осуществлении или организации осуществления автоматизированной обработки (ст. 226-16); 2.2. Нарушение мер обеспечения безопасности персональных данных, включающих несанкционированное изменение, повреждение или передачу третьим лицам (ст. 226-17); 2.3. Нарушение правил уведомления надзорного органа о несанкционированном доступе к персональным данным (ст. 226-17-1)[1]; 2.4. Нарушение правил обработки персональных данных, выразившееся в использовании оператором персональных данных в целях проведения исследований и опросов, при несогласии на то лица (ст. 226-18.1); 2.5. Нарушение цели сбора персональных данных, когда они используются вопреки законодательным положениям или регламенту (ст. 226-21); 2.6. Нарушение правил передачи персональных данных в международные организации или государства, не являющиеся членами Европейского Союза (ст. 226-22-1); 2.7. Нарушение срока хранения персональных данных, за исключением их использования для исторических, статистических или научных исследований (ст. 226-20).

---

[1] Здесь преследуется нарушение защиты персональных данных. Им считается «любое нарушение безопасности, случайное или намеренное, повлекшее за собой разрушение, утрату, изменение, обнародование или неправомерный доступ к персональным данным, являющимся объектом обработки в рамках предоставления электронно-коммуникационных услуг». Поставщик услуг обязан сообщить о нарушении защиты персональных данных в Национальную комиссию информатики и свободы, иначе он подлежит тюремному заключение на пять лет и штрафу в размере 300 тыс. евро. См.: Талапина Э.В. Правовая защита персональных данных во Франции // Право. 2012. № 4. С. 152.

3. *Посягательства, связанные с нарушениями правил обработки и хранения специальных персональных данных.* Нарушение установленных правил касается: 3.1 обработки персональных данных, включающих идентификацию человека (регистрационный номер физического лица, содержащийся в национальном справочнике) (ст. 226-16-1); 3.2. обработки персональных данных, целью которой являются медицинские исследования (ст. 226-19-1)[1]; 3.3. хранения в памяти компьютера персональных данных, касающихся расового или этнического происхождения, политических, религиозных взглядов, принадлежности к профсоюзам, состояния здоровья либо интимной жизни, лица без его согласия (ст. 226-19); 3.4. хранения в памяти компьютера без согласия лица персональных данных о правонарушениях, обвинительных приговорах или мерах безопасности (ст. 226-19).

Согласно ст. 179 novies Третьего раздела «Преступные деяния против чести и в области тайной и частной сферы» *Уголовного кодекса Швейцарской конфедерации*[2], ответственности подлежит любое лицо, которое без разрешения незаконно получает из баз персональных данных или личных дел особо конфиденциальные («чувствительные») личные сведения или профили о личности, которые не являются общедоступными[3]. При этом за нарушение неприкосновенности частной жизни предусмотрена уголовная ответственность в ст. 179 quarter «Нарушение тайной и частной сферы путем использования звукозаписывающей и съёмочной аппаратуры».

В Швеции идея закрепления наказания за нарушение правил обработки персональных данных получила развитие после принятия в 2018 г. специального Закона «О защите данных» (2018: 218) и Регламента о защите данных (2018:219),

---

[1] К примеру, во Франции в 2020 г. разразился скандал: интернет-сайт «Doctissimo» собирал конфиденциальную информацию с онлайн-тестами о состоянии здоровья граждан, которая затем передавалась третьим лицам для использования в рекламных целях. См.: URL: https://tekdeeps.com/doctissimo-accused-of-collecting-and-reselling-your-health-data/ (дата обращения: 05.03.2022).

[2] Уголовный кодекс Швейцарской Конфедерации (Swiss Criminal Code) (с изм. и доп. от 01.07.2021). URL: https://www.legislationline.org/download/id/8991/file/SWITZ_Criminal%20Code_as%20of%202020-07-01.pdf (дата обращения: 07.08.2022).

[3] Сапранкова Т.Ю. Указ. соч. С. 125.

нормы которого по защите информации частного характера действуют самостоятельно, за рамками шведского *Уголовного кодекса*[1]. Эта модель уголовно-правовой защиты конфиденциальной информации о человеке похожа на французскую. Аналогично УК Франции по ст. 49 шведского закона наказывается тот, кто с использованием своего служебного положения или профессиональных навыков умышленно или по небрежности осуществляет обработку персональных данных в нарушение установленного порядка. Им может быть, к примеру, неполучение разрешения об использовании персональных данных в Комитете по научной этике. Субъектами содеянного признаются сотрудники научно-исследовательских организаций, учреждений здравоохранения, социального обеспечения, статистики и др., которые используют личные данные для научных целей.

При тех же условиях наказуема и обработка личных данных о правонарушителях. Она включает информацию о самом преступлении, мерах уголовно-процессуального принуждения, приговоре и наказании по нему. Преступлением по ст. 49 считается и передача персональных данных шведских подданных другим государствам, присоединившимся к Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных»[2], у которых, по мнению законодателя, нет надлежащего уровня защиты персональных данных. Оценка степени защищенности передачи конфиденциальной информации проводится с учетом характера личных данных, цели их обработки и ее продолжительности, страны происхождения, страны назначения и установленных правил обработки данных в государстве, куда они передаются Швецией. В самом же УК по ст. 8 части 2 главы 4 «О преступлениях против свободы и общественного спокойствия» преступлением признается

---

[1] Уголовный кодекс Швеции (Criminal code of the Kingdom of Sweden) (с изм. и доп. от 12.03.2022). URL: http://www.legislationline.org/documents/section/criminal-codes (дата обращения: 14.08.2022).

[2] Конвенция о защите физических лиц при автоматизированной обработке персональных данных: заключена в г. Страсбурге 28.01.1981 (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // СЗ РФ. 2014. № 5, ст. 419.

нарушение частной тайны (переписки, разговоров), поскольку «уважение к частной жизни есть один из аспектов индивидуальной свободы»[1]. По ст. 9с наказывается нарушение секретности данных. Оно включает незаконные доступ к записи в системе автоматической обработки данных, изменение, уничтожение или внесение такой записи в реестр.

Согласно ст. ст. 13 и 35 Конституции Японии, ее граждане обладают правом на защиту частной жизни (право на приватность), составной частью которого является защита неприкосновенности персональных данных[2]. Еще в 1964 г. суд г. Токио по резонансному делу экс-министра иностранных дел Арита Хатиро признал законным право на частную жизнь и его гарантию от умышленного раскрытия общественности личной или семейной тайны. Это решение суда о праве на неприкосновенность частной жизни и защиту персональных данных стало судебным прецедентом, применяемым к делам этой категории[3]. Через сорок лет институт неприкосновенности персональных данных получил свое развитие в Законе 2003 г. «О защите персональных данных» (с изм. и доп. от 01.04.2022), положения которого направлены на обеспечение защиты приватности сферы частной жизни, в том числе уголовно-правовыми средствами[4]. В нем предусмотрена уголовная ответственность для специальных субъектов – должностных лиц организаций, связанных с доступом, обработкой и хранением персональных данных, которые обязаны соблюдать порядок работы с персональной информацией и ее защиты. При несоблюдении этих требований должностные лица могут быть наказаны штрафом в размере до 30 тыс. иен либо лишены свободы сроком на шесть месяцев (ст. 56 Закона). Такому же наказанию

---

[1] Мачковский Л.Г. Ответственность за нарушение неприкосновенности частной жизни в уголовном законодательстве России и зарубежных стран // Известия высших учебных заведений. Правоведение. 2003. № 5 (250). С. 156.

[2] Савинцева М.И. Конституционно-правовые проблемы регулирования информационных отношений в Японии: история и современность: автореф. дис. … канд. юрид. наук. М., 2007. С. 21.

[3] Речь шла о книге Юкио Мисима «После банкета», в которой писатель накануне выборов Арито Хатира на должность губернатора Токио рассказал о его сексуальных развлечениях с официанткой. См.: Савинцева М.И. Конституционно-правовые основы защиты персональной информации в Японии // Конституционное и муниципальное право. 2006. № 9. С. 41.

[4] Act on the Protection of Personal Information (Act № 57 of 2003). URL: http:// www.cas.go.jp/jp/seisaku/hourei/data/APPIHAO.pdf (дата обращения: 11.08.2022).

подвергается должностное лицо организации, если представляется отчет о выполнении мер по защите персональных данных либо он содержит ложные сведения (ст. 57 Закона). В самом же *Уголовном кодексе Японии*[1] нет специальной нормы о защите персональных данных. Главу 13 «Преступления, состоящие в нарушении тайны» образуют два состава преступления, посягающие на неприкосновенность частной жизни. Ими являются ст. 133 «Вскрытие корреспонденции» и ст. 134 «Разглашение профессиональной тайны» с перечислением субъектов нарушения врачебной, нотариальной, адвокатской тайны, ставшей им известной «в связи с осуществлением ими своей профессиональной деятельности».

Отличный от УК РФ и большинства кодексов других стран бывшего СССР концептуальный подход к защите чужих личных данных наблюдается в Латвии и Узбекистане.

Статья 145 «Незаконные действия с данными физического лица» главы XIV «Преступные деяния против основных прав и свобод личности» *Уголовного кодекса Латвийской Республики*[2] интересна тем, что в ней содержатся три состава преступления. В части первой говорится о незаконных действиях в отношении персональных данных человека, которые не конкретизируются, а в части второй – о тех же действиях, совершенных с целью мести, корысти или шантажа специальным субъектом – заведующим обработкой личных данных или оператором. Отдельно, в части третьей, криминализированы действия, связанные с применением насилия либо угроз, или с использованием доверия или обмана в отношении заведующего обработкой личных данных или оператора либо субъекта данных с целью осуществления незаконных действий с данными физического лица.

---

[1] Уголовный кодекс Республики Японии (Criminal code of the Republic of Japan) (с изм. и доп. от 23.11.2021). URL: http://www.cas.go.jp/jp/seisaku/hourei/data/PC.pdf (дата обращения: 15.08.2022).
[2] Уголовный кодекс Латвийской Республики (Krimināllikums) (с изм. и доп. от 23.05.2022). URL: https://www.legislationline.org/documents/section/criminal-codes/country/19/Kyrgyzstan/show (дата обращения: 06.08.2022).

После принятия Закона от 02.07.2019 № ЗРУ-547 «О персональных данных»[1] в 2021 г. в главу VII «Преступления против конституционных прав и свобод граждан» *Уголовного кодекса Республики Узбекистан*[2] вводится ст. 141^2 об ответственности за нарушение законодательства о персональных данных[3]. И это при том, что в национальном уголовном праве уже действует норма о нарушении неприкосновенности частной жизни (ст. 141^1). Отметим ряд особенностей конструкции новой нормы. Наказуемыми, во-первых, являются незаконный сбор, систематизация, хранение, изменение, дополнение, использование, предоставление, распространение, передача, обезличивание и уничтожение персональных данных; во-вторых, несоблюдение при обработке персональных данных граждан Республики Узбекистан с использованием информационных технологий, в том числе во всемирной информационной сети Интернет, требований по сбору, систематизации и хранению персональных данных на технических средствах, физически размещенных на территории Республики Узбекистан, и в базах персональных данных, зарегистрированных в установленном порядке в Государственном реестре баз персональных данных. Названные деяния становится преступными, если они совершены после применения административного взыскания за те же действия (административная преюдиция).

В сравнении с другими странами-участницами СНГ и ближнего зарубежья узбекский УК отличает множество отягчающих признаков, которым отведена вторая часть ст. 141^2, а именно пп. «а»–«д». Их перечень включает деяния, совершенные по предварительному сговору группой лиц (а); повторно или опасным рецидивистом (б); из корыстных или иных низменных побуждений (в); с

---

[1] О персональных данных: закон Республики Узбекистан от 02.07.2019 № ЗРУ-547 (с изм. и доп. от 14.01.2021) // Национальная база данных законодательства. 2019. 03 июля.

[2] Уголовный кодекс Республики Узбекистан (с изм. и доп. от 23.06.2022) // Законодательство стран СНГ. URL: https://online.zakon.kz/Document/?doc_id=30421110&pos=1670;56#pos=1670;56 (дата обращения: 27.07.2022).

[3] О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан: закон Республики Узбекистан от 29.10.2021 № ЗРУ-726 // Народное слово. 2021. 30 окт.

использованием служебного положения (г) или повлекшие тяжкие последствия (д).

Подводя итог рассмотрению уголовного законодательства зарубежных стран об ответственности за преступления в отношении персональных данных, можно сделать *следующие выводы*:

1. Уголовное законодательство зарубежных стран обнаруживает тенденцию придания самостоятельного уголовно-правового значения персональным данным как *предмету преступления* и (или) *средству совершения преступления в составе охраны тайны частной жизни* (Дания, Испания, Лихтенштейн, Нидерланды, ФРГ), *наряду с ней* (Беларусь, Грузия, Казахстан) или *самостоятельно* (Великобритания, США, Латвия, Узбекистан, Франция, Швейцария, Швеция, Япония).

2. Национальные уголовные законы многих зарубежных стран снабжены нормами, законодательная формулировка которых содержит разные способы конструирования и закрепления видов незаконных действий с персональными данными, чрезмерную или недостаточную их детализацию. Разница в технико-юридическом оформлении зарубежных уголовно-правовых норм препятствует их четкой систематизации по причине сложности самого феномена персональных данных и новизны деяний, с их помощью причиняющих вред или создающих угрозу его причинения охраняемым уголовным законом благам и интересам.

С учетом сложившихся подходов в зарубежном праве можно выделить *две основные группы преступлений*, обеспечивающих неприкосновенность персональных данных. *Первой* является *группа уголовно наказуемых деяний*, не связанных с обработкой персональных данных: незаконные собирание, похищение, получение, распространение, уничтожение, хранение, продажа и использование (Беларусь, Великобритания, Грузия, Дания, Испания, Казахстан, Лихтенштейн, Нидерланды, ФРГ).

Вторую группу преступлений составляют посягательства, связанные с нарушениями операторами персональных данных требований получения, автоматизированной обработки, хранения и передачи, установленных для

обеспечения их безопасности, повлекшие несанкционированные доступ, введение, изменение (фальсификацию), обезличивание, повреждение, сокрытие, уничтожение, распространение (передача третьим лицам), а также предоставление заведомо ложных персональных данных или отказ в их предоставлении (Латвия, США, Узбекистан, Франция, Швеция, Швейцария, Япония).

3. В ряде стран дальнего зарубежья и бывшего СССР имеются концептуальные новации охраны персональных данных, аналогов которых в отечественном уголовном праве. Вполне обоснованными представляются зарубежные модели самостоятельной охраны персональных данных, которые могут быть введены в российскую юридическую практику. Национальным правом может быть заимствована идея уголовной ответственности за незаконные действия с персональными данными из ведомственных баз данных о человеке, включая их незаконное копирование, распространение (передачу третьим лицам).

§ 3. Состояние норм российского уголовного закона об ответственности за незаконные действия с персональными данными

В отличие от уголовных правопорядков зарубежных стран нормами российского уголовного закона персональные данные, как уже отмечалось, непосредственно не охраняются, в связи с чем их защита может обеспечиваться вместе (или наряду) с другими видами конфиденциальной информации. В доктрине уголовного права не все ученые единодушны в понимании того, какими из действующих составов преступлений персональные данные могут охраняться. Изучив российскую следственную и судебную практику, М.А. Филатова пишет, что отдельные категории персональных данных охраняют такие составы преступлений, как: нарушение неприкосновенности частной жизни (ст. 137 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), разглашение тайны усыновления (удочерения) (ст. 155 УК РФ), незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ), неправомерный доступ к компьютерной информации (ст. 272 УК

РФ), разглашение данных предварительного расследования (ст. 310 УК РФ)[1]. Размышляя на эту тему, Д.А. Гарбатович дополняет систематизированный М.А. Филатовой перечень статьей 140 УК РФ «Отказ в предоставлении гражданину информации»[2]. В трактовке А.В. Губаревой и А.Н. Гулемина только две статьи УК РФ можно рассматривать как устанавливающие ответственность за незаконное использование и распространение персональных данных – ст. 137 УК РФ и ст. 272 УК РФ[3]. В.А. Чукреев, отмечая отсутствие в УК РФ составов преступлений, которые устанавливали бы наказание за нарушения в сфере оборота персональных данных, признает, что в этом смысле деяниями, имеющими предметом личную информацию, выступают ст. 137 «Нарушение неприкосновенности частной жизни» УК РФ, ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» УК РФ, ст. 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» УК РФ и ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ[4]. Н.Е. Рязанова, как и В.А. Чукреев, называет те же посягательства[5]. По мнению С.И. Гутника, посягательствами, связанными с персональными данными, с учетом исследования следственно-судебной практики, являются ст. 137 и 183 УК РФ[6].

Обращает на себя внимание, что все составы преступлений, могущие потенциально иметь своим предметом и (или) средством персональные данные человека, о которых пишут правоведы, не обособлены структурно, а

---

[1] Филатова М.А. Персональные данные как предмет преступного посягательства журнал // Уголовное право. 2021. № 11. С. 38.

[2] Гарбатович Д.А. Защита персональных данных уголовным правом // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2 (4). С. 12.

[3] Губарева А.В., Гулемин А.Н. Угрозы безопасности персональных данных: проблемы современности // Политика и общество. 2015. № 2. С. 154.

[4] Чукреев В.А. Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 3 (91). С. 109.

[5] Рязанова Е.Н. Ответственность за распространение персональных данных как способ противодействия правонарушениям в сфере информационно-коммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. 2022. № 3 (95). С. 119.

[6] Гутник С.И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: дис. … канд. юрид. наук. Красноярск, 2017. С. 66.

«разбросаны» по разным разделам и главам. Они сгруппированы в уголовном законе по принципу «включенности» персональных данных в конкретные общественные отношения, элементом которых они являются, а потому разнится и содержание объектов посягательств. Это объясняется тем, что, *во-первых*, персональные данные и есть подвид информации согласно ее определению в ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1]. *Во-вторых*, сложность отнесения того или иного посягательства с информационной составляющей к совокупности деяний, запрет совершения которых распространяется и на персональные данные, состоит в том, что нет специальной нормы, предусматривающей уголовную ответственность за незаконные действия с персональными данными, за исключением ст. 173^2 «Незаконное использование документов для образования (создания, реорганизации) юридического лица» УК РФ. *В-третьих*, существует неопределенность в самом перечне персональных данных, их видах и потребности в уголовно-правовой охране.

Ввиду отсутствия четкого понятия персональных данных и специальной нормы для их охраны на основании сообщений СМИ и следственно-судебной практики представляется возможным выделить, с определенной долей условности, составы преступлений, совершаемых в отношении персональных данных или с их использованием, в которых *они могут являться*:

– *предметом преступления* (ст. 137 «Нарушение неприкосновенности частной жизни», ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», ст. 140 «Отказ в предоставлении гражданину информации», ст. 155 «Разглашение тайны усыновления (удочерения)», ст. 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», ст. 272 «Неправомерный доступ к компьютерной информации», ст. 274^1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской

[1] Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ (с изм. и доп. от 31.07.2023, № 408-ФЗ) // Рос. газета. 2006. 29 июля; 2023. 3 авг.

Федерации, ст. 275 «Государственная измена», ст. 276 «Шпионаж», ст. 283 «Разглашение государственной тайны», ст. 283^1 «Незаконное получение сведений, составляющих государственную тайну», ст. 283^2 «Нарушение требований по защите государственной тайны», ст. 284 «Утрата документов, содержащих государственную тайну», ст. 310 «Разглашение данных предварительного расследования», ст. 311 «Разглашение сведений о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса», ст. 320 «Разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа», ст. 325 «Похищение или повреждение документов, штампов, печатей либо похищение акцизных марок, специальных марок или знаков соответствия», ст. 327 «Подделка, изготовление или оборот поддельных документов, государственных наград, штампов, печатей или бланков», ст. 330^1 «Уклонение от исполнения обязанностей, предусмотренных законодательством Российской Федерации об иностранных агентах», ст. 330^2 «Неисполнение обязанности по подаче уведомления о наличии у гражданина Российской Федерации гражданства (подданства) иностранного государства либо вида на жительство или иного действительного документа, подтверждающего право на его постоянное проживание в иностранном государстве» УК РФ);

– *средством совершения преступления* (ст. 142 «Фальсификация избирательных документов, документов референдума, документов общероссийского голосования», ст. 159^1 «Мошенничество в сфере кредитования», ст. 173^2 «Незаконное использование документов для образования (создания, реорганизации) юридического лица» УК РФ).

В механизме противодействия незаконным действиям с персональными данными могут быть задействованы и иные уголовно наказуемые деяния, напрямую не связанные с информацией. Материалы следственно-судебной практики свидетельствуют о росте количества посягательств, где в качестве средства совершения преступления используются базы персональных данных.

Например, приговором Петрозаводского городского суда осуждены по ч. 4 ст. 159 УК РФ за мошенничество к семи годам лишения свободы с отбыванием в исправительной колонии общего режима участницы организованной преступной группы. Как следует из судебного акта, соучастницы в 2018–2019 годах, используя базу персональных данных Пенсионного фонда РФ, звонили потерпевшим от имени его сотрудниц и сообщали ложную информацию о якобы наличии у них права на дополнительные выплаты. Осужденные убеждали граждан пенсионного возраста перевести деньги посредством электронного кошелька на указанный ими банковский счет. Всего установлено 16 эпизодов мошеннических действий, причинивших ущерб на сумму более 630 тыс. руб.[1].

Практика фиксирует злоупотребления с персональными данными и при совершении должностных преступлений. Так, В., являясь оперуполномоченным отдела уголовного розыска ОМВД России по Тбилисскому району Краснодарского края, желая получить материальную выгоду, скопировал персональные данные из электронных баз ИПС «Следопыт-М» с использованием индивидуального логина и пароля, установленных на его служебном компьютере. Затем он выгрузил текстовые сообщения и фотоснимки с личными сведениями о 12 потерпевших (серия, номер, дата выдачи паспорта, место регистрации) в мессенджер «Telegram» и передал их неустановленному лицу, за что получил путем электронного перевода на банковскую карту 1090750 руб.[2]

Очевидно, что содержательно уголовно-правовой механизм противодействия злоупотреблениям с персональными данными может включать самые разнообразные группы преступных посягательств: против конституционных прав и свобод, семьи и несовершеннолетних, экономические, должностные, компьютерные, против правосудия и порядка управления. Вместе с тем исследовательская задача видится не только в определении группы

---

[1] В Петрозаводске вынесен приговор по уголовному делу о мошенничестве в составе организованной группы // Прокуратура Республики Карелия. URL: https://epp.genproc.gov.ru/web/proc_10/mass-media/news?item=62606760 (дата обращения: 09.04.2023).

[2] Приговор Тбилисского районного суда Краснодарского края от 11.07.2019 по делу № 1-125/2019 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/gGB9phbVHUg0/?regular (дата обращения: 08.02.2023).

преступлений, которые в настоящее время используются или гипотетически могут быть задействованы для решения социально-политической задачи противодействия рассматриваемым правонарушениям. Требуется установить, насколько эти нормы отвечают концептуальной идее уголовно-правовой охраны персональных данных, имеются ли пробелы, снижающие ее качество, достаточны или избыточны имеющиеся уголовно-правовые средства, охватывают ли они всю совокупность незаконных действий с персональными данными, требуется ли их реформирование.

Думается, что говорить об уголовно-правовой охране персональных данных с точки зрения существующих уголовно-правовых запретов в отсутствие специальной нормы вряд ли возможно. Они созданы законодателем в иных целях и выполняют иную уголовно-политическую функцию, а потому являются не прямыми, а опосредованными средствами уголовно-правового предупреждения незаконных действий с персональными данными и их последствий. По этой причине нельзя согласиться с мнением С.И. Гутника, который полагает, что «при введении специальной уголовно-правовой охраны преступных посягательств в отношении персональных данных неизбежно возникнет избыточность криминализации», поскольку правовой режим конфиденциальности персональных данных «подпадает под уголовно-правовое воздействие посредством соответствующих норм Уголовного кодекса РФ (ст. 137, ст. 183)»[1].

Правильность этой научной позиции опровергают результаты мониторинга приговоров и иных правоприменительных актов. Отсутствие специальной нормы породило противоречивые интерпретационные подходы в отношении одних и тех же деяний, совершенных при одних и тех же обстоятельствах, когда субъект квалификации каждый раз применяет одну норму из указанной выше группы преступлений или даже их совокупность. Такой разброс в квалификации привел к неединообразной практике. Во многих случаях следователи вынужденно искажают оценку содеянного, не имея правовых инструментов для уголовного

[1] Гутник С.И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: дис. … канд. юрид. наук. Красноярск, 2017. С. 149.

преследования – обнаружения и доказывания признаков незаконных действий с персональными данными ввиду отсутствия отдельной нормы о противодействии им.

К примеру, Самарский районный суд г. Самары вынес обвинительный приговор по п. «а», «в» ч. 5 ст. 290 УК РФ бывшему начальнику отдела полиции № 6 г. Самары Б. и его подчиненному Ч. Судом установлено, что сотрудники полиции получили взятку в размере 596 тыс. руб. за продажу персональных данных граждан из базы МВД «Розыск-Магистраль» (содержит информацию о пассажирах рейсового транспорта). Из показаний Ч. правоохранителям стало известно, что конфиденциальная информация была использована в материалах расследования отравления оппозиционера Алексея Навального[1].

Или другой пример. Богородский городской суд Нижегородской области признал установленным, что подсудимые, являясь оперуполномоченными уголовного розыска ОМВД России по Богородскому району, за денежное вознаграждение осуществляли незаконное копирование персональных данных из ведомственных банков данных МВД и передачу их третьим лицам. Личные сведения о гражданах включали в том числе информацию о привлечении к уголовной ответственности, адреса проживания, наличие транспортных средств и др. Осужденные получили от заказчиков, проживающих в 20 субъектах РФ, денежные средства в размере не менее 800 тыс. руб. Суд согласился с позицией государственного обвинителя относительно квалификации преступления по ст. 286 УК РФ[2].

И третий вариант квалификации. Во Владивостоке Следственным комитетом РФ было возбуждено дело по ч. 5 ст. 290 УК РФ и ч. 3 ст. 272 УК РФ в отношении трех полицейских. Как следует из обвинения, сотрудники МВД РФ передавали за денежное вознаграждение персональные данные граждан,

---

[1] В Самаре экс-полицейским вынесли приговор за слив базы МВД // РИА Новости. URL: https://ria.ru/20220622/prigovor-1797366783.html (дата обращения: 09.04.2023).

[2] Рассмотрено уголовное дело в отношении бывших сотрудников полиции, которые продавали персональные данные граждан // Прокуратура Нижегородской области. URL: https://epp.genproc.gov.ru/web/proc_52/mass-media/news/archive?item=46470953 (дата обращения: 09.02.2023).

полученные из служебных информационных банков данных МВД РФ лицам, незаконно их собирающим. Деньги за информацию о гражданах из баз МВД РФ, к которым у обвиняемых имелся доступ в силу служебного положения, перечислялись на банковские счета фигурантов[1].

О нехватке уголовно-правовых средств говорит и невозможность дать адекватную оценку незаконным действиям в отношении информационных массивов, содержащих персональные данные граждан. С развитием информационных технологий, связанных с обработкой значительных по объему массивов информации, в современном обществе возникла потребность их систематизации для обеспечения простоты использования. По прогнозам Cybersecurity Ventures, к 2025 г. во всем мире глобальное хранение данных с использованием информационно-коммуникационных технологий превысит 200 zettabytes (1 зеттабайт равен 1099511627776 ГБ). Такие информационные базы, составляющие систематизированную совокупность структурированных данных, подвергаются неправомерному доступу в целях умышленного изменения, уничтожения, копирования, использования или распространения[2]. Только в 2022 г. в результате 40 крупных утечек с высоким уровнем критичности было раскрыто 168 баз клиентов российских банков, сервисов доставки, транспортных, медицинских организаций, телефонных компаний, оказывающих услуги мобильной связи[3]. Согласимся с С.В. Бариновым в том, что их распространение и использование может причинить вред значительному количеству граждан, личные данные которых деаномизированы[4].

---

[1] Во Владивостоке возбуждено уголовное дело по факту получения взятки и неправомерного доступа к компьютерной информации // Следственное управление Следственного комитета РФ по Приморскому краю. URL: https://primorsky.sledcom.ru/news/item/1671004/ (дата обращения: 04.02.2023).

[2] Корчемкина О.А. Понятие и признаки базы данных как объекта права // Российский юридический журнал. 2012. № 1. С. 120.

[3] С начала 2022 года в открытый доступ попало не менее 40 баз данных россиян // Коммерсантъ. URL: https://www.kommersant.ru/doc/5504156 (дата обращения: 09.04.2023).

[4] Баринов С.В. О криминализации преступного нарушения неприкосновенности частной жизни, совершаемого в форме распространения баз персональных данных // Российский следователь. 2017. № 4. С. 36; *Его же*. Содержание и особенности проведения тактической операции «задержание с поличным» по делам о преступных нарушениях неприкосновенности частной жизни // Актуальные проблемы российского права. 2018. № 11 (96). С. 224.

Статистика инцидентов с разглашением личных сведений подтверждает попадание миллионов записей о россиянах в открытые источники. По подсчетам экспертов «Лаборатория Касперского», в Глобальной сети оказалось почти 300 млн пользовательских данных, и в том числе адрес проживания, банковские реквизиты, копии паспортов и др.[1]. Так, по сообщениям РБК, на специализированном сайте на продажу была выставлена база клиентов микрофинансовой организации «Быстроденьги» с 1,2 млн записей (ФИО, паспортные данные, номера телефонов, адрес электронной почты), которые могут быть использованы и для оформления онлайн-займов[2]. По прогнозам специалистов, в 2023 г. количество «сливов» преступниками персональных данных, аккумулированных в базах, увеличится еще на 20 %, что уже доказано статистикой января-февраля 2023 г., за которые в три раза – с 7 до 21 – возросли показатели потерь относительно того же периода 2022 г.[3]. О масштабе проблемы компрометации личных данных граждан свидетельствует решение Министерства цифрового развития, связи и массовых коммуникаций РФ об организации мониторинга даркнета, хакерских форумов и каналов в Telegram на предмет кражи персональных данных киберпреступниками[4]. Приведенные статистические показатели подтверждаются и следственно-судебной практикой.

Согласно изученным приговорам, информационные массивы с персональными данными граждан выступают предметом похищений злоумышленниками с целью последующей их продажи.

К примеру, Генеральная прокуратура РФ в феврале 2023 г. утвердила обвинительное заключение по уголовному делу в отношении десяти

---

[1] 300 млн данных пользователей. Названы лидеры по масштабу утечек в России. Ими оказались сервисы доставки и ритейлеры // РБК. URL: https://www.rbc.ru/life/news/63fc38ef9a79474882d03e46 (дата обращения: 09.04.2023).

[2] Персональные данные клиентов МФО выставили на продажу в интернете // РБК. URL: https://www.rbc.ru/finances/06/02/2020/5e3971cc9a79472fd1048e1a (дата обращения: 09.04.2023).

[3] Эксперт Новикова: Более 1,5 млрд записей с персональными данными попали в сеть в 2022 году // Российская газета. URL: https://rg.ru/2022/12/08/bolee-15-mlrd-zapisej-s-personalnymi-dannymi-popali-v-set-v-2022-godu.html (дата обращения: 09.03.2023).

[4] Персональные сданные: как будут отслеживать продавцов незаконных баз // Известия. URL: https://iz.ru/1262783/valerii-kodachigov/personalnye-sdannye-kak-budut-otslezhivat-prodavtcov-nezakonnykh-baz (дата обращения: 09.04.2023).

организаторов и членов преступного сообщества (преступной организации). По версии следствия, организаторы преступного сообщества Ю. и С., которые с целью получения финансовой выгоды собирали и продавали конфиденциальные сведения о гражданах, объединили несколько организованных групп – свои и группы Ф., М. и Г. В период с 2018 по 2020 гг. они неоднократно взламывали доступ к личным данным из баз данных ФНС России, Пенсионного фонда России, Бюро кредитных историй, МВД России и банков. Незаконно полученные в отношении не менее 6,5 тыс. физических лиц персональные данные продавались заказчикам через даркнет на площадке Hydra Market с использованием электронных устройств[1].

И другой пример. В 2020 г. были похищены и предлагались к продаже секретные информационные базы Главного управления по контролю за оборотом наркотиков МВД РФ, которые содержали не только персональные данные (фамилии и фото) наркоманов, но и агентов-осведомителей и граждан, сообщивших по телефону доверия адреса наркопритонов и их клиентах. Вся информация включала сведения на 153 тыс. наркозависимых россиян из 27 регионов страны и местоположение действующих наркопритонов[2]. Обнаруживались на закрытых площадках в Сети и базы ВИЧ-инфицированных, пациентов психоневрологических диспансеров, больных алкоголизмом, самоубийц[3]. Как следует из сообщений СМИ, на «черном» киберрынке осуществляется торговля базами об уголовном преследовании и судимости с описанием подозреваемых, осужденных и их примет, сведений о потерпевших, а также спецучета членов организованных преступных групп (ФИО, дата рождения,

---

[1] В России будут судить продавцов персональных данных в даркнете // Про Пермь. URL: https://properm.ru/news/2023-02-12/v-rossii-budut-sudit-prodavtsov-personalnyh-dannyh-v-darknete-2683588 (дата обращения: 09.04.2023).

[2] Персональные данные общего пользования // Комсомольская правда. URL: https://www.msk.kp.ru/daily/26333/3217332/ (дата обращения: 09.04.2023).

[3] СМИ: база данных о ВИЧ-инфицированных и наркозависимых доступна для продажи // Газета.ru. URL: https://www.gazeta.ru/tech/news/2016/09/12/n_9103151.shtml (дата обращения: 09.04.2023).

адрес проживания, статус в ОПГ, кличка, комментарии, сфера интересов и др.), этнических чеченцев и др.[1].

Возрастание количества обращений граждан об утечках их персональных данных из баз данных государственных учреждений, банков, правоохранительных органов и др. отмечает и Роскомнадзор[2].

Очевидные преимущества цифровой формы хранения ограниченной информации при помощи информационных систем и их дальнейшая востребованность позволяют прогнозировать высокие риски прироста показателей преступлений в отношении баз персональных данных, а также тяжкие последствия их использования в преступных целях[3]. А потому систематизированная в базы конфиденциальная информация нуждается в повышенной защите средствами уголовного права. Справедливо замечание О.С. Капинус о том, что «скорость и объемы обращающейся информации, а также относительная доступность ее противоправного получения, в том числе из государственных и частных баз данных, образуют необходимость усиления защиты конституционных прав и свобод человека и гражданина, закрепленных в ст. ст. 23 и 24 Конституции Российской Федерации, в том числе связанных с неприкосновенностью частной жизни, личной и семейной тайны при аккумулировании, передаче, копировании и использовании персональных данных»[4].

Как показало исследование, в отличие от уголовного законодательства зарубежных стран отечественный уголовный закон не позволяет своевременно реагировать на совершение незаконных действий с персональными данными и

---

[1] СПИД пустили в народ. Базы данных по ВИЧ-инфицированным Тольятти и областным наркоманам открыто продаются // Новости Самары. URL: https://www.samru.ru/society/novosti_samara/21998.html (дата обращения: 09.04.2023).

[2] Халиулина Э.Т., Журавлева А.С. Преступления, совершаемые с использованием персональных данных: характеристика состояния // Военное право. 2021. № 2 (66). С. 290.

[3] Алихаджиева И.С. Криминологические риски персональных данных: основные тенденции и прогнозы // Известия Юго-Западного государственного университета. Серия: История и право. 2023. Т. 13, № 3. С. 95.

[4] Капинус О.С. Безопасность персональных данных как один из важнейших объектов конституционно-правовой охраны // Вестник Университета прокуратуры Российской Федерации. 2018. № 6 (68). С. 11.

противостоять им. В арсенале российского уголовного закона отсутствует выверенный механизм непосредственной уголовно-правовой охраны персональных данных, что и порождает трудности квалификации незаконных действий с ними. Для разрешения выявленных проблем необходимо реформировать уголовный закон путем введения в УК РФ самостоятельной нормы, обеспечивающей должную охрану неприкосновенности персональных данных (*проектируемая ст. 137[1] УК РФ*) и разработать специальную методику квалификации преступных посягательств в отношении персональных данных или с их использованием (об этом далее в настоящем исследовании).

Таким образом, изучив состояние российского уголовного права об ответственности за незаконные действия с персональными данными, автор пришел *к следующим выводам*:

1. В уголовно-правовом предупреждении незаконных действий с персональными данными задействована группа норм, выполняющих иные уголовно-политические функции. По задумке законодателя и своей уголовно-правовой сути они предназначены для противодействия иным преступлениям, непосредственно не связанным с персональными данными (против конституционных прав и свобод, семьи и несовершеннолетних, экономическим, должностным, компьютерным, против правосудия и порядка управления). В силу неразработанности понятий персональных данных как предмета преступления и их неприкосновенности как объекта преступления, корреспондирующего предмету, правоприменитель вынужден приспосабливать существующие уголовно-правовые средства для их защиты.

2. Социальная необходимость борьбы с преступлениями в отношении персональных данных требует создания особого механизма их уголовно-правовой охраны, включающего наряду с уже существующими нормами, специальную норму об ответственности за незаконные действия с персональными данными. Одним из основных аргументов в пользу специальной криминализации деяний, совершаемых с персональными данными или против них, служит ревизия имеющихся уголовно-правовых средств защиты персональной информации,

которые в силу многократного повышения общественной опасности незаконных действий с персональными данными не решают и объективно не могут решить задачи уголовного права по эффективному противодействию им. Их низкий предупредительный потенциал, кроме прочего, обусловлен и появлением новых трендов преступности в отношении персональных данных, проявляемых в ее цифровизации, «монетизации» личной конфиденциальной информации, сверхизменчивости и высокой вероятности наступления разрушительных последствий, в том числе отсроченных по времени. Незаконные действия с персональными данными сами по себе обладают высокой степенью общественной опасности, поскольку продуцируют новые посягательства против них (совершение преступлений с использованием персональных данных) и способствуют причинению вреда или угрозе его причинения другим охраняемым отношениям.

ГЛАВА II. ПОНЯТИЕ И ПРИЗНАКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ИМЕЮЩИЕ УГОЛОВНО-ПРАВОВОЕ ЗНАЧЕНИЕ

§ 1. Понятие персональных данных для целей уголовного закона

Для определения границ надлежащей уголовно-правовой охраны персональных данных и не нарушения пределов невмешательства в частную жизнь человека следует разработать точную их дефиницию. Понятие персональных данных дается во множестве нормативных правовых актах и разнится в зависимости от предмета регулирования тех либо иных общественных отношений[1]. Легальное определение персональных данных сформулировано и в статье 3 федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных» (далее также – Закон о персональных данных, ФЗ № 152), а потому авторский анализ не мог не учитывать интерпретацию персональных данных в официальном праве. Введенное в ФЗ № 152 определение персональных данных не может быть применимо для целей уголовного права, потому что он регулирует иную сферу общественных отношений – отношения, связанные с обработкой персональных данных государственными, муниципальными органами, юридическими и физическими лицами средствами автоматизации для поиска персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к ним. Иными словами, речь идет о правовом регулировании вопросов организационной (принципы и условия) и технической обработки операторами персональных данных человека для его социализации с установлением требований, обеспечивающих защиту прав на неприкосновенность частной жизни, личную и семейную тайну и других его благ и интересов. Являясь юридическим, оно видится неоднозначным с учетом специфики области применения, а потому применительно к уголовному праву требует уточнения.

---

[1] Об утверждении Перечня сведений конфиденциального характера: указ Президента РФ от 06.03.1997 № 188 (с изм. и доп. от 13.07.2015, № 357) // Рос. газета. 1997. 14 мар.; СЗ РФ. 2015. № 29 (ч. II), ст. 4473; Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела: указ Президента РФ от 30.05.2005 № 609 (с изм. и доп. от 29.04.2023, № 319) // Рос. газета. 2005. 07 июня; СЗ РФ. 2023. № 18, ст. 3297.

Актуализирует потребность в определении этого понятия для целей уголовного права, *во-первых*, его различное толкование в доктринальных источниках по объему – применяется узкий или чрезвычайно широкий подход, что позволяет относить к личным сведениям о человеке ограниченную либо, напротив, практически любую информацию о нем[1]. Подобный разброс в позициях, как пишут исследователи, порождает «некоторую правовую неопределенность, не позволяя однозначно ответить на вопрос о том, какие данные могут считаться персональными»[2], то есть подлежат охране средствами уголовного права. Выделение критериев отнесения той или иной информации к личным данным человека важно для теоретического исследования персональных данных и как самостоятельного предмета преступных посягательств, и как средства совершения общественно опасных деяний.

Другая сложность в установлении наличия признаков уголовно наказуемого деяния в отношении персональных данных обусловлена разными правовыми режимами их безопасности (личная и семейная, коммерческая, банковская, врачебная, адвокатская, налоговая тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений), включая вид и содержание персональных данных, и установленные по ним запреты и ограничения[3]. Для оценки наличия признаков уголовно наказуемого деяния правоприменитель вынужденно прибегает к толкованию норм позитивного права[4], подзаконным актам[5], позволяющим предметно детализировать, что же

---

[1] Мираев А.Г. Понятие персональных данных в Российской Федерации и Европейском союзе // Юридическая наука. 2019. № 5. С. 77.

[2] Проскурякова М.И. Защита персональных данных в праве России и Германии: конституционно-правовой аспект: автореф. дис. ... канд. юрид. наук. СПб., 2017. С. 7.

[3] Радова М.А. Профессиональная тайна в системе уголовно-процессуальных гарантий защиты сведений о частной жизни лица // Криминалистика: вчера, сегодня, завтра. 2023. № 2 (26). С. 143.

[4] См.: Ст. 6 федерального закона от 25.01.2002 № 8-ФЗ «О Всероссийской переписи населения» (с изм. и доп. от 24.04.2020, № 147-ФЗ) // Рос. газета. 2002. 29 янв.; 2020. 29 апр.; п. 2 ст. 6 федерального закона от 01.04.1996 № 27-ФЗ (с изм. и доп. от 28.12.2022, № 569-ФЗ) «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» // Рос. газета. 1996. 10 апр.; 2022. 30 дек.

[5] Об утверждении Положения о защите персональных данных работников Федерального фонда обязательного медицинского страхования: приказ Федерального фонда ОМС от 19.08.2008 № 180 (с изм. и доп. от 23.03.2009, № 53) // Рос. газета. 2008. 17 сент.; 2009. 28 апр.

считается персональными данными при регулировании того или иного правоотношения. *Во-вторых*, отсутствие единообразного толкования этого термина порождает противоречивую правоприменительную практику и, как следствие, не служит эффективной защите тех фундаментальных благ личности, которые поставлены под охрану самим законодателем.

Чтобы сформулировать понятие персональных данных для целей уголовного права, следует выделить *признаки персональных данных* на основе разработок международного права, специального (регулятивного) российского законодательства и отечественной правовой доктрины.

1. *Персональные данные – это* ***информация*** *независимо от ее восприятия и использования.* Из текста ст. 3 Закона о персональных данных следует, что отечественный правотворец пошел по пути их атрибуции через «любую информацию», относящуюся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)[1]. Ориентируясь на него, правоведы-специалисты по конституционному и информационному праву выводят персональные данные через категорию «информация»: «информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу»[2]; «информация, неразрывно связанная с личностью ее обладателя»[3]; «информация (зафиксированная на любом носителе) о конкретном человеке, которая отождествляется или может быть отождествлена с ним»[4] и др. Для уголовного права определение персональных данных сформулировал С.И. Гутник, предлагая считать ими информацию, позволяющую идентифицировать физическое лицо и в отношении которой на основе федерального закона может устанавливаться режим её

---

[1] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (с изм. и доп. от 06.02.2023, № 8-ФЗ) // Рос. газета. 2006. 29 июля; 2023. 9 февр.

[2] Кротов А.В. Опыт обработки персональных данных работника в компании // Информационное право. 2007. № 2. С. 18.

[3] Петров М.И. Комментарий к Федеральному закону «О персональных данных» (постатейный): от 27 июля 2006 г. № 152-ФЗ. М.: Юстицинформ, 2007. С. 34.

[4] Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право / под ред. Б.Н. Топорнина. 2-е изд., с изм. и доп. СПб.: Юрид. центр Пресс, 2005. С. 244.

конфиденциальности[1]. Думается, с точки зрения юридической техники его очевидным недостатком является отсутствие всех признаков персональных данных, которые позволяют добиться более высокого уровня формальной определенности[2].

Синонимами «информации», используемыми теоретиками при построении определения «персональные данные», являются также термины «сведения» и «данные»: «сведения конфиденциального характера»[3]; «сведения о фактах, событиях, и обстоятельствах жизни физического лица, его семьи, а также позволяющие отождествить их с конкретным индивидом и отражающие особенности последнего по отношению к другим людям (обществу)»[4]; «сведения, использование которых без согласия их субъекта может нанести вред его чести, достоинству, деловой репутации, доброму имени, иным нематериальным благам и имущественным интересам»[5]; «данные в автоматизированной форме, содержащие информацию о частной (личной, семейной) жизни индивида, который может быть идентифицирован на основании этой информации (или с помощью этой и иной информации), если, с точки зрения любого нормального человека, наделенного обычной чувствительностью, субъект данных вправе считать такую информацию конфиденциальной и контролировать ее распространение»[6]; «сведения о

---

[1] Гутник С.И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: дис. … канд. юрид. наук. Красноярск, 2017. С. 66.

[2] Принцип формальной определенности закона, сформулированный в практике Конституционного Суда РФ, вытекает из ч. 1 ст. 1, ч. 2 ст. 4, ч. 2 ст. 6, ч. 2 ст. 15 и ч. 1 ст. 19 Конституции РФ и предполагает точность, ясность и недвусмысленность правовых норм, без чего не может быть обеспечено единообразное понимание и применение таких норм, а значит, и равенство всех перед законом (см., напр., Постановление Конституционного Суда РФ от 08.04.2014 № 10-П «По делу о проверке конституционности положений пункта 6 статьи 2 и пункта 7 статьи 32 Федерального закона «О некоммерческих организациях», части шестой статьи 29 Федерального закона «Об общественных объединениях» и части 1 статьи 19.34 Кодекса РФ об административных правонарушениях в связи с жалобами Уполномоченного по правам человека в Российской Федерации, фонда «Костромской центр поддержки общественных инициатив», граждан Л.Г. Кузьминой, С.М. Смиренского и В.П. Юкечева».

[3] Никитин Е.Л., Тимошенко А.А. К вопросу о правовой природе персональных данных работника // Журнал российского права. 2006. № 7. С. 44.

[4] Просветова О.Б. Защита персональных данных: дис. … канд. юрид. наук. М., 2005. С. 27–28.

[5] Бачило И.Л. Информационное право: учебник. С. 284.

[6] Иванский В.П. Теоретические проблемы правовой защиты частной жизни в связи с использованием информационных технологий: автореф. дис. … канд. юрид. наук. М., 1998. С. 21.

физическом лице или относящиеся к прямо или косвенно к определенному или определяемому на основании таких сведений физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, а также другая информация, которая, как правило, представлена в формализованном виде, обеспечивающем возможность их обработки в информационных системах, преимущественно с помощью средств автоматизации, полностью или частично»[1] и др. Очевидно, что многочисленные дефиниции, во многом схожие между собой, достаточно сложны и громоздки в том числе и потому, что на сегодняшний день, как справедливо замечает Л.А. Букалерова, нет легального определения термина «информация» для целей уголовного права, хотя уголовный закон им оперирует»[2].

В этой части дискуссия обычно сводится к тому, допустима ли замена термина «информация» иными, похожими по смыслу понятиями, среди которых «персональная информация», «сведения», «данные», «информация о личной жизни лица», «информация личного характера» и др.[3]. Теоретико-прикладного значения в контексте настоящего исследования она не имеет, *во-первых*, потому, что согласно легальному определению видами информации являются сведения (сообщения, данные) независимо от формы их представления (ст. 2 федерального закона «Об информации, информационных технологиях и о защите информации», далее – ФЗ об информации, ФЗ № 149[4]), *во-вторых*, ввиду их использования для разгрузки текста от многократных повторов одного и того же понятия

---

[1] Бундин М.В. Персональные данные в системе информации ограниченного доступа: дис. ... канд. юрид. наук. М., 2017. С. 53.

[2] Букалерова Л.А. Уголовно-правовая охрана официального информационного оборота / под ред. В.С. Комиссарова, Н.И. Пикурова. М.: Юрлитинформ, 2006. С. 10.

[3] Бачило И.Л. Информация и информационные отношения в праве // НТИ. Сер. 1. 1999. № 8. С. 27; Шутова А.А. Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности: теоретический и прикладной аспекты: дис. ... канд. юрид. наук. Н. Новгород, 2017. С. 9; Бундин М.В. Указ. соч. С. 53; Гутник С.И. Указ. соч. С. 45.

[4] Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ (с изм. и доп. от 31.07.2023, № 408-ФЗ) // Рос. газета. 2006. 29 июля; 2023. 3 авг.

(персональные данные)[1], *в-третьих*, в составах преступлений, имеющихся в уголовном законе, понятия «информация» и «сведения» тождественны, однако авторы предлагают использовать один термин «информация» для унификации норм УК[2].

Следует оговориться в этой части, что для целей уголовного права сочетание слов «*любая* информация» неприемлемо в силу его юридической абстрактности. В науке неудачность прилагательного «любая» применительно к информации критикуется за его широту, поскольку «оно может включать в себя как данные, являющиеся информацией ограниченного доступа о субъекте, так и данные, не являющиеся персональными данными ввиду каких-либо особенностей. Такое широкое толкование, часто используемое судами, далеко не всегда свидетельствует о повышении уровня защиты прав субъекта персональных данных, поскольку формальное обращение к защите таких сведений способно привести к существенному нарушению прав, гарантированных другими законодательными актами, зачастую более важными, нежели право на защиту персональных данных»[3]. Думается, *во-первых*, как разновидность конфиденциальной информации о человеке персональные данные должны быть не любыми и не «вообще», а такими, которые позволяют увеличить степень осведомлённости о нем[4]. Причем осведомленность означает буквально достоверную и однозначную их принадлежность только этому лицу. *Во-вторых*, не вся информация является одинаково значимой для целей идентификации. Ведь если она «не привязана» к номинативной, т.е. знаковой в этом смысле информации (фамилия, имя, отчество, дата и место рождения), то сами по себе данные об образовании, семейном и имущественном положении, состоянии здоровья или профессии не могут повлечь причинения вреда человеку[5]. И потому

---

[1] Бундин М.В. Указ. соч. С. 49.
[2] Шутова А.А. Указ. соч. С. 9.
[3] Симонова Е.В. Определение понятия персональных данных в Российской Федерации // Молодой ученый. 2017. № 10. С. 324.
[4] Гутник С.И. Указ. соч. С. 45.
[5] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. М.: Статут, 2011. С. 21.

правоприменитель должен учитывать, что комбинация находящихся в свободном обороте номинативных данных с информацией о судимости, болезни, банковских вкладах, сексуальной ориентации, индивидуальных средствах коммуникации и др. создает опасность нарушения прав и свобод идентифицированного человека. Как подчеркивает в этой связи В.Н. Лопатин, к персональным данным могут быть отнесены сведения, использование которых без согласия их субъекта может нанести вред его чести, достоинству, деловой репутации, доброму имени, иным нематериальным благам и имущественным интересам[1]. А потому при установлении признаков уголовно наказуемого деяния в каждом конкретном случае следует, прежде всего, определять только ту совокупность (или набор) данных о человеке, которая позволяет его идентифицировать, а, следовательно, обладает потенциалом причинения вреда или угрозы его причинения любым охраняемым законом отношениям. В теории уголовного права С.И. Гутник такую совокупность информации именует объемом персональных данных, и он должен быть достаточным, чтобы их субъект мог быть достоверно идентифицирован[2]. Это может быть один или несколько признаков человека, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности[3].

2. *Персональные данные – это информация, относящаяся* ***к физическому лицу*** *(субъекту персональных данных), ее связь с индивидом*. Она становится персональной как раз тогда, когда есть связь между субъектом и данными о нем. Именно потому, что персональные данные признаются информацией, позволяющей идентифицировать человека, их субъектами могут быть исключительно физические лица[4]. Примечательно, что в зарубежном праве обладателем персональных данных могут быть юридические лица (Австрия,

---

[1] Бачило И.Л. Информационное право: учебник. С. 284.
[2] Гутник С.И. Указ. соч. С. 190.
[3] Вабищевич В.В. Определение персональных данных в целях их уголовно-правовой охраны // Вестник Полоцкого государственного университета: научно-теоретический журнал. 2019. № 14. С. 137.
[4] Камалова Г.Г. О способе отнесения сведений к информации ограниченного доступа // Вестник Удмуртского университета. Экономика и право. 2015. № 2. С. 109.

Исландия, Швейцария)[1] или не просто физические лица, а живые. К примеру, в новом Акте о защите данных 2018 г. Великобритании в ч. 1 ст. 3 об этом указано прямо: «идентифицируемое живое лицо»[2]. В российском ФЗ № 152 такого уточнения нет, хотя его положения говорят об аналогичном подходе. К тому же к персональным данным относятся не только сведения, собираемые для идентификации неизвестного лица, но и уже известного[3].

3. *Информация относится* ***к определенному или определяемому*** *физическому лицу*. Особенностью персональных данных как вида информации ограниченного доступа является соотносимость с конкретным лицом. После внесения федеральным законом от 25.07.2011 № 261-ФЗ[4] поправок в понятие персональных данных ими стала являться и информация, которая должна позволять определять конкретное физическое лицо. Об определенном или поддающемся определению физическом лице («субъект данных») через любую информацию говорит и Конвенция о защите физических лиц при автоматизированной обработке персональных данных (далее Конвенция 108, ратифицирована федеральным законом от 19.12.2005 № 160-ФЗ[5]), закрепляя понятие персональных данных[6]. Комментаторы в этой связи считают персональными данными информацию, с помощью которой лицо можно установить. Так, по мнению Н.Е. Циулиной, определяемым является лицо, которое может быть «определено, прямо или косвенно, в частности, через

---

[1] Добробаба М.Б. Понятие персональных данных: проблема правовой определенности // Вестник Университета имени О. Е. Кутафина. 2023. № 2 (102). С. 45.

[2] Закон о защите данных 2018 г. (Data Protection Act 2018 (DPA 2018)). URL: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (дата обращения: 21.09.2022).

[3] Калятин В.О. Персональные данные в Интернете // Журнал российского права. 2002. № 5. С. 79.

[4] О внесении изменений в Федеральный закон «О персональных данных»: федер. закон от 25.07.2011 № 261-ФЗ // СЗ РФ. 2011. № 31, ст. 4701.

[5] О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных: федер. закон от 19.12.2005 № 160-ФЗ // Рос. газета. 2005. 22 дек.

[6] Конвенция о защите физических лиц при автоматизированной обработке персональных данных: заключена в г. Страсбурге 28.01.1981 (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) // СЗ РФ. 2014. № 5, ст. 419.

идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности»[1].

Между тем большинство предлагаемых в научных трудах по изучаемой теме понятий персональных данных верно строится на признаке «идентифицируемости» их субъекта. Так, А.С. Минзов, А.Ю. Невский, О.Р. Баронов отмечают, что «идентификация – это определение пользователя в автоматизированной системе по его уникальному признаку – идентификатору[2]. В роли идентификатора может выступать имя пользователя в системе (логин), числовой или буквенно-числовой код, электронная подпись, ИНН, СНИЛС, электронная почта, номер мобильного телефона или другая информация»[3]. Тем самым соавторы понимают под идентификацией техническую процедуру проверки принадлежности идентификатора списку или базе данных[4]. То же самое происходит и при установлении признаков состава преступления, когда осуществляется процедура распознавания (идентификации) человека и его соответствия тем данным, которые без его согласия и в отсутствие законных оснований противоправно собирались, были похищены или обнародованы.

---

[1] Циулина Н.Е. Формирование и развитие правовой категории «персональные данные» // Вестник УрФО. Безопасность в информационной сфере. 2013. № 1. С. 49.

[2] В этом контексте под идентификатором понимается информация о физическом лице, которая сама по себе отдельно или с другими данными может идентифицировать человека. Система российского учета представляет собой набор персональных данных о гражданах в государственных и муниципальных информационных системах, плохо связанных между собой множеством идентификаторов (свидетельство о рождении, паспорт, ИНН, СНИЛС и т.д.). Между тем в РФ активно обсуждается перспектива введения универсального идентификатора сведений о физических лицах, тем более что в проекте ФЗ № 152 имелась статья о присвоении персональным данным субъектов индивидуальных идентификационных номеров. В окончательную редакцию она не вошла, поскольку подверглась критике со стороны представителей религиозных конфессий. См. подроб.: Волошкин И.Г., Андреева Е.В. Универсальный идентификатор сведений о гражданине: мировой опыт и возможности введения в Российской Федерации // Вестник университета. 2014. № 15. С. 260; Петрыкина Н.И. К вопросу о конфиденциальности персональных данных // Законы России: опыт, анализ, практика. 2007. № 6. С. 115.

[3] Минзов А.С., Невский А.Ю., Баронов О.Р. Безопасность персональных данных: новый взгляд на старую проблему // Вопросы кибербезопасности. 2022. № 4 (50). С. 4.

[4] ГОСТ Р 58833-2020. Защита информации. Идентификация и аутентификация. Общие положения: утв. приказом Федерального агентства по техническому регулированию и метрологии от 10.04.2020 № 159-ст. Доступ из Справ.-прав. системы «КонсультантПлюс».

Соглашаясь с аргументами ученых в этой части, для упрощения интерпретации данных как персональных предлагается использовать в качестве их признака (свойства) идентификацию конкретного лица как более удачный по причине его формальной определенности термин. Он точнее передает смысл формулировки персональных данных, позволяет выделить из общего массива информации о человеке те данные, с помощью которых он может быть идентифицирован доподлинно, без ошибки. В качестве аргумента укажем и то, что редакции ряда законопроектов о персональных данных использовали именно это слово, однако в итоговом документе появились слова «определенный» и «определяемый»[1].

В тематических трудах находит место и позиция о том, что распознавание человека или его идентификация, а также иные синонимы – отождествление[2], определение личности – не могут использоваться как критерий разграничения персональных от иных, не конфиденциальных данных, ввиду возникновения дискуссии о возможности или невозможности установить лицо на основании той или иной совокупности сведений о нем[3]. О.Б. Просветова, в частности, пишет, что сужение значения персональных данных лишь до сведений, позволяющих идентификацию личности, не соответствует ст. 24 Конституции РФ, которая охватывает все сведения о частной жизни лица[4]. Полагаем, что постановка проблемы о неприемлемости признака идентификации надумана, *во-первых*, потому что не вся возможная совокупность сведений о частной жизни лица, охраняемых конституционными нормами, может считаться персональными

---

[1] Хохлова Е.В. О признаках персональных данных как предмете и средстве совершения преступлений // Уголовная политика и культура противодействия преступности: матер. междунар. науч.-практ. конф. (30 сентября 2022 г.) / ред. кол.: А.Л. Осипенко (отв. ред.) [и др.]. Краснодар: Изд-во Краснодар. ун-та МВД России, 2022. С. 425–427.

[2] К примеру, в Модельном законе от 16.10.1999 № 14-19 «О персональных данных» персональные данные – это: а) информация (зафиксированная на материальном носителе) о конкретном человеке; б) информация отождествлена или может быть отождествлена с ним.

[3] Алексашина М.Н. Защита персональных данных как условие обеспечения безопасности личности // Право и безопасность. 2014. № 1. С. 69.

[4] Просветова О.Б. Указ. соч. С. 26.

данными, а только относящаяся к «чувствительным данным»[1], и только та, которая идентифицирует субъекта. Здесь должно быть достаточно объёма персональных данных, чтобы их субъект мог быть идентифицирован достоверно[2]; *во-вторых*, российское и международное законодательство активно использует именно термин «идентификация». Так, в действующем Указе Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» понятие персональных данных было сформулировано как «сведения о фактах, событиях и обстоятельствах частной жизни гражданина», позволяющие *идентифицировать* его личность (персональные данные)»[3]. В п. 1 ст. 4 Общего регламента по защите персональных данных Европейского союза (General Data Protection Regulation, GDPR) (по содержанию это Регламент (EU) № 2016/679 и Директива (EU) № 2016/680) персональные данные – любая информация, относящаяся *к идентифицированному или идентифицируемому* физическому лицу; «субъект данных» может быть *идентифицирован* прямо или косвенно[4]; *в-третьих*, без признака идентификации исключается соотносимость персональных данных с конкретным лицом, а значит утрачивается какой-либо смысл в их охране, и в том числе уголовно-правовыми средствами.

---

[1] Это наименование специальных данных основано на сложившемся в судебной практике стран общего права принципе, что распространение определенного факта частной жизни (персональных данных) признается посягательством на частную жизнь, если это распространение «высокопредосудительно для любого благоразумного человека, наделенного обычной чувствительностью». Цит. по: Минбалеев А.В. Проблемные вопросы понятия и сущности персональных данных // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2 (4). С. 5. Статья 6 Конвенции 108 к «высокочувствительным» относит данные о расовом или национальном происхождении, политических взглядах, религиозных и иных убеждениях, а также данные, касающиеся здоровья, сексуальной жизни, судимости, подлежащие специальной охране.

[2] Гутник С.И. Указ. соч. С. 190.

[3] Об утверждении Перечня сведений конфиденциального характера: указ Президента РФ от 06.03.1997 № 188 (с изм. и доп. от 13.07.2015, № 357) // Рос. газета. 1997. 14 марта; СЗ РФ. 2015. № 29 (ч. II), ст. 4473.

[4] О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных: регламент (EU) от 27.04.2016 № 2016/679. URL: https://ogdpr.eu/ru/gdpr-2016-679 (дата обращения: 21.05.2022); О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования уголовных преступлений, ведения розыскных или судебных действий или исполнения уголовных наказаний, а также за свободное перемещение таких данных: директива (EU) от 27.04.2016 № 2016/680. URL: https://ogdpr.eu/ru/gdpr-2016-680 (дата обращения: 21.05.2022).

В Общем регламенте по защите персональных данных 2018 г. (или GDPR) появилось важное уточнение, что специальные категории данных являются персональными, если, используя некую их совокупность, человека можно идентифицировать *однозначно* (of *uniquely* identifying a natural person, ст. 9). У термина «однозначность» имеется множество синонимов, однако в контексте персональных данных он понимается нами как «очевидный», «единственный», «конкретный», «четкий», «недвусмысленный», «одновариантный», «тождественный» и др. А потому «однозначная» идентификация означает точное совпадение уникальных признаков субъекта с закрытыми личными данными о нем. Напротив, «неоднозначная» идентификация человека по персональным данным есть использование вероятностного подхода к его установлению, что не допустимо при осуществлении квалификации деяний, посягающих на неприкосновенность частной жизни, личной или семейной тайны и других видов тайны. Неоднозначно определенными персональными данными могут быть сведения, включающие: маркетинговые и социологические исследования, расследование инцидентов, криминологию, судебную деятельность, в которых имеют значение не индивидуальные признаки субъектов конфиденциальных данных, а групповые. Признак однозначности идентификации персональных данных в этом смысле свидетельствует о единственно возможной принадлежности данных конкретному физическому лицу. Придание же иного смысла этому термину не отвечало бы принципу вины. В этой связи предлагается учитывать новый признак персональных данных в их определении применительно к характеристике идентификации.

4. *Информация относится к* ***прямо или косвенно*** *определенному или определяемому физическому лицу.* Теоретики пишут о расширении понятия персональных данных, ибо по смыслу ФЗ № 152 персональными признаются и те личные данные, которые даже косвенно, как следует из его текста, могут определить того или иного человека или создают эту возможность[1], и потому выделяют этот характеризующий признак. Думается, что использование

[1] Минбалеев А.В. Указ. соч. С. 6.

в отношении персональных данных понятий «прямо» и «косвенно» лишено всяческого смысла ввиду того, что любая личная информация о физическом лице, позволяющая его идентификацию, и есть персональные данные[1]. Это следует и из перечня персональных данных Общего регламента по защите персональных данных (или GDPR), классифицировать которые на прямые и косвенные нельзя. Так, согласно ст. 4 GDPR идентифицируемое физическое лицо – это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, фамилия, идентификационный номер, данные о местоположении, онлайн-идентификатор или один или несколько характерных для указанного лица физических, физиологических, генетических, духовных, экономических, культурных факторов или ссылаясь на факторы социальной идентичности. Изучение актуальной судебной практики показывает, что в приговорах понятия «прямо» или «косвенно» в отношении персональных данных не используются. А потому для устранения неопределенности в толковании правоприменителем признаков персональных данных следует исключить понимание информации особого вида, относящейся к человеку, как прямой или косвенной, тем более что такое ее деление не имеет практического смысла.

Проблема видится и в том, что такая формулировка персональных данных закрепляет неверный подход, по которому абсолютно любая косвенная информация может относиться к физическому лицу, поскольку понятие персональных данных не содержит оговорки «*на основании такой информации*»[2]. Очевидно, что информация об образовании или профессии, заболевании, судимости без другой достоверно идентифицирующей информации, не может быть персональными данными[3]. А потому для формальной определенности

---

[1] Минзов А.С., Невский А.Ю., Баронов О.Р. Указ. соч. С. 5.

[2] Наумов В.Б., Архипов В.В. Понятие персональных данных: интерпретация в условиях развития информационно-телекоммуникационных технологий // Российский юридический журнал. 2016. № 2. С. 189.

[3] Бучакова М.А. Персональные данные и их защита в условиях цифровизации общества // Алтайский юридический вестник. 2021. № 2 (34). С. 45.

дефиниция персональных данных должна содержать уточнение о том, что лицо может идентифицироваться исключительно «на основании такой информации».

5. *Персональные данные являются разновидностью информации, обладающей признаком* ***конфиденциальности***.

Для того, чтобы понять, какие персональные данные подлежат уголовно-правовой охране, следует оговориться, что не все из них для исключения их использования с целью причинения вреда публичным или частным интересам находятся в ограниченном доступе. Персональные данные отличает от иных видов информации особого вида, находящейся под защитой (адвокатская, коммерческая, банковская тайна, тайна усыновления) то, что многие из них либо открытые или общедоступные (фамилия, имя, отчество лица, место работы, ученая степень), либо свободный доступ к ним и использование запрещены в зависимости от определенных обстоятельств или в определенный период времени. К примеру, в постановлении Правительства РФ от 24.11.2009 № 953 (с изм. и доп. от 10.11.2022, № 2025) «Об обеспечении доступа к информации о деятельности Правительства Российской Федерации и федеральных органов исполнительной власти» фамилии, имена, отчества Председателя и членов Правительства РФ, руководителей федеральных органов исполнительной власти и их структурных подразделений и некоторых других должностных лиц не могут быть отнесены к сведениям ограниченного доступа[1]. И в этом случае, как пишет М.В. Бундин, действует «презумпция конфиденциальности» (наличие однозначного согласия или изъятия специальным законом)[2]. Иными словами, не все персональные данные – *конфиденциальная* информация, поскольку в тексте ФЗ № 152 упоминается категория общедоступных персональных данных (фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, ст. 8).

Тем же ФЗ № 152 в 2020 г. была добавлена ещё одна категория персональных данных – «разрешённые для распространения» (пункт

---

[1] Рос. газета. 2009. 2 дек.; СЗ РФ. 2022. № 46, ст. 8027.

[2] Бундин М.В. Персональные данные как информация ограниченного доступа // Информационное право. 2009. № 1. С. 11.

1.1 ст. 3)[1]. По смыслу новеллы ими признаются такие персональные данные, чей владелец сам предоставил доступ к ним неограниченному кругу лиц. Здесь субъектом личной информации дается отдельное от иных согласие не только на обработку, а именно на их распространение. Из пояснительной записки № 101234-8 к законопроекту следует, что цель поправки – ограничить неконтролируемое использование персональных данных, размещенных в открытых источниках. Любые данные человека о себе, опубликованные в сети Интернет в свободном доступе (социальные сети, сайты маркетинговых площадок, развлекательные платформы и др.), или, к примеру, для оказания определенных услуг, связанных с его профессиональной деятельностью, не могут быть использованы третьими лицами в иных целях. Такой подход имеет значение для решения вопроса о наличии признаков состава преступления при использовании персональных данных, опубликованных самим пользователем, что будет исследовано в других параграфах работы. Очевидно, не все персональные данные считаются информацией, при обороте которой действуют определенные ограничения и запреты, в отношении далеко не всех персональных данных действует принцип сохранения их конфиденциальности и уголовно наказуемый запрет их сбора и (или) распространения. При этом одни и те же персональные данные могут охраняться и разными способами защиты – самостоятельно, собственными мерами; в режиме совместной охраны (профессиональная, служебная тайна); в режиме государственной тайны; в режиме охраны иного вида информации ограниченного доступа.

Режимом конфиденциальности по ФЗ № 152 наделены специальные (ст. 10) и биометрические персональные данные (ст. 11). Попытка установить, что же включают в себя специальные персональные данные, была предпринята в ст. 10 ФЗ № 152, где называются расовая, национальная принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья, интимная жизнь. Причем законодатель закрыл этот перечень персональных

[1] О внесении изменений в Федеральный закон «О персональных данных»: федер. закон от 30.12.2020 № 519-ФЗ // Рос. газета. 2021. 11 янв.

данных, запрещенных к обработке, не включив в них судимость, сведения о которой упоминаются в п. 3 той же статьи 10. Закон их именует «категориями персональных данных» с разным правовым режимом, суть которых, как верно подмечает Л.К. Терещенко, «сводится в основном к режиму доступа»[1] (*или режиму охраны – курсив наш*). В комментарии под редакцией В.М. Лебедева разъясняется, что охраняемой является информация, для которой в законах, иных нормативных правовых актах установлен специальный режим ее правовой защиты, например, государственная, служебная, коммерческая и банковская тайны, персональные данные и т.д.[2]. Таким образом, все персональные данные по категориям делятся на разрешённые для распространения, общедоступные, специальные, биометрические и иные. Последними согласно абз. 4 п. 5 постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[3] являются группы сведений о человеке, которые нельзя отнести к трем другим.

«Конфиденциальная» информация и «конфиденциальность» информации – не одно и то же. Это подтверждает и множество теоретических работ, авторы которых комментируют попытку законодателя использовать второе понятие в действующем законе об информации вместо уже имевшегося термина «конфиденциальная» информация. Так, по смыслу ст. 9 «Ограничение доступа к информации» Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» государственная, коммерческая, профессиональная, служебная, личная, семейная и иная тайна признаются информацией с ограниченным доступом. А «конфиденциальность» информации согласно п. 7 ст. 2 этого закона рассматривается как обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее

---

[1] Терещенко А.К. К вопросу о правовом режиме информации // Информационное право. 2008. № 1. С. 23.
[2] Комментарий к Уголовному кодексу Российской Федерации / отв. ред. В.М. Лебедев.13-е изд., перераб. и доп. М.: Юрайт, 2013. С. 339.
[3] Рос. газета. 2012. 7 нояб.

обладателя[1]. Напротив, одноименный закон 1995 г. использовал иное понятие, обозначающее ограниченную информацию – «*конфиденциальная* информация», которой признавалась документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ (п. 8 ст. 2)[2]. Такую замену терминов многие авторы справедливо называют неоправданной ввиду порождения ею большей путаницы[3]. Отметим, что и ФЗ № 152 содержит понятие конфиденциальности персональных данных (ст. 7), а не прилагательное «конфиденциальный».

Конфиденциальность не абсолютна и может подвергаться изъятию – быть устранена или уменьшена самим носителем персональных данных (при согласии на их обнародование) или Конституцией РФ (ч. 3 ст. 55), федеральным законом, когда нарушение их анонимной сохранности не зависит от его воли. К примеру, в пп. 2.1-9 п. 2 ст. 10 ФЗ № 152 перечислены основания обработки персональных данных без согласия их владельца, что исключает и обеспечение их конфиденциальности (Всероссийская перепись населения; осуществление правосудия, проведение следствия[4], дознания, оперативно-розыскных мероприятий и др.). Изложенное определяет вывод о том, что для установления персональных данных физического лица в качестве предмета преступления значение имеет признак «конфиденциальность», означающий их неприкосновенность, обеспечиваемую в том числе уголовно-правовой охраной от их незаконного получения (собирания) или разглашения (распространения), а также использования в преступных целях. Нарушение же конфиденциальности

---

[1] Несмелов П.В. К вопросу о конфиденциальной информации в административном праве // Полицейская деятельность. 2012. № 4. С. 60.

[2] Об информации, информатизации и защите информации: федер. закон от 20.02.1995 № 24-ФЗ (утратил силу) // Рос. газета. 2006. 11 июля.

[3] Бундин М.В. Система информации ограниченного доступа и конфиденциальность // Вестник Нижегородского университета им. Н.И. Лобачевского. 2015. № 1. С. 127.

[4] Дударева М.А. Сведения о частной жизни лица как составляющая данных предварительного расследования: особенности запрета на разглашение // Закон и право. 2022. № 10. С. 164; Радова М.А. Соотношение сведений о частной жизни человека и его персональных данных в уголовном процессе России // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. 2022. № 4 (93). С. 158.

персональных данных состоит в необеспечении соответствующего режима их сохранности.

6. *Персональные данные являются* ***фиксированной*** *(обособленной) информацией.* ФЗ № 152 не содержит в определении персональных данных такого признака, как их фиксация в идеальной или материальной форме на определённом материальном носителе, что позволяет расширительно их толковать, считать ими в том числе слухи, домыслы и сплетни[1]. И.А. Юрченко пишет о том, что особенностью информации является то, что ее невозможно представить без какой-либо материальной основы, она является атрибутом (свойством) материи и неотделима от нее[2]. По мнению В.П. Числина, охраняемая законом информация – это документированная информация, содержащая сведения, отнесенные законом к государственной тайне или конфиденциальной информации[3]. Разделяют эту позицию и другие исследователи[4]. Напротив, С.А. Стяжкина отмечает, что для целей уголовного права информация может и не иметь материальной формы фиксации (например, устная передача информации)[5]. А.С. Озерова считает, что значимая и неизвестная неопределенному кругу лиц информация не обязательно фиксируется на материальном носителе и имеет определенные реквизиты; носителем информации способен выступать человек, а значит путем угроз и иных противоправных действий информация может быть получена от ее законного владельца[6]. Не углубляясь в дискуссию о том, что является предметом преступления – информация в любой форме или ее физический носитель, отметим как верный подход юристов второй группы, поскольку в противном случае необоснованно сужается предмет уголовно-

---

[1] Платонова Н.И. Современный подход к пониманию персональных данных // Право и современные государства. 2017. № 5. С. 11.

[2] Юрченко И.А. Информация как предмет уголовно-правовой охраны: дис. ... канд. юрид. наук. М., 2000. С. 40.

[3] Числин В. П. Уголовно-правовые меры защиты информации от неправомерного доступа: дис. ... канд. юрид. наук. М.: Коломенский государственный педагогический институт, 2004. С. 36.

[4] Козороиз Н.Л. Законодательство защищает информацию // Право в вооруженных силах. 2013. № 9. С. 107–111.

[5] Стяжкина С.А. Информация как объект уголовно-правовой охраны: понятие, признаки, виды // Вестник Удмуртского университета. Экономика и право. 2015. № 2. С. 158.

[6] Озерова А.С. О необходимости изменения подхода к понятию «информация» в законодательстве и судебной практике // Правоведение. 2019. № 1. С. 142.

правовой охраны. Учитывая, что персональные данные – это ставшая достоверно известной другому лицу после ознакомления информация, полученная в результате любой деятельности, то предметом преступления следует признавать зафиксированные в документах или на иных носителях, а также в устной (сообщения, полученные в ходе беседы), в идеальной (в памяти человека) форме персональные данные. Легальная дефиниция информации подтверждает правильность такого заключения (информация – сведения (сообщения, данные) независимо от формы их представления, п. 1) ст. 2 ФЗ № 149). Полагаем, что это могут быть недокументированные и документированные персональные данные на бумаге или в электронном виде[1], видео и аудиофайлы, снимки экрана, распечатанные копии интернет-страниц, прочих интернет-ресурсов (социальные сети, сайты), т.е. материальные носители, зафиксировавшие информацию в том числе из виртуальной реальности. Понимание персональных данных с юридической точки зрения как обособленной, зафиксированной тем или иным образом информации, наделяет их юридическим статусом и позволяет правоприменителю отграничить от прочей информации о частной жизни человека, основанной на неточных, непроверенных или заведомо неверных, нарочито измышленных сведениях.

Таким образом, на основе анализа международного и российского законодательства, теории права и систематизированных из специального федерального законодательства оригинальных признаков персональных данных, перечисленных в пп. 1–6, автор сформулировал определение персональных данных для целей уголовного права. Как предмет преступления или как средство его совершения ***персональные данные*** представляют собой зафиксированную с помощью материального носителя или в нематериальной (идеальной) форме информацию (сведения) о физическом лице (субъекте персональных данных),

---

[1] См., напр.: О перечне персональных данных, записываемых на электронные носители информации, содержащиеся в основных документах, удостоверяющих личность гражданина Российской Федерации, по которым граждане Российской Федерации осуществляют выезд из Российской Федерации и въезд в Российскую Федерацию: постановление Правительства РФ от 04.03.2010 № 125 (с изм. и доп. от 10.02.2014, № 94) // Рос. газета. 2010. 10 мар.; 2014. 14 февр.

охраняемую в режиме конфиденциальности (ограниченного доступа), на основании которой может быть осуществлена его однозначная идентификация.

§ 2. Соотношение персональных данных со смежными категориями, имеющими уголовно-правовое значение

Предметом активного обсуждения в российской научной среде является вопрос о соотношении между собой понятий «персональные данные» и «частная жизнь», «личная тайна», «семейная тайна» как категорий, характеризующих личную информацию. Пробелы в терминологии не всегда позволяют их четко отмежевать потому, что одни и те же виды информации могут быть и сведениями о частной жизни, и личной, и семейной тайной, и персональными данными. Неопределённость связи между собой этих понятий «осложняет системное толкование законодательства и правоприменения»[1]. Потребность в терминологической ясности отмечается и экспертами (*54 %*), что объективно вызывает необходимость уточнить для правоприменителя весь информационный массив, составляющий рассматриваемые категории. Поиск ответов на проблему их соотношения в теории уголовного права породил неоднозначные решения и в том числе потому, что легального понятия частной жизни нет, как и закона о неприкосновенности частной жизни и персональной информации[2]. Как верно отмечает В. Новиков, в России нет нормативного правового акта, который давал бы точное определение частной жизни и регулировал порядок обращения со сведениями, составляющими личную и семейную тайну. Отдельные нормы можно найти в разных законах и подзаконных актах, но этого недостаточно для эффективной защиты неприкосновенности частной жизни[3].

---

[1] Войниканис Е.А., Машукова Е.О., Степанов-Егиянц В.Г. Неприкосновенность частной жизни, персональные данные и ответственность за незаконные сбор и распространение сведений о частной жизни и персональных данных: проблемы совершенствования законодательства // Законодательство: право для бизнеса. 2014. № 12. С. 77.

[2] Афанасьева О.В. Право на неприкосновенность частной жизни. Укрепляет ли его закон о персональных данных? // Общественные науки и современность. 2011. № 6. С. 83.

[3] Новиков В. Понятие частной жизни и уголовно-правовая охрана ее неприкосновенности // Уголовное право. 2011. № 1. С. 43.

Предваряя исследование по вынесенной в название параграфа проблеме, оговоримся, что труды по праву содержат огромное число определений частной жизни как охраняемой информации, однако единой и универсальной формулировки не выработано. Не углубляясь в научную дискуссию, коей посвящены многие оригинальные публикации, по смыслу, придаваемому авторами, частная жизнь – это физическая и духовная область индивида, которая, *во-первых*, не связана с его публичной деятельностью, службой или работой и включает «родственные и дружеские связи, домашний уклад, интимные и другие личные отношения, привязанности, образ мыслей, увлечения и творчество»[1]. Конституционный Суд РФ интерпретировал правовую позицию с учетом строгого различия частной жизни с иными сферами жизнедеятельности человека: «В частную жизнь включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит непротивоправный характер»[2].

Во-вторых, частная жизнь сохраняется человеком в тайне от посторонних, «это область его общения, им контролируемая, свободная от внешнего вмешательства и воздействия, которым человек не придает гласность, если это не требуется законом»[3]. По воле человека, субъективно, согласно его образу жизни, представлениям о морали и нравственности, положению в обществе осуществляется формирование границ, очерчивающих содержательный компонент права на частную жизнь и т.п. Судьями Конституционного Суда РФ трижды подтверждалось, что право на неприкосновенность частной жизни (ч. 1 ст. 23 Конституции РФ) означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе,

---

[1] Петрухин И.Л. Личные тайны (Человек и власть). М.: ИГиП РАН, 1998. С. 11.

[2] Пункт 2.1 постановления Конституционного Суда РФ от 25.05.2021 № 22-П «По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона «О персональных данных» в связи с жалобой общества с ограниченной ответственностью «МедРейтинг» // Рос. газета. 2021. 8 июня.

[3] Судакова О.В. Личные неимущественные права, направленные на обеспечение неприкосновенности и тайны личной жизни граждан // Балтийский гуманитарный журнал. 2020. № 1 (30). С. 382.

препятствовать разглашению *сведений личного, интимного характера*[1]. Такая позиция соответствует и другому решению Конституционного Суда РФ, сформулированному им в определении от 28.06.2012 № 1253-О: « ... Лишь само лицо вправе определить, какие именно сведения, имеющие отношение к его частной жизни, должны оставаться в тайне, а потому и сбор, хранение, использование и распространение такой информации, не доверенной никому, не допускается без согласия данного лица, как того требует Конституция Российской Федерации»[2].

В-третьих, производным от понятия «частная жизнь» является часто употребляемое в активной лексике в качестве замены словосочетание «сведения о частной жизни». Для разрешения поставленной задачи выявить соотношение категории «персональные данные» с разными видами личной информации следует использовать общеправовое понятие – «частная жизнь». Оперирование же термином «сведения» более предпочтительно в значении предмета преступления, поскольку здесь имеется в виду не вся, а незаконно собранная и (или) распространённая виновным и охраняемая уголовным законом информация о частной жизни человека. В такой редакции словосочетание используется в диспозиции применяемой для охраны персональных данных статьи 137 «Нарушение неприкосновенности частной жизни» УК РФ, по которой ответственность наступает за незаконное собирание или распространение *сведений о частной жизни лица, составляющих его личную или семейную тайну*,

---

[1] Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом «б» части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации»: определение Конституционного Суда РФ от 09.06.2005 № 248-О; Об отказе в принятии к рассмотрению жалобы гражданина Усенко Дмитрия Николаевича на нарушение его конституционных прав положениями статьи 8 Федерального закона «Об оперативно-розыскной деятельности»: определение Конституционного Суда РФ от 26.01.2010 № 158-О-О; Об отказе в принятии к рассмотрению жалобы гражданина Богородицкого Сергея Николаевича на нарушение его конституционных прав статьей 5 Закона Российской Федерации «О милиции»: определение Конституционного Суда РФ от 27.05.2010 № 644-О-О. Доступ из Справ.-прав. системы «КонсультантПлюс».

[2] Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации: определение Конституционного Суда РФ от 28.06.2012 № 1253-О. Доступ из Справ.-прав. системы «КонсультантПлюс».

без его согласия. Пленум Верховного Суда РФ в постановлении «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138[1], 139, 144[1], 145, 145[1] Уголовного кодекса Российской Федерации)» (далее ППВС № 46) на вопрос, что в содержательном смысле считать сведениями личного или семейного характера для целей квалификации, не ответил[1]. Идеи российских ученых-правоведов сводятся к перечислению всех возможных такого рода сведений личного или семейного характера, относящихся к частной жизни гражданина[2]. Заслуживает внимания позиция тех авторов, которые относят к таковым состояние физического и психического здоровья человека и его близких; внутренний мир человека, его образ мыслей и различные формы их выражения; взаимоотношения с близкими и друзьями, в том числе интимные отношения; привычки, досуг лица и его семьи (за исключением сведений о совершенных преступлениях); имущественные отношения и источники существования; отношение к религии и вопросы вероисповедания[3]. Для чистоты юридической терминологии следует признать, что понятия «сведения о частной жизни», «информация о частной жизни», «сведения личного характера», «сведения семейного характера», а равно прочие похожие вариации словосочетаний, характеризующие саму информационную составляющую феномена частной жизни, в правовом понимании являются близкими по своему смыслу. Как уже отмечалось, сведения (сообщения и данные) согласно ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ФЗ об информации)[4] и есть информация, что говорит об отсутствии в легальной

---

[1] О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138[1], 139, 144[1], 145, 145[1] Уголовного кодекса Российской Федерации): постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 // Бюллетень Верховного Суда РФ. 2019. № 2.

[2] Елин В.М. Уголовно-правовая охрана некоторых категорий информации ограниченного доступа. М.: Академия сферы социальных отношений, 2010. С. 19.

[3] Кадников Б.Н. Уголовно-правовая охрана неприкосновенности частной жизни: научно-практическое пособие / под ред. Н.Г. Кадникова. 2-е изд., доп. М.: Юриспруденция, 2017. С. 49.

[4] Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ (с изм. и доп. от 31.07.2023, № 408-ФЗ) // Рос. газета. 2006. 29 июля; 2023. 3 авг.

дефиниции различий, а значит тождестве этих понятий. Вместе с тем они трактуются как неравнозначные понятию «частная жизнь». Их соотношение видится как форма (сфера частной жизни) и содержание (информационное наполнение), что доказывается на примере определения Л.О. Красавчиковой, выделившей множество сторон частной жизни (интимная, семейная, организационная, оздоровительная, досуг, коммуникативная)[1].

Неопределенность соотношения понятий частной жизни и персональных данных как особой категории информации не находит единообразного теоретического и правоприменительного разрешения. Эту проблему М.А. Филатова описывает так: «Как соотносятся между собой термины «частная жизнь» и «персональные данные», это по содержанию абсолютно разные понятия или что-то является общим по отношению к другому? Данный вопрос имеет принципиальное значение, так как в УК РФ уже имеется запрещенное деяние в виде нарушения неприкосновенности частной жизни (ст. 137 УК РФ)»[2]. В целях формирования единообразной судебной практики и устранения существующих пробелов в области охраны персональных данных средствами уголовного права необходимо уяснить, как трактуется наукой их взаимосвязь. Одни авторы-представители *первого* доктринального *подхода* считают, что не все персональные данные являются информацией о частной жизни человека, а потому категория «частная жизнь» является более общей по отношению к персональным данным. Так, Э.А. Цадыкова, исходя из того, что более широким, чем персональные данные понятием является информация о частной жизни, аргументирует это утверждение тем, что персональные данные – это лишь информация, позволяющая идентифицировать личность. Само по себе распространение персональных данных не столько наносит ущерб личности, сколько создает возможность для причинения ущерба; защита персональных данных подстраховывает от возможных нарушений неприкосновенности частной жизни, т. к. отдельные данные о человеке могут сложиться в обобщающую картину его

---

[1] Красавчикова Л.О. Личная жизнь граждан под охраной закона. М.: Юрид. лит., 1983. С. 15–16.
[2] Филатова М.А. Персональные данные как предмет преступного посягательства журнал // Уголовное право. 2021. № 11. С. 38.

личности[1]. По мнению Е.А. Миндровой, персональные данные являются по своему содержанию сегментом информации о частной жизни лица[2]. Д.А. Гарбатович приходит к тому же выводу, отмечая, что тайна частной жизни является общей родовой категорией, включающей профессиональные и непрофессиональные (иные) тайны; тайна персональных данных – одна из видов тайн[3]. Схожей точки зрения придерживаются и другие отечественные ученые[4].

Второй подход представляют исследователи, которые, напротив, признают персональные данные более широкой категорией информации, которую составляют среди прочего и сведения о частной жизни[5]. В основании такой интерпретации соотношения персональных данных и частной жизни лежит утверждение юристов о том, что персональные данные не являются однородными и в их структуре, помимо идентифицирующей информации, следует выделять и информацию о конкретном человеке, к которой относится и информация о частной жизни, моральных, деловых качествах и др.[6]

Сторонники *третьего подхода* считают понятия частной жизни и персональных данных не идентичными по объему, но частично совпадающими по содержанию. Судья Конституционного Суда РФ Г.А. Гаджиев эту точку зрения обосновывает следующим образом: «С точки зрения требований ч. 1 ст. 24 Конституции наиболее уязвимой является такая информация, по которой можно персонифицировать отдельную личность и которая находится вне пределов

---

[1] Цадыкова Э.А. Гарантии охраны и защиты персональных данных человека и гражданина // Конституционное и муниципальное право. 2007. № 14. С. 16.

[2] Миндрова Е.К. Коллизия права граждан на доступ к информации и права на неприкосновенность частной жизни в условиях информационного общества: автореф. дис. ... канд. юрид. наук. М., 2007. С. 8.

[3] Гарбатович Д.А. Защита персональных данных уголовным правом // Вестник УрФО. Безопасность в информационной сфере. 2012. № 2 (4). С. 12.

[4] Гришаев С.П. Право на неприкосновенность частной жизни // Гражданин и право. 2012. № 11. С. 26; Малеина М.Н. Право на тайну и неприкосновенность персональных данных // Журнал российского права. 2010. № 11. С. 22; Бачило И.Л., Сергиенко Л.А., Кристальный Б.В., Арешев А.Г. Персональные данные в структуре информационных ресурсов. Основы правового регулирования. Минск: Беллитфонд, 2006. С. 16 и др.

[5] Ветров Д.М. Защита персональных данных и защита информации на предприятии. Некоторые спорные вопросы применения // Проблемы права. 2010. № 1. С. 119.

[6] Климович Е.В. О сущности понятия «персональные данные» как конфиденциальной информации особой категории // Международные юридические чтения: матер. ежегод. междунар. науч.-практ. конф. (14 апреля 2005 г.). Омск, 2005. Ч. 2. С. 27.

постоянного контроля данного лица. Законодательство РФ выделяет информацию такого рода в отдельную категорию «персональные данные», которая хотя и пересекается с формулой «информация о частной жизни», но не вполне идентична ей»[1]. В теории эту позицию разделяет Н.И. Пикуров, отмечая, что сведения о частной жизни и персональные данные не совпадают по содержанию, хотя и в значительной своей части пересекаются по объему[2]. М.А. Филатова считает наиболее точным понимание персональных данных и неприкосновенности частной жизни самостоятельными понятиями, которые «пересекаются в определенной области, пусть и существенной, однако не совпадают по объему»[3]. В.Л. Гейхман[4], С.Ю. Головина[5] и А.М. Лушников[6] также обращают внимание на то, что понятия «персональные данные» и «частная жизнь» лица пересекаются, а элементы частной жизни могут составлять персональные данные. Правоведы приводят в пример анкетные данные, включающие имя и место жительства лица, сведения о дате и месте рождения, паспорте, об образовании, профессиональной подготовке, о предыдущей трудовой деятельности и др. в качестве персональных данных, не затрагивающих частную жизнь. Эта идея нашла развернутое разъяснение у С.Г. Пилипенко и А.С. Федосина: «Понятия «персональные данные» и «информация о частной жизни» не идентичны по объему, вместе с тем их содержание пересекается следующим образом: вся информация о частной жизни персонифицирует личность путем отображения процесса ее жизнедеятельности в сфере частной жизни, следовательно, является сегментом категории персональных данных. Однако имеется большой объем персональных

---

[1] Комментарий к Конституции Российской Федерации / под ред. В.Д. Зорькина, Л.В. Лазарева. С. 240.

[2] Пикуров Н.И. Проблемы квалификации преступных посягательств на частную жизнь: теория и судебная практика // Уголовное право. 2019. № 2. С. 53.

[3] Филатова М.А. Указ. соч. С. 38.

[4] Трудовое право: учебник для вузов / В.Л. Гейхман, И.К. Дмитриева. М.: РПА, 2002. С. 159.

[5] Трудовое право России: учебник для вузов / М.В. Молодцов, С.Ю. Головина. М.: Норма, 2003. С. 191–193.

[6] Лушников А.М. Защита персональных данных работника: сравнительно-правовой комментарий главы 14 Трудового кодекса Российской Федерации // Трудовое право. 2009. № 9. С. 95.

данных, который хотя и идентифицирует личность, но не составляет сведений о частной жизни»[1].

Обобщая приведенные научные взгляды, думается, для целей уголовного права более обоснованным является третий подход, согласно которому персональные данные – самостоятельная категория информации, содержательное наполнение которой разнится относительно сходного, но не тождественного ему понятия «частная жизнь». Для разъяснения позиции автора приведем разделяемые им суждения М.А. Важоровой, разработавшей критерии разграничения двух рассматриваемых терминов. Оперируя дефиницией персональных данных из ФЗ № 152, исследователь пишет о том, что оба понятия разнятся по содержанию. Персональные данные – это фамилия, имя, отчество, дата и место рождения, адрес, сведения о семейном, социальном, имущественном положении, об образовании, профессии, доходах, о состоянии здоровья, об интимной жизни, о взглядах и убеждениях человека и др. Сюда же она относит и идентификаторы (номер пенсионного свидетельства, идентификационный номер налогоплательщика). Информацию же о частной жизни составляют сведения об определенном человеке, о тех сторонах его жизнедеятельности, которые не связаны с его профессиональной и общественной деятельностью (сведения о родственных, дружеских и иных связях, пристрастиях, пороках, о социальном и финансовом положении, о взглядах и убеждениях, образе жизни, отдельных фактах биографии и т.п.)[2]. И действительно, многие персональные данные не идентичны информации о частной жизни, они не включаются одно в другое, а являются понятиями, содержание которых пересекается только в отдельных случаях. По нашему мнению, косвенно разграничивать частную жизнь и персональные данные, хотя бы и имеющих определенную схожесть и взаимные пересечения, но являющихся разными, позволяет и текст Федерального закона от 27.07.2006 № 149-ФЗ (с изм. и доп. от 31.07.2023, № 408-ФЗ) «Об информации,

---

[1] Федосин А.С. Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации: автореф. дис. ... канд. юрид. наук. Саранск, 2009. С. 14.

[2] Важорова М.А. Соотношение понятий «Информация о частной жизни» и «Персональные данные» // Вестник Саратовской государственной юридической академии. 2012. № 4 (87). С. 57.

информационных технологиях и о защите информации». В нем говорится о том, что никто не вправе требовать от гражданина (физического лица) против его воли информацию о частной жизни, в том числе составляющую личную или семейную тайну (п. 8). Отдельным пунктом оговаривается, что порядок доступа к персональным данным устанавливается федеральным законом (п. 9)[1]. В этом смысле мы солидарны с теми юристами, которые верно указывают на специфику персональных данных, «проявляемую в том, что каждое из них, взятое по отдельности, может не иметь отношения к частной жизни, но их совокупность становится социально-экономической характеристикой субъекта»[2]. Истолкование персональных данных всего лишь как элемента права на неприкосновенность частной жизни означало бы, что охране средствами уголовного права подлежат только такие из них, которые содержат исключительно сведения о частной жизни, а иные, таких сведений не содержащие, однако включающие личную информацию, оказываются ее лишёнными.

Вторым дифференцирующим информацию о частной жизни от персональных данных признаком, по мнению М.А. Важоровой, является возможность идентификации физического лица, в то время как не всегда сведения о частной жизни позволяют хоть как-то лицо определить[3].

Сформулировали содержательные отличия двух категорий информации не только теоретики, но и правоприменитель. По мнению судей Конституционного Суда РФ, как показывает его практика, «личные данные (имя, адрес места жительства, почтовый адрес, контактный телефон) лица, заявляющего о правонарушении …, личные данные свидетеля, которые фиксируются в процессуальных документах, не относятся к сведениям о частной жизни таких лиц»[4]. Доказательством тому служит и судебная практика. По свидетельству

---

[1] Рос. газета. 2006. 29 июля; 2023. 3 авг.

[2] Михайлова И.А. Персональные данные и их правовая охрана: некоторые проблемы теории и практики // Законы России: опыт, анализ, практика: правовой журнал. 2017. № 10. С. 13.

[3] Важорова М.А. Указ. соч. С. 57.

[4] Об отказе в принятии к рассмотрению жалобы гражданина Кудрякова Антона Васильевича на нарушение его конституционных прав положением части 1 статьи 25.1 Кодекса Российской Федерации об административных правонарушениях: определение Конституционного Суда РФ от 23.04.2015 № 1075-О; Об отказе в принятии к рассмотрению жалобы гражданина Кудрякова

В.Б. Наумова и В.В. Архипова, российские суды признавали персональными следующие данные: фамилии, имена и отчества, размер задолженности по оплате коммунальных платежей; дату и место рождения, адрес места регистрации и фактического проживания, номера рабочего и мобильного телефонов и номер паспорта, а также дату его выдачи и наименование органа, выдавшего паспорт, сведения о работе, супруге и детях, датах их рождения, указанные в заявлении-анкете на получение потребительского кредита; копии материалов пенсионного дела; данные, содержащиеся в техническом паспорте на дом; сведения о пересечении Государственной границы России; данные трудового договора[1]. М.А. Филатова, изучив отечественное правоприменение, со ссылкой на источники, также обобщила информацию, оцениваемую как персональные данные: год и место рождения, сведения о профессии, о заработной плате, абонентский номер и адрес электронной почты физического лица, семейное, социальное, имущественное положение, образование, профессию, доходы, фото- и видеоизображения человека, площадь помещения, сумму начисления и (или) задолженности, номер и показания электрического счетчика[2]. Очевидно, что далеко не все из них можно отнести к сведениям о частной жизни человека, составляющих личную или семейную тайну, тайну корреспонденции, следуя смыслу диспозиций ст. 137, 138 УК РФ.

Нетождественность понятий «персональные данные» и «частная жизнь» подтверждается и КоАП РФ. В ст. 13.11. «Нарушение законодательства Российской Федерации в области персональных данных» КоАП РФ ни о каком праве на неприкосновенность частной жизни, личную или семейную тайну не упоминается, а названы запрещенные действия в отношении персональных данных. И в этом смысле следует поддержать правоведов, исходящих из

Антона Васильевича на нарушение его конституционных прав положением части 1 статьи 25.1 Кодекса Российской Федерации об административных правонарушениях: определение Конституционного Суда РФ от 16.07.2013 № 1217-О. Доступ из Справ.-прав. системы «КонсультантПлюс».

[1] Наумов В.Б., Архипов В.В. Понятие персональных данных: интерпретация в условиях развития информационно-телекоммуникационных технологий // Российский юридический журнал. 2016. № 2. С. 189.

[2] Филатова М.А. Указ. соч. С. 38.

автономного характера притязания на защиту персональных данных, т.е. как самостоятельного конституционного права гражданина, наполненного собственным содержанием, отдельно от более общего права на неприкосновенность частной жизни (право на защиту персональных данных приобрело во многом самостоятельное значение[1]). Думается, что дальнейшая эволюция конституционного права на неприкосновенность частной жизни, обусловленная в том числе и стремительным развитием информационно-коммуникационных технологий, аккумулирующих и обрабатывающих огромные объёмы информации о людях, приведет к многократному возрастанию значимости защиты персональных данных и их конечной автономии как института. Это положение доказывается на страницах диссертаций российскими учеными. К примеру, А.В. Кучеренко, обосновывая самостоятельность института персональных данных в рамках информационного права, указывает на его специфику, отраженную в предмете – информации ограниченного доступа, призванной идентифицировать физических лиц (персональными данными)[2]. «Понятия «частная жизнь» и «персональные данные» частично пересекаются, однако не всегда совпадают. … Важнее то, что исследуемые категории представляют собой два различных (хотя и смежных) правовых института. Следовательно, правовое регулирование этих двух институтов будет различным»[3].

Новые международные акты в области защиты прав человека, принимаемые в условиях стремительного развития информационных технологий, когда многие положения международных и наднациональных правовых актов устарели, уже формируют этот подход. Так, Хартия Европейского Союза об основных правах закрепила право человека на защиту относящихся к нему данных личного характера, подчеркнув в тексте его самостоятельный и независимый от иных

---

[1] Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». М.: Статут, 2017. С. 18–20.

[2] Кучеренко А.В. Правовое регулирование персональных данных в Российской Федерации: автореф. дис. ... канд. юрид. наук. Челябинск, 2010. С. 8.

[3] Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. М.: Статут, 2011. С. 39.

естественных прав характер. Разработчики Хартии обособили в разных статьях право на частную и семейную жизнь (ст. 7) и право на защиту данных личного характера (ст. 8)[1]. Перспектива модернизации права на защиту персональных данных в новое право, поименованное как право на неприкосновенность персональных данных, вполне вероятна, если вспомнить, что признаваемые суверенными право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ч. 2 ст. 23 Конституции РФ) и право на неприкосновенность жилища (ст. 25 Конституции РФ) исторически формировались как права, охраняющие частную жизнь человека. Отсюда для решения проблем охраны персональных данных, обозначенных научно-юридической мыслью и следственно-судебной практикой, представляется перспективной разработка уголовно-правового механизма обеспечения конституционных гарантий их неприкосновенности, учитывая широкую распространенность и общественную опасность незаконных действий с персональными данными.

Категория «персональные данные» в юридической литературе рассматривается и в контексте личной или семейной тайны, ибо персональные данные охватываются понятием информации (сведений). Переходя к анализу соотношения персональных данных и личной и семейной тайн, отметим множественность в юридической литературе их определений[2]. Согласно изученным научным источникам, граница между ними проводится через принадлежность тайны одному или нескольким лицам: если личная тайна непосредственно касается интересов лишь конкретного индивидуума, то семейная тайна затрагивает интересы нескольких лиц, находящихся друг с другом в семейных отношениях[3]. Характеристику иных различий этих видов тайны

---

[1] Хартия Европейского Союза об основных правах: принята в г. Страсбурге 12.12.2007 // Журнал № С 202, 7.6.2016. С. 389.

[2] Комментарий к Конституции Российской Федерации / под ред. В.Д. Зорькина, Л.В. Лазарева; Конституционный Суд Российской Федерации. М.: Эксмо, 2009. С. 157.

[3] Елисеева А.А. Семейная тайна: вопросы содержания и правовой охраны // Актуальные проблемы российского права. 2018. № 4 (89). С. 71–76; Мартышин М.Ю. Государственная тайна как объект конституционно-правового регулирования: дис. … канд. юрид. наук. М., 2009. С. 62.

аргументированно формулирует Н.И. Пикуров: «Семейная тайна отличается от личной по кругу ее носителей и по характеру сведений, которые составляют ее содержание. Семейная тайна в основном касается всех членов семьи, их взаимоотношений между собой, образа жизни, бытовых условий и т.п. Личная тайна имеет отношение к конкретному человеку. Сведения личного характера могут храниться в тайне от других членов семьи»[1]. С.Ю. Пашаев к этому добавляет, что такие тайны обеспечиваются защитой самого индивида либо государством: «Личная тайна – это неизвестная третьим лицам охраняемая человеком информация о себе, а также об отношениях с другими людьми, правомерный доступ к которой закрыт. Семейная тайна – это неизвестная третьим лицам охраняемая людьми, связанными правами и обязанностями, вытекающими из братства, родства, усыновления или иной формы принятия детей на воспитание, информация о взаимоотношениях внутри семьи, об их общих взглядах и интересах, правомерный доступ к которой закрыт»[2]. Существенный недостаток данного подхода видится в том, что обе категории тайн при определенных обстоятельствах совпадают либо могут быть обособленными друг от друга: в одной и той же семье у каждого ее члена может быть и семейная, и личная тайна, которая охраняется им[3]. Здесь следует поддержать позицию тех авторов, которые приходят к выводу об их условной границе, полагая, что личная и семейная тайна являются близкими, родственными, однако различными понятиями[4], что не позволяет найти четкий критерий разграничения сравниваемых понятий.

Чтобы отграничить персональные данные и личную или семейную тайну, следует установить, что является тайной вообще, и как она коррелирует с другой

---

[1] Уголовный закон в практике мирового судьи: научно-практическое пособие / под ред. А.В. Галаховой. 2-е изд., доп. М.: Норма, 2007. С. 143.

[2] Пашаев С.Ю. Конституционно-правовое регулирование личной и семейной тайны в Российской Федерации: автореф. дис. ... канд. юрид. наук. М., 2010. С. 11.

[3] Телина Ю.С. Конституционное право гражданина на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных в России и зарубежных странах: дис. ... канд. юрид. наук. М., 2016. С. 45.

[4] Пашаев С.Ю. Проблемы обеспечения права на личную и семейную тайну в Российской Федерации: теоретико-правовой аспект // Современное право. 2010. № 10. С. 21.

схожей категорией – «конфиденциальная информация». Это соотношение не имеет общепризнанной точки зрения до настоящего времени. Одни правоведы, ссылаясь на толковые словари русского языка[1], полагают, что такие понятия, как «конфиденциальная информация», «тайна», «секрет», «конфиденциальный», «секретный», «тайный», «доверительный», «не подлежащий огласке», являются синонимами[2], а значит равнозначными и взаимозаменяемыми. Другие авторы, напротив, считают, что тайна выступает разновидностью конфиденциальной информации, то есть она уже, несмотря на свою обеспеченность властной силой государства[3]. Собирательное определение тайны можно сформулировать как «представленную в нематериальной форме или на физических носителях и имеющую потенциальную духовно-нравственную, этическую, коммерческую либо иную общественно значимую ценность информацию (сведения), известную или доверенную узкому кругу субъектов в силу исполнения ими служебных, профессиональных либо иных обязанностей, доступ к которой ограничен действующим федеральным законодательством, в связи с чем собственник либо иной законный владелец информации принимает необходимые меры к охране ее конфиденциальности, и разглашение которой влечет за собой юридическую ответственность»[4]. Исходя из анализа доктринальных взглядов, думается, что и тайна, и конфиденциальная информация, а также прочие производные от них, являются разновидностью информации с ограниченным доступом, а потому оба понятия означают практически одно и то же – характеристику (свойство, признак)

---

[1] См., напр.: Ожегов С.И. Словарь русского языка: 70000 слов / под ред. Н.Ю. Шведовой. М.: Рус. яз., 1991. С. 293.

[2] Алексеенцев А.И. О составе защищаемой информации // Безопасность информационных технологий. 1999. № 2. С. 5–7; Ефремов А.А. Понятие и виды конфиденциальной информации // Russianlaw. URL: http://www.russianlaw.net/law/doc/a90.htm (дата обращения: 12.10.2023); Ткачук И.Б. Коммерческая тайна: организация защиты, расследование посягательств. М., 1999; Жигалов А.Ф. Коммерческая и банковская тайна в коммерческом и уголовном законодательстве: дис. … канд. юрид. наук. Н. Новгород, 2000.

[3] Паршин С.М. Тайна в уголовном законодательстве (теоретико-прикладное исследование): дис. ... канд. юрид. наук. Н. Новгород, 2006. С. 27; Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. ... докт. юрид. наук. М., 2017. С. 45.

[4] Бондарь И.В. Тайна по российскому законодательству (проблемы теории и практики): дис. … канд. юрид. наук. Н. Новгород, 2004. С. 74; Жигалов А.Ф. Коммерческая и банковская тайна в коммерческом и уголовном законодательстве: дис. … канд. юрид. наук. Н. Новгород, 2000. С. 13.

информации как закрытых для свободного доступа и распространения сведений. Так, по указу Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» к информации, которая является конфиденциальной, относятся, кроме персональных данных, различные виды тайн (служебная, тайна следствия и судопроизводства, врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений, коммерческая), в отношении которых должна обеспечиваться их конфиденциальность[1].

По-другому обстоит дело с взаимосвязью тайны и конфиденциальности, ведь, как уже отмечалось, «конфиденциальная» информация и «конфиденциальность» информации – разнопорядковые категории. Во многих научных публикациях прослеживается мысль о том, что сохранность конфиденциальной информации обеспечивается режимом тайны (государственная, служебная, коммерческая, налоговая и др.). Иначе говоря, тайна – это обладающие определенной ценностью сведения, которые неизвестны другим лицам и находятся в ограниченном доступе в связи с установлением специального правового режима. Формулируя понятие тайны для уголовного права, А. Кибальник и И. Соломоненко пишут, что под ней следует понимать сведения (информацию), доступ к которой ограничен в соответствии с положениями федерального законодательства, и за несанкционированное нарушение конфиденциальности которых установлена уголовная ответственность[2]. Добавим к этому, что персональные данные – уникальные по своей природе разновидности личной информации (сведений) о человеке, а всякое их собирание или распространение, за исключением, указанным в законе, допускается с согласия субъекта, а потому конфиденциальность и тайна – режимы или формы ограничения доступа к ним. Режимный характер тайны подтверждает и А.А. Ефремов, отмечая, что «тайна является не только конфиденциальной

---

[1] Об утверждении Перечня сведений конфиденциального характера: указ Президента РФ от 06.03.1997 № 188 (с изм. и доп. от 13.07.2015, № 357) // Рос. газета. 1997. 14 мар.; СЗ РФ. 2015. № 29 (ч. II), ст. 4473.

[2] Кибальник А., Соломоненко И. Понятие и виды тайны в уголовном праве // Российская юстиция. 2001. № 2. С. 53.

информацией, но и правовым режимом информации»[1]. Иными словами, тайна – это не только «сведения личного характера», «сведения семейного характера», а еще правовой режим, содержащий ограничения и запреты в отношении их собирания, использования или распространения.

Проведенный анализ теоретических работ на тему взаимосвязи персональных данных и тайны (личная или семейная) и судебной практики убеждает, что речь идет о некорректном отождествлении двух понятий. Первое из них определяет огромный массив индивидуальных сведений, и в том числе о личной и (или) семейной жизни человека, запечатленных на материальных носителях, в устной или идеальной форме. Второе обозначает исключительно ту конкретную информацию о личной и семейной жизни индивида, которая обретает режим тайны по его усмотрению[2]. Как пишет С.Ю. Пашаев, «какая конкретно информация является личной или семейной тайной – это вопрос, решаемый лицом, которого она касается, то есть с субъективной стороны тайна – это те сведения о личной жизни, которые не подлежат оглашению по мнению лица, интересы которого они затрагивают»[3]. Оговоримся, что в отличие от сведений личного или семейного характера, охраняемых ст. 137 УК РФ, персональные данные в «чистом виде» больше являются фактической характеристикой индивидуума, отражающей физическую, социально-демографическую составляющую информации о личности, или «анкетные» данные. Суть персональных данных состоит в том, что личной или семейной тайной они могут и не быть по объективным причинам, однако по воле их носителя могут ограничиваться для свободного распространения и использования. К примеру, сведения о месте учебы, работы или жительства могут характеризовать персональные данные человека, однако не могут быть личной или семейной

---

[1] Ефремов А.А. Понятие и виды конфиденциальной информации // Russianlaw. URL: http://www.russianlaw.net/law/confidential_data/a90/ (дата обращения: 25.12.2022).

[2] Хохлова Е.В. Частная жизнь, личная и семейная тайна в уголовном праве: проблемы соотношения понятий // Роль юридических и социальных наук в развитии современного общества: сб. науч. ст. науч.-практ. конф. (30–31 марта 2023 г.) / ред. кол.: Е.Ю. Антонова (отв. ред.) [и др.]. Владивосток: Изд-во Дальневост. федерал. ун-та, 2023. С. 252.

[3] Пашаев С.Ю. Проблемы обеспечения права на личную и семейную тайну в Российской Федерации: теоретико-правовой аспект. С. 23.

тайной, но могут быть конфиденциальными. В режиме конфиденциальности человек самостоятельно определяет круг людей (или юридических лиц) и условия, которым и при которых он открывает доступ к информации о себе[1]. Иначе говоря, сокрыть все персональные данные в социуме нельзя, однако в конкретном общественном отношении и для кого-то в силу конфиденциальности «становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных» (п. 9 ст. 3 ФЗ № 152).

Не случайно в зарубежных источниках в отношении термина «конфиденциальность» применяется более точный подход. Выделяются две ее формы: тайны (секреты) (secrecy) и иные формы ограничения доступа к конкретным видам информации (privacy)[2]. Тайность (секретность) (secrecy) информации – это форма сокрытия тех или иных сведений, которая носит принудительный характер, предусматривая санкции за их разглашение (государственные, профессиональные, служебные, коммерческие, личные, семейные и др.). Приватность (privacy) – это форма ограничения доступа к личным сведениям человека, когда любое их использование допускается только с его согласия. Режим приватности распространяется на персональную информацию, тайной (секретом) не являющейся, но использование которой другими лицами допустимо при соблюдении определенных правил[3]. В ст. 2 Закона об информации именно как privacy понимается конфиденциальность информации, или «обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя». В случае персональных данных по ст.

---

[1] Рожкова М.А. Персональные данные: можно ли относить их к имуществу? (взгляд цивилиста) // Закон.ру. URL: https://zakon.ru/blog/2019/02/28/personalnye_dannye_mozhno_li_otnosit_ih_k_imuschestvu_vzglyad_civilista (дата обращения: 25.12.2022).

[2] Shils Edward A. The Torment of Secrecy: the Background and Consequences of American Security Policies. Chicago: Ivan R. Dee. 1956, reissued 1996. P. 112.

[3] Рожкова М.А. Являются ли персональные данные действительно конфиденциальными, или как соотносятся категории «персональные данные» и «тайны» (взгляд цивилиста) // Закон.ру. URL: https://zakon.ru/blog/2019/3/18/yavlyayutsya_personalnye_dannye_dejstvitelno_konfidencia1 (дата обращения: 25.12.2022).

7 ФЗ № 152 privacy означает запрет или ограничение на использование и распространение личных сведений граждан без их согласия операторами и другими лицами, получившими доступ к этим сведениям[1], или, как пишет Н.И. Петрыкина, правовой режим использования личной информации индивида для осуществления предоставленных ему законом прав и исполнения возложенных на него законом обязанностей[2]. Применительно же к охранительному уголовному праву речь идет о персональных данных, ставших известными или доступными другим лицам, в том числе в силу личных отношений, служебной или иной профессиональной деятельности, на которых в соответствии со специальным правовым режимом персональных данных (личной, семейной, банковской, налоговой, врачебной тайны, тайны усыновления, предварительного следствия и др.) возлагается императивная обязанность (или устанавливается требование) их нераспространения и неиспользования. Как пишет И.В. Винюкова, «люди доверяют свои личные тайны представителям определённых профессий, необходимым атрибутом которых выступает сохранность тайн, в числе которых адвокаты, депутаты, врачи, психологи, нотариусы, налоговые инспекторы, журналисты, органы опеки и попечительства, банковские работники и священнослужители. Соответственно, законодатель несёт публично-правовую обязанность регламентации и формализации деятельности этих субъектов правоотношений в целях реализации конституционного права граждан на неприкосновенность частной жизни»[3]. Обозначенный вывод вполне укладывается в концепцию Б.Н. Кадникова, предлагающего понимать частную жизнь в широком и узком смыслах этого слова. В первом случае речь должна идти о сведениях личного или семейного характера, во втором – о специальных тайнах и персональных данных человека. По его мнению, эта классификация и

---

[1] Рожкова М.А. Указ. соч.

[2] Петрыкина Н.И. К вопросу о конфиденциальности персональных данных // Законы России: опыт, анализ, практика. 2007. № 6. С. 119.

[3] Винюкова И.В., Кузахметова С.Е. Неприкосновенность частной жизни как принцип правового регулирования отношений в сфере защиты информации // Правовая культура. 2007. № 1 (2). С. 148–154.

есть основа для построения системы уголовно-правовых норм, охраняющих в том числе и персональные данные[1].

Таким образом, подводя итог терминологическому осмыслению соотношения понятия «персональные данные» с иными, близкими по уголовно-правовому смыслу категориями, сформулируем наиболее значимые *выводы* проведенного исследования:

1. Понятия «частная жизнь» и «персональные данные» взаимопересекаются, исключают полное содержательное совпадение, а потому не могут толковаться как тождественные и даже синонимичные. Эти феномены представляют собой ряд близких, обусловленных объективной неразрывной связью понятий, но имеющих не только неодинаковое сущностное, но и правовое значение. Различаются они и режимами правовой охраны: в случае с персональными данными их конфиденциальность предполагает иную форму ограничения доступа к ним, отличающуюся от режима личной или семейной тайны применительно к частной жизни (обеспечение их неприкосновенности третьими лицами, согласие обладателя на их распространение), что должно учитываться при конкретизации объекта уголовно-правовой охраны и предмета преступлений, связанных с персональными данными.

2. Понятия «сведения личного или семейного характера» и «персональные данные», являясь информацией о человеке, *во-первых*, разнятся между собой содержательно. По своему уголовно-правовому смыслу персональные данные отличаются тем, что они необязательно характеризуют те или иные сведения личного или семейного характера как области частной жизни. *Во-вторых*, сведения о личной или семейной жизни, которые должны оставаться сокрытыми, определяет само лицо и сохраняет их по своей воле, субъективно в режиме тайны от других лиц. Персональные данные в силу своей специфичности могут быть открытыми ввиду объективной невозможности обеспечить их тайность (номинативные персональные данные) либо доверяются третьим лицам, однако

[1] Кадников Б.Н. Уголовно-правовая охрана неприкосновенности частной жизни: научно-практическое пособие / под ред. Н.Г. Кадникова. 2-е изд., доп. М.: Юриспруденция, 2017. С. 49.

при наличии тех или иных обстоятельств субъект персональных данных может установить запрет на их собирание или распространение без его согласия. В отличие от личной или семейной тайны на персональные данные распространяется иной правовой режим – режим конфиденциальности. Это принципиальное различие в режимах должно учитываться в качестве основания для проектирования самостоятельного состава преступления, осуществляющего специальную защиту персональных данных, которая в настоящее время осуществляется средствами, несоответствующими современному состоянию преступности с персональными данными.

3. В целях совершенствования механизма уголовно-правовой охраны неприкосновенности персональных данных и учитывая положения международного права и зарубежный опыт в этой сфере, требуется специальная их защита путем установления уголовной ответственности за общественно опасные деяния в отношении персональных данных или с их использованием как особого (непоименованного) предмета преступления с определением круга общественно опасных деяний и местоположения новой нормы.

§ 3. Общедоступность персональных данных и ее значение для уголовно-правовой оценки содеянного

Российская научная дискуссия представлена разными вариантами юридической оценки открытого доступа к персональным данным. В практических комментариях и учебниках и в теории уголовного права научные споры вызывают подходы к установлению вины: они касаются неопределенности в понимании того, когда тайна персональных данных может быть нарушена правомерно. Верховный Суд РФ через разделительный союз «либо» в п. 2 ППВС № 46 назвал три условия уголовной ненаказуемости сбора или распространения сведений о частной жизни гражданина: если они, сведения, «*ранее стали общедоступными* либо *были преданы огласке самим гражданином или по его воле*», либо собирались или распространялись в государственных, общественных или иных

публичных интересах[1]. Следуя этому разъяснению, теоретики ставят вопрос о том, при каких условиях общедоступны персональные данные, и когда нарушена сохранность тайны самим их обладателем или по его воле. Следственно-судебная практика и экспертный опрос (*33,6 % респондентов)* подтверждают, что разночтения в квалификации противоправных деяний с персональными данными обусловлены приданием правоприменителем разного, взаимоисключающего смысла термину «общедоступность». *Во-первых*, проблема тому – неясность в понимании соотношения понятий конфиденциальности и общедоступности персональных данных, размещенных в различных информационных системах, в том числе социальных сетях, иных ресурсах в сети Интернет, что требует специального рассмотрения второй категории более подробно. По сути, названные в п. 2 ППВС № 46 обстоятельства, исключающие уголовную ответственность за сбор или распространение сведений о частной жизни гражданина, можно толковать как санкционированное нарушение конфиденциальности, то есть формы ограничения доступа к персональным данным. А оно допускается только в соответствии со специальным законом или с согласия их субъекта.

Во-вторых, вопрос об общедоступности персональных данных важен и в связи с предложениями о придании идентифицирующим данным о физических лицах статуса общедоступных сведений с выделением такой категории персональных данных. Речь идет о ЕГН – едином государственном регистре населения, включающем идентификаторы персональных данных всех физических лиц, постоянно или временно проживающих в РФ (уникальные номера, присваиваемые физическим лицам, как это сделано во многих зарубежных странах), однако от этой идеи в ФЗ № 152 отказались на время (ввиду необходимости точной юридической проработки). В качестве пригодных для идентификации рассматриваются паспортные и другие данные о человеке,

[1] О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138[1], 139, 144[1], 145, 145[1] Уголовного кодекса Российской Федерации)»: постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 // Бюллетень Верховного Суда РФ. 2019. № 2.

позволяющие его отождествить, которые имеются у государственных структур, однако другим субъектам доступ к системе данных о гражданах закрыт. Недостаток информации о физических лицах, позволяющей их идентифицировать, порождает спрос, в том числе криминальный, на персональные данные, чем объясняется существование «серых» баз в организациях и учреждениях для обеспечения безопасности своей деятельности. Осложняет проблему и то, что сам человек множество раз сообщает свои персональные данные, в том числе анкетные данные, ИНН, биометрию[1], сведения, удостоверяющие личность, юридическим лицам и другим гражданам для получения каких-либо государственных и иных услуг, покупок и др.

О том, что судебная практика разнородна в подходе к термину «общедоступность», покажем на примере статьи 152.1 ГК РФ об охране от неправомерного использования изображения человека, выступающего основным идентификатором (Правительство РФ в постановлении от 30.06.2018 № 772 определило в качестве вида биометрических персональных данных физического лица изображение лица человека, полученное с помощью фото-, видеоустройств[2]. Роскомнадзор дважды разъяснял, что изображение человека (фотография и видеозапись), позволяющее установить его личность, относится к персональным данным человека[3]). Содержание юридического понятия «общедоступность» не

---

[1] К слову, в теории предлагается создание национальной системы биометрической идентификации личности, в том числе предусматривающей идентификации по биометрии для оказания банковских, образовательных и иных услуг. См.: Дивольд В.Е. Предпосылки создания национальной системы биометрической идентификации личности // Научный вестник Омской академии МВД России. 2021. Т. 27. № 2 (81). С. 140.

[2] Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации»: постановление Правительства РФ от 30.06.2018 № 772 // СЗ РФ. 2018. № 28, ст. 4234.

[3] О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки»: разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30.08.2013: разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки // Доступ из Справ.-прав. системы

разъяснялось судьями в ППВС № 46, сославшимися на принятое ранее постановление от 23.06.2015 № 25 «О применении судами некоторых положений раздела I части первой Гражданского кодекса Российской Федерации». В нем Верховный Суд РФ отметил: «Обнародование изображения гражданина, в том числе размещение его самим гражданином в сети «Интернет», и *общедоступность такого изображения сами по себе не дают иным лицам права на свободное использование такого изображения без получения согласия изображенного лица»*. И в этом же пункте высшая судебная инстанция сделала противоречивую оговорку: «Обстоятельства размещения гражданином своего изображения в сети «Интернет» могут свидетельствовать о выражении таким лицом согласия на дальнейшее использование данного изображения, например, если это предусмотрено условиями пользования сайтом, на котором гражданином размещено такое изображение»[1].

Такое разночтение не могло не повлиять на единообразие судебной практики при размещении гражданином своего изображения и других персональных данных в социальных сетях и на веб-сайтах: если пользователь согласился с политикой распространения информации на интернет-платформе (сайте, социальной сети), суды признают персональные данные, им размещенные, общедоступными, руководствуясь в том числе п. 4 ст. 7 Федерального закона «Об информации, информационных технологиях и о защите информации»[2]. Он гласит: «Информация, размещаемая ее обладателями в сети «Интернет» в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является *общедоступной информацией*, размещаемой в форме открытых данных».

Так, Савеловский районный суд г. Москвы, отказывая в иске о защите права на изображение, в решении от 16.12.2011 по делу № 11-2538 привел следующий

«Гарант»; Роскомнадзор пояснил, относится ли фотография гражданина к биометрическим персональным данным // Доступ из Справ.-прав. системы «Гарант».

[1] Рос. газета. 2015. 30 июня.

[2] Хохлова Е.В. К вопросу о защите изображения человека как персональных данных (на основе судебной практики по ст. 137 УК РФ) // Вестник Воронежского института МВД России. 2023. № 3. С. 300–304.

довод: ответчик получил фотографию заявителя «из социальной сети на сайте «…», где она была размещена самим истцом наравне с другими своими изображениями для обозрения неопределенным кругом лиц, имеющим доступ к данному сайту». Подтвердив позицию нижестоящего суда, Судебная коллегия по гражданским делам Московского городского суда в Апелляционном определении от 30.03.2012 указала: «Данные истца, такие как фамилия, имя, возраст, а также его фотография, которые были опубликованы в журнале, были размещены на личной странице С.С.В. в социальной сети «…», открытой для доступа неограниченному кругу лиц и не защищенной никакими настойками приватности. …Разместив спорную фотографию на сайте в открытом для неопределенного круга лиц доступе, истец фактически своими действиями выразил добровольное волеизъявление на обнародование своего изображения, его обсуждение, дачу пользователями сайта своих оценок фотографиям истца»[1].

Вторым вариантом решения судов, противоположным первому, является непризнание персональных данных общедоступными в отсутствие у социальных сетей какого-либо подтвержденного согласия на обнародование личных данных. В мотивировочной части суды дополнительно приводят ссылку на п. 4 ст. 8 ФЗ об информации: информация относится к общедоступной, если она прямо упомянута как источники, доступ к которым не может быть ограничен. Среди них: нормативные правовые акты, затрагивающие права, свободы и обязанности граждан; информация о состоянии окружающей среды; информация о деятельности государственных органов, об использовании бюджетных средств, а также информация, накапливаемая в открытых фондах библиотек, музеев и архивов. Аналогичная мотивировка судами используется и применительно к ст. 8 «Общедоступные источники персональных данных» ФЗ № 152 (справочники, адресные книги).

К примеру, АО «НБКИ» обратилось в суд с заявлением о признании недействительными пунктов 1 и 4 предписания Управления Роскомнадзора по

[1] Апелляционное определение Судебной коллегии по гражданским делам Московского городского суда от 30.03.2012 по делу № 11-2538. Доступ из Справ.-прав. системы «Гарант».

ЦФО № П-77/07/524-нд/1/230 от 26.08.2016, которыми, в частности, указывалось на нарушение требований п. 1 ч. 1 ст. 6 и ч. 3 ст. 22 ФЗ № 152 в виде отсутствия согласия на обработку содержащихся в социальных сетях и интернет-порталах персональных данных заемщика либо потенциального клиента финансовой организации. Для оценки потенциальных и действующих клиентов АО «НБКИ» использовались IT-программы, позволяющие найти и собрать множество дополнительных скоринговых факторов из социальных сетей и других открытых интернет-источников для 60 % заемщиков и их окружения, и в том числе аккаунты заемщика в соцсетях, электронную почту, номера мобильных телефонов, личные фотографии, семейное положение, место работы и должность, образование и др. Решение Арбитражного суда г. Москвы от 05.05.2017 по делу № А40-5250/17-144-51 было основано на выводе, что «…персональные данные, сделанные общедоступными субъектом персональных данных, могут содержаться только в общедоступных источниках персональных данных. Для этих целей статьей 8 Закона введено определение общедоступных источников персональных данных. … Информация о субъекте (в том числе персональные данные), содержащаяся в социальных сетях (в сети Интернет), не может быть отнесена к персональным данным, сделанным субъектом общедоступными, поскольку социальные сети не являются источником общедоступных персональных данных применительно к положению ст. 8 Закона»[1]. Суд подчеркнул, что без письменного согласия обладателя страницы в социальных сетях с персональных данными нельзя утверждать, что имеется согласие владельца персональных данных, и сведения предоставлены именно им.

Девятый Арбитражный апелляционный суд, оставив в силе решение Арбитражного суда г. Москвы, отметил: «Применительно к положениям ч. 1 ст. 8, п. 4 ч. 2 ст. 22 Закона о персональных данных не являются общедоступными обрабатываемые обществом персональные данные, содержащиеся в открытых источниках (социальных сетях: ВКонтакте, Одноклассники, МойМир, Instragram,

[1] Решение Арбитражного суда г. Москвы от 05.05.2017 по делу № А40-5250/17-144-51 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/arbitral/doc/YLVZ7F3cAwU0/ (дата обращения: 15.12.2022).

Twitter; интернет-порталов Авито и Авто.ру). По смыслу Закона о персональных данных размещение персональных данных в указанных открытых источниках не делает их автоматически общедоступными. Следовательно, не допускается обработка таких данных без согласия субъекта»[1]. Постановлением Арбитражного суда Московского округа от 09.11.2017 № Ф05-16382/17 это постановление было оставлено без изменения[2]. Не нашел оснований для отмены обжалуемых судебных актов и Верховный Суд РФ[3].

В качестве еще одного примера служит решение Арзамасского городского суда Нижегородской области от 14.06.2016 по делу № 2-2307/2016 по иску К. к АО «ФОРУС Банк» об уничтожении персональных данных и взыскании компенсации морального вреда. Суд не принял доводы ответчика о том, что согласие пользователя на обработку общедоступных персональных данных в любых не противоречащих закону целях не требуется, поскольку информация с телефонным номером размещена самим истцом в сети Интернет на общедоступных сайтах. В мотивировочной части он сослался на то, что «телефонный номер истца был размещен в сети Интернет в целях оказания юридических услуг, в то время как ответчик воспользовался персональными данными истца *с другой целью*, а именно с целью доведения до Г. через К. информации в связи с задолженностью по кредиту»[4]. На этом основании суд признал действия банка по собиранию и обработке персональных данных истца незаконными, поскольку он согласия на них не давал. Апелляционным определением от 11.10.2016 Нижегородский

---

[1] Постановление Девятого арбитражного апелляционного суда от 27.07.2017 № 09АП-31744/2017 по делу № А40-5250 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/arbitral/doc/ADkm2q8j8irQ/ (дата обращения: 04.11.2022).

[2] Постановление Арбитражного суда Московского округа от 09.11.2017 № Ф05-16382/17 по делу № А40-5250 // Гарант. URL: https://base.garant.ru/41915854/ (дата обращения: 04.11.2022).

[3] Определение Верховного Суда РФ от 29.01.2018 № 305-КГ17-21291 по делу № А40-5250/2017 // Гарант. URL: https://www.garant.ru/files/0/1/1294310/opredelenie_vs_rf_ot_29_yanvarya_2018_goda_po_delu_305_kg17_21291.pdf. (дата обращения: 04.02.2023).

[4] Решение Арзамасского городского суда Нижегородской области от 14.06.2016 по делу № 2-2307/2016 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/YTC0pcVgf4o8/ (дата обращения: 04.02.2023).

областной суд отказал в удовлетворении жалобы ответчика на тех же основаниях[1].

Как показывает текст приведенных судебных решений, социальные сети и другие интернет-ресурсы признаются открытыми источниками, но не общедоступными; персональные данные, размещенные самими пользователями в социальных сетях, не являются общедоступными; на обработку персональных данных из социальных сетей требуется письменное согласие их субъекта в связи с иной ее целью в сравнении с целью пользователя интернет-ресурса, поделившегося своими персональными данными.

Для толкования критерия «общедоступность» следует проанализировать наиболее значимые синонимичные понятия, характеризующие свободный доступ к персональным данным, и только после этого давать юридическую оценку позиции судов. В трудах по праву и в законодательстве активным применением в отношении персональных данных отличаются *следующие термины*:

1) *«Открытый доступ»* (англ. open access), хотя в России он не является легальным. В международном праве он впервые упоминается в 2002 г. на конференции Будапештской инициативы свободного доступа применительно к научным исследованиям в сети Интернет (книги, статьи, диссертации и проч.). В ее Декларации открытый доступ определяется как «открытые для всех публикации в Интернете, которые можно читать, разгружать, копировать, распространять, распечатывать, находить или присоединять к полным текстам соответствующих статей, использовать для составления указателей, вводить их как данные в программное обеспечение или использовать для других законных целей при отсутствии финансовых, правовых и технических преград, за исключением тех, которые регулируют доступ к собственно Интернету. Единственным ограничением на воспроизводство и распространение публикаций и единственным условием копирайта в этой области должно быть право автора контролировать целостность своей работы и обязательные ссылки на его имя при

[1] Апелляционное определение Нижегородского областного суда от 11.10.2016 по делу № 33-12355/2016. URL: https://www.audar-info.ru/na/article/view/type_id/7/doc_id/26195/ (дата обращения: 04.02.2023).

использовании работы и ее цитировании»[1]. Другими словами, открытый доступ к научно-исследовательским публикациям в сети Интернет разрешает их любое использование со ссылкой на автора, за исключением внесения изменений в чужие работы;

2) *Общедоступная информация* (ч. 1 ст. 7 Закона об информации). В российском праве используется эта юридическая категория, которая по закону делится на две группы, но не раскрывается им – общеизвестные сведения и иная информация, доступ к которой не ограничен. Исходя из понимания общеизвестности, ею будет обладать информация, известная широкому кругу лиц и доступная для ознакомления в общедоступных и проверяемых источниках (данные государственной статистики, сведения о научных открытиях, содержащиеся в открытых государственных реестрах или размещенные на официальных сайтах государственных органов). А потому она может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации (ч. 2 ст. 7 Закона об информации). Комментируя эту норму, Л.К. Терещенко определяет режим общедоступной информации как максимально возможную свободу не только доступа, но и использования информации[2]. А.И. Савельев отмечает, что она устанавливает презумпцию открытости информации: любая информация, кроме той, к которой ограничен доступ, является общедоступной. А значит «любое лицо без указания причин и целей может получать такую информацию и использовать по своему усмотрению, с соблюдением установленных федеральным законом ограничений на ее распространение»[3]. Очевидно, что общеизвестные сведения и иная

---

[1] Декларация Будапештской инициативы «Открытый доступ». URL: https://www.budapestopenaccessinitiative.org/translations/russian-translation (дата обращения: 24.12.2022).

[2] Терещенко Л.К. Правовой режим информации. М.: Юриспруденция, 2007. С. 49.

[3] Савельев А.И. Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (постатейный). М.: Статут, 2015. С. 181.

информация, доступ к которой не ограничен, могут содержать персональные данные (к примеру, номинативные);

3) *Общедоступная информация, размещаемая в форме открытых данных* (ч. 4 ст. 7 Закона об информации). Концепция открытых данных тесно связана с идеей открытого правительства, прозрачность деятельности которого обеспечивается информационно-телекоммуникационными технологиями в целях взаимодействия с населением, для ознакомления и последующего использования информации заинтересованными лицами. Открытыми данными признается, например, информация, создаваемая и аккумулируемая государственными органами и органами местного самоуправления (Минфин, МВД, Росстат и др.) о своей деятельности, размещаемая в сети Интернет в формате, допускающем ее последующую обработку без вмешательства человека[1]. Правительством РФ определяется перечень информации, которая подлежит размещению в форме открытых данных[2]. Ссылаясь на ч. 4 ст. 7 Закона об информации, М.А. Рожкова пишет, что общедоступная информация, размещаемая в форме открытых данных, является разновидностью общедоступных данных, которую из прочих общедоступных данных выделяет то, что она размещена в сети Интернет в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования. Проведя аналогию с персональными данными, она считает, что в случае их размещения в открытом доступе в сети Интернет они автоматически становятся общедоступными, что

[1] Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления на их официальных сайтах в информационно-телекоммуникационной сети «Интернет» в форме открытых данных: постановление Правительства РФ от 10.07.2013 № 583 (с изм. и доп. от 10.11.2022, № 2025) // СЗ РФ. 2013. № 30 (ч. II), ст. 4107; 2022. № 46, ст. 8027.

[2] О Перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети Интернет в форме открытых данных: распоряжение Правительства РФ от 10.07.2013 № 1187-р (с изм. и доп. от 10.11.2022, № 2025) // Доступ из Справ.-прав. системы «Гарант» (дата обращения: 22.02.2023).

разрешает их свободное использование, за исключением распространения, требующего согласия в соответствии со ст. 9 ФЗ № 152[1].

4) *Общедоступные источники персональных данных* (ст. 8 ФЗ № 152). По замыслу законодателя, к ним относятся справочники, адресные книги, открытые любому человеку, и создаваемые по инициативе оператора, а не в силу обязанности по закону раскрыть или опубликовать определенную информацию (как в случае с открытыми данными). В прежней редакции ФЗ № 152 для обозначения этих ресурсов применялся термин «общедоступные персональные данные», определяемый как «персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных либо на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности». После внесения поправок произошла его замена на термин «общедоступные источники персональных данных». Исходя из смысла, заложенного в эту норму, речь идет, к примеру, о справочнике работников учреждения и т.п. в целях информационного обеспечения трудовой деятельности, однако она не действует в отношении их персональных данных, не связанных с работой. В ст. 8 оговаривается, что фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии *могут* включаться с письменного согласия их владельца, и он же является источником иных персональных данных, на что однозначно указывает слово «сообщаемые».

5) *Персональные данные, разрешенные субъектом персональных данных для распространения* (п. 1.1 ст. 3 ФЗ № 152). Этот новый термин, применяемый в значении общедоступной информации, был дефинирован в 2020 г.[2] как персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для

---

[1] Рожкова М.А. «Общедоступная информация», «открытые данные» и «персональные данные, разрешенные субъектом для распространения» – что это такое и как они между собой связаны? // Закон.ру. 2021. 13 янв.

[2] О внесении изменений в Федеральный закон «О персональных данных»: федер. закон от 30.12.2020 № 519-ФЗ // Рос. газета. 2021. 11 янв.

распространения в порядке, предусмотренном ФЗ № 152[1]. В пояснительной записке к законопроекту внесение поправок объяснялось необходимостью ограничения неконтролируемого использования персональных данных человека, размещенных им на сайтах и в других открытых источниках. По мысли депутатов, это касается случаев распространения чужих персональных данных «в целях, отличных от цели их первоначального распространения, а равно с ориентиром на иные целевые аудитории»[2]. Согласно новой статье 10.1 оператор персональных данных для их распространения (например, размещение на сайте компании) обязан получить отдельное от иных согласие (ранее он мог распространять персональные данные (публиковать или передавать третьим лицам) при письменном согласии их владельца на обработку). У субъекта персональных данных есть право выбирать персональные данные и условия распространениям их оператором, получившим к ним доступ. Если обладатель персональных данных дал свое согласие только на обработку его данных, то оператор может их хранить, уточнять, использовать и др., но не наделен правом передавать кому-либо еще (п. 4 ст. 10.1), за исключением государственных структур (военкомат, полиция, Следственный комитет, ФНС, ФСС, ПФР и т.д.).

Проанализировав содержание режимов информации, установленных законодательными актами и определяющих информацию как открытую; общедоступную; открытую и общедоступную, можно увидеть, что законодатель устанавливает один и тот же общий режим информации, предоставляющий любому заинтересованному лицу получить доступ к информации и использовать ее по своему усмотрению[3]. Разграничив указанные понятия, автор вправе прокомментировать решения Арбитражного суда г. Москвы от 05.05.2017 по делу

---

[1] Ранее ФЗ № 152 в п. 4 ч. 2 ст. 22 (утратил силу в соответствии с федеральным законом от 14.07.2022 № 266-ФЗ) правотворец использовал иное понятие – «персональные данные, сделанные субъектом персональных данных общедоступными».

[2] О внесении изменений в Федеральный закон «О персональных данных» в части установления особенностей обработки общедоступных персональных данных»: пояснительная записка к проекту федерального закона № 1057337-7 // Официальный сайт Государственной Думы РФ. URL: https://sozd.duma.gov.ru/bill/1057337-7 (дата обращения 19.01.2022).

[3] Рагимханова Д.А., Аливердиева М.А. Правовой режим общедоступной информации // Вестник Дагестанского государственного университета. Серия 3: Общественные науки. 2013. № 2. С. 59.

№ А40-5250/17-144-51 и Арзамасского городского суда Нижегородской области от 14.06.2016 по делу № 2-2307/2016. Напомним, что логика решений судебных инстанций была основана на положениях ст. 8 ФЗ № 152: общедоступными являются только те персональные данные, которые, *во-первых*, поименованы в качестве источников персональных данных. Персональные данные, размещенные в аккаунтах социальных сетей, на веб-сайтах или на других пабликах, не могут считаться, по мнению судов, общедоступными, поскольку эти интернет-платформы прямо не указаны в ст. 8 ФЗ № 152. Последнее обоснование вызвало критику одних ученых, другие же считают позицию судов подлежащей нормативному оформлению. Так, В.И. Солдатова предложила законодательно закрепить указанную позицию судов по использованию персональных данных граждан, содержащихся в базах социальных сетей[1]. М.А. Рожкова, напротив, полагает, что общедоступные источники персональных данных неверно толкуются судами как прямо названные ресурсы (справочники, адресные книги), что влечет ошибочный вывод о необщедоступности непоименованных персональных данных с открытым доступом в сети Интернет. По ее мнению, что ст. 8 ФЗ № 152 не исключает иных общедоступных источников персональных данных, а в условиях цифровой трансформации ограничивать их справочниками и адресными книгами, как это сделали арбитражные суды в приведенных выше решениях, нельзя[2]. Возражая против такого подхода, укажем, что М.А. Рожкова считает понятия «общедоступные источники персональных данных» и «общедоступные персональные данные» равнозначными, а это, как верно подмечает А.В. Кучеренко, не одно и то же[3]. Действительно, применительно к положению статьи 8 ФЗ № 152 социальные сети источником общедоступных персональных данных не являются. Тот же вывод следует из проведенного ранее

---

[1] Солдатова В.И. Защита персональных данных в условиях применения цифровых технологий // Lex Russica. 2020. № 2 (159). С. 36.

[2] Рожкова М.А. «Общедоступная информация», «открытые данные» и «персональные данные, разрешенные субъектом для распространения» – что это такое и как они между собой связаны? // Закон. ру. 2021. 13 янв.

[3] Кучеренко А.В. Правовое регулирование персональных данных в Российской Федерации: дис. ... канд. юрид. наук. Челябинск, 2010. С. 86.

авторского анализа терминологии, применяемой к персональным данным, а потому решения судов в этой части следует признать соответствующими закону;

Во-вторых, персональные данные, размещенные в социальных сетях самими пользователями, являются общедоступными. За безопасность своих личных данных отвечает пользователь, ведь он сам выбирает условия доступа к своей личной странице, и решает, какие персональные данные, и кому он желает демонстрировать. Так, согласно п. 5.11. Пользовательского соглашения сайта «ВКонтакте» после регистрации пользователь получает право самостоятельно в личных целях создавать, использовать и определять содержание собственной страницы и условия доступа других пользователей к ее содержанию. Как обладатель информации, размещённой пользователем на персональной странице, он осознаёт, что администрация сайта не принимает участия в формировании и использовании содержания и контроле доступа других пользователей к персональной странице пользователя. Размещая на персональной странице свои персональные данные, пользователь осознаёт и соглашается с тем, что указанная информация может быть доступна другим пользователям сети Интернет (п. 5.12.) и может быть использована в том числе и в противоправных целях. К примеру, интернет-ресурс http://botsman.org/ предлагает услуги по извлечению данных о пользователе Интернета из открытых ресурсов сети. В его базе находится более 18 млн персональных данных пользователей социальных сетей. Поиск данных осуществляется при помощи бота по фамилии, месту обучения или проживания и др. сведениям из открытых источников, охватывающих более 100 площадок, включая социальные сети «ВКонтакте», «FaceBook», «Одноклассники», «Twitter», «Instagram», «Pinterest», «Tumblr» и др. На странице сайта его владельцы разъясняют право использования чужих персональных данных так: «Вы сами публикуете свои данные в сети Интернет (социальные сети, форумы и т.д.), что делает Ваши данные общедоступными!»[1]. Социальные сети и другие платформы в Глобальной сети активно используются и правоохранительными органами для определения местонахождения преступников, правонарушителей и должников, а

[1] URL: https://botsman.org (дата обращения 26.12.2022).

также их имущества[1]. Среди ресурсов сети Интернет, которые могут быть использованы в целях поиска информации о должниках и их имуществе, Методические рекомендации ФССП РФ от 30.11.2010 № 02-7, например, называют профили в социальных сетях, личные блоги, сайты онлайн объявлений, массив личных данных близких родственников, друзей и коллег по работе[2]. Думается, что для вменения вины в совершении нарушения или преступления правоприменителю необходимо детально изучить правила ресурса для того, чтобы определить, как он ограничивает использование персональных данных пользователей. Та же социальная сеть «ВКонтакте» в пункте 7.1.3. Правил пользования сайтом закрепляет положение о том, что пользователь, размещая на сайте принадлежащий ему на законных основаниях контент, предоставляет другим пользователям неисключительное право на его использование путём просмотра, воспроизведения (в том числе копирования) и иные права исключительно с целью личного некоммерческого использования, кроме случаев, когда такое использование причиняет или может причинить вред охраняемым законом интересам правообладателя.

В-третьих, обработка сделанных общедоступными персональных данных, как решил суд, требует согласия пользователя сайтов объявлений и социальных сетей. Полномочия неизвестных лиц, предоставивших персональные данные неопределенному кругу лиц, операторами (владельцами) социальных сетей и сайтов объявлений не проверялись. Согласие здесь, считает суд, должно быть предоставлено верифицированным субъектом и в письменной форме. Исследованный же в судебном заседании порядок размещения личных данных пользователей в социальных сетях был признан не обеспечивающим достоверность согласия на обработку персональных данных. В качестве его доказательства судебные органы не приняли электронную «галочку-согласие»

---

[1] Павлюков В.В. Правовая и практическая возможность объединения данных в информационно-поисковых системах МВД РФ с информацией из сети Интернет // Вестник Костромского государственного университета. 2016. № 3. С. 227.

[2] Методические рекомендации по использованию сети Интернет в целях поиска информации о должниках и их имуществе (утв. ФССП РФ 30.11.2010 № 02-7) // Службы судебных приставов. 2011. № 1.

ввиду невозможности идентифицировать пользователя. Этот вывод подытожил в своем определении Верховный Суд РФ: «Обрабатываемые персональные данные, содержащиеся в открытых источниках (социальных сетях: Вконтакте, Facebook, Instagram, Одноклассники, МойМир и т.д.), не являются общедоступными, т.к. согласно требованию п. 1 ч. 1 ст. 6 ФЗ № 152 «О персональных данных» согласия субъектов ПД на обработку их персональных данных получено не было»[1].

Анализируя решения судов в этой части, отметим противоречивость такого требования к операторам социальных сетей. Суд ссылается на ст. 7 «Конфиденциальность персональных данных» ФЗ № 152, где прописана обязанность оператора, получившего доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия их субъекта, если иное не предусмотрено федеральным законом. Между тем социальные сети и сайты объявлений, указанные в решениях, не являются операторами персональных данных. По авторскому запросу на официальном сайте Роскомнадзора в Реестре операторов, осуществляющих обработку персональных данных, социальная сеть «Вконтакте» не значится[2], а при этом платформой ежемесячно пользуются более 100 млн человек в России и СНГ, просматривающих 9 млрд записей. В п. 5.1. Правил пользования сайтом «ВКонтакте» говорится, что регистрация и/или авторизация на сайте означает согласие с этими правилами и политикой конфиденциальности. Иными словами, интернет-порталы и социальные сети при размещении пользователем своих персональных данных в режиме общей доступности вводят правило свободной воли и предупреждают о том, что в этом случае обязанность принимать меры к их сохранности возлагается на самого пользователя. Испрашивать отдельное и письменное согласие именно на обработку ставших общедоступными

---

[1] Определение Верховного Суда РФ от 29.01.2018 № 305-КГ17-21291 по делу № А40-5250/2017 // Гарант. URL: https://www.garant.ru/files/0/1/1294310/opredelenie_vs_rf_ot_29_yanvarya_2018_goda_po_delu_305_kg17_21291.pdf. (дата обращения: 04.02.2023).

[2] Реестр операторов, осуществляющих обработку персональных данных (по состоянию на 05.03.2023) // Росреестр. URL: https://pd.rkn.gov.ru/operators-registry/operators-list/ (дата обращения: 04.02.2023).

персональных данных, как посчитали суды, по ФЗ № 152 необязательно, кроме их распространения (ч. 2 ст. 10.1 ФЗ № 152). Именно потому сам Роскомнадзор на своем официальном сайте разъяснил, когда для обработки персональных данных не требуется согласия субъекта персональных данных (дата публикации 27.03.2012). Ведомство дало следующий ответ: когда осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее персональные данные, сделанные общедоступными субъектом персональных данных)[1].

В-четвертых, отсутствие согласия на обработку общедоступных персональных данных пользователей в целях, несовместимых с целями сбора персональных данных, поскольку заявленные им цели обнародования своих персональных данных и цели оператора (в нашем случае кредитно-финансовые организации) разнятся. Юридическим основанием признания Роскомнадзором по ЦФО нарушителем положений ст. 6 и ст. 8 ФЗ № 152 организации, осуществлявшей скоринг пользователей интернет-ресурсов (или оценку добросовестности заемщика), явилось отсутствие согласия на обработку общедоступных персональных данных пользователей для определения их потенциальной кредитоспособности. Финансово-кредитные организации, упомянутые в судебных актах, фактически осуществляли противоправную обработку общедоступных персональных данных пользователей социальных сетей и сайтов объявлений в целях, несовместимых с целями сбора персональных данных указанных платформ и самих пользователей без их согласия (оценка кредитоспособности пользователей; информирование друга заемщика о долге по кредиту), в связи с чем в действиях заявителя усматриваются нарушения п. 1 ч. 1 ст. 6 ФЗ № 152. Следовательно, финансово-кредитные организации совершили правонарушение, предусмотренное ч. 1 ст. 13.11 КоАП РФ, а именно обработку персональных данных, несовместимую с целями сбора персональных данных

---

[1] Обращения в сфере персональных данных // Роскомнадзор. URL: https://26.rkn.gov.ru/p8926/p10713/ (дата обращения: 15.12.2022).

социальными сетями и другими интернет-ресурсами. Возражая против такой оценки, отметим, что, единожды выразив свою волю на предоставление доступа неограниченному кругу лиц к своим персональным данным, размещенным на общедоступных сайтах, субъект тем самым автоматически подтверждает согласие каждому на обработку указанных данных в любых не противоречащих закону целях. Хорошей иллюстрацией последнему утверждению являются положения ст. 10.1 ФЗ № 152. Как уже говорилось, размещая свои персональные данные на странице в сети, владелец дает тем самым свободное согласие на доступ к ним, но отнюдь не делает их разрешенными для иных действий, кроме использования. Если субъект, сделав публичными персональные данные, не дал согласия оператору на их обработку *для распространения*, то при установлении вины в их последующем распространении или иной обработке следует исходить из доказательства незаконности этих действий с чужими персональными данными (п. 2 ст. 10.1 ФЗ № 152). Возлагается такая обязанность и на участников социальных сетей. Например, согласно п. 6.1. Правил пользования сайтом «ВКонтакте» пользователь обязуется хранить в тайне и не предоставлять другим пользователям и третьим лицам ставшие ему известными в результате использования сайта персональные данные (включая, но не ограничиваясь, домашними адресами, номерами телефонов, адресами электронной почты, ICQ, паспортными данными, банковской информацией) и информацию о частной жизни других пользователей и третьих лиц без получения соответствующего предварительного разрешения последних. Другими словами, требуется согласие на распространение сделанных самим человеком общедоступными персональных данных, а для собирания и систематизации персональных данных пользователей социальной сети и сайтов объявлений, профили которых открыты и являются публичными, оно не обязательно. Фактически кредитно-финансовая организация осуществляла не противоправную обработку общедоступных персональных данных пользователей социальных сетей и сайтов объявлений в форме их сбора, систематизации, накопления, хранения, уточнения (обновление, изменение), извлечения и использования без распространения. Подтверждается такая позиция

и разбором понятия «обработка персональных данных». Ею, обработкой, является любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (п. 3 ч. 1 ст. 1 ФЗ № 152). Правомерное же использование персональных данных по смыслу допускается при условии легального свободного доступа к ним (кроме утечки, хакерской атаки). И если говорить о каких-либо нарушениях заявителя, то они могут быть выражены исключительно в способах сбора информации. Правилами пользования сайтом социальной сети «ВКонтакте» запрещается использование автоматизированных скриптов (программы, боты, краулеры) для сбора информации на сайте без специального на то разрешения администрации (п. 6.3.9.)[1]. Между тем для поиска клиента или потенциального клиента и обработки его профиля в открытых источниках информации заявителями применялись сервисы Double Data Social Link и Double Data Social Attributes (а между тем программа самого сайта «VK Parser» позволяет собирать персональные данные каждого подписчика группы или публичной страницы[2])[3]. Учитывая приведённые аргументы, суды допустили ошибку в толковании ст. ст. 6, 8 и 9 ФЗ № 152 и вопреки им признали, что обрабатываемые в социальных сетях персональные данные не являются общедоступными. Не соответствует закону и требование о письменном согласии пользователя на обработку им же открытых своих

---

[1] Правила пользования Сайтом «ВКонтакте». URL: https:// vk.com/terms (дата обращения 26.12.2022).

[2] VK Parser и его друзья. URL: http://vkparser.ru/ (дата обращения 26.12.2015).

[3] Такие прецеденты уже имеются. К примеру, «ВКонтакте» обратилась в суд с иском к ООО Дабл, использовавшей программное обеспечение для поиска и проверки в открытых источниках этой сети персональных данных физических лиц (дело № А40-18827/17-110-180). См. подроб.: Орешин Е. Дело ВКонтакте VS Дабл об использовании общедоступных данных пользователей // Закон.ру. URL: https://zakon.ru/blog/2018/6/15/delo_vkontakte_vs_dabl_ob_ispolzovanii_obschedostupnyh_dannyh_polzovatelej_poziciya_dabl_v_sude_po_i/ (дата обращения 26.12.2022).

персональных данных и в других целях, несовместимых с целями сбора персональных данных социальными сетями и интернет-ресурсами.

При авторском выводе о неверном толковании правоприменителем понятия «общедоступные персональные данные» следует оговориться, что суды не случайно давали оценку наличию именно подтвержденного письменного, а не виртуального, согласия пользователя персональных данных на их общедоступность, поскольку конфиденциальные личные сведения могут быть сделаны публичными не их субъектом. Если персональные данные были раскрыты вопреки согласию их обладателя или помимо него вследствие правонарушения, преступления или обстоятельств непреодолимой силы, то и на этот случай распространяется правило об обязанности доказывания законности своих действий каждым лицом, кто распространил или иным способом осуществлял обработку чужих персональных данных (п. 3 ст. 10 ФЗ № 152). Наглядным примером подобной ситуации служат фейковые аккаунты в социальных сетях, созданные в том числе для совершения преступлений с использованием сети Интернет, регистрация которых допускается без идентификации личности пользователя по официальным документам. Так, согласно пункту 5.5. Пользовательского соглашения регистрацию на сайте «ВКонтакте» необходимо подтвердить путем: 1) распознания автоматизированного теста, предназначенного для различия компьютеров и людей; 2) активации персональной страницы через сообщение, отправленное администрацией сайта на электронную почту пользователя; 3) введения в соответствующую форму на сайте кода, полученного пользователем в виде sms-сообщения от администрации сайта на номер предоставленного пользователем мобильного телефона[1]. Удостоверительная процедура не включает требование легального, к примеру, по паспорту, распознавания человека. И это несмотря на то, что практически все онлайн-сервисы, сайты и социальные сети ведут политику «настоящих имен» – не только предоставлять при регистрации достоверные и

[1] Правила пользования Сайтом «ВКонтакте». URL: https://vk.com/terms (дата обращения 23.12.2022).

полные данные пользователя, не допуская псевдонимов, но и следить за их актуализацией[1].

Исследователи давно обращают внимание на необходимость урегулирования в нормах права отсутствия доступных форм выражения согласия на действия третьих лиц в отношении чужих персональных данных, в т.ч. в сети Интернет. По их мнению, регистрация могла бы выполняться посредством применения квалифицированной электронной подписи пользователя или путем реализации протокола, в результате которого устанавливается личность (код активации учетной записи направляется почтой и получается пользователем по предъявлению паспорта, как это было при регистрации на портале «Госуслуги»)[2]. Предлагается и практика свободного отказа от обработки части персональных данных, которые могут регулироваться посредством настроек в браузере[3]. Не случайно в пояснительной записке к проекту федерального закона № 1057337-7 им предусматривалось получение согласия субъекта персональных данных, сделавшего их общедоступными, как исключительного правового основания на их обработку оператором с перечнем интернет-ресурсов, на которых планируется их размещать. С учетом замечаний Правового управления ГД РФ от 23.11.2020 после первого чтения из законопроекта обязательное согласие на обработку персональных данных, сделанных общедоступными, было исключено.

А есть ли в этом предложении теоретиков и правотворцев практический смысл и разумное обоснование? Полагаем, отчасти. Аргументировать обязательность испрашивания согласия лица на использование его персональных данных, размещенных на открытых страницах в Глобальной сети, позволяет широкое применение цифровых технологий и массовой вовлеченности граждан в виртуальный мир для различных коммуникаций. И, действительно, «современные социальные связи немыслимы без интенсивного обмена информацией, в том

---

[1] Наумов В.Б., Панова Н.В., Лебедева Т.В. Персональные данные в соцсетях и социальных медиа: правовые проблемы защиты и использования // Закон. 2012. № 5. С. 121.

[2] Ильютович Д.А. Юридическое содержание права гражданина на изображение // Правовая информатика. 2015. № 3. С. 49.

[3] Серебряков К.Д. Некоторые проблемы реализации механизма правовой защиты персональных данных в социальной сети «Вконтакте» // Вопросы российской юстиции. 2022. № 21. С. 688.

числе непосредственно касающейся частной жизни человека. Пользование технологиями мобильного банкинга, покупки и получение самых разных услуг посредством интернет-контактов предполагает жертвование не только материальными, но и определенными личными благами, в том числе и своим правом на неприкосновенность частной жизни»[1]. В информационном обществе согласие людей на передачу (обработку) персональных данных и регистрацию на различных онлайн-платформах является нередко вынужденным, или условно добровольным. Оно дается в обмен на получение государственных и прочих услуг, продвижение товаров в самых разных сферах (открытое правительство, личные кабинеты на сайтах маркетплейсов, косметики, объявлений) и возможность осуществления профессиональной деятельности на площадках с многомиллионной аудиторией (заработок фрилансеров, блогеров, реклама товаров, оказания услуг и др.). Научно-технический прогресс будет способствовать последующему росту получения услуг, связанных с цифровыми технологиями, и вовлеченности в них сограждан. Как отмечают аналитики, реализация разработанных на основе указов Президента РФ В.В. Путина[2] Концепции «Цифровая трансформация 2030» и программы «Цифровая экономика Российской Федерации» приведет к увеличению доли массовых социально значимых услуг, доступных в электронном виде, в том числе здравоохранения и образования, до 95 %[3]. Это означает, что пользователи, получившие аккаунт или личную страницу, и дальше будут предоставлять информацию о себе, в том числе и персональные данные, а потому и в теории уголовного права вокруг отграничения допустимого сбора или распространения персональной информации, размещенной на сайтах или в социальных сетях самим гражданином

---

[1] Пикуров Н. Проблемы квалификации преступных посягательств на частную жизнь: теория и судебная практика // Уголовное право. 2019. № 2. С. 56.

[2] О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: указ Президента РФ от 09.05.2017 № 203 // СЗ РФ. 2017. № 20, ст. 2901; О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: указ Президента РФ от 07.05.2018 № 204 (с изм. и доп. от 21 июля 2020 г. № 474) // СЗ РФ. 2018. № 20, ст. 2817; 2020. № 30, ст. 4884.

[3] Бугера М.А. Борьба с хищениями сотовых телефонов и персональных данных, содержащихся в них: проблемы и пути решения // Вестник Санкт-Петербургского университета МВД России. 2022. № 2 (94). С. 110.

ведется оживленная полемика. Ее суть объясняет Н.И. Пикуров: «Настоящий бум обмена сведениями, относящимися к частной жизни конкретного лица, связан с появлением социальных сетей. Возникает проблема отграничения допустимого сбора и распространения информации, прежде всего визуального характера, размещенной на сайтах самим гражданином, от незаконных действий, нарушающих право такого гражданина на неприкосновенность частной жизни при дальнейшем распространении информации иными лицами»[1].

В попытке изыскать пути решения этой проблемы одни правоведы прибегают к приравниванию регистрации в пабликах (блогах, страницах в соцсетях, приложениях, иных сайтах) как публичном пространстве к согласию на совершение каких-либо действий с персональными данными другого человека, размещаемыми им в социальных сетях. Согласно позиции Р.И. Дремлюги, информация, размещенная в блогах, не подпадает под определение охраняемых законом сведений: «Все персональные данные, которые размещаются на таких страницах, являются общедоступными в силу п. 2 ч. 2. ст. 10 ФЗ «О персональных данных», так как размещены самим субъектом персональных данных. Неправомерный доступ будет рассматриваться как доступ к неохраняемой законом информации. В то же время такие действия могут привести к существенным негативным последствиям. Упомянутый подход оставляет без уголовно-правовой защиты ключевую фигуру цифровой экономики – лицо, генерирующее информацию»[2]. По мнению А.К. Жаровой и В.М. Елина, если личная информация размещается в сети самим субъектом персональных данных, то дальнейшее ее использование возможно[3].

Другие же авторы предлагают оценивать правомерность действий с чужими персональными данными с позиции принятых пользователем мер по защите своего аккаунта. Н.И. Пикуров доказывает, что признанием персональной информации пользователя социальных сетей охраняемой служит установление им

---

[1] Пикуров Н. Указ. соч. С. 55.

[2] Дремлюга Р.И. Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ // Уголовное право. 2018. № 4. С. 56–57.

[3] Жарова А.К., Елин В.М. Источники понятий «персональные данные» и частная жизнь лица в российском праве // Вестник Академии права и управления. 2017. № 1 (46). С. 73.

пароля для входа на свою страницу. Взлом пароля и будет подтверждать осознание виновным того факта, что потерпевшим охраняются в том числе и персональные данные от доступа других лиц[1]. Как уже отмечалось при анализе понятия общедоступности, когда сам субъект раскрывает свои персональные данные, к примеру, на своей странице в социальной сети, т.е. в открытом доступе, без режима приватности, то они становятся общедоступными и выводятся из-под запрета их собирания, использования или распространения, если они не носят цели совершения преступления. А потому публикуя свои персональные данные на разных ресурсах в сети Интернет, участник свободно, своей волей и в своем интересе выражает согласие на то, что они доступны для ознакомления или распространения другими участниками онлайн-площадки.

При изложенных обстоятельствах возникает и другой вопрос, являются ли предметом уголовно-правовой охраны правдивые персональные данные, ставшие общедоступными помимо воли их обладателя, в результате их открытия неопределенному кругу лиц нарушителем или злоумышленником? Практикующие юристы полагают, что если персональные данные размещены неустановленным лицом и не проверены на подлинность, нельзя их рассматривать их как персональные[2]. Правовую позицию о фейковых аккаунтах в соцсетях сформулировал и Роскомнадзор, указав, что они являются примером нарушения закона о персональных данных. В сообщении ведомства разъясняется: «Если персональные данные другого человека – будь то ФИО или его фотография – будут использоваться для создания фальшивого аккаунта, то имеет место нарушение закона, поскольку «цель его создания не может быть признана социально значимой. Правила пользования большинства популярных соцсетей (например, Facebook) предполагают соблюдение политики «реальных имен». Если такое нарушение имело место, следует обратиться к администраторам сайта с требованием удалить аккаунт. При этом можно апеллировать к правовой

[1] Филатова М.А. Персональные данные как предмет преступного посягательства журнал // Уголовное право. 2021. № 11. С. 38.

[2] Емельянников М.Ю. Судебное решение: соцсети и сайты объявлений в России теперь незаконны? // Emeliyannikov.blogspot. URL: https://emeliyannikov.blogspot.com/2017/12/blog-post.html (дата обращения 26.12.2022).

позиции в соответствии с российским законодательством по защите персональных данных»[1].

При использовании чужих персональных данных только для создания поддельного аккаунта при отсутствии умысла на совершение преступлений регистрация фейковой страницы может быть квалифицирована как несанкционированная обработка персональных данных, предусмотренная ч. 1 ст. 13.11 «Нарушение законодательства Российской Федерации в области персональных данных» КоАП РФ. Уголовная же ответственность будет зависеть от того, с какой целью ложная страница от имени другого лица регистрировалась. Действия, выражающиеся в создании фальшивого аккаунта в виде страницы-клона с указанием действительных персональных данных реально существующего человека («кража личности») с добавлением в друзья его контактов и получение злоумышленником от них денежных средств якобы в качестве долга, будут квалифицироваться по ст. 159 УК РФ как мошенничество. Если же фейковая страница создавалась для распространения сведений о частной жизни, составляющих личную и семейную тайну (например, фото обнаженного человека), то содеянное содержит признаки нарушения неприкосновенности частной жизни (ст. 137 УК РФ). Клеветой (ст. 128^1 УК РФ) могут признаваться размещенные на фальшивой странице сведения, порочащие честь и достоинство скомпрометированного человека, связанные, к примеру, с рассылкой якобы от его имени предложения об оказании платных секс-услуг.

Таким образом, результаты проведенного исследования общедоступности персональных данных позволили изложить ряд теоретических выводов:

1. Персональные данные не имеют одного правового режима и могут находиться в режиме личной или семейной тайны, информации ограниченного доступа (конфиденциальность) или в режиме доступной информации (общедоступность). Конфиденциальность – дискретный признак, влияющий на

---

[1] Ведомости: «Фейковые» аккаунты в соцсетях нарушают закон о персональных данных // Роскомнадзор. URL: https://rkn.gov.ru/press/publications/news29215.htm (дата обращения: 15.12.2022).

наличие состава преступления в случае сбора или распространения персональных данных, охраняемых в режиме конфиденциальности (ограниченного доступа), а общедоступность его исключает. Для целей уголовного права, исходя из разности правового режима открытой информации и информации ограниченного доступа, предлагается толковать понятия «общедоступность» и «конфиденциальность» применительно к персональным данным кардинально противоположными и взаимоисключающими.

2. Исходя из понимания персональных данных как конфиденциальной информации, уголовную ответственность за нарушение их неприкосновенности как самую репрессивную должно исключать, *во-первых*, согласие лица на предание огласке личных данных о себе и (или), *во-вторых*, их общедоступность. Право на неприкосновенность персональных данных является абсолютным личным правом, а потому от волеизъявления лица зависит юридически значимый факт: в случае, если дано согласие обладателя этого права на доступ к персональным данным, состав преступления отсутствует.

3. Не подлежит уголовной ответственности собирание или распространение чужих персональных данных, сделанных общедоступными самим их владельцем, в том числе путем размещения в сети «Интернет» (публичный профиль в социальной сети, на сайтах, форумах и иных онлайн ресурсах). В этом случае согласие на собирание, хранение, систематизацию и распространение общедоступных персональных данных презюмируется. В иных обстоятельствах при отсутствии общедоступности персональных данных согласие их субъекта должно быть конкретным, информированным и сознательным и в любой подтверждающей его наличие форме.

4. При решении вопроса о виновности в совершении указанных деяний необходимо устанавливать, охватывалось ли умыслом лица, что персональные данные другого человека хранятся им в тайне. Следует иметь в виду, что установление обладателем персональных данных порядка обращения с ними (ограничение доступа, режим конфиденциальности с закрытым доступом) свидетельствует о желании контролировать и самостоятельно определять степень

их открытости. Любое деяние, направленное на получение персональных данных, находящихся в режиме приватности, следует признавать совершенным против или помимо воли их владельца и квалифицировать как посягательство в отношении неприкосновенности чужих персональных данных.

ГЛАВА III. ОПТИМИЗАЦИЯ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

§ 1. Совершенствование уголовно-правовой оценки незаконных действий с персональными данными (de lege lata)

Уголовно-правовая защита конфиденциальных личных данных, как уже отмечалось, может обеспечиваться при их пересечении с иными видами охраняемой информации. Анализ следственно-судебной практики и экспертного мнения представителей правоохранительных органов и судов показывает, что посягательства в отношении персональных данных квалифицируются правоприменителем чаще всего по ст. 137 «Нарушение неприкосновенности частной жизни» и ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» УК РФ[1]. В иных случаях, когда персональные данные становятся предметом преступлений, совершаемых сотрудниками правоохранительных органов, кредитно-финансовых учреждений, операторов мобильной связи, других государственных и коммерческих организаций, уголовное преследование осуществляется по разным нормам уголовного закона при тождественных обстоятельствах содеянного. Противоречивые интерпретационные подходы в отношении одних и тех же деяний в процессе правоприменения закономерно порождают неоднозначную практику.

Согласно проведенному автором исследованию обвинительных заключений, судебных постановлений и приговоров, а также сообщений СМИ из выборки по делам о преступлениях, связанных с персональными данными, не отличается единообразием квалификация действий сотрудников компаний–операторов мобильной связи. Имея доступ к клиентской базе данных, они осуществляют неправомерный доступ, копирование и распространение (разглашение) путем передачи, в том числе за плату, персональных данных абонентов. В целях обеспечения потребностей сотрудников следственных и судебных органов в единых алгоритмах толкования деяний этой категории

[1] См.: Приложение 2, содержащее результаты опроса экспертов.

субъектов в отношении персональных данных опишем сложившиеся варианты уголовно-правовой оценки:

1) *нарушение неприкосновенности частной жизни (ч. 2 ст. 137 УК РФ)*. Б., сотрудник АО «Мегафон Ритейл», находясь в офисе продаж, воспользовавшись открытой учетной записью С. на служебном компьютере, осуществил доступ в специализированную систему (SBMS) с базами данных. Просмотрев и сфотографировав на мобильное устройство «Huawei P20 Lite» личные данные потерпевшей И. (фамилия, имя и отчество, паспортные данные, сведения о месте регистрации, дата рождения). Используя свое мобильное устройство, Б. через мессенджер «Telegram» переслал сделанную им фотографию с личными данными И. неустановленному пользователю под псевдонимом «Zer2122», за что последний перевел Б. 200 руб. через платежную систему «Яндекс.Кошелек»[1];

2) *неправомерный доступ к компьютерной информации (ст. 272 УК РФ).* При этом если персональные данные копировались сотрудником из базы данных мобильного оператора и передавались за денежное вознаграждение, то содеянное квалифицируется по ч. 2 ст. 272 УК РФ, а в иных случаях вменяется использование служебного положения по ч. 3 ст. 272 УК РФ.

К примеру, оператор обособленного подразделения ООО «Т2 Мобайл» М., находясь на своем рабочем месте, действуя умышленно, из корыстной заинтересованности под своими индивидуальными учетными данными осуществила доступ в компьютерную программу «InVoice», которая используется сотрудниками компании «Т2 Мобайл» для сервисного обслуживания абонентов оператора «Tele2». Далее М. передала неустановленному следствием лицу по средствам сети Интернет за вознаграждение в сумме 500 руб. информацию о SIM-карте, карточке абонента с персональными данными и скопированный ею PUK-код абонентского номера №. PUK-код представляет собой персональный код для защиты данных, хранящихся на SIM-карте, в том числе персональных данных (скан паспорта, платёжных карт, получение доступа к мобильному банку

[1] Приговор Фрунзенского районного суда г. Владимира от 18.05.2020 по делу № 1-77/2020 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/JFXOOMXHQdQx/?regular (дата обращения: 04.02.2023).

клиента). Согласно вынесенному приговору Октябрьского районного суда г. Ростова-на-Дону М. обвинялась в девяти эпизодах неправомерного копирования компьютерной информации из корыстной заинтересованности, что предусмотрено ч. 2 ст. 272 УК РФ[1]. Напротив, при тех же обстоятельствах и тем же судом за аналогичные действия был осужден по ч. 3 ст. 272 УК РФ Л., оператор группы абонентского обслуживания «Т2 Мобайл». Посредством системы «InVoice» он осуществил неправомерный доступ к компьютерной информации – персональным данным абонента, скопировал PUK-код и передал его неустановленному лицу за вознаграждение. Всего Л. было предъявлено двадцать эпизодов копирования и передачи персональных данных клиентов «Т2 Мобайл»[2].

В другом уголовном деле Мокшанский районный суд Пензенской области, постановивший приговор в отношении Ч. по ч. 3 ст. 272 УК РФ, руководствовался иным подходом. Характеризуя вину подсудимой, суд отметил, что преступные действия Ч. совершила «для демонстрации значимости и возможностей, которыми она обладает в процессе осуществления трудовой деятельности, для поднятия собственного авторитета перед иными лицами». Являясь специалистом офиса обслуживания и продаж Казанского филиала ПАО «ВымпелКоммуникации», Ч. по просьбе подруги Ю. осуществила вход в компьютерную программу «Amdocs» с неправомерным доступом к электронной карточке абонента Я. Его персональные данные, включающие фамилию, дату рождения, адрес места жительства, реквизиты паспорта, наименование тарифного плана и остаток на лицевом счете, Ч. скопировала на свой мобильный телефон и с использованием сервиса SMS-сообщений отправила на мобильный телефон Ю.[3];

---

[1] Приговор Октябрьского районного суда г. Ростова-на-Дону от 22.04.2019 по делу № 1-306/2019 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/MEIPEhOnVY5T/?regular (дата обращения: 10.04.2023).

[2] Приговор Октябрьского районного суда г. Ростова-на-Дону от 04.02.2020 по делу № 1-119/2020 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/Mieif03BN1b4/?regular-(дата обращения: 10.04.2023).

[3] Приговор Мокшанского районного суда Пензенской области от 28.06.2019 по делу № 1-36/2019 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/OVzzuMQ72gHB/?page=4&regular (дата обращения: 10.04.2023).

3) *незаконное разглашение сведений, составляющих коммерческую тайну (ст. 183 УК РФ) и неправомерный доступ к компьютерной информации (ст. 272 УК РФ).* С.И. Гутник, изучивший судебную практику о преступлениях против персональных данных, заметил, что ему «не встретилось ни одного уголовного дела с обвинительным приговором, в котором действия виновного были бы квалифицированы по совокупности ст. 183 и ст. 272 УК РФ»[1]. Другие авторы, напротив, учитывая масштабы незаконного разглашения сведений, составляющих банковскую или налоговую тайну, когда она была доверена или стала известна по службе или работе, предлагают криминализировать хранение и распространение больших массивов информации[2]. Настоящее исследование также подтверждает сложившуюся практику постановления приговоров по указанной совокупности преступлений.

Л., оператор контактного центра ООО «Т2 Мобайл», находясь в офисе, использовал выданный ему логин и персональный пароль для входа с рабочего компьютера в программы «Invoice» и «Umbrella». Осуществив неправомерный доступ к электронным карточкам пятнадцати абонентов с их персональными данными, включающими фамилию, имя, отчество, реквизиты документов, удостоверяющих личность, сведения о денежных средствах на лицевом счете, скопировал их на мобильный телефон и с использованием мессенджера «Telegram» передал пользователю с аккаунтом «N» за вознаграждение в размере 35 тыс. руб. Органом предварительного следствия действия Л. квалифицированы по ч. 3 ст. 272 УК РФ как неправомерный доступ к охраняемой законом компьютерной информации, повлёкший копирование компьютерной информации, из корыстной заинтересованности, с использованием служебного положения, и по ч. 3 ст. 183 УК РФ как незаконное разглашение сведений, составляющих

---

[1] Гутник С.И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: дис. … канд. юрид. наук. Красноярск, 2017. С. 120.

[2] Бронников Д.А. Передача и распространение массивов персональных данных. Общественная опасность и перспективы криминализации подобных деяний // Молодые учёные России: сб. ст. VI всерос. науч.-практ. конф. Пенза, 2021. С. 166; Сысенко А.Р., Белова К.С., Горденко А.С. Особенности расследования неправомерного доступа к компьютерной информации (ст. 272 УК РФ) // Криминалистика: вчера, сегодня, завтра. 2022. № 4 (24). С. 187.

коммерческую тайну, без согласия их владельца, ставших ему известными по работе, из корыстной заинтересованности[1];

4) *нарушение неприкосновенности частной жизни с использованием служебного положения (ч. 2 ст. 137 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ч. 2 ст. 138 УК РФ) и незаконное разглашение сведений, составляющих коммерческую тайну (ст. 183 УК РФ).*

Дзержинским районным судом г. Новосибирска осуждены Н. по ч. 2 ст. 137, ч. 2 ст. 138 и ст. 183 УК РФ, а Б. и С. – по ч. 4 ст. 33 ч. 2 ст.137 УК РФ, ч. 4 ст. 33 ч. 2 ст. 138 УК РФ, ч. 4 ст. 33 ч. 3 ст. 183 УК РФ. Б., действуя умышленно, группой лиц по предварительному сговору, из корыстных побуждений получал заказы через мессенджеры от неустановленных лиц для копирования персональных данных абонентов МТС и передавал их С. Занимая должность старшего инженера отдела развития сервисных сетей в ПАО МТС, С. не имела доступа к информационной системе персональных данных (далее ИСПДн), а потому передавала полученные от Б. поручения Н., специалисту группы обслуживания абонентов массового сегмента. Вход в систему осуществлялся Н. с использованием логина и пароля, который предоставлялся ей при трудоустройстве для выполнения своих обязанностей. Следствием было установлено 24 эпизода копирования и передачи за денежное вознаграждение полных персональных данных абонентов сотовой связи ПАО МТС и сведений о дате и времени соединений, номерах исходящих и входящих соединений[2];

5) *неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274[1] УК РФ).*

---

[1] Постановление Пролетарского районного суда г. Саранска от 11.09.2019 по делу № 1-288/2019 о применении судебного штрафа // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/l4O9LJQ90WHR/?page=3&regular (дата обращения: 04.02.2023).

[2] Бывшую сотрудницу МТС признали виновной в продаже информации о звонках абонентов // Новости Новосибирска. URL: https://novosibirsk-news.net/other/2018/04/19/77809.html; приговор Дзержинского районного суда г. Новосибирска от 02.10.2017 по делу № 1-389/2017 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/kN7MkWMrBlUK/?regular-txt=Необутова+приговор&regular-case_doc=&regular (дата обращения: 09.05.2023).

По сообщениям прокуратуры Калужской области, в отношении 23-летнего жителя г. Калуги утверждено обвинительное заключение по ч. 4 ст. 274[1] УК РФ. Работая в офисе продаж компании сотовой связи, он имел доступ к сведениям о детализации телефонных соединений, персональным данным абонентов, которые копировал и передавал третьим лицам. В течение нескольких месяцев обвиняемый осуществлял незаконную выгрузку из соответствующих баз данных, делал снимки экрана рабочего компьютера на свой телефон, впоследствии незаконно скопированную информацию передавал через мессенджер «Telegram» за денежное вознаграждение. Базы данных оператора связи были включены в реестр объектов критической информационной инфраструктуры РФ (КИИ РФ), чем была нарушена целостность данных в автоматизированной системе. Действия виновного были квалифицированы как неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ с использованием своего служебного положения[1].

Мониторинг обвинительных заключений и судебных актов показывает, что при одних и тех же обстоятельствах правоприменитель каждый раз использует противоречивый алгоритм квалификации, вызывающий возражение, *во-первых*, в том, что при передаче персональных данных третьим лицам сотруднику вменяется разглашение коммерческой тайны (ст. 183 УК РФ), а другому, с аналогичным функционалом, не всегда. Вопреки ссылке в приговоре на то, что персональная информация об абонентах, их личные данные и сведения о соединениях являются сведениями, составляющими коммерческую тайну оператора мобильной связи, о чем предупреждался виновный при приеме на работу, следственные органы обвинение по ст. 183 УК РФ зачастую не предъявляют. *Во-вторых,* по многим уголовным делам исключается обвинение и в неправомерном доступе к компьютерной информации (ст. 272 УК РФ) вне зависимости от того, использовал ли виновный собственные логин и пароль, рабочий компьютер с его идентификатором и персональным именем для входа в

[1] Возбуждено уголовное дело по факту незаконного копирования информации из баз данных оператора сотовой связи // Генеральная прокуратура РФ. URL: https://epp.genproc.gov.ru/web/proc_40/mass-media/news?item=61325179 (дата обращения: 09.05.2023).

систему с персональными данными абонентов либо воспользовался учетной записью другого работника. К тому же работники операторов сотовой связи не всегда признаются лицами, использующими служебное положение при осуществлении неправомерного доступа вопреки обязанности соблюдать конфиденциальность информации ограниченного доступа в должностной инструкции (ч. 3 ст. 272 УК РФ). *В-третьих*, действия лиц, допустивших нарушение конфиденциальности информации путём копирования из баз данных операторов мобильной связи персональных данных с их последующей передачей заказчику, квалифицируются только по ст. 137 и (или) ст. 138 УК РФ[1]. *В-четвертых*, в приговорах, вынесенных после введения в УК РФ ст. 274[1] УК РФ Федеральным законом от 26.07.2017 № 194-ФЗ не усматривается попытка установления органом предварительного расследования, относится ли информационная система (база данных) мобильного оператора к объекту критической информационной инфраструктуры, включена ли она в Реестр значимых объектов критической информационной инфраструктуры (ст. 8 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[2])[3].

С изложенными вариантами квалификационных решений правоприменителя, который дает содеянному в похожих случаях разную уголовно-правовую оценку, согласиться нельзя, и вот почему. Решая вопрос о виновности лица в совершении преступления, предусмотренного статьей 183 УК РФ, следует иметь в виду, что персональные данные являются конфиденциальной информацией, доступ к которой ограничен. Доказательством тому являются

---

[1] В юридической литературе теоретиками актуализируется проблема ответственности при виртуализированном соучастии, когда, к примеру, установлен только один из соучастников, а второй, заказавший услугу «слива» персональных данных в мессенджерах, неизвестен. См.: Русскевич Е.А. О некоторых аспектах квалификации соучастия в преступлениях в сфере компьютерной информации // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2019. № 3 (57). С. 30.

[2] Рос. газета. 2017. 31 июля.

[3] Дремлюга Р.И., Зотов С.С., Павлинская В.Ю. Критическая информационная структура как предмет преступного посягательства // Азиатско-Тихоокеанский регион: экономика, политика, право. 2019. № 21 (2). С. 133; Русскевич Е.А., Чекунов И.Г. Квалификация неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Уголовное право. 2022. № 5 (141). С. 28.

особые условия для работников на вход в информационную систему персональных данных клиентов (ИСПДн) операторов связи и др., включающие установление индивидуального логина и пароля для осуществления его служебных обязанностей. Прав М.А. Ершов, утверждая, что «клиентские базы коммерческих организаций, которые, главным образом, состоят из персональных данных клиентов, охраняются уголовным законом и подпадают под режим коммерческой тайны только в том случае, если в отношении них введён такой режим и при этом предпринимаются все усилия для того, чтобы эта информация не была доступна третьим лицам. Если же злоумышленник совершил посягательство на данную информацию, то он подлежит уголовной ответственности по ст. 183 УК РФ»[21]. Иными словами, сама система защиты информации подтверждает умышленные действия персонала, использовавшего личную или чужую учетную запись в системе управления абонентской базой для копирования и передачи личных данных. Разглашение путем передачи третьим лицам персональных данных клиентов организаций и компаний образует состав преступления, предусмотренный ст. 183 УК РФ в том числе и потому, что принимаемые на работу сотрудники дают обязательство о неразглашении сведений, составляющих охраняемую законом тайну – коммерческую, служебную и персональных данных (*такая оценка нашла поддержку у 92 % опрошенных респондентов*).

В силу бланкетности норм, предусмотренных ч. 2-4 ст. 183 УК РФ, следователь или суд должны привести названия и выходные данные локальных нормативных актов, которыми устанавливался режим коммерческой тайны[1].

Так, в обвинительном приговоре Чебаркульского городского суда Челябинской области в отношении специалиста офиса продаж и обслуживания ПАО «Вымпел-Коммуникации» Д. говорится о том, что он был обязан обеспечить соблюдение тайны в соответствии с обязательством о неразглашении информации ограниченного доступа, в том числе информации, составляющей коммерческую

---

[1] Крылова Н.Е., Леонтьев Б.М. Незаконные разглашение или использование сведений, составляющих коммерческую тайну: проблемы правоприменения // Вестник Московского университета. Серия 11: Право. 2017. № 3. С. 8.

тайну; трудовым договором, согласно которому признает, что он обязан не разглашать прямо или косвенно предоставляемые сведения, составляющие коммерческую, служебную, персональные данные и иную информацию ограниченного доступа, являющуюся таковой на основании внутренних документов работодателя; Порядком «Обращение с информацией ограниченного доступа», утвержденным президентом ПАО «Вымпел-Коммуникации»[1].

Другими словами, критерием определения границ незаконности разглашения персональных данных выступает режим коммерческой и других видов тайны, заключающийся в ограничениях и запретах в целях экономической безопасности хозяйствующего субъекта. В случаях соучастия лиц, не являющихся сотрудниками организаций, откуда произошла умышленная утечка персональных данных, квалификация содеянного в зависимости от роли каждого осуществляется по ст. 33 и ст. 183 УК РФ.

Тот же подход должен использоваться и в отношении банковской и налоговой тайны, однако если статьей 102 Налогового кодекса РФ персональные данные налогоплательщика и плательщика страховых взносов отнесены к налоговой тайне[2], то в Федеральном законе от 02.12.1990 № 395-1 «О банках и банковской деятельности» в понятие банковской тайны персональные данные клиентов банков не входят[3]. При этом банк обрабатывает персональные данные не только клиентов (потенциального клиента, партнера, контрагента), а работников банка, заемщика (залогодателя, поручителя, потенциального заемщика), которые находятся в автоматизированной банковской системе (АБС) и системе «Клиент-Банк»[4]. Разъясняя понятие тайны частной жизни,

---

[1] Приговор Чебаркульского городского суда Челябинской области от 26.12.2019 по делу № 1-349/2019 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/i8uMeLpvrKQh/?page=2&regular-court=&regular-date_from=&regular (дата обращения: 09.05.2023).

[2] Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ (с изм. и доп. от 04.08.2023, № 425-ФЗ) // Рос. газета. 1998. 6 авг.; 2023. 09 авг.

[3] О банках и банковской деятельности: федер. закон от 02.12.1990 № 395-1 (с изм. и доп. от 04.08.2023, № 417-ФЗ) // Рос. газета. 1996. 10 февр.; 2023. 8 авг.

[4] Бартошко Т.В., Стерхов А.П. Защита персональных данных как важная составляющая общей безопасности банка // Вестник Иркутского государственного технического университета. 2015. № 5 (100). С. 179.

Конституционный Суд РФ в п. 3 постановления от 14.05.2003 № 8-П отметил: «Из конституционных гарантий неприкосновенности частной жизни, личной тайны и недопустимости распространения информации о частной жизни лица без его согласия вытекают как право каждого на сохранение в тайне сведений о его банковских счетах и банковских вкладах и иных сведений, виды и объем которых устанавливаются законом, так и соответствующая обязанность банков, иных кредитных организаций хранить банковскую тайну, а также обязанность государства обеспечивать это право в законодательстве и правоприменении»[1]. Пробел в законе видится в том, что согласно ст. 857 «Банковская тайна» ГК РФ банк гарантирует тайну банковского счета и банковского вклада, операций по счету и *сведений о клиенте*. Именно потому при трудоустройстве сотрудники банков подписывают соглашения о служебной тайне, что трактуется судом как доказательство того, что она была доверена или стала известна по работе в банке.

Так, Искитимский районный суд Новосибирской области признал Б. виновной в незаконном разглашении и использовании сведений, составляющих банковскую тайну (ч. 2 ст. 183 УК РФ). Будучи кредитным специалистом в банке «Хоум Кредит энд Финанс Банк», она передала своей знакомой С. персональные данные клиента М. Используя их, С. подготовила фиктивный договор потребительского кредита на имя потерпевшей в «РусфинансБанке», а полученные деньги перевела на свой счет и поделила их с Б. Суд пришел к выводу, что Б. «умышленно разгласила и использовала без согласия владельца из корыстной заинтересованности данные, составляющие информацию ограниченного доступа, *содержащие банковскую тайну*, а именно данные о клиенте ООО «Хоум Кредит энд Финанс Банк», содержащие сведения о фамилии, имени, отчестве, дате и месте рождения, месте жительства, реквизиты паспорта, телефон, тем самым незаконно разгласила сведения, составляющие в ООО «Хоум Кредит энд Финанс Банк» банковскую тайну без согласия владельца, использовав

---

[1] Ершов М.А. Законы и иные нормативные правовые акты как юридический аргумент применения бланкетных норм об уголовной ответственности за посягательства на экономическую конфиденциальную информацию // Юридическая техника. 2013. № 7 (ч. 1). С. 120.

их в дальнейшем по своему усмотрению в целях получения денежных средств по договору потребительского кредита на имя М.»[1].

Данный подход по делам о преступлениях, предусмотренных ст. 183 УК РФ, применяется и в отношении сотрудников других коммерческих организаций.

К примеру, Кировским районным судом г. Ростова-на-Дону по ч. 3 ст. 30 ч. 3 ст. 183 УК РФ был осужден Г., системный администратор в ООО, который в период своей работы сделал резервную копию клиентской базы данных, сохранив ее на флэш-карте. При передаче флэш-карты и получения денежного вознаграждения от «конкурирующей» фирмы Г. был задержан. Суд решил, что действия Г., ознакомленного с приказом «Об утверждении положения о коммерческой тайне» и обязательством «О неразглашении коммерческой тайны», «могли нанести ООО тяжкие последствия в случае получения списка клиентов с их личными данными, сведениями об автомобилях и их повреждениях, стоимости и поставщиках автомобильных запчастей, в связи с чем конкуренты получили возможность предложить клиентам услуги по более низкой цене»[2].

Предъявляя обвинение по ст. 272 УК РФ, правоприменитель должен исходить из того, что субъектами рассматриваемого преступления являются лица, в том числе имеющие легальный доступ к закрытым базам данных клиентов (абонентов). В наработках общей теории уголовного права встречаются разные мнения об оценке его правомерности[3]. Согласимся с Е.А. Русскевичем в том, что неправомерным является доступ к компьютерной информации при совершении любых высокотехнологичных либо примитивно-бытовых действий, предоставляющих лицу возможность распоряжения информацией (ее уничтожение, модификация, блокирование, копирование) по собственному

---

[1] Приговор Искитимского районного суда Новосибирской области от 01.12.2016 по делу № 1-627/2016 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/IKwb4kGNFudC/?regular-txt=приговор+бубело&regular-case_doc=&regular (дата обращения: 04.02.2023).

[2] Приговор Кировского районного суда г. Ростова-на-Дону от 10.06.2011 по делу № 1-223 // Судебные и нормативные и акты РФ. URL: https://rospravosudie.com/court-kirovskij-rajonnyj-sud-g-rostova-na-donu-rostovskaya-oblast-s/act-102576386/ (дата обращения: 04.02.2023).

[3] Грибанова Д., Филатова М. Неправомерный доступ к сведениям, составляющим тайну, в России, США и Великобритании // Уголовное право. 2020. № 5. С. 15.

усмотрению без согласия на то законного владельца[1]. Вне зависимости от имеющейся учетной записи с личным паролем и логином для входа в информационную систему сотрудники банков, операторов мобильной связи, других коммерческих организаций и компаний не имеют права знакомиться с персональными данными, составляющими банковскую, коммерческую или налоговую тайны клиента, если это не связано с выполнением служебных обязанностей. Об этом говорят и тексты обвинительных заключений и приговоров. Признавая доступ к информационным системам неправомерным, суды усматривают обоснование вменения этого состава преступления в положениях локальных нормативных актов, с которыми был ознакомлен подсудимый при подписании трудового договора.

Так, в Порядке «Обращение с информацией ограниченного доступа» ПАО «Вымпел – Коммуникации», который был принят Серпуховским городским судом Московской области в качестве доказательства вины, указывается, что «работники должны запрашивать и получать доступ к документам с информацией ограниченного доступа только в пределах и объеме, необходимом для выполнения ими своих должностных обязанностей и при наличии согласия абонентов на предоставление третьим лицам сведений о них. … Запрещается копировать информацию ограниченного доступа, в том числе содержащую персональные данные, на не принадлежащие компании информационные ресурсы; передавать информацию ограниченного доступа любыми способами, в том числе через Интернет, по электронной почте либо с помощью компьютерных носителей информации; передавать информацию ограниченного доступа, в том числе персональные данные, по каналам связи сети общего пользования и сети Интернет, включая системы обмена сообщениями без соответствующих разрешений и применения мер и средств защиты информации»[2].

---

[1] Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. ... д-ра юрид. наук. М., 2021. С. 252.

[2] Приговор Серпуховского городского суда Московской области от 14.01.2019 по делу № 1-27/2019 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/XikJ89Z5aBJ0/?page=5&regular (дата обращения: 04.02.2023).

Другой значимой проблемой квалификации преступлений, совершаемых с персональными данными, является возможность вменения служебного положения в случаях неправомерного доступа к информационным системам, когда деяние объективно совершено лицом, которое осуществило несанкционированный вход в ИСПДн с использованием своих возможностей по службе или работе. В уголовно-правовой науке давно предложен новый подход к оценке деяний лиц, являющихся сотрудниками организаций, не наделенными организационно-распорядительными или административно-хозяйственными функциями. Их, по мнению правоведов, следует относить к иным служащим организаций независимо от формы собственности, то есть не признавать использование ими служебного положения[1]. Вместе с тем судебные приговоры демонстрируют осуждение рядовых специалистов по обслуживанию клиентов, имеющих доступ к базам данных в результате выполняемой работы (по трудовому, гражданско-правовому договору), неправомерно копировавших и распространяющих личные сведения.

К примеру, Дзержинский районный суд г. Новосибирска вынес обвинительный приговор, в котором указал: «Квалифицирующий признак «с использованием своего служебного положения» по всем эпизодам преступной деятельности нашёл своё полное подтверждение в ходе судебного разбирательства, поскольку совершение всех преступлений стало возможным при наличии у Н. доступа в силу занимаемой должности правомочий по доступу к информационному массиву данных, содержащих сведения как частной жизни лиц, составляющих их личную тайну, так и о телефонных переговорах (ИСПДн)»[2].

Из этих соображений, учитывая, что именно у работника имеется возможность войти (под своим или чужим паролем) в такую систему для совершения преступления, обвинение, на наш взгляд, должно включать признак

---

[1] Егорова Н.А. Ответственность за «служебные» мошенничества: необходимость новых подходов // Российская юстиция. 2014. № 8. С. 20.

[2] Приговор Дзержинского районного суда г. Новосибирска от 02.10.2017 по делу № 1-389/2017 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/kN7MkWMrBlUK/?regular-txt=Необутова+приговор&regular-case_doc=&regular (дата обращения: 09.05.2023).

использования лицом своего служебного положения (ч. 3 ст. 272 УК РФ)[1]. Прав Е.А. Русскевич в том, что «проблема более строгой ответственности лиц, обязанных в силу выполняемых ими трудовых функций, соблюдать и (или) обеспечивать информационную безопасность организации, требует отказа от классического (ограничительного) толкования лиц, использующих служебное положение, и отнесения к данной категории по сути любых сотрудников, которые на законных основаниях используют компьютерную информацию компании или учреждения, а также средства ее обращения (системные инженеры, программисты, менеджеры, продавцы-консультанты и специалисты по обслуживанию клиентов, обладающие полномочиями по использованию баз данных и др.)[2]. В пользу такого квалификационного решения говорят и разъяснения Генеральной прокуратуры Российской Федерации[3].

Исследователи задаются и другим логичным вопросом, если данные составляют одну из тайн в контексте ст. 183 УК РФ, разве они перестают подлежать охране по ст. 137 и (или) 138 УК РФ, если речь идет о разных потерпевших и разных объектах?[4] Как представляется, в любых случаях передачи третьим лицам, а значит и разглашения, персональных данных сотрудниками кредитных и иных государственных или коммерческих организаций вне выполнения служебных обязанностей нарушается неприкосновенность личной информации. А все потому, что клиент или абонент не давал согласия на ознакомление с его персональными данными работниками юридических лиц, их

---

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 // Рос. газета. 2022. 28 дек.

[2] Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. ... д-ра юрид. наук. М., 2021. С. 271; Русскевич Е.А. О квалификации преступлений в сфере компьютерной информации, совершаемых с использованием служебного положения // Российское правосудие. 2019. № 2. С. 37.

[3] Методические рекомендации Генеральной прокуратуры Российской Федерации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. Доступ из Справ.-прав. системы «КонсультантПлюс».

[4] Филатова М.А. Персональные данные как предмет преступного посягательства журнал // Уголовное право. 2021. № 11. С. 41.

использование и передачу помимо тех целей, для которых он стал потребителем той или иной услуги. Отказ от идеальной совокупности со ст. 137 и ст. 138 УК РФ по делам, связанным с охраны коммерческой, налоговой или банковской тайны, где предметом преступлений являлись персональные данные, объясняется тем, что правоприменитель «при конкуренции тайн» толкует их вменение как двойную вину. В пользу такой уголовно-правовой оценки говорит и неоднозначность признания персональных данных тайной личной жизни по смыслу ст. 137 УК РФ, сводимому к узкому пониманию правоохранителями персональных данных как разновидности банковской, налоговой или коммерческой тайны. Разрешению проблемы неполноты квалификации посягательств, связанных с персональными данными, будет способствовать выделение в уголовном законе специальной нормы о защите персональных данных (*такой вывод нашел поддержку у 86 % опрошенных экспертов*).

Следственно-судебная практика свидетельствует и об отсутствии унифицированного толкования деяний, связанных с персональными данными, когда фигурантами уголовных дел становятся сотрудники правоохранительных органов. От усмотрения правоприменителя зависит квалификация действий тех полицейских, которые, имея доступ к информационным базам данных МВД, ГИБДД РФ, незаконно передавали их другим лицам, в том числе за денежное вознаграждение. Как показывают изученные правоприменительные акты, к уголовно-правовой оценке однородных деяний с аналогичными обстоятельствами также имеется несколько подходов, когда виновному вменяется:

1) *получение взятки* (ст. 290 УК РФ). К примеру, Ленинский районный суд г. Комсомольска-на-Амуре Хабаровского края вынес обвинительный приговор по ч. 3 ст. 290 УК РФ в отношении сотрудника полиции Г. Судом установлено, что Г. получил взятку в размере 35 тыс. руб. за передачу работнику ритуального агентства персональных данных семи умерших граждан на территории

обслуживания, ставших ему известными в связи с выполнением служебных обязанностей[1];

2) *злоупотребление полномочиями* (ст. 285 УК РФ)[2] (фабула приговора приводилась в §3 главы I);

3) *превышение полномочий (ст. 286 УК РФ)*[3] (фабула приговора приводилась в §3 главы I);

4) *получение взятки (ст. 290 УК РФ) и неправомерный доступ к компьютерной информации (ч. 3 ст. 272 УК РФ)*.

Например, Жуковским районным судом Брянской области С. признан виновным в совершении преступлений, предусмотренных ч. 3 ст. 272 и п. «в» ч. 5 ст. 290 УК РФ. Являясь помощником оперативного дежурного дежурной части МО МВД России «Жуковский», С., находясь в служебном помещении, используя логины и пароли оперативных дежурных, незаконно, не менее 1470 раз, выгрузил из ИПС «Следопыт-М» информацию в виде досье в отношении не менее 1366 потерпевших, содержащих их персональные данные (анкетные, паспортные, фотоснимки, сведения об имуществе, транспортных средствах, информацию о привлечении к административной ответственности). Скопировав конфиденциальную информацию со служебного компьютера на мобильный телефон при помощи USB-кабеля и путем фотографирования изображения информации с экрана компьютера, С. при помощи интернет-мессенджера передавал ее неустановленному лицу, за что получил путем безналичного

---

[1] Приговор Ленинского районного суда г. Комсомольска-на-Амуре от 27.05.2020 по делу № 1-47/2020 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/5w1bXYMWarN8/?regular (дата обращения: 08.02.2023).

[2] Приговор Тбилисского районного суда Краснодарского края от 11.07.2019 по делу № 1-125/2019 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/gGB9phbVHUg0/?regular (дата обращения: 08.02.2023).

[3] Рассмотрено уголовное дело в отношении бывших сотрудников полиции, которые продавали персональные данные граждан // Прокуратура Нижегородской области. URL: https://epp.genproc.gov.ru/web/proc_52/mass-media/news/archive?item=46470953 (дата обращения: 09.02.2023).

перевода на его электронное средство платежа в качестве взятки денежные средства в сумме 573200 руб.[1];

5) *нарушение неприкосновенности частной жизни (ч. 2 ст. 137 УК РФ) и злоупотребление должностными полномочиями (ч. 1 ст. 285 УК РФ)*.

Так, участковому инспектору одного из райотделов полиции в Челябинской области было предъявлено обвинение по указанным статьям за продажу персональных данных двух человек из базы данных МВД РФ[2]. По другому уголовному делу Центральный районный суд г. Новосибирска признал С., инспектора патрульно-постовой службы отдела полиции № 1 «Центральный» УМВД России по г. Новосибирску, виновным по ч. 1 ст. 285 УК РФ в злоупотреблении должностными полномочиями (56 эпизодов) и по ч. 2 ст. 137 УК РФ в нарушении неприкосновенности частной жизни по ч. 2 ст. 137 УК РФ (56 эпизодов). Из текста приговора следует, что С. «по просьбе своих знакомых из иной личной заинтересованности, выразившейся в желании сохранить с ними дружеские отношения и создать взаимовыгодные условия дальнейшего сотрудничества, злоупотребляя своими полномочиями», копировал из базы ИЦ ГУ МВД России составляющие личную тайну персональные данные третьих лиц на электронный носитель. Затем подсудимый передавал собранную на электронный носитель информацию о персональных данных 56 человек, составляющую их личную тайну, с использованием своего электронного почтового адреса в сети «Интернет» на адрес электронной почты заказчиков. Суд пришел к выводу, что «своими преступными действиями С. существенно нарушил права и интересы граждан на защиту персональных данных, охраняемых ст. 24 Конституции РФ и федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», а также охраняемые законом интересы общества и государства в сфере правоохранительной деятельности, регламентированные ст.

---

[1] Приговор Жуковского районного суда Брянской области от 21.05.2020 по делу № 1-127/2019 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/Jir03EOSNHgb/?regular (дата обращения: 04.02.2023).

[2] В Челябинской области будут судить полицейского за слив данных из базы МВД // Комсомольская правда. Челябинск. URL: https://www.chel.kp.ru/online/news/4713959/ (дата обращения: 04.02.2023).

ст. 2, 17, 24 Конституции РФ, ст. 5 ФЗ «О полиции». По каждому эпизоду имеется идеальная совокупность двух преступлений – ч. 2 ст.137 «Нарушение неприкосновенности частной жизни с использованием служебного положения» УК РФ и ч. 1 ст. 285 «Злоупотребление должностными полномочиями» УК РФ»[1];

6) *нарушение неприкосновенности частной жизни с использованием служебного положения (ч. 2 ст. 137 УК РФ)*.

Так, приговором Белозерского районного суда Курганской области по ч. 2 ст. 137 УК РФ осужден Ю., занимавший должность дознавателя отдела полиции № 6 УМВД России по г. Тюмени, который под своим паролем зашел в базу «ИДБ-Регион» и нашел полные данные потерпевшего, его супруги и сына. Затем, используя логин и пароль своего коллеги, Ю. вошел в базу ФИС «ГИБДД-М», доступа к которой не имел, и скопировал сведения о зарегистрированных на членов семьи потерпевшего автотранспортных средствах. Полученные данные он передал своему знакомому Н. по его просьбе[2].

При аналогичных обстоятельствах прокуратурой Калининского района г. Тюмени в отношении сотрудника полиции было утверждено обвинительное заключение по ч. 2 ст. 137 УК РФ, который по просьбе своего знакомого предоставил сведения о местонахождении и передвижении жителя г. Тюмени[3].

Во всех приведенных примерах с копированием и передачей сведений, которые относятся к персональным данным, возникает вопрос, не толкуют ли суды чрезмерно широко или, напротив, ограничительно, деяния специальных субъектов, усматривая в них и получение взятки, и злоупотребление или превышение должностных полномочий, и неправомерный доступ к компьютерной информации? Правоприменительные акты обнаруживают

---

[1] Приговор Центрального районного суда г. Новосибирска от 07.12.2012 по делу № 1-566/2012 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/mdwYfSwTqVYB/?page=2&regular-court=&regular (дата обращения: 04.02.2023).

[2] Кассационное определение Седьмого кассационного суда общей юрисдикции от 10.06.2020 № 77-889/2020 // Доступ из Справ.-прав. системы «КонсультантПлюс».

[3] В Тюмени перед судом предстанет сотрудник полиции по обвинению в незаконном распространении информации в отношении местного жителя // Прокуратура Тюменской области. URL: https://epp.genproc.gov.ru/web/proc_72/mass-media/news?item=74056760 (дата обращения: 10.04.2023).

примеры, когда следственно-судебные органы не признают наличия служебного положения при совершении компьютерного преступления сотрудником полиции. Сам доступ к информационным базам данных не квалифицируется как неправомерный потому, как следует из приговоров, осужденный имел право доступа к ним в связи с занимаемой должностью и присвоением соответствующих логина и пароля.

Например, осуществляя переквалификацию содеянного В. на ч. 1 ст. 285 УК РФ, Тбилисский суд Краснодарского края обосновал ее следующим образом: «Действия В. по предоставлению лицам, не являющимся работниками правоохранительных органов, сведений, содержащихся в ИПС «Следопыт-М», которые подлежали использованию исключительно в служебных целях, не входило в круг его должностных обязанностей. В. фактически совершены действия, которые хотя и были связаны с осуществлением им своих прав и обязанностей, поскольку он имел доступ в силу занимаемой должности к ИПС «Следопыт-М», однако его действия по предоставлению сведений из этой информационно-поисковой системы сторонним лицам не вызывались служебной необходимостью и противоречили как общим задачам и требованиям, предъявляемым к сотруднику полиции, так и тем целям и задачам, для достижения которых сотрудники полиции наделены своими должностными полномочиями, потому его действия подлежат квалификации по ч. 1 ст. 285 УК РФ»[1].

Иной является позиция судов, усматривающих в деянии сотрудников полиции неправомерный доступ к компьютерной информации вне зависимости, использовал ли виновный свои данные для входа в систему или чужие. Использование должностным лицом своих служебных полномочий отнюдь не исключает вменения ч. 3 ст. 272 УК РФ.

Так, Жуковский районный суд Брянской области признал неправомерным доступ С. к персональным данным физических лиц, размещенных в

[1] Приговор Тбилисского районного суда Краснодарского края от 11.07.2019 по делу № 1-125/2019 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/gGB9phbVHUg0/?regular (дата обращения: 08.02.2023).

Информационно-поисковом сервисе, разработанном в интересах оперативных подразделений МВД РФ «Следопыт-М» в соответствии с п. 4 Регламента доступа к нему. Он гласит, что при работе с ИПС не допускается использовать доступ к его информационным ресурсам и электронным базам *в целях, не связанных с выполнением служебных обязанностей*, *распространять сведения, полученные с использованием его информационных ресурсов и электронных баз*, за исключением случаев, предусмотренных законодательством РФ. Квалифицируя действия С. по эпизоду неправомерного доступа к компьютерной информации, суд указал, что подсудимый, *не обладая необходимыми полномочиями*, *использовал возможность получения компьютерной конфиденциальной информации* – персональных данных физических лиц, размещенных в ИПС и переносил копии полученной им информации на другой носитель[1].

При таких обстоятельствах следует принять за основу следующее правило квалификации. Действия должностных лиц правоохранительных органов, состоящие в неправомерном доступе к ведомственным информационно-поисковым системам (базам данных), должны быть квалифицированы по ч. 3 ст. 272 УК РФ как использование своего служебного положения вне зависимости от наличия или отсутствия легального доступа к компьютерной информации (собственный или других лиц логин и пароль)[2].

Дополнительной квалификации по ст. 285 или ст. 286 УК РФ не требуется, потому что копирование персональных данных вопреки интересам службы является специальной формой злоупотребления должностными полномочиями в силу имеющейся у обвиняемого возможности получить чужие персональные

---

[1] Приговор Жуковского районного суда Брянской области от 21.05.2020 по делу № 1-127/2019 // Судебные и нормативные и акты РФ. URL: https://sudact.ru/regular/doc/Jir03EOSNHgb/?regular (дата обращения: 04.02.2023).

[2] Хохлова Е.В. О практике квалификации преступлений с персональными данными // Уголовное законодательство: вчера, сегодня, завтра: матер. междунар. науч.-практ. конф. (9–10 июня 2023 г.) / ред. кол.: Т.А. Огарь (отв. ред.) [и др.]. СПб.: Изд-во С.-Петерб. ун-та МВД России, 2023. С. 287.

данные в связи с занимаемой должностью[1]. Как верно отмечает Е.А. Русскевич, в подобных случаях часть 3 ст. 272 УК РФ точнее выражает направленность деяния, а также более полно описывает его признаки. В силу ч. 1 ст. 17 УК РФ подобного рода действия должностных лиц полностью охватываются ч. 3 ст. 272 УК РФ и дополнительной квалификации по ст. 285 УК РФ или ст. 286 УК РФ не требуют[2].

Вместе с тем совокупность преступлений наличествует, если за копирование персональных данных и их передачу, которые не были обусловлены служебной необходимостью, сотрудник правоохранительных органов получил денежное вознаграждение. В подобных обстоятельствах диспозиции ч. 3 ст. 272 УК РФ и ст. 290 УК РФ точнее всего характеризуют признаки деяний, совершенных лицами, использующими свое служебное положение для копирования персональных данных с их передачей за плату.

Таким образом, в целях совершенствования уголовно-правовой оценки незаконных действий с персональными данными автором сформулированы *следующие выводы*:

1. При незаконном копировании и передаче персональных данных из информационных систем правоохранительных органов должностным лицом содеянное следует квалифицировать по части 3 статьи 272 УК РФ как неправомерный доступ к компьютерной информации с использованием своего служебного положения. В частности, как использование служебного положения должны квалифицироваться действия виновного, которые не вызывались служебной необходимостью (отсутствовали обязательные условия или основания для их совершения) и противоречили целям и задачам службы, для достижения которых должностное лицо правоохранительного органа было наделено соответствующими служебными полномочиями (доступ к информационной системе персональных данных с получением персонального логина и пароля).

---

[1] См. подроб.: Борков В.Н. Квалификация должностных преступлений. М.: Юрлитинформ, 2018. С. 110; Рясов А.В. Понятие и сущность признака «использование служебного положения» в российском уголовном праве // Юристъ-Правоведъ. 2007. № 6 (25). С. 22 и др.

[2] Русскевич Е.А. Указ. соч. С. 272.

Решая вопрос о квалификации по статье 272 УК РФ, надлежит выяснять, какими именно ведомственными документами (должностные инструкции, иные локальные нормативные акты) установлены права и обязанности обвиняемого в копировании и передаче персональных данных должностного лица, злоупотребление какими из этих прав и обязанностей вменяется ему в вину со ссылкой на конкретные нормы (статью, часть, пункт).

Наличие у виновного официального доступа к информационной системе персональных данных (собственный логин и пароль) не исключает возможности его осуждения по статье 272 УК РФ, поскольку им совершены незаконные действия, связанные с неправомерным доступом к персональным данным, имевшие целью их копирование и последующую передачу третьим лицам вопреки интересам службы. Если использование должностным лицом своих служебных полномочий выразилось в незаконном копировании персональных данных, когда фактически произошло их незаконное распространение, содеянное дополнительно не подлежит квалификации по статье 137 УК РФ или статье 138 УК РФ.

Получение должностным лицом незаконного вознаграждения за копирование и передачу персональных данных из ведомственных информационных систем надлежит квалифицировать как получение взятки по статье 290 УК РФ. Совершение должностным лицом указанных действий за взятку образует самостоятельный состав преступления, однако не охватывается объективной стороной преступлений, предусмотренных статьей 290 УК РФ. В таких случаях содеянное взяткополучателем подлежит квалификации по совокупности преступлений как получение взятки за незаконные действия по службе и по части третьей статьи 272 УК РФ как неправомерный доступ к компьютерной информации с использованием служебного положения.

2. Действия лица, имевшего на законных основаниях доступ к компьютерной информации в результате выполняемой работы (трудовой, гражданско-правовой договор), надлежит квалифицировать по статье 272 УК РФ, если установлено, что им совершен неправомерный доступ к компьютерной

информации в специализированной системе (служебных программах и информационно-поисковых базах данных), с целью копирования и передачи (распространения) персональных данных клиентов (абонентов). Неправомерным следует признавать доступ к компьютерной информации для получения и (или) использования персональных данных без согласия их обладателя виновным, не наделенным необходимыми для этого полномочиями (отсутствие специального (авторизованного) доступа) либо в нарушение установленного нормативными правовыми актами его условий и порядка независимо от формы такого доступа. Осуществление указанными лицами технических функций (администраторы баз данных, инженеры, специалисты, служащие банков, офисов продаж операторов мобильной связи) при наличии к тому оснований не исключает уголовную ответственность по части 3 статьи 272 УК РФ за использование своего служебного положения. Решая вопрос о квалификации содеянного по статье 272 УК РФ, надлежит установить, осуществляло ли лицо неправомерный доступ к персональным данным вопреки специальному режиму защиты сведений, составляющих персональные данные, а также коммерческую, служебную, личную, семейную или иную тайну, а также возложена ли на это лицо обязанность соблюдать указанные правила.

При установлении обязанности соблюдения лицом конфиденциальности такой информации и предупреждении об ответственности за разглашение в целях обеспечения ее неприкосновенности в соответствии с локальными нормативными актами коммерческой или иной организации (трудовой договор, должностные инструкции, порядок обращения с информацией ограниченного доступа, обязательство о неразглашении информации ограниченного доступа, в том числе составляющей коммерческую, налоговую, служебную тайны, тайну персональных данных), содеянное следует дополнительно квалифицировать по статье 183 УК РФ.

3. Действия лица квалифицируются по статье 274^1 УК РФ, если установлено, что информационная система (база данных) правоохранительных органов, кредитно-финансового учреждения, мобильного оператора и других

государственных или коммерческих учреждений и организаций относится к объекту критической информационной инфраструктуры и включена в Реестр значимых объектов критической информационной инфраструктуры (ст. 8 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»). В ином случае действия лица при наличии на то оснований квалифицируются по статье 272 УК РФ.

§ 2. Концептуальная модель уголовно-правовой охраны персональных данных (de lege ferenda)

Идея введения уголовной ответственности за совершение с персональными данными или в отношении них незаконных действий стала предметом научных споров задолго до принятия федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»[1], а появление правового института персональных данных только активизировало дискуссию в научных кругах. Одни юристы критикуют нерасторопность законодателя за отсутствие прямой нормы, устанавливающей наказание за незаконные собирание или распространение персональных данных[2]. На их взгляд, этот пробел уголовного закона является «существенным упущением в условиях развивающегося информационного общества, когда подобного рода информация приобретает все большую ценность»[3]. Сторонники такого подхода считают необходимым конструирование отдельной уголовно-правовой нормы, предметом которой будут персональные данные, ссылаясь на то, что они «фактически остаются незащищенными»[4]. Так,

---

[1] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (с изм. и доп. от 06.02.2023, № 8-ФЗ) // СЗ РФ. 2006. № 31 (ч. I), ст. 3451; Рос. газета. 2023. 9 февр.

[2] Чукреев В.А. Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны // Вестник Университета имени О.Е. Кутафина (МГЮА). 2022. № 3 (91). С. 116; Рязанова Е.Н. Ответственность за распространение персональных данных как способ противодействия правонарушениям в сфере информационно-коммуникационных технологий // Вестник Санкт-Петербургского университета МВД России. 2022. № 3 (95). С. 123.

[3] Губарева А.В., Гулемин А.Н. Угрозы безопасности персональных данных: проблемы современности // Политика и общество. 2015. № 2. С. 154.

[4] Кадников Б.Н. Уголовно-правовая охрана неприкосновенности частной жизни: научно-практическое пособие / под ред. Н.Г. Кадникова. 2-е изд., доп. М.: Юриспруденция, 2017. С. 49.

В.В. Вабищевич, отвергая соподчиненность понятия персональных данных категории «частная жизнь», предлагает совершенствование уголовного закона «путем формирования нового состава преступления, диспозицией которого станут неправомерные посягательства на персональные данные как на самостоятельный объект уголовно-правовой защиты»[1].

Представители второй группы исследователей считают более выверенной модернизацию редакции уже имеющегося в ст. 137 УК РФ состава преступления путем наделения его диспозиции конструктивными и квалифицирующими признаками[2]. Такая новелла, по мнению ученых, повлечет изменение названия статьи 137 УК РФ «Нарушение неприкосновенности частной жизни и законодательства Российской Федерации о персональных данных и их защите»[3]. Разделяя убеждения о специальной криминализации деяний, совершаемых с персональными данными или против них, отметим, что основным аргументом, из которых мы исходим, служит, *во-первых*, неодинаковость по объему понятий «частная жизнь» и «персональные данные» при содержательном их совпадении в какой-то части, о чем подробно говорилось в §2 главы II.

Во-вторых, расширение границ общественной опасности уже криминализированных деяний не позволяет осуществлять эффективное противодействие преступлениям, связанным с персональными данными. Объяснением тому служит трансформация преступности, связанной с личными данными человека, которая во многом обусловлена инновационными технологическими трендами, позволяющими накапливать, хранить и обрабатывать огромные объемы информации об индивиде. Общественная опасность преступлений, посягающих на сохранность закрытых для общего

---

[1] Вабищевич В. В. Персональные данные: пределы и объем их уголовно-правовой охраны // Вестник Гродненского государственного университета имени Янки Купалы. Серия 4. Правоведение. 2020. Т. 10, № 2. С. 84.

[2] Новиков В. Понятие частной жизни и уголовно-правовая охрана ее неприкосновенности // Уголовное право. 2011. № 1. С. 43; Карелин Д.В., Мацепуро Д.М., Селита Ф. Уголовно-правовая охрана генетических данных человека: к постановке проблемы // Вестник Томского государственного университета. Право. 2018. № 29. С. 90.

[3] Шутова А.А. Социальная обусловленность существования норм об уголовной ответственности за посягательства на персональные данные // Вестник Нижегородской академии МВД России. 2015. № 4 (32). С. 334.

доступа личных данных, выражается не только в угрозах новых массовых криминальных эксцессов против них. Она отличается высокой долей концентрации в таких деяниях отдаленных разрушительных последствий, с большей вероятностью способных причинить тяжкий вред иным охраняемым отношениям. В связи с негативной тенденцией «монетизации» от сбыта чужих персональных данных и сверхизменчивости «цифровой» преступности требуется переосмысление социальной ценности личных благ, касающихся приватности персональных данных человека, и переоценка предупредительного потенциала имеющихся в уголовном законе средств их защиты. Как пишет М.А. Ефремова, становление информационного общества в России требует переосмысления иерархии охраняемых уголовным законом общественных отношений, что должно, на наш взгляд, учитываться при определении местоположения и содержания составов преступлений, обеспечивающих защиту конфиденциальности и в виртуальном пространстве[1]. Думается, что ревизия эффективности имеющихся уголовно-правовых запретов, напрямую не связанных с нарушением неприкосновенности персональных данных, должна осуществляться посредством формулирования нового, специального состава преступления, предметом уголовно-правовой охраны которого будут именно персональные данные.

В-третьих, следует учитывать и неэффективность гражданско- и административно-правовых средств борьбы с нарушениями, связанными с персональными данными человека, и отсутствие аналога состава правонарушения в КоАП РФ, предметом охраны которого выступают персональные данные с запретом их собирания или распространения. Ст. 13.11 «Нарушение законодательства РФ в области персональных данных» КоАП РФ предусматривает ответственность за нарушение правил обработки персональных данных. По ст. 17.13. «Незаконное распространение сведений о защищаемых лицах» КоАП РФ осуществляется защита персональных данных не всех граждан, а судей, прокурорских работников, следователей, лиц, производящих дознание,

[1] Ефремова М.А. Социальная обусловленность уголовно-правовой охраны информационной безопасности Российской Федерации // Вестник Пермского университета. Юридические науки. 2017. № 36. С. 224.

сотрудников МВД, ФСБ, органов государственной охраны, внешней разведки РФ, Следственного комитета РФ, военнослужащих и др. Имеющиеся в арсенале административного законодательства составы правонарушений не обладают достаточным превентивным потенциалом для предупреждения противоправных деяний, связанных с персональными данными, хотя бы потому, что применяемые размеры штрафов не способны обеспечить их надлежащую охрану. По ч. 6 ст. 13.11 КоАП РФ в случае необеспечения сохранности персональных данных, если это повлекло в том числе распространение либо иные неправомерные действия в отношении персональных данных, первый штраф для юридических лиц составляет от пятидесяти тысяч до ста тысяч рублей. Так, штраф, который назначил суд по ст. 13.11 КоАП РФ компании «Гемотест» за утечку 30 млн личных данных клиентов, составил всего 60 тыс. руб.[1]

О том, что только административно- и гражданско-правовыми мерами обеспечить защиту граждан от незаконного доступа и оборота их персональных данных невозможно, подтверждает и неэффективность административных средств борьбы с правонарушениями в этой сфере. В 2021 г. Роскомнадзором выявлено, что из 3,9 тыс. контрольных проверок операторов при обработке персональных данных граждан более 80 % допускали несоблюдение законодательства о защите персональных данных (не назначен ответственный за обработку, нет организованного внутреннего контроля и необходимых мер безопасности, правовых оснований для обработки данных). По этим фактам Росреестром составлено всего 220 протоколов о привлечении к административной ответственности по выявленным нарушениям требований Федерального закона «О персональных данных», а в АИС «Реестр нарушителей прав субъектов персональных данных» на основании судебных решений включено 93 ресурса. Для сравнения в этот же год была допущена масштабная компрометация личных данных ГИБДД РФ (данные 50 млн автовладельцев (имена, даты рождения, номера телефонов, VIN-коды и номера машин, их марки и модели, а также год

[1] «Гемотест» оштрафовали на 60 тыс. руб. за утечку персональных данных // Коммерсантъ. URL: https://www.kommersant.ru/doc/5480244 (дата обращения: 17.08.2022).

постановки на учет))[1]; сайтом компании Hyundai (1,3 млн автовладельцев)[2]; «Яндекс» (5 тыс. e-mail пользователей)[3]; компанией Oriflame (1,5 млн паспортов)[4]. Очевидно, что административно-правовых средств, направленных на минимизацию уровня преступлений с персональными данными, совершаемых посредством и в отношении них, недостаточно. Вместе с тем изложенные суждения позволяют уточнить авторскую позицию о нецелесообразности введения состава административного правонарушения, включающего только сами противоправные деяния (собирание или распространение) в отношении персональных данных с точки зрения потребностей правоприменительной практики для предупреждения преступлений. Масштабность проблемы защиты информации ограниченного доступа в России со всей очевидностью свидетельствует о необходимости и оправданности установления именно уголовно-правовых запретов в отношении деяний, совершаемых с использованием персональных данных человека или против них. Пробел в части ответственности за противоправные деяния с личной информацией должен быть восполнен дополнением УК РФ соответствующим составом преступления.

В-четвертых, на процесс криминализации посягательств в отношении личной информации с ограниченным доступом существенное влияние оказывают и социально-психологические основания, включающие правовые традиции, обычаи, характер межличностного общения, уровень правосознания, а также приоритетные в обществе социальные ценности и интересы[5]. А.И. Коробеев справедливо замечает, что уголовно-правовой запрет должен соответствующим

---

[1] РКН начал расследование утечки базы данных водителей Москвы и Подмосковья // РБК: URL: https://www.rbc.ru/technology_and_media/25/10/2021/6175eeb89a794778b01c0189 (дата обращения: 27.08.2022).

[2] СМИ узнали об утечке базы данных 1,3 млн российских клиентов Hyundai // РБК. URL: https://www.rbc.ru/technology_and_media/11/01/2021/5ffbf4af9a79476933c5f164 (дата обращения: 27.08.2022).

[3] «Яндекс» сообщил об утечке данных 5 тыс. почтовых ящиков // РБК. URL: https://www.rbc.ru/technology_and_media/12/02/2021/602645dc9a79472c62786d55 (дата обращения: 27.08.2022).

[4] Хакеры продают сканы паспортов 1,5 млн россиян, украденных у компании Oriflame: эксперт рассказал, что грозит жертвам // Комсомольская правда. URL:: https://www.kp.ru/daily/28321/4464204/ (дата обращения: 28.11.2022).

[5] Бодаевский В.П., Соловьёв Е.А. Социальная обусловленность уголовно-правового положения // Научный вестник Омской академии МВД России. 2020. № 1 (76). С. 22.

образом восприниматься общественной психологией и правосознанием[1]. К тому же обществом должна осознаваться и необходимость такого запрета, оценка его как преступления. Результаты опроса ВЦИОМ подтверждают, что россияне усматривают особую опасность в получении и использовании своих персональных данных третьими лицами, их передаче от одних компаний к другим в коммерческих и иных целях. 59 % соотечественников информированы о возможности передачи личных данных третьим лицам; 70 % россиян относятся к этому отрицательно; 58 % респондентов считают, что доступ третьих лиц к их данным может представлять для них личную угрозу[2]. А потому фиксируется ежегодный рост количества обращений по данным фактам в госорганы[3]. Если в 2020 г. в Роскомнадзор поступило 42255 жалоб граждан на владельцев интернет-сайтов (в т.ч. социальных сетей), организаций ЖКХ, кредитных учреждений, коллекторских агентств за неправомерное размещение их персональных данных в сети Интернет, передачу банками коллекторам личных данных без согласия граждан и обработку коллекторскими агентствами персональных данных граждан без их согласия, то в 2021 г. их зарегистрировано уже 49939[4]. В исследовании платформы онлайн-рекрутинга hh.ru и веб-браузера Vivaldi отмечается, что наши сограждане более всего опасаются за потерю паспортных и банковских данных (90 % опрошенных). «Чувствительной» для респондентов является и утрата конфиденциальной информации о месте жительства и доходах (70 %), а также данных о детях – 58 %[5].

В-пятых, отдельной защиты персональных данных требуют международно-правовые стандарты охраны персональных данных человека.

---

[1] Коробеев А.И. Советская уголовно-правовая политика: проблемы декриминализации и пенализации. Владивосток: Изд.-во Дальневост. ун-та, 1987. С. 67.

[2] Персональные данные в интернете: угроза утечки и как с ней бороться // ВЦИОМ. URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/personalnye-dannye-v-internete-ugroza-utechki-i-kak-s-nei-borotsja (дата обращения: 17.08.2022).

[3] Россияне стали чаще жаловаться на незаконное использование их персональных данных // Ведомости. URL: https://www.vedomosti.ru/technology/articles/2019/07/22/807016-rossiyane-personalnih (дата обращения: 17.08.2022).

[4] Итоги работы с обращениями граждан в Роскомнадзоре в 2021 году // Роскомнадзор. URL: https://rkn.gov.ru/treatments/p436/ (дата обращения: 17.08.2022).

[5] Россияне испугались кражи личных данных и перешли на VPN // News. URL: https://news.mail.ru/society/49789704/ (дата обращения: 11.09.2022).

Среди правовых оснований криминализации деяний, посягающих на безопасность персональных данных человека, особое значение приобретают положения международных актов. Мировым сообществом фундаментальное право на неприкосновенность частной жизни, включая право на защиту персональных данных, признается особо охраняемой категорией, о чем провозглашается в преамбуле Конвенции Совета Европы «О защите личности в связи с автоматизированной обработкой персональных данных» (далее Конвенция 108)[1]. Государства, ее подписавшие, «исходят из необходимости *расширения гарантий права на уважение частной жизни*, вызванной увеличением трансграничного потока персональных данных, подвергающихся автоматизированной обработке». Они подтверждают приверженность свободе информации, невзирая на границы, и признают необходимость уважения неприкосновенности частной жизни и свободного обмена информацией между народами. Как участница Конвенции 108 с 2001 г. Российская Федерация, ратифицировавшая ее федеральным законом от 19.12.2005 № 160-ФЗ[2], возложила на себя международно-правовые обязательства по принятию надлежащих санкций по защите личных данных национальным правом[3].

Подписала Россия и принятый через тридцать семь лет протокол Совета Европы о внесении изменений в Конвенцию 108[4], внесший множество поправок в правовой механизм защиты персональных данных физических лиц в рамках национальных юрисдикций и в том числе при их трансграничной передаче. Цель новаций – дополнение правил по перемещению потоков данных личного характера с учетом возросших угроз использования новых информационных и

---

[1] Конвенция о защите физических лиц при автоматизированной обработке персональных данных: заключена в Страсбурге 28.01.1981. Доступ из Справ.-прав. системы «КонсультантПлюс».

[2] О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных: федер. закон от 19.12.2005 № 160-ФЗ // СЗ РФ. 2005. № 52 (ч. I), ст. 5573.

[3] Афанасьева О.В. Право на неприкосновенность частной жизни. Укрепляет ли его закон о персональных данных? // Общественные науки и современность. 2011. № 6. С. 83.

[4] Протокол о внесении изменений в Конвенцию о защите физических лиц при автоматизированной обработке персональных данных (ETS № 223) // Бюллетень Европейского суда по правам человека. 2018. № 12. С. 102–111.

коммуникационных технологий. В обновленной преамбуле Конвенции 108 содержится призыв учитывать диверсификацию, интенсификацию и глобализацию обработки данных и потоков персональных данных, «принцип личной автономии» – право человека контролировать персональные данные и их обработку.

Идеи этого основополагающего, первого и единственного, международного договора о правах человека в области защиты персональных данных оказали влияние на формирование позитивного права[1] и уголовно-правового механизма обеспечения безопасности личной информации в российском законодательстве. В Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы национальными интересами в области цифровой экономики названо обеспечение правомерного использования персональных данных[2]. Для защиты таких данных необходимо проводить мероприятия по противодействию незаконным обработке и сбору сведений о персональных данных граждан, неуполномоченными и неустановленными лицами, а также используемым ими техническим средствам[3]. А уголовным кодексом на основе международных стандартов и гарантий должно быть установлено наказание за нарушение права на неприкосновенность персональных данных.

Осознавая насущную необходимость установления самостоятельной уголовной ответственности за незаконные действия с персональными данными, 04.12.2023г. группа депутатов внесла на рассмотрение Государственной Думы РФ законопроект № 502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации». Они выступили с инициативой криминализации соответствующего деяния в рамках гл. 28 «Преступления в сфере компьютерной информации» и предложили включить в неё ст. 272[1] об ответственности, по сути,

---

[1] О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (с изм. и доп. от 06.02.2023, № 8-ФЗ) // СЗ РФ. 2006. № 31 (ч. I), ст. 3451; Рос. газета. 2023. 9 февр.

[2] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: указ Президента РФ от 09.05.2017 № 203 // СЗ РФ. 2017. № 20, ст. 2901.

[3] Осипенко А.Л., Соловьев В.С. Основные направления развития криминологической науки и практики предупреждения преступлений в условиях цифровизации общества // Всероссийский криминологический журнал. 2021. Т. 15, № 6. С. 681.

за два самостоятельных преступления: незаконные использование и (или) передачу (распространение, предоставление, доступ), сбор и (или) хранение компьютерной информации, содержащей персональные данные, полученной путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование, либо иным незаконным путем (ч. 1 проектной статьи) и создание и (или) обеспечение функционирования информационных ресурсов (сайта в сети «Интернет» и (или) страницы сайта в сети «Интернет», информационной системы, программы для электронных вычислительных машин), заведомо предназначенных для незаконного хранения, передачи (распространения, предоставления, доступа) компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконного хранения и (или) распространения (ч. 6).

Признаками, отягчающими (особо отягчающими) ответственность за совершение действий, перечисленных в первой части проектной статьи, называется их совершение в отношении компьютерной информации, содержащей специальные категории персональных данных и (или) биометрические персональные данные (ч. 2); из корыстной заинтересованности; повлекшее причинение крупного ущерба; группой лиц по предварительному сговору; с использованием своего служебного положения (ч. 3); сопряженное с трансграничной передачей компьютерной информации, содержащей персональные данные, и (или) трансграничным перемещением носителей, содержащих такие данные (ч. 4); повлекшее тяжкие последствия, либо организованной группой (ч. 5).

Статья снабжена тремя примечаниями. В первом особо оговаривается, что её действие не распространяется на случаи обработки персональных данных физическими лицами исключительно для личных и семейных нужд; во втором и третьем раскрываются понятия «трансграничное перемещение носителей» и «тяжкие последствия» соответственно.

В законопроекте также предложено дополнить ч. 1 ст. 137 и ч.1 ст. 272 УК РФ указанием на то, что они не распространяются на случаи, предусмотренные проектной уголовно-правовой нормой[1].

Соглашаясь с позицией нормотворцев в части криминализации незаконных действий с персональными данными, принципиальные возражения вызывает концепция предложенного ими законопроекта. Его существенными *недостатками являются*:

1. *Нивелирование интересов личности.* Для злоумышленников важна не сама по себе информация, содержащая персональные данные (в том числе и компьютерная), а те потенциальные возможности, которые она таит в себе (идентификация личности) и которые могут быть использованы и обычно используются для совершение самых разнообразных преступлений, причем не только в Сети, но и (или) в объективной действительности (например, так называемая кража личности, убийства, телефонное мошенничество, фальсификация избирательных документов и др.) Как некий специфический товар информация, содержащая персональные данные, может быть продана и продается независимо от её носителя (бумажный или электронный документ).

2. *Игнорирование регулятивного законодательства*, определяющего порядок обработки персональных данных, который не ограничивает осуществление соответствующей деятельности использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях (ст.1 ФЗ № 152). Зачастую первичные сбор, хранение и обработка информации, содержащей персональные данные, осуществляется без применения специального оборудования и возможностей Сети и только в процессе вторичной обработки переводится в «цифру».

3. *Искусственное создание объекта уголовно-правовой охраны*. По мнению разработчиков, специальный объект предлагаемого ими к криминализации посягательства – «компьютерная информация, содержащая персональные данные,

[1]Законопроект № 502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации» // Официальный сайт государственной Думы РФ. URL: https://sozd.duma.gov.ru/bill/502113-8 (дата обращения: 04.02.2023).

полученная путем неправомерного доступа к средствам ее обработки, хранения или иного вмешательства в их функционирование, либо иным незаконным путем»[1]. Во-первых, такой подход противоречит уголовно-правовой доктрине, поскольку смешиваются различные уголовно-правовые категории – «предмет» и «объект» преступления. Во-вторых, осуществляется подмена понятий – «персональные данные» и «компьютерная информация». Они имеют самостоятельное правовое значение и являются пересекающимися по объему и содержанию. По этим причинам компьютерная информация не может выступать родовым по отношению к персональным данным понятием. Неслучайно законодательные правопорядки зарубежных стран не определяют незаконные действия с персональными данными в качестве компьютерных преступлений. Как правило, они относят их к преступлениям против личности или против конституционных прав и свобод человека. Такой подход избрали законодатели бывших союзных республик. Например, ст. 147 УК Республики Казахстан, предусматривающая ответственность за нарушение неприкосновенности частной жизни и законодательства Республики Казахстан о персональных данных и их защите находится в гл. 3 «Уголовные правонарушения против конституционных и иных прав и свобод человека и гражданина». Глава 23 «Преступления против конституционных прав и свобод человека и гражданина» УК Беларуси содержит ст. 203[1] об ответственности за незаконные действия в отношении информации о частной жизни и персональных данных.

4. *Неверное определение границ криминализации*. Если в КоАП РФ установлена ответственность за незаконные действия с персональными данными независимо от формы их фиксации и способа совершения нарушений (ст. 13.11), то предлагаемые к криминализации деяния ограничены исключительно компьютерной сферой. Вместе с тем, четких критериев разграничения с аналогичными административными деяниями предлагаемая редакция ч.1 ст. 272[1] УК РФ не содержит, на что вполне справедливо обратил внимание Верховный

[1] Пояснительная записка к законопроекту№ 502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации» // Официальный сайт государственной Думы РФ. URL: https://sozd.duma.gov.ru/bill/502113-8 (дата обращения: 04.02.2023).

Суд РФ в своём заключении на законопроект, отметив отсутствие каких-либо дополнительных признаков, повышающих общественную опасность деяния. Это вполне «может привести к конкуренции данного уголовно-правового запрета со статьей 13.11 КоАП РФ и существенно усложнить применение проектной нормы на практике»[1].

5. *Технико-юридические недостатки.* Обращает на себя внимание громоздкость и сложная архитектоника проектной статьи. Как отмечалось ранее, она состоит из 6 частей, объединяет два самостоятельных состава преступления, 6 квалифицирующих (особо квалифицирующих) признаков одного из них, три примечания. Формулирование основных составов в полной мере не соотносится с регулятивным и охранительным законодательством, призванными обеспечивать безопасность операций с персональными данными, кроме того, изобилует оценочными признаками: «обработка персональных данных для личных и семейных нужд», «нарушение целостности информационной системы персональных данных», «обеспечение функционирования информационных ресурсов» и др. Это препятствует формированию четкого представления об уголовно-правовых запретах нарушающего поведения и его границах.

6. *Проблемы дифференциации ответственности.* Некоторые из признаков, отягчающих ответственность за совершение деяний, перечисленных в ч. 1 проектной статьи, вызывают вопросы. Например, повышенную ответственность предлагается установить в случае, если такие деяния сопряжены с трансграничной передачей компьютерной информации, содержащей персональные данные, и (или) трансграничным перемещением носителей, содержащих такие данные (ч.4 проектной статьи). Вместе с тем, данных об их распространенности (обязательного условия установления повышенной ответственности) разработчиками законопроекта не приводится. При подготовке настоящего исследования мы не встречали подобные случаи ни в судебной практике, ни в

[1] Официальный отзыв на проект федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации». Исх. №4-ВС-79/23 от 11 января 2023 г. // Официальный сайт государственной Думы РФ. URL: https://sozd.duma.gov.ru/bill/502113-8. (дата обращения: 04.02.2023).

аналитических материалах. В пояснительной записке не обоснована необходимость усиления ответственности за совершение соответствующих деяний, в отношении компьютерной информации, содержащей специальные категории персональных данных (ч.2 проектной статьи), к которым ФЗ № 152 относит сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни. И доктрина, и судебная практика в настоящее время исходят из того, что такие деяния получают юридическую оценку в рамках ст. 137 УК РФ. Критериев разграничения проектная норма не содержит.

Таким образом, предлагаемый законопроект не отвечает современным потребностям в уголовно-правовой охране персональных данных, противоречит принципу формальной определенности норм и доктринальным представлениям о криминализации деяния, дифференциации ответственности, технико-юридическим правилам конструирования уголовно-правовых норм.

Полагаем, что видовым объектом уголовно-правовой охраны при совершении преступных посягательств в отношении персональных данных являются не информационная (компьютерная) безопасность, а конституционные права и свободы человека и гражданина. Не противоречит этому предложению довод теоретиков уголовного права, что персональные данные как специальный объект защиты в Конституции РФ не упоминаются[1]. Об этом пишут и специалисты по конституционному праву, комментируя этот пробел Основного закона как нехватку юридических гарантий по защите персональных данных[2]. Другие правоведы-конституционалисты, напротив, полагают, что не упоминание в Конституции персональных данных не препятствует тому, что предметом конституционной защиты они все же выступают. Содержательное разъяснение этого вывода приводит М.И. Проскурякова: «В процессе истолкования Конституции РФ, при котором ее положения анализируются не изолированно, а с учетом «конкретно-исторических реалий», удается выявить конституционные

---

[1] Войниканис Е.А., Машукова Е.О., Степанов-Егиянц В.Г. Указ. соч. С. 77.

[2] Давыдова М.Л. Средства юридической техники и проблема ограничения прав и свобод человека // Юриспруденция. 2010. № 2. С. 33; Афанасьева О.В. Указ. соч. С. 82.

основания защиты персональных данных в ч. 1 ст. 23 в совокупности с ч. 1 ст. 24, закрепляющей право на неприкосновенность частной жизни; ч. 2 ст. 23, провозглашающей право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; ст. 25, закрепляющей право на неприкосновенность жилища»[1]. Определенную ясность в обсуждение этого вопроса вносят и С.Г. Пилипенко и А.С. Федосин: «Право на защиту персональных данных является элементом комплексного права на неприкосновенность частной жизни. Концептуальный подход к данному вопросу основан на положениях ч.1 ст. 23 и ч.1 ст. 24 Конституции Российской Федерации. Они фактически формируют конституционно-правовую основу права человека на защиту персональных данных в структуре его права на неприкосновенность частной жизни»[2]. Верную интерпретацию учеными положений Конституции РФ подтверждает и практика Конституционного Суда РФ. В своих определениях от 29.09.2011 № 1063-О-О и от 29.01.2009 № 3-О-О, ранее признав, что Конституция РФ допускает возможность установления режима ограничения свободного доступа к информации со стороны граждан, суд констатирует: «Исключение информации, относящейся к персональным данным, из режима свободного доступа полностью соответствует предписаниям ч. 2 ст. 24 Конституции. В противном случае под угрозой оказалось бы гарантированное ч. 1 ст. 23 и ч. 1 ст. 24 Конституции право на неприкосновенность частной жизни»[3].

---

[1] Проскурякова М.И. Конституционно-правовые рамки защиты персональных данных в России // Вестник Санкт-Петербургского университета. Право. 2016. № 2. С. 18.

[2] Пилипенко С.Г., Федосин А.С. К вопросу о реализации права на защиту персональных данных при их обработке в электронной форме // Пробелы в российском законодательстве. 2009. № 3. С. 214.

[3] Об отказе в принятии к рассмотрению жалобы гражданина Багадурова Магомеда Магомедовича на нарушение его конституционных прав подпунктом 1 пункта 3 статьи 6 Федерального закона «Об адвокатской деятельности и адвокатуре в РФ» статьей 10 Федерального закона «О персональных данных» и частью второй статьи 57 ГПК Российской Федерации»: определение Конституционного Суда РФ от 29.09.2011 № 1063-О-О; Об отказе в принятии к рассмотрению жалобы гражданина Глушкова Николая Петровича на нарушение его конституционных прав статьями 3, 5, 6 и 9 Федерального закона «Об информации, информационных технологиях и о защите информации» и статьями 8 и 9 Федерального закона «О персональных данных»: определение Конституционного Суда РФ от 29.01.2009 № 3-О-О. Доступ из Справ.-прав. системы «КонсультантПлюс».

Отметим, однако, что исследователи не пришли и к общему мнению о том, что же охраняется – право на неприкосновенность частной жизни или персональных данных. Н.М. Малеина, используя понятие «право на тайну и неприкосновенность персональных данных», пишет, что это право на неприкосновенность персональных данных[1]; Э.А. Цадыкова[2], М.Ю. Авдеев[3], напротив, считают, что юридической охране подлежит право на неприкосновенность частной жизни, ибо неприкосновенность персональных данных как личной информации выступает его составной частью. Используя наработки специалистов конституционного права, отметим, что объектом уголовно-правовой охраны должно выступать право на неприкосновенность персональных данных. Идею его формирования как одного из фундаментальных прав личности еще в 2006 г. в кандидатской диссертации по конституционному праву предложил И.А. Вельдер[4]. Поддерживая ее, Н.Г. Белгородцева указывает, что право на защиту персональных данных является одной из разновидностей юридических гарантий конституционных прав человека[5]. Действительно, высокие темпы развития информационных технологий способствовали расширению способов идентификации человека в социуме через личные данные. Многократно возрастающие объемы конфиденциальной информации о человеке в условиях информатизации общества потребовали усиления защиты его личных прав, что обусловило формирование в структуре конституционного права на неприкосновенность частной жизни нового элемента – права на защиту персональных данных[6]. Обособление нового права М.В. Бундин справедливо

---

[1] Малеина М.Н. Указ. соч. С. 20.

[2] Цадыкова Э.А. Конституционное право на неприкосновенность частной жизни: сравнительно-правовое исследование: автореф. дис. … канд. юрид. наук. М., 2007. С. 19.

[3] Авдеев М.Ю. Нормативное содержание права на неприкосновенность частной жизни // Новый юридический журнал. 2013. № 1. С. 50.

[4] Вельдер И.А. Система правовой защиты персональных данных в Европейском союзе: дис. ... канд. юрид. наук. Казань, 2006. С. 10.

[5] Белгородцева Н.Г. Теоретико-правовые аспекты защиты персональных данных: автореф. дис. ... канд. юрид. наук. М., 2012. С. 10–11.

[6] Федосин А.С. Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации: автореф. дис. ... канд. юрид. наук. Саранск, 2009. С. 7; Сергиенко Л.А. Правовая

объясняет тем, что оно представляется «необходимым элементом информационной культуры современного общества, без которого невозможно было бы обеспечить необходимый уровень защиты личности»[1]. Еще одно подтверждение необходимости самостоятельного развития права на защиту персональных данных ученые усматривают в даче согласия на обработку персональных данных как правомочия человека контролировать данные о себе[2].

Систематизируя представленные мнения, укажем, что ввиду не совпадения, а пересечения двух правовых феноменов – частной жизни и персональных данных, неприкосновенность персональных данных в целях повышенной охраны должна получить самостоятельное значение, то есть охраняться за рамками неприкосновенности частной жизни. Только такой подход к соотношению этих понятий позволяет обосновать тезис о рассмотрении неприкосновенности персональных данных в качестве объекта уголовно-правовой защиты, поскольку в действующей редакции ст. 137 УК РФ является непонятным, что именно подлежит охране уголовным законом – право на неприкосновенность частной жизни, неприкосновенность персональных данных или сами персональные данные. Исходя из доказанного в работах большинства ученых-конституционалистов и не вызывающего дискуссии положения о том, что право на неприкосновенность персональных данных как информации ограниченного доступа, имеет конституционную природу, предлагается осуществлять его уголовно-правовую защиту в рамках главы 19 «Преступления против конституционных прав и свобод человека и гражданина».

Дополнительным аргументом в пользу такой модели ответственности служит, *во-первых*, следственно-судебная практика, подтверждающая причинение или угрозу причинения вреда конституционным правам и свободам собственника

защита персональных данных. Цели и принципы правового регулирования // Проблемы информатизации. 1995. № 1. С. 37.

[1] Бундин М.В. Персональные данные в системе информации ограниченного доступа: дис. ... канд. юрид. наук. М., 2017. С. 53.

[2] Филатова М.А. Указ. соч. С. 37; Проскурякова М.И. Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе // Сравнительное конституционное обозрение. 2016. № 6. С. 87.

(владельца) персональных данных (вред здоровью, жизни, вмешательство в его личную жизнь, шантаж или угрозы с использованием персональных данных, распространение порочащих сведений, имущественный вред и др.). Подчеркивая значение охраны персональных данных, В.Н. Лопатин точно подмечает, что к ним могут быть отнесены сведения, использование которых без согласия их субъекта может нанести вред его чести, достоинству, деловой репутации, доброму имени, иным нематериальным благам и имущественным интересам[1]. И, действительно, «разглашение информации само по себе может наносить ущерб личности того, к кому относится такая информация – в первую очередь, страдают нематериальные блага потерпевшего субъекта: честь, достоинство и деловая репутация»[2]. И в этой связи «защищаются скорее не персональные данные как таковые, а их носитель, человек, от противоправного или нежелательного для него использования таких данных»[3], а потому «в конечном итоге, защита персональных данных – это не защита информации, а защита персоналий»[4]. Иными словами, первоначально подвергаются угрозе и претерпевают куда более значимый в социальном отношении вред блага, принадлежащие человеку и гражданину, нежели информационная безопасность или порядок управления.

Во-вторых, показатели социологических опросов населения свидетельствуют о росте уровня тревожности россиян относительно вреда от деаномизации персональных данных, выраженного, прежде всего, в нарушении их прав и свобод, не ограниченных частной жизнью (ст. ст. 23, 24, 25 Конституции РФ). Подтверждается это фиксируемым следственно-судебной практикой и СМИ широким спектром злоупотреблений с персональными данными человека, затрагивающих его личные неимущественные, социальные, экономические и политические права. Как следует из результатов Всероссийского

---

[1] Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: учебник. СПб.: Юрид. центр Пресс, 2001. С. 284.

[2] Гутник С.И. Указ. соч. С. 109.

[3] Лушников А.М. Защита персональных данных работника: сравнительно-правовой комментарий главы 14 Трудового кодекса Российской Федерации // Трудовое право. 2009. № 9. С. 95.

[4] Дятленко В.В., Волчинская Е.К. Законодательство о защите персональных данных: проблемы и решения // Информационное право. 2006. № 1. С. 13.

исследования, проводившегося в течение четырех лет в городах всех федеральных округов России с участием 28 тыс. респондентов, наблюдается значительное увеличение доли граждан, опасающихся утечки своих персональных данных ввиду их криминального использования (с 33 % до 63 %). Из возможных вариантов негативных последствий такого сценария максимальную значимость для респондентов представляют следующие: незаконное завладение паспортными и банковскими данными (90 %), информацией о месте жительства и доходах (70 %), данными о детях (58 %), потеря денежных средств (55 %), злоупотребление персональными данными в преступных целях (52 %), создание фальшивых документов (47 %), вторжение в частную жизнь (39 %), вред для членов семьи (25 %) и распространение ложной информации о владельце данных (19 %)[1]. При этом 33 % опрошенных не осведомлены о способах защиты от кражи и другой несанкционированной утраты персональных данных[2].

В-третьих, национальными интересами в информационной сфере признаны *обеспечение и защита конституционных прав и свобод человека и гражданина* при получении и использовании информации, неприкосновенности частной жизни при использовании информационных технологий (Доктрина информационной безопасности РФ, утвержденная указом Президента РФ от 05.12.2016 № 646 (п. 1 ст. 8)[3]). В качестве цели ФЗ № 152 заявлено *обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных*, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну. Объектом защиты конституционных прав и свобод граждан называет персональные данные и международное право. Так, целью ратифицированной с участием России Конвенции Совета Европы «О защите частных лиц в отношении автоматизированной обработки данных личного

---

[1] Почему россияне боятся расстаться с персональными данными, и кому они готовы их доверить. Исследование Sostav и OMI // Sostav. URL: https://www.sostav.ru/publication/pochemu-rossiyane-boyatsya-rasstatsya-s-personalnymi-dannymi-i-komu-oni-gotovy-ikh-doverit-issledovanie-sostav-i-omi-38865.html (дата обращения: 03.12.2022).

[2] Россияне испугались кражи личных данных и перешли на VPN // News. URL: https://news.mail.ru/society/49789704/?frommail=1 (дата обращения: 25.12.2022).

[3] Доктрина информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646 // Рос. газета. 2016. 6 дек.

характера» (Конвенция 108) ее авторы провозгласили *обеспечение для каждого физического лица* независимо от его гражданства или местожительства, *уважения его прав и основных свобод*, и в частности его *права на неприкосновенность частной жизни, в отношении автоматизированной обработки касающихся его персональных данных* («защита данных»)[1]. Выражение «защита данных» здесь понимается в контексте защиты не самих по себе персональных данных, а прав и основных свобод человека, которые могут быть нарушены при их автоматизированной обработке.

В-четвертых, месторасположение проектируемой нормы (Раздел VII) будет являться показателем первостепенности защиты уголовным законом прав и свобод человека и гражданина, его приоритетной задачей.

Разрешая вопрос о том, какие именно деяния в отношении персональных данных следует признать уголовно наказуемыми, представителями уголовно-правовой науки предлагаются разные варианты, и в том числе их изготовление, фальсификация, хранение, уничтожение[2]. Полагаем, что понятия «собирание» и «распространение» охватывают все незаконные действия в отношении персональных данных, за исключением их использования и в целом соответствует концепции ФЗ №152, использующего для этих целей понятие «обработка персональных данных» (п.3 ст.3), к тому же, исключит перегруженность соответствующей уголовной нормы.

Этот вывод подтверждается разъяснением собирания и распространения применительно к ст. 137 УК РФ Пленума Верховного Суда РФ[3]. В соответствии с п. 3 постановления от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138[1], 139, 144[1], 145, 145[1] Уголовного кодекса

---

[1] Конвенция о защите физических лиц при автоматизированной обработке персональных данных: зЗаключена в Страсбурге 28.01.1981. Доступ из Справ.-прав. системы «КонсультантПлюс».

[2] Чукреев В.А. Указ. соч. С. 116; Рязанова Е.Н. Указ. соч. С. 123.

[3] О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138[1], 139, 144[1], 145, 145[1] Уголовного кодекса Российской Федерации): постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 // Бюллетень Верховного Суда РФ. 2019. № 2.

Российской Федерации)» под собиранием сведений о частной жизни лица понимаются умышленные действия, состоящие в получении этих сведений любым способом, например путем личного наблюдения, прослушивания, опроса других лиц, в том числе с фиксированием информации аудио-, видео-, фотосредствами, копирования документированных сведений, а также путем похищения или иного их приобретения. Распространением сведений о частной жизни лица судьи Верховного Суда РФ признают сообщение (разглашение) их одному или нескольким лицам в устной, письменной или иной форме и любым способом (в частности, путем передачи материалов или размещения информации с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»). Здесь оговоримся, что собирание персональных данных само по себе не представляет той общественной опасности, степень которой обусловливает установление за него уголовной ответственности. По нашему мнению, если поиск (как первоначальный этап) и сбор персональных данных завершились получением искомых сведений, то уголовно-правовое значение имеет не сам факт незаконного собирания чужой персональной информации, а ее использование именно в преступных целях. Иными словами, для квалификации незаконных действий с персональными данными имеет значение не сам результат незаконного сбора охраняемых персональных данных с их систематизацией и накоплением, а цель их собирания, создающая опасность нарушения других прав человека (право на жизнь, здоровье, собственность, честь, достоинство и т.д.). Ведь незаконное собирание персональных данных, ограниченных в свободном доступе, не может причинить вред их обладателю, если они после сбора виновным лицом не используются для совершения преступления или используются иначе. Той же позиции придерживаются опрошенные нами эксперты, поддержавшие предложение о конкретизации цели при собирании персональных данных (44 %). Именно такая формулировка конструктивного признака дополнительно повысит предупредительный потенциал новой нормы, что актуально в условиях значительного роста незаконных действий с персональными данными.

Во избежание излишнего загромождения уголовного закона законодателю следует предложить четкие объективные и субъективные признаки нового состава преступления. А.А. Шутова, констатируя, что нормы административной ответственности, охраняющие персональные данные, неэффективны, предлагает дополнить часть 1 ст. 137 УК РФ признаком причинения существенного вреда правам и законным интересам человека в результате незаконного сбора или распространения информации (персональных данных) с его дефиницией в примечании[1]. В науке уголовного права принято считать, что существенный вред может быть выражен в причинении физического, морального вреда, в материальном ущербе (имущественном вреде), организационном вреде и в нарушении конституционных прав и законных интересов граждан и организаций[2]. Предлагаемый в качестве конструктивного признак существенности вреда должен быть применен, на наш взгляд, в его традиционной для уголовного закона редакции, ведь в случае совершения преступлений с персональными данными многочисленные риски существуют и для прав и законных интересов организаций, охраняемых законом интересов общества или государства. Прирост доли инцидентов с личными данными в 2022 г. наблюдался в крупных транспортных компаниях, медицинских организациях, государственных учреждениях, службах доставки, банках и ритейлах с последующим неправомерным доступом к инфраструктуре клиентов и нарушением бизнес-процессов из-за сбоев в работе сервисов[3]. По свидетельству специалистов IT, взлом виртуальных ресурсов позволяет атаковать пользователей для сбора персональной информации о них, когда киберпреступники встраивают вредоносный код в скомпрометированные веб-страницы. Украденная в результате хакерских атак информация продавалась на теневых форумах и использовалась в качестве метода социальной инженерии, ставшего популярным по причине

---

[1] Шутова А.А. Указ. соч. С. 45.

[2] Крылова А.В. Понятие существенного вреда правам и законным интересам граждан и организаций в составе «Управленческого» злоупотребления» // Вестник Московского университета. Серия 11: Право. 2014. № 6. С. 69.

[3] Актуальные киберугрозы: итоги 2022 года // Ptsecurity. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения: 09.04.2023).

массовости «сливов». Деанонимизированные данные могут быть применяться для составления цифрового «портрета» жертв и проведения более интенсивных атак в целях доступа к закрытой информации. Жертвы злоумышленников, укравших чужие персональные данные, для устранения последствий преступлений вынуждены менять свои документы, сим-карты мобильных телефонов, подавать иски в суд для оспаривания получения оформленных на их имя кредитов, являться участниками затяжного уголовного судопроизводства[1]. Юридические лица, в которых допущена утечка персональных данных, даже в случае хакерских атак и невиновности сотрудников, в судебном порядке возмещают понесенные гражданами убытки и моральный вред, а также подвергаются административному штрафу, приостановлению или запрету деятельности по обработке персональных данных. К примеру, в 2022 г. клиенты СДЭК, сервиса экспресс-доставки, подали в суд коллективный иск на сумму 2,2 млн руб. после того, как в сеть Интернет попали их персональные данные. Такой же иск заявили пострадавшие от утечки своих личных данных клиенты «Яндекс.Еды», требуя от компании по 100 тыс. руб.[2]

О том, что проблема причинения вреда приобрела особую актуальность, подтверждает издание Роскомнадзором приказа от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»». Если ранее критерии потенциального вреда субъектам персональных данных устанавливались организациями самостоятельно, то с 1 марта 2023 г. стали применяться единые правила оценки операторами и владельцами баз персональных данных возможного ущерба их субъектам[3]. По сообщениям СМИ, в России может появиться фонд материальной

---

[1] Рязанова Е.Н. Указ. соч. С. 119.

[2] Фонд защиты сданных // Коммерсантъ. URL: https://www.kommersant.ru/doc/5515449 (дата обращения: 09.04.2023).

[3] Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»: приказ Роскомнадзора от 27.10.2022 № 178. Доступ из Справ.-прав. системы «КонсультантПлюс».

компенсаций для граждан, пострадавших от утечек их персональных данных из компаний. По задумке авторов законопроекта, денежными средствами, наполняющими фонд, будут штрафы компаний, в которых произошел инцидент. Идея предполагает введение в КоАП РФ поправок, по которым компания может быть оштрафована на 1 % от годового оборота. Размер штрафа вырастет до 3 %, если компания попыталась скрыть проблему[1].

Оценивая существенность вреда, правоприменитель должен учитывать влияние преступного посягательства на нормальную работу организации, характер и размер причинённого материального ущерба, в том числе сумму денежных средств на компенсацию вреда потерпевшим, устранение последствий компрометации персональных данных (например, реквизитов банковских счетов, пластиковых карт и др.). Под «существенностью» можно понимать нарушение прав и свобод граждан (честь и достоинство личности, тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений и др.) и юридических лиц, количество потерпевших и тяжесть причиненного им морального или имущественного вреда и др. Существенный вред может выражаться и в разглашении персональных данных лиц, осуществляющих разведывательную деятельность, обеспечивающих государственную безопасность, охрану руководителей страны, свидетелей по уголовным делам, что может повлечь их персонификацию и создать угрозу их жизни и здоровью, их близких, ущерб внутренней и внешней безопасности и иным жизненно важным интересам РФ.

По данным опроса экспертов, характерной особенностью преступности данного вида является ее организованный характер (*76 %*) с увеличением количества преступных посягательств с участием группы лиц по предварительному сговору или организованных групп. Соучастие существенно увеличивает общественную опасность преступных посягательств, связанных с

[1] Утечки возьмут в оборот // Коммерсантъ. URL: https://www.kommersant.ru/doc/5379590 (дата обращения: 09.04.2023).

персональными данными[1]. О высокой степени распространенности соучастия при совершении исследуемого преступления свидетельствуют результаты изучения следственно-судебной практики. Например, сотрудниками МВД России были задержаны члены организованной группы, которая занималась продажей персональных данных в Интернете. Они создали площадки, где можно было купить или продать персональные данные россиян, реквизиты их банковских карт, а также получить доступ к серверам через удаленный рабочий стол. Среди задержанных шесть фигурантов из Санкт-Петербурга, Саратова и Перми. В ходе обысков по адресам их проживания и в офисах обнаружены компьютерная техника, мобильные телефоны, носители информации. Полицейскими изъяты 24 золотых слитка 999-й пробы, три машины премиум-класса и 12 млн руб.[2] Для повышения потенциала уголовно-правовых средств реагирования на организованные формы преступной деятельности, и в том числе в виртуальном пространстве, представляется необходимым снабдить проектируемый состав преступления, ст. 137[1] УК РФ, особо квалифицирующим признаком – признаком его совершения группой лиц по предварительному сговору или организованной группой (*с таким предложением согласны 48 % респондентов-экспертов; 28 % высказались за группу лиц по предварительному сговору*).

Правоприменительная практика подтверждает и бóльшую степень общественной опасности деяний, совершаемых с персональными данными или в отношении них, с помощью информационно-телекоммуникационных сетей, включая сеть Интернет. Преступники используют данные электронной почты жертв, осуществляя рассылку писем с фишинговыми ссылками, фальшивые интернет-сайты-копии банков и государственных учреждений, приложений государственных услуг, мобильных телефонов для отправки сообщений

---

[1] Соловьев В.С., Осипенко А.Л. Основные направления развития криминологической науки и практики предупреждения преступлений в условиях цифровизации общества // Всероссийский криминологический журнал. 2021. Т. 15, № 6. С. 684.

[2] МВД России накрыло группировку, продававшую персональные данные. Среди участников есть пермяки // 59.ru. URL: https://59.ru/text/incidents/2022/02/22/70461209/ (дата обращения: 09.04.2023).

в мессенджеры, а также социальные сети[1]. Распространена криминальная практика взлома личной страницы в социальной сети, когда злоумышленниками осуществляется рассылка контактам с чужого аккаунта с просьбой перевести деньги[2]. В научных работах описаны не только риски виртуальной «кражи личности» документов и внешности для использования персональных данных человека, но и его черт характера, переживаемых эмоций и манер поведения для эксплуатации уже самой личности[3].

По причине дистанционного характера эти преступления раскрываются и расследуются правоохранителями существенно сложнее ввиду анонимности злоумышленников и проблем фиксирования материальных (цифровых) следов, составляющих доказательства содеянного. Это подтверждается показателями предварительного расследования уголовных дел по исследуемым преступлениям (по данным авторского опроса, почти *30 %* возбужденных дел остаются нераскрытыми). Количество жертв, данные которых были украдены, а впоследствии использованы для совершения против них различных посягательств, насчитывает десятки, если не сотни тысяч, однако установить их точно не представляется возможным ввиду гиперлатентности этих преступлений (*46 % экспертов, считающих гиперлатентностью 75-100 % незарегистрированных преступлений; 24 % экспертов определяют латентность на уровне 25–49 %*). В условиях цифровой реальности с переходом на удаленную идентификацию, повлекшую изменение «качества» преступности, уже сейчас возможен прогноз о появлении в будущем новых способов похищения и использования личных данных россиян посредством информационно-коммуникационных технологий, а значит и новых потенциальных угроз

---

[1] Кузьмин Ю.А. Кража персональных данных (криминологический аспект) // Oeconomia et Jus. 2020. № 3. С. 50; Соловьев В.С. Преступность в социальных сетях интернета (криминологическое исследование по материалам судебной практики) // Всероссийский криминологический журнал. 2018. Т. 10, № 1. С. 77.

[2] Соловьев В.С. Мошеннические действия в социальном сегменте сети интернет (криминологическое исследование по результатам интернет-опроса пользователей) // Известия Юго-Западного государственного университета. Серия: История и право. 2018. Т. 8, № 3 (28). С. 104.

[3] Атагимова Э.И., Потёмкина А.Т., Цопанова И.Г. «Кража личности» как самостоятельное преступление или разновидность мошенничества // Правовая информатика. 2017. № 3. С. 17.

состоянию защищенности прав и законных интересов личности, охраняемых законом интересов общества и государства. А потому проектируемая норма об общественно опасных, противоправных деяниях, совершаемых в отношении и (или) посредством персональных данных значительно распространенным способом – с использованием информационно-коммуникационных сетей (включая сеть «Интернет»), должна быть наделена соответствующим квалифицирующим признаком (*это мнение поддержали 23,2 % экспертов*).

Правоведами в разных вариантах юридической техники внесены предложения о признании баз персональных данных предметом преступления[1], которые следует поддержать, однако не в части формулирования дополнительного квалифицирующего признака ст. 137 УК РФ, а нового состава преступления в качестве его отягчающего обстоятельства (проектируемой ст. 137[1] УК РФ). Подобное правотворческое решение позволит преодолеть неэффективность действующих уголовно-правовых инструментов защиты личных данных человека. Для использования термина «база данных» в формулировке квалифицирующего признака необходима определенная ясность в самом его понимании. По сути, единственное легальное определение базы данных в ГК РФ (ст. 1260)[2] критикуется за утрату его актуальности, неопределенность и узость, а также относимость только к результатам интеллектуальной деятельности[3]. Специалисты по IT трактуют базы данных как «большие массивы информации о какой-либо сфере производственной или общественной деятельности, предназначенные для коллективного использования и допускающие компьютерную обработку этой информации»[4]. В федеральном законе

---

[1] Баринов С.В. О криминализации преступного нарушения неприкосновенности частной жизни, совершаемого в форме распространения баз персональных данных. 2017. № 4. С. 37.

[2] Согласно абз. 2 п. 2 ст. 1260 ГК РФ базой данных является представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ).

[3] Иванов И.С. Правовые признаки государственной информационной системы // Вестник Воронежского государственного университета. Право. 2020. № 2 (41). С. 179–187.

[4] Зафиевский А.В., Короткин А.А., Лататуев А.Н. Базы данных: учеб. пособие. Ярославль, 2012. С. 6.

«О полиции» (далее ФЗ о полиции) законодатель использует два термина – «база данных» (п. 10 ст. 13) и «банк данных». Банком данных ФЗ о полиции именует оперативно-справочную, экспертно-криминалистическую, разыскную и иную информацию о лицах, предметах и фактах; банки данных о гражданах; банки данных других государственных органов и организаций, в том числе персональные данные граждан (п. 33 ст. 13 «Права полиции»)[1]. Пунктом 3 ст. 17 «Формирование и ведение банков данных о гражданах» установлен исчерпывающий перечень видов информации, подлежащей внесению в банки данных. В п. 8 ст. 17 указано, что персональные данные, содержащиеся в банках данных, подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей. В то же время ведомственные приказы МВД РФ оперируют и термином «база данных»[2]. Думается, что банки данных или базы данных употребляются в значении информационного ресурса, в котором информация систематизируется по всем категориям учета, хранится, обрабатывается и поддерживается в актуальном состоянии[3].

В п. 10 ст. 13 «Права полиции» говорится не только о базах данных, но и государственных информационных системах. Согласно ст. 2 ФЗ об информации, информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств[4] (подп. 3). Сам термин «база данных», упоминаемый более тридцати раз в тексте закона, остался без определения. Государственные информационные системы создаются в целях реализации полномочий

---

[1] О полиции: федер. закон от 07.02.2011 № 3-ФЗ (с изм. и доп. от 04.08.2023, № 440-ФЗ) // Парламентская газета. 2011. 11-17 февр.; Рос. газета. 2023. 11 авг.

[2] Об утверждении Порядка формирования и ведения базы данных о лицах, состоящих в органах внутренних дел Российской Федерации на учете для получения единовременной социальной выплаты для приобретения или строительства жилого помещения, а также снятых с данного учета: приказ МВД России от 25.01.2022 № 70. Официальный интернет-портал правовой информации (pravo.gov.ru) 30 августа 2022 г. № 0001202208300004.

[3] Тюрина Е.Н. Интегрированные банки данных и сетевые каналы связи как особенный объект правоотношений, возникающих в деятельности органов внутренних дел // Труды Академии управления МВД России. 2012. № 2 (22). С. 127.

[4] Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ (с изм. и доп. от 31.07.2023, № 408-ФЗ) // Рос. газета. 2006. 29 июля; 2023. 3 авг.

государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях. К примеру, федеральной государственной информационной системой Минюста РФ является «Учет адвокатов Российской Федерации и адвокатов иностранных государств, осуществляющих адвокатскую деятельность на территории Российской Федерации». В приказах МВД РФ федеральная государственная информационная система (ФГИС) МВД РФ, ГИБДД – это интегрированный банк данных федерального уровня с возможностями распределенного хранения и обработки информации (ИБД)[1]. Иными словами, информационная система предназначена для хранения, поиска и обработки информации, результатом функционирования которой является информационная продукция – документы, информационные массивы, базы данных и информационные услуги[2]. На основании изложенного, при юридико-техническом оформлении диспозиции следует применять устоявшийся термин «база данных», используемый в специальном законе об информации (ФЗ № 149).

Правоприменитель при расследовании преступлений, связанных с похищением персональных данных, не может дать отдельную правовую оценку тому, каким образом были использованы «украденные» данные, облегчившие наступление негативных последствий для их обладателей. Некоторые исследователи предлагают ввести наказание при условии, что похищенные личные данные использовались для совершения других преступлений[3]. Правоприменительная практика подтверждает криминологическую обоснованность такого законотворческого решения.

Так, прокуратура Волгоградской области утвердила обвинительное заключение по уголовному делу в отношении жителя г. Волгограда и других соучастников. Они обвиняются в совершении преступлений, предусмотренных ч. 1 ст. 173[1] УК РФ «Незаконное образование юридического лица», ч. 2 ст. 173[2] УК

---

[1] О порядке эксплуатации специального программного обеспечения федеральной информационной системы Госавтоинспекции: приказ МВД России от 05.02.2016 № 60. Доступ из Справ.-прав. системы «КонсультантПлюс».

[2] Петров В.Н. Информационные системы. СПб.: Питер, 2002. С. 11.

[3] Рязанова Е.Н. Указ. соч. С. 120.

РФ «Незаконное использование документов для создания юридического лица», а также по ч. 3 ст. 159 УК РФ «Мошенничество в крупном размере». По версии СУ ГУ МВД России по Волгоградской области, обвиняемый А. с целью хищения денежных средств банков зарегистрировал два юридических лица, которые якобы оказывали посреднические услуги при организации туристических туров. Между фирмой обвиняемого и банком был заключен договор, по которому фирма имела право оформлять от имени банка документы на выдачу кредитов клиентам на оплату туристических услуг. Используя сеть Интернет для получения доступа к персональным данным граждан, фигурант составил договоры на получение потребительских кредитов на оплату туров. После этого денежные средства были перечислены на счет подконтрольной ему фирмы. Соучастники А. аналогичным способом похитили денежные средства двух других кредитных организаций. Сумма причиненного трем банкам ущерба составила 2 млн 750 тыс. руб.[1]

И другой пример. Октябрьским районным судом г. Архангельска О. был признан виновным в совершении преступления, предусмотренного ч. 3 ст. 183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» из корыстной заинтересованности, а С. – по ч. 4 и ч. 5 ст. 33 ч. 3 ст. 183 УК РФ подстрекателем и пособником. О., специалист кредитно-кассового офиса «Альфа-банка» в г. Архангельске, по предварительному сговору с С., другим сотрудником банка, осуществлял продажу персональных данных клиентов банка без их согласия третьим лицам. Фигуранты скопировали персональные данные шести вкладчиков, включая сведения об их банковских счетах и остатках средств на них, и передавали их за плату третьим лицам, за что получили 140 тыс. руб. Покупателями персональных данных являлись жители Москвы, воспользовавшись которыми, они подделали паспорта клиентов банка и открыли на имена трех из них банковские карты, с помощью которых получили доступ к

[1] Прокуратура Волгоградской области утвердила обвинительное заключение по уголовному делу о мошенничестве при получении кредитов для оплаты туристических путевок // Прокуратура Волгоградской области. URL: https://epp.genproc.gov.ru/web/proc_34/mass-media/news?item=56232080 (дата обращения: 09.04.2023).

счетам. В результате незаконных действий злоумышленники успели похитить с трех счетов вкладчиков денежные средства на сумму, превышающую 8 млн руб.[1]

Учитывая российскую следственно-судебную практику, сообщения СМИ о крупных утечках личных данных в открытый доступ и мнение опрошенных экспертов (*76 %*), более предпочтительным будет дополнение УК РФ все же не наделением диспозиций уголовно-правовых норм квалифицирующим признаком, а новым отягчающим обстоятельством – «с использованием персональных данных». Его надлежит включить в институт обстоятельств, отягчающих наказание (ст. 63 УК РФ), для соблюдения требований системного характера новеллы. Предлагаемое законодателю решение выглядит логичным и с позиции уголовно-правовой теории, поскольку объясняется повышением ответственности, в частности, уже потому, что незаконные действия в отношении персональных данных совершаются, в том числе, с целью их дальнейшего использования в методах социальной инженерии для мошеннических действий, опорочивания чести и достоинства человека, рейдерских захватов чужого бизнеса, совершения тяжких преступлений против личности, в том числе убийств, террористических актов и др. В контексте сказанного следует предложить ввести указанное обстоятельство в п. «т» ч. 1 ст. 63 УК РФ с формулировкой – «совершение преступления с использованием персональных данных». Придание указанному обстоятельству статуса универсального инструмента, усиливающего наказание комплексно, за все преступления, совершенные с помощью персональных данных, будет способствовать достижению эффективности противодействия незаконным действиям с ними.

Таким образом, на основе международных стандартов, опыта зарубежных стран, правоприменительной практики и научной доктрины содержание модели криминализации незаконных действий в отношении персональных данных (de lege ferenda) можно сформулировать *следующими положениями*:

---

[1] Сотрудники Альфа-банка продавали персональные данные клиентов. Их гонорар больше штрафа за разглашение банковской тайны // Cnews. URL: https://zoom.cnews.ru/news/item/511675 (дата обращения: 09.04.2023).

1. Для эффективности реализации уголовно-правового механизма охраны персональных данных предлагается сконструировать новую норму и изложить ее в *следующей редакции*:

«**Статья 137[1]. Нарушение неприкосновенности персональных данных**

1. Незаконные собирание и (или) распространение персональных данных в целях совершения преступления, либо повлекшие причинение существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства, –

наказываются …

2. Те же деяния, совершенные:

а) группой лиц по предварительному сговору или организованной группой;

б) с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

в) в отношении информационно-поисковых систем (баз данных), –

наказываются …».

2. Для концептуального единства уголовной ответственности проектируемый состав преступления предлагается ввести в главу 19 УК РФ по признаку общности видового объекта со ст. 137 УК РФ (частная жизнь) и прочими посягательствами против конституционных прав и свобод человека и гражданина. Объектом здесь следует признать общественные отношения, обеспечивающие неприкосновенность персональных данных, а предметом – конкретные сведения, при определенных признаках характеризующиеся как персональные данные. Уголовно-правовому охранению здесь подлежит та часть права на неприкосновенность персональных данных, которая даже в условиях действия запрета на вторжение в частную жизнь остается незащищенной, подвергается посягательству помимо или против воли человека. Воплощение идеи нового понимания неприкосновенности персональных данных как объекта специального состава преступления с его структурным расположением в разделе о преступлениях против личности повысит качество уголовно-правового инструментария по противодействию этому виду преступности. Объективная

потребность в независимой от частной жизни, а самостоятельной охране персональных данных уголовным правом обусловлена и обеспечением защиты других личных, социальных, экономических, политических прав человека, страдающих от сопутствующих преступлений.

3. В связи с необходимостью придания самостоятельного значения персональным данным как объекту уголовно-правовой охраны и для восполнения пробела уголовно-правовой доктрины в части неразработанности понятия неприкосновенности персональных данных предлагается ввести в научный оборот ее определение. Под неприкосновенностью персональных данных предлагается понимать самостоятельное право человека, представляющее собой гарантированные государством правомочия контролировать свои персональные данные, разрешать или ограничивать доступ к ним с определением порядка и условий такого доступа и требовать защиты в случае его нарушения.

4. Принимая во внимание, что персональные данные – это информация, непосредственно связанная с человеком, уголовно-правовой механизм охраны неприкосновенности персональных данных следует понимать в *двух значениях*: как совокупность норм, обеспечивающих конституционные гарантии неприкосновенности персональных данных, и в том числе при автоматизированной или иной их обработке в различных сферах общественных отношений, и как элемент государственной защиты других прав и свобод человека (личных, социальных, экономических, политических), подвергающихся угрозе через противоправные деяния с чужими персональными данными или в отношении них.

5. В целях предупреждения совершения преступлений с персональными данными в перечень обстоятельств, отягчающих наказание, надлежит включить новое обстоятельство «совершение преступления с использованием персональных данных» (п. «т» ч. 1 ст. 63 УК РФ).

Заключение

В диссертационной работе в рамках поставленных целей были исследованы вопросы уголовно-правовой охраны персональных данных. К новым научным результатам, которые могут быть использованы для модернизации уголовного закона и дальнейшего развития науки уголовного права могут служить следующие *основные положения и выводы проведенного исследования*:

1. На основе имеющихся в доктрине разрозненных доктринальных знаний о феномене персональных данных, обобщения следственно-судебной практики и статистических данных для теории уголовного права впервые сформулированы основания уголовной ответственности за незаконные действия с персональными данными.

2. Для разрешения проблемы отсутствия единообразного понимания и правильной оценки персональных данных как предмета преступления или его средства предложен новый теоретико-правовой подход к понятию персональных данных, выявлены их сущностные признаки для науки уголовного права и правоприменительной практики.

3. В целях совершенствования механизма уголовно-правового обеспечения неприкосновенности персональных данных проведен анализ норм международного права и сравнительно-правовое исследование уголовного законодательства зарубежных государств об охране персональных данных. С учетом сложившихся подходов в зарубежном праве выделены *две основные группы преступлений*, обеспечивающих неприкосновенность персональных данных человека. *Первой* является *группа уголовно наказуемых деяний*, не связанных с получением и обработкой персональных данных; *вторую группу преступлений* составляют посягательства, связанные с нарушениями операторами персональных данных требований получения, автоматизированной обработки, хранения и передачи, установленных для обеспечения их безопасности. На основании приведенной классификации определена основная тенденция развития зарубежного законодательства, состоящая в придании самостоятельного уголовно-правового значения персональным данным и установлении уголовной

ответственности за незаконные действия в отношении информационных баз персональных данных.

4. Проведено комплексное исследование схожих по смыслу сперсональными данными понятий, затрагивающих область частной жизни человека. На основе системного анализа понятий «персональные данные», «частная жизнь», «личная тайна» и «семейная тайна», их соотношения и разграничения в сущностных признаках сформулированы выводы о том, что понятия «частная жизнь» и «персональные данные» пересекаются, однако исключают полное содержательное совпадение, а потому не могут толковаться как тождественные и даже синонимичные. Эти феномены представляют собой ряд близких, обусловленных объективной неразрывной связью понятий, но имеющих не только неодинаковое сущностное, но и правовое значение. Различаются они и режимами правовой охраны: в случае с персональными данными их конфиденциальность предполагает иную форму ограничения доступа к ним, использования и распространения, отличающуюся от режима тайны применительно к частной жизни, личной или семейной тайне, что должно учитываться при конкретизации объекта уголовно-правовой охраны и предмета преступлений, связанных с персональными данными.

5. По результатам исследования правоприменительной практики по толкованию категории «общедоступность» сформулированы подходы к пониманию персональных данных, размещенных в социальных сетях и других открытых онлайн-ресурсах, как доступной информации, собирание или распространение которой не влечет уголовную ответственность. Для целей уголовного права, исходя из разности правового режима открытой информации и информации ограниченного доступа, предлагается толковать понятия «общедоступность» и «конфиденциальность» применительно к персональным данным противоположными и взаимоисключающими.

6. Аргументирована специальная защита персональных данных путем установления уголовной ответственности за общественно опасные деяния против них. Проектируемый состав преступления о нарушении неприкосновенности

персональных данных (ст. 137^1 УК РФ) предлагается ввести в главу 19 УК РФ по признаку общности видового объекта со ст. 137 УК РФ (частная жизнь) и прочими посягательствами против конституционных прав и свобод человека и гражданина. Объектом здесь следует признать неприкосновенность персональных данных, а предметом – конкретные сведения, при определенных признаках характеризующиеся как персональные данные. Уголовно-правовой охране здесь подлежит та часть права на неприкосновенность персональных данных, которая даже в условиях действия запрета на вторжение в частную жизнь остается незащищенной, подвергается посягательству помимо или против воли человека. Воплощение идеи нового понимания неприкосновенности персональных данных как объекта специального состава преступления с его структурным расположением в разделе о преступлениях против личности повысит качество уголовно-правового инструментария по противодействию этому виду преступности. Объективная потребность в независимой от частной жизни, а самостоятельной охране персональных данных уголовным правом обусловлена и обеспечением защиты других личных, социальных, экономических, политических прав человека, страдающих от сопутствующих преступлений.

7. Уголовно-правовой механизм охраны неприкосновенности персональных данных следует понимать в *двух значениях*: как совокупность норм, обеспечивающих конституционные гарантии неприкосновенности персональных данных, и в том числе при автоматизированной или иной их обработке в различных сферах общественных отношений, и как элемент государственной защиты других прав и свобод человека (личных, социальных, экономических, политических), подвергающихся угрозе через противоправные деяния с чужими персональными данными или в отношении них.

8. Раскрыто содержание наиболее дискуссионных вопросов, возникающих в научной доктрине при характеристике объективных и субъективных признаков преступлений с персональными данными, и определены проблемы правоприменительной практики по вопросам их квалификации. В целях совершенствования специальной методики оценки незаконных действий с

персональными данными в механизме совершения должностных, служебных преступлений, преступлений против конституционных прав и свобод человека и гражданина, преступлений в сфере компьютерной информации и ограничения правоприменительного усмотрения разработаны рекомендации по устранению квалификационных ошибок, представленные в формате разъяснений Пленума Верховного Суда РФ (в качестве дополнения ППВС № 46) (*Приложение* 1).

9. Неэффективность действующих уголовно-правовых инструментов обусловила разработку авторской модели перспективных направлений развития российского уголовного законодательства. На основе международных стандартов, опыта зарубежных стран, правоприменительной практики и научной доктрины в работе представлен проект новой нормы для введения ее в УК России ст. 137^1 УК РФ «Нарушение неприкосновенности персональных данных».

В завершение исследования вопросов уголовно-правового противодействия преступлениям, совершаемым в отношении персональных данных или с их использованием, следует наметить пути, по которым должна развиваться наука уголовного права и правоприменение. Из результатов исследования приговоров и других уголовно-процессуальных актов (обвинительных заключений, постановлений о прекращении уголовных дел, применении судебного штрафа) об использовании уголовно-правовых норм, прямо или косвенно обеспечивающих охрану персональных данных, следует, что фактически отсутствует какая-либо судебная практика привлечения к уголовной ответственности так называемых «покупателей» персональных данных. В постановленных приговорах они значатся как «неустановленные следствием лица». Между тем именно они, «приобретатели персональных данных», «заказчики» этих услуг, инициируют и поддерживают спрос, способствуя массовому копированию и распространению чужих личных данных теми, кто имеет доступ к персональным данным по службе или по должности, и которые используются в дальнейшем, как правило, для совершения преступлений в отношении их владельцев.

Внимания законодателя требует и юридическая защита приватности персональных данных в социальных сетях, иных интернет-платформах и онлайн-

ресурсах, где конфиденциальная персональная информация о человеке предается огласке без его согласия или помимо его воли, либо не соответствует действительности ввиду несвоевременной ее актуализации.

В ряде стран дальнего зарубежья и бывшего СССР имеются концептуальные новации охраны персональных данных, аналогов которых в российской уголовно-правовой модели нет. Многие из них представляются вполне обоснованными и могут быть введены в российскую юридическую практику. Национальным правом может быть заимствована идея уголовной ответственности за незаконное использование изображений человека как биометрических персональных данных без его согласия в СМИ, социальных сетях, по ТВ (фото, видео). Подводя итоги работы, следует предложить и расширение перечня защищаемых персональных данных, включив в него генетические данные человека для обеспечения их надлежащей защиты, и разработку в этой связи нового направления научных исследований в праве. Думается, что эти и другие предложения автора будут способствовать созданию единой концепции уголовно-правовой борьбы с преступлениями в отношении персональных данных или с их использованием, что позволит в ближайшей перспективе осуществлять эффективное уголовно-правовое и иное противодействие всему комплексу незаконных действий с персональными данными.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ

Международные нормативные правовые акты и иные официальные документы

1. Декларация Будапештской инициативы «Открытый доступ» [Электронный ресурс]. – URL: https://www.budapestopenaccessinitiative.org/translations/russian-translation (дата обращения: 24.12.2022).

2. Закон о защите данных 2018 г. (Data Protection Act 2018 (DPA 2018)) [Электронный ресурс]. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (дата обращения: 21.09.2022).

3. Конвенция о защите физических лиц при автоматизированной обработке персональных данных: заключена в г. Страсбурге 28.01.1981 (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15.06.1999) [Текст] // СЗ РФ. – 2014. – № 5, ст. 419.

4. О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных: регламент (EU) от 27.04.2016 № 2016/679 [Электронный ресурс]. – URL: https://ogdpr.eu/ru/gdpr-2016-679 (дата обращения: 21.05.2022).

5. О защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования уголовных преступлений, ведения розыскных или судебных действий или исполнения уголовных наказаний, а также за свободное перемещение таких данных: директива (EU) от 27.04.2016 № 2016/680 [Электронный ресурс]. – URL: https://ogdpr.eu/ru/gdpr-2016-680 (дата обращения: 21.05.2022).

6. О персональных данных: Модельный закон: принят на четырнадцатом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ постановлением от 16.10.1999 № 14-19 [Текст] // Информационный бюллетень Межпарламентской ассамблеи государств-участников СНГ. – 2000. – № 23.

7. Протокол о внесении изменений в Конвенцию о защите физических лиц при автоматизированной обработке персональных данных (ETS № 223) [Текст] // Бюллетень Европейского суда по правам человека. – 2018. – № 12. – С. 102 –111.

8. Хартия Европейского Союза об основных правах: принята в г. Страсбурге 12.12.2007 [Текст] // Журнал № С 202. – 7.6.2016. – С. 389.

Нормативные правовые акты

и иные официальные документы Российской Федерации

9. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. (с изм. и доп. от 04.10.2022, № 5-ФКЗ, № 6-ФКЗ, № 7-ФКЗ, № 8-ФКЗ) [Текст] // Рос. газета. – 1993. – 25 декабря; Официальный интернет-портал правовой информации (www.pravo.gov.ru). – 2022. – 06 окт. – № 0001202210060013.

10. Уголовный кодекс Российской Федерации (с изм. и доп. от 04.08.2023, № 413-ФЗ) [Текст] // СЗ РФ. – 1996. – № 25, ст. 2954; Рос. газета. – 2023. – 08 авг.

11. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (с изм. и доп. от 04.08.2023, № 426-ФЗ) [Текст] // Рос. газета. – 2001. – 31 дек.; 2023. – 09 авг.

12. Налоговый кодекс Российской Федерации (часть первая) от 31.07.1998 № 146-ФЗ (с изм. и доп. от 04.08.2023, № 425-ФЗ) [Текст] // Рос. газета. – 1998. – 6 авг.; 2023. – 09 авг.

13. О банках и банковской деятельности: федер. закон от 02.12.1990 № 395-1 (с изм. и доп. от 04.08.2023, № 417-ФЗ) [Текст] // Рос. газета. – 1996. – 10 февр.; 2023. – 8 авг.

14. О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных: федер. закон от 19.12.2005 № 160-ФЗ [Текст] // Рос. газета. – 2005. – 22 дек.

15. О персональных данных: федер. закон от 27.07.2006 № 152-ФЗ (с изм. и доп. от 06.02.2023, № 8-ФЗ) [Текст] // Рос. газета. – 2006. – 29 июля; 2023. – 9 февр.

16. Об информации, информационных технологиях и о защите информации: федер. закон от 27.07.2006 № 149-ФЗ (с изм. и доп. от 31.07.2023, № 408-ФЗ) [Текст] // Рос. газета. – 2006. – 29 июля; 2023. – 3 авг.

17. О внесении изменений в Федеральный закон «О персональных данных»: федер. закон от 25.07.2011 № 261-ФЗ [Текст] // СЗ РФ. – 2011. – № 31, ст. 4701.

18. О внесении изменений в Федеральный закон «О персональных данных»: федер. закон от 30.12.2020 № 519-ФЗ [Текст] // Рос. газета. – 2021. – 11 янв.

19. Об утверждении Перечня сведений конфиденциального характера: указ Президента РФ от 06.03.1997 № 188 (с изм. и доп. от 13.07.2015, № 357) [Текст] // Рос. газета. – 1997. – 14 марта; СЗ РФ. – 2015. – № 29 (ч. II), ст. 4473.

20. Доктрина информационной безопасности Российской Федерации: указ Президента РФ от 05.12.2016 № 646 [Текст] // Рос. газета. – 2016. – 6 дек.

21. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: указ Президента РФ от 09.05.2017 № 203 [Текст] // СЗ РФ. 2017. № 20, ст. 2901.

22. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: указ Президента РФ от 07.05.2018 № 204 (с изм. и доп. от 21 июля 2020 г. № 474) [Текст] // СЗ РФ. 2018. № 20, ст. 2817; 2020. № 30, ст. 4884.

23. О Стратегии национальной безопасности Российской Федерации: указ Президента РФ от 02.07.2021 № 400 [Текст] // СЗ РФ. – 2021. – № 27 (ч. II), ст. 5351.

24. Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления на их официальных сайтах в информационно-телекоммуникационной сети «Интернет» в форме открытых данных: постановление Правительства РФ от 10.07.2013 № 583 (с изм. и доп. от 10.11.2022, № 2025) [Текст] // СЗ РФ. – 2013. – № 30 (ч. II), ст. 4107; 2022. – № 46, ст. 8027.

25. Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку,

включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации»: постановление Правительства РФ от 30.06.2018 № 772 [Текст] // СЗ РФ. – 2018. – № 28, ст. 4234.

26. О случаях и сроках использования биометрических персональных данных, размещенных физическими лицами в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица»: постановление Правительства РФ от 15.06.2022 № 1067 [Текст] // СЗ РФ. – 2022. – № 25, ст. 4337.

27. О Перечнях информации о деятельности государственных органов, органов местного самоуправления, размещаемой в сети Интернет в форме открытых данных: распоряжение Правительства РФ от 10.07.2013 № 1187-р [Электронный ресурс]. Доступ из справ.-прав. системы «Гарант».

28. О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки»: разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30.08.2013: разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки [Электронный ресурс]. Доступ из справ.-правовой системы «Гарант».

29. Об утверждении Положения о защите персональных данных работников Федерального фонда обязательного медицинского страхования: приказ Федерального фонда ОМС от 19.08.2008 № 180 (с изм. и доп. от 23.03.2009, № 53) [Текст] // Рос. газета. – 2008. – 17 сент.; 2009. – 28 апр.

30. Методические рекомендации Генеральной прокуратуры Российской Федерации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс]. Доступ из справ.-прав. системы «КонсультантПлюс».

31. О внесении изменений в Федеральный закон «О персональных данных» в части установления особенностей обработки общедоступных персональных данных»: пояснительная записка к проекту федерального закона № 1057337-7 [Электронный ресурс] // Официальный сайт Государственная Думы РФ. URL: https://sozd.duma.gov.ru/bill/1057337-7 (дата обращения 19.01.2022).

32. ГОСТ Р 58833-2020. Защита информации. Идентификация и аутентификация. Общие положения: утв. приказом Федерального агентства по техническому регулированию и метрологии от 10.04.2020 № 159-ст [Электронный ресурс]. Доступ из справ.-прав. системы «КонсультантПлюс».

Нормативные правовые акты Российской Федерации, утратившие юридическую силу

33. Об информации, информатизации и защите информации: федер. закон от 20.02.1995 № 24-ФЗ (утратил силу) [Текст] // Рос. газета. – 2006. – 11 июля.

Зарубежные нормативные правовые акты

34. Уголовный кодекс Республики Армения (с изм. и доп. от 24.05.2022) [Электронный ресурс] // Законодательство стран СНГ. – URL: https://base.spinform.ru/show_doc.fwx?rgn=7472 (дата обращения: 04.08.2022).

35. Уголовный кодекс Республики Беларусь (с изм. и доп. от 13.05.2022) [Электронный ресурс] // Законодательство стран СНГ. – URL: https://online.zakon.kz/Document/?doc_id=30414984&doc_id2=30414984#activate_doc=2&pos=6;-98&pos2=1840;-97 (дата обращения: 24.07.2022).

36. Уголовный кодекс Грузии (Criminal Code of Georgia) (с изм. и доп. от 18.04.2022) [Электронный ресурс]. – URL: https://www.legislationline.org/download/id/8847/file/Georgia_Criminal_Code_am2020_ru.pdf (дата обращения: 22.07.2022).

37. Уголовный кодекс Испании (Codigo Penal de Espana) (с изм. и доп. от 13.03.2022) [Электронный ресурс]. – URL: http://noticias.juridicas.com/base_datos/Penal/lo10-1995.html (дата обращения: 13.08.2022).

38. Уголовный кодекс Республики Казахстан от 03.07.2014 № 226-V (с изм. и доп. от 27.06.2022) [Текст] // Казахстанская правда. – 2014. – 09 июля; 2022. – 28 июня.

39. Уголовный кодекс Королевства Дания (Danish Criminal Code) (с изм. и доп. от 11.08.2021) [Электронный ресурс]. – URL: http://www.unodc.org/tldb/pdf/Denmark_Criminal_Code_2016.pdf (дата обращения: 29.07.2022).

40. Уголовный кодекс Королевства Нидерланды (Wetboek van Strafrecht van Nederland) (с изм. и доп. от 14.04.2021) [Электронный ресурс]. – URL: http://www.wetboek-online.nl/wet/Sr.html (дата обращения: 12.08.2022).

41. Уголовный кодекс Кыргызской Республики (с изм. и доп. от 09.08.2022) [Электронный ресурс] // Законодательство стран СНГ. – URL: https://base.spinform.ru/show_doc.fwx?rgn=94723 (дата обращения: 14.08.2022).

42. Уголовный кодекс Латвийской Республики (Krimināllikums) (с изм. и доп. от 23.05.2022) [Электронный ресурс]. – URL: https://www.legislationline.org/documents/section/criminal-codes/country/19/Kyrgyzstan/show (дата обращения: 06.08.2022).

43. Уголовный кодекс Лихтенштейна [Текст] / под ред. А.В. Серебренниковой. – М.: МАКС Пресс, 2013. – 188 с.

44. Уголовный кодекс Республики Таджикистан (с изм. и доп. от 19.07.2022) [Электронный ресурс] // Законодательство стран СНГ. – URL: http://base.spinform.ru/show_doc.fwx?rgn=2324 (дата обращения: 27.07.2022).

45. Уголовный кодекс Республики Узбекистан (с изм. и доп. от 23.06.2022) [Электронный ресурс] // Законодательство стран СНГ. – URL: https://online.zakon.kz/Document/?doc_id=30421110&pos=1670;56#pos=1670;56 (дата обращения: 27.07.2022).

46. Уголовный кодекс Украины (с изм. и доп. от 14.04.2022) [Электронный ресурс] // Законодательство стран СНГ. – URL: https://online.zakon.kz/Document/?doc_id=30418109&pos (дата обращения: 04.08.2022).

47. Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия (German criminal code) (с изм. и доп. от 19.06.2021) [Электронный ресурс]. – URL: http://www.gesetze-im-internet.de/englisch_stgb/ (дата обращения: 15.08.2022).

48. Уголовный кодекс Французской Республики (Code pénal France) (с изм. и доп. от 01.06.2022) [Электронный ресурс]. – URL: https://www.legifrance.ouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 (дата обращения: 21.07.2022).

49. Уголовный кодекс Швейцарской Конфедерации (Swiss Criminal Code) (с изм. и доп. от 01.07.2021) [Электронный ресурс]. – URL: https://www.legislationline.org/download/id/8991/file/SWITZ_Criminal%20Code_as%20of%202020-07-01.pdf (дата обращения: 07.08.2022).

50. Уголовный кодекс Швеции (Criminal code of the Kingdom of Sweden) (с изм. и доп. от 12.03.2022) [Электронный ресурс]. – URL: http://www.legislationline.org/documents/section/criminal-codes (дата обращения: 14.08.2022).

51. Уголовный кодекс Республики Японии (Criminal code of the Republic of Japan) (с изм. и доп. от 23.11.2021) [Электронный ресурс]. – URL: http://www.cas.go.jp/jp/seisaku/hourei/data/PC.pdf (дата обращения: 15.08.2022).

52. О персональных данных: закон Азербайджанской Республики от 11.05.2010 № 998-IIIQ (с изм. и доп. от 03.04.2018) [Текст] // Азербайджан. – 2010. – 06 июня; 2018. – 06 мая.

53. О защите персональных данных от 13.06.2015 № ЗР-49 [Текст] // Официальные ведомости Республики Армения. – 2015. – 18 июня; 2019. – 25 июля.

54. Об изменении кодексов по вопросам уголовной ответственности: закон Республики Беларусь от 26.05.2021 № 112-З [Электронный ресурс] //

Национальный правовой Интернет-портал Республики Беларусь. – 2021. – 8 июня, № 2/2832.

55. О персональных данных и их защите: закон Республики Казахстан от 21.05.2013 № 94-V (с изм. и доп. от 30.12.2021) [Текст] // Казахстанская правда. – 2013. – 25 мая; 2021. – 31 дек.

56. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информатизации: закон Республики Казахстан от 24.11.2015 № 419-V [Текст] // Казахстанская правда. – 2015. – 26 нояб.

57. О персональных данных: закон Республики Узбекистан от 02.07.2019 № ЗРУ-547 (с изм. и доп. от 14.01.2021) [Текст] // Национальная база данных законодательства. – 2019. – 03 июля.

58. О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан: закон Республики Узбекистан от 29.10.2021 № ЗРУ-726 [Текст] // Народное слово. – 2021. – 30 окт.

59. О соответствии Конституции Республики Беларусь Закона Республики Беларусь «Об изменении кодексов по вопросам уголовной ответственности»: решение Конституционного Суда Республики Беларусь от 17.05.2021 № Р-1270/2021 [Текст] // Вестник Конституционного Суда Республики Беларусь. – 2021. – № 2.

Монографии

60. *Бачило, И.Л.* Персональные данные в структуре информационных ресурсов. Основы правового регулирования [Текст] / И.Л. Бачило, Л.А. Сергиенко, Б.В. Кристальный, А.Г. Арешев. – Минск: Беллитфонд, 2006. – 474 с.

61. *Букалерова, Л.А.* Уголовно-правовая охрана официального информационного оборота / под ред. В.С. Комиссарова, Н.И. Пикурова [Текст] / Л.А. Букалерова. – М.: Юрлитинформ, 2006. – 354 с.

62. *Елин, В.М.* Уголовно-правовая охрана некоторых категорий информации ограниченного доступа [Текст] / В.М. Елин. – М.: Академия сферы социальных отношений, 2010. – 215 с.

63. *Кадников, Б.Н.* Уголовно-правовая охрана неприкосновенности частной жизни: научно-практическое пособие / под ред. Н.Г. Кадникова [Текст] / Б.Н. Кадников. 2-е изд., доп. – М.: Юриспруденция, 2017. – 119 с.

64. *Коган, В.М.* Социальный механизм уголовно-правового воздействия [Текст] / В.М. Коган. – М.: Наука, 1983. – 183 с.

65. *Коробеев, А.И.* Уголовная наказуемость общественно опасных деяний (основания установления, характер и реализация в деятельности органов внутренних дел): учебное пособие [Текст] / А.И. Коробеев. – Хабаровск: Хабаровская высшая школа МВД СССР, 1986. – 79 с.

66. *Коробеев, А.И.* Советская уголовно-правовая политика: проблемы декриминализации и пенализации [Текст] / А.И. Коробеев. – Владивосток: Изд-во Дальневост. ун-та, 1987. – 268 с.

67. *Красавчикова, Л.О.* Личная жизнь граждан под охраной закона [Текст] / Л.О. Красавчикова. – М.: Юрид. лит., 1983. – 160 с.

68. *Маркунцов, С.А.* Уголовно-правовой запрет: теоретический аспект [Текст] / С.А. Маркунцов. – М.: Юрлитинформ, 2007. – 112 с.

69. Основания уголовно-правового запрета. Криминализация и декриминализация [Текст] / отв. ред.: В.Н. Кудрявцев, А.М. Яковлев. – М.: Наука, 1982. – 303 с.

70. *Петров, В.Н.* Информационные системы [Текст] / В.Н. Петров. – СПб.: Питер, 2002. – 687 с.

71. *Петрухин, И.Л.* Личные тайны (Человек и власть) [Текст] / И.Л. Петрухин. – М.: Изд-во ИГиП РАН, 1998. – 232 с.

72. *Петрыкина, Н.И.* Правовое регулирование оборота персональных данных. Теория и практика [Текст] / Н.И. Петрыкина. – М.: Статут, 2011. – 131 с.

73. *Терещенко, Л.К.* Правовой режим информации [Текст] / Л.К. Терещенко. – М.: Юриспруденция, 2007. – 133 с.

Учебники, учебные и иные пособия, лекции, комментарии

74. *Бачило, И.Л.* Информационное право: учебник [Текст] / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов. – СПб.: Юрид. центр Пресс, 2001. – 789 с.

75. *Бачило, И.Л.* Информационное право [Текст] / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов; под ред. Б.Н. Топорнина. 2-е изд., с изм. и доп. – СПб.: Юридический центр Пресс, 2005. – 723 с.

76. Комментарий к Федеральному закону «О персональных данных» (постатейный): от 27 июля 2006 г. № 152-ФЗ [Текст] / М.И. Петров. – М.: Юстицинформ, 2007. – 155 с.

77. Комментарий к Конституции Российской Федерации [Текст] / под ред. В.Д. Зорькина, Л.В. Лазарева. – М.: Эксмо, 2009. – 1056 с.

78. Комментарий к Уголовному кодексу Российской Федерации [Текст] / отв. ред. В.М. Лебедев. 13-е изд., перераб. и доп. – М.: Юрайт, 2013. – 1359 с.

79. Криминология. 5-е изд., перераб. и доп. [Текст] / под ред. В.Н. Кудрявцева и В.Е. Эминова. – М.: Норма-ИНФРА-М, 2022. – 800 с.

80. *Мазуров, В.А.* Тайна: государственная, коммерческая, банковская, частной жизни. Уголовно-правовая защита: учебное пособие [Текст] / В.А. Мазуров. – М.: Дашков и К°, 2003. – 152 с.

81. *Савельев, А.И.* Комментарий к Федеральному закону от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (постатейный) [Текст] / А.И. Савельев. – М.: Статут, 2015. – 318 с.

82. *Савельев, А.И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» [Текст] / А.И. Савельев. – М.: Статут, 2017. – 543 с.

83. *Савельев, А.И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных» [Текст] / А.И. Савельев. 2-е изд., перераб. и доп. – М.: Статут, 2021. – 466 с.

84. Уголовный закон в практике мирового судьи: научно-практическое пособие [Текст] / под ред. А.В. Галаховой. 2-е изд., доп. – М.: Норма, 2007. – 623 с.

85. Уголовное право. Особенная часть: учебник [Текст] / под ред. В.Н. Петрашева. – М.: Приор: Эксперт. Бюро, 1999. – 607 с.

86. Уголовное право. Общая часть: специализированный учебник для юридического колледжа [Текст] / под ред. В.П. Бодаевского, В.М. Зимина, А.И. Чучаева. – М.: Проспект, 2017. – 251 с.

87. Уголовное уложение (Уголовный кодекс) Федеративной Республики Германия: Strafgesetzbuch (StGB): научно-практический комментарий и перевод текста закона [Текст] / П.В. Головненков. – Постдам: Universitätsverlag Potsdam, 2021. – 311 с.

88. Федеральный закон «О персональных данных»: научно-практический комментарий [Текст] / под ред. заместителя руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций А.А. Приезжевой. – М.: Редакция «Российской газеты», 2015. – Вып. 11. – 176 с.

Статьи в сборниках, материалы конференций, тезисы выступлений, доклады, информационные сообщения

89. *Абламейко, М.С.* Правовое регулирование персональных данных с учетом введения ID-карт и биометрических паспортов [Текст] / М.С. Абламейко // Журнал Белорусского государственного университета. – 2018. – № 1. – С. 14–20.

90. *Авдеев, М.Ю.* Нормативное содержание права на неприкосновенность частной жизни [Текст] / М.Ю. Авдеев // Новый юридический журнал. – 2013. – № 1. – С. 49–54.

91. *Алексашина, М.Н.* Защита персональных данных как условие обеспечения безопасности личности [Текст] / М.Н. Алексашина // Право и безопасность. – 2014. – № 1. – С. 68–73.

92. *Алексеенцев, А.И.* О составе защищаемой информации [Текст] / А.И. Алексеенцев // Безопасность информационных технологий. – 1999. – № 2. – С. 5–7.

93. *Алихаджиева, И.С.* Криминологические риски персональных данных: основные тенденции и прогнозы [Текст] / И.С. Алихаджиева // Известия Юго-Западного государственного университета. Серия: История и право. – 2023. – Т. 13, № 3. – С. 90–101.

94. *Антонов, А.Д.* Принципы криминализации общественно опасных деяний в уголовно-правовой науке [Текст] / А.Д. Антонов // Вестник Московского университета. Серия 11: Право. – 2000. – № 4. – С. 79–90.

95. *Атагимова, Э.И.* «Кража личности» как самостоятельное преступление или разновидность мошенничества [Текст] / Э.И. Атагимова, А.Т. Потемкина, И.Г. Цопанова // Правовая информатика. – 2017. – № 3. – С. 14–22.

96. *Афанасьева, О.В.* Право на неприкосновенность частной жизни. Укрепляет ли его закон о персональных данных? [Текст] / О.В. Афанасьева // Общественные науки и современность. – 2011. – № 6. – С. 76–88.

97. *Баринов, С.В.* О криминализации преступного нарушения неприкосновенности частной жизни, совершаемого в форме распространения баз персональных данных [Текст] / С.В. Баринов // Российский следователь. – 2017. – № 4. – С. 35–38.

98. *Баринов, С.В.* Содержание и особенности проведения тактической операции «задержание с поличным» по делам о преступных нарушениях неприкосновенности частной жизни [Текст] / С.В. Баринов // Актуальные проблемы российского права. – 2018. – № 11 (96). – С. 222–229.

99. *Бартошко, Т.В.* Защита персональных данных как важная составляющая общей безопасности банка [Текст] / Т.В. Бартошко, А.П. Стерхов // Вестник Иркутского государственного технического университета. – 2015. – № 5 (100). – С. 177–182.

100. *Бачило, И.Л.* Информация и информационные отношения в праве [Текст] / И.Л. Бачило // НТИ. Сер. 1. – 1999. – № 8. – С. 22–28.

101. *Бегишев, И.Р.* Проблемные вопросы уголовно-правовой охраны персональных данных [Текст] / И.Р. Бегишев, Д.В. Кирпичников // Уголовная юстиция. – 2020. – № 15. – С. 11–16.

102. *Бодаевский, В.П.* Социальная обусловленность уголовно-правового положения [Текст] / В.П. Бодаевский, Е.А. Соловьев // Научный вестник Омской академии МВД России. – 2020. – № 1 (76). – С. 20–25.

103. *Бронников, Д.А.* Передача и распространение массивов персональных данных. Общественная опасность и перспективы криминализации подобных деяний [Текст] / Д.А. Бронников // Молодые учёные России: сб. ст. VI всерос. науч.-практ. конф. – Пенза, 2021. – С. 165–167.

104. *Бугера, М.А.* Борьба с хищениями сотовых телефонов и персональных данных, содержащихся в них: проблемы и пути решения [Текст] / М.А. Бугера // Вестник Санкт-Петербургского университета МВД России. – 2022. – № 2 (94). – С. 108–113.

105. *Букалерова, Л.А.* Информация, содержащая фотографии (изображения) человека, нуждается в уголовно-правовой защите [Текст] / Л.А. Букалерова, А.В. Остроушко // Правовые вопросы связи. – 2007. – № 1. – С. 42–44.

106. *Бундин, М.В.* Персональные данные как информация ограниченного доступа [Текст] / М.В. Бундин // Информационное право. – 2009. – № 1. – С. 10–14.

107. *Бундин, М.В.* Система информации ограниченного доступа и конфиденциальность [Текст] / М.В. Бундин // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2015. – № 1. – С. 120–130.

108. *Буркова, А.Ю.* Определение понятия «персональные данные» [Текст] / А.Ю. Буркова // Право и экономика. – 2015. – № 4. – С. 20–24.

109. *Бучакова, М.А.* Персональные данные и их защита в условиях цифровизации общества [Текст] / М.А. Бучакова // Алтайский юридический вестник. – 2021. – № 2 (34). – С. 44–48.

110. *Вабищевич, В.В.* Определение персональных данных в целях их уголовно-правовой охраны [Текст] / В.В. Вабищевич // Вестник Полоцкого государственного университета: научно-теоретический журнал. – 2019. – № 14. – С. 134–139.

111. *Вабищевич, В.В.* Зарубежный опыт уголовно-правовой охраны персональных данных [Текст] / В.В. Вабищевич // Журнал Белорусского государственного университета. Право. – 2019. – № 1. – С. 72–80.

112. *Вабищевич, В.В.* Опыт уголовно-правовой охраны персональных данных Казахстана и Германии [Текст] / В.В. Вабищевич // Борьба с преступностью: теория и практика: тез. докл. VIII междунар. науч.-практ. конф. (23 апреля 2020 г.). – Могилев: Изд-во Могил. ин-та МВД РБ, 2020. – С. 23–25.

113. *Вабищевич, В.В.* К вопросу об уголовно-правовой защите от посягательств на персональные данные с использованием компьютерных и сетевых технологий [Текст] / В.В. Вабищевич // Право.by: научно-практический журнал. – 2020. – № 5. – С. 43–48.

114. *Вабищевич, В.В.* Персональные данные: пределы и объем их уголовно-правовой охраны [Текст] / В.В. Вабищевич // Вестник Гродненского государственного университета имени Янки Купалы. Серия 4: Правоведение. – 2020. – Т. 10, № 2. – С. 83–90.

115. *Важорова, М.А.* Соотношение понятий «Информация о частной жизни» и «Персональные данные» [Текст] / М.А. Важорова // Вестник Саратовской государственной юридической академии. – 2012. – № 4 (87). – С. 55–59.

116. *Ветров, Д.М.* Защита персональных данных и защита информации на предприятии. Некоторые спорные вопросы применения [Текст] / Д.М. Ветров // Проблемы права. – 2010. – № 1 (21). – С. 114–121.

117. *Винюкова, И.В.* Неприкосновенность частной жизни как принцип правового регулирования отношений в сфере защиты информации [Текст] / И.В. Винюкова, С.Е. Кузахметова // Правовая культура. – 2007. – № 1 (2). – С. 148–154.

118. *Войниканис, Е.А.* Неприкосновенность частной жизни, персональные данные и ответственность за незаконные сбор и распространение сведений о частной жизни и персональных данных: проблемы совершенствования законодательства [Текст] / Е.А. Войникас, Е.О. Машукова, В.Г. Степанов-Егиянц // Законодательство: право для бизнеса. – 2014. – № 12. – С. 74–80.

119. *Волошкин, И.Г.* Универсальный идентификатор сведений о гражданине: мировой опыт и возможности введения в Российской Федерации [Текст] /

И.Г. Волошкин, Е.В. Андреева // Вестник университета. – 2014. – № 15. – С. 260–265.

120. *Гарбатович, Д.А.* Защита персональных данных уголовным правом [Текст] // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 2 (4). – С. 10–13.

121. *Грибанова, Д.* Неправомерный доступ к сведениям, составляющим тайну, в России, США и Великобритании [Текст] / Д. Грибанова, М. Филатова // Уголовное право. – 2020. – № 5. – С. 13–24.

122. *Гришаев, С.П.* Право на неприкосновенность частной жизни [Текст] / С.П. Гришаев // Гражданин и права. – 2012. – № 11. – С. 24–27.

123. *Губарева, А.В.* Угрозы безопасности персональных данных: проблемы современности [Текст] / А.В. Губарева, А.Н. Гулемин // Политика и общество. – 2015. – № 2. – С. 151–158.

124. *Гуде, С.В.* Защита персональных данных в Российской Федерации: исторический аспект и современное состояние [Текст] / С.В. Гуде, П.В. Арбузов, А.Г. Карпика // Юристъ-Правоведъ. – 2015. – № 2 (69). – С. 93–97.

125. *Давыдова, М.Л.* Средства юридической техники и проблема ограничения прав и свобод человека [Текст] / М.Л. Давыдова // Юриспруденция. – 2010. – № 2. – С. 29–36.

126. *Дагель, П.С.* Условия установления уголовной наказуемости [Текст] / П.С. Дагель // Правоведение. – 1975. – № 4. – С. 67–74.

127. *Дивольд, В.Е.* Предпосылки создания национальной системы биометрической идентификации личности [Текст] / В.Е. Дивольд // Научный вестник Омской академии МВД России. – 2021. – Т. 27. – № 2 (81). – С. 139–143.

128. *Добробаба, М.Б.* Понятие персональных данных: проблема правовой определенности [Текст] / М.Б. Добробаба // Вестник Университета имени О.Е. Кутафина. – 2023. – № 2 (102). – С. 42–52.

129. *Дремлюга, Р.И.* Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ [Текст] / Р.И. Дремлюга // Уголовное право. – 2018. – № 4. – С. 56–57.

130. *Дремлюга, Р.И.* Критическая информационная структура как предмет преступного посягательства [Текст] / Р.И. Дремлюга, С.С. Зотов, В.Ю. Павлинская // Азиатско-Тихоокеанский регион: экономика, политика, право. – 2019. – № 21 (2). – С. 130–139.

131. *Дударева, М.А.* Сведения о частной жизни лица как составляющая данных предварительного расследования: особенности запрета на разглашение // Закон и право. – 2022. – № 10. – С. 164–166.

132. *Дятленко, В.В.* Законодательство о защите персональных данных: проблемы и решения [Текст] / В.В. Дятленко, Е.К. Волчинская // Информационное право. – 2006. – № 1. – С. 11–16.

133. *Егорова, Н.А.* Ответственность за «служебные» мошенничества: необходимость новых подходов [Текст] / Н.А. Егорова // Российская юстиция. – 2014. – № 8. – С. 19–22.

134. *Елисеева, А.А.* Семейная тайна: вопросы содержания и правовой охраны [Текст] / А.А. Елисеева // Актуальные проблемы российского права. – 2018. – № 4 (89). – С. 71–76.

135. *Ершов, М.А.* Законы и иные нормативные правовые акты как юридический аргумент применения бланкетных норм об уголовной ответственности за посягательства на экономическую конфиденциальную информацию [Текст] / М.А. Ершов // Юридическая техника. – 2013. – № 7 (ч. 1). – С. 118–121.

136. *Ефремова, М.А.* Уголовно-правовая охрана сведении, составляющих коммерческую, банковскую и налоговую тайны [Текст] / М.А. Ефремова // Вестник Пермского университета. Юридические науки. – 2015. – № 1 (27). – С. 124–132.

137. *Ефремова, М.А.* Социальная обусловленность уголовно-правовой охраны информационной безопасности Российской Федерации [Текст] / М.А. Ефремова // Вестник Пермского университета. Юридические науки. – 2017. – № 36. – С. 222–230.

138. *Жарова, А.К.* Опыт правового обеспечения безопасности персональных данных в Великобритании [Текст] / А.К. Жарова // Государство и право. – 2017. – № 6. – С. 70–78.

139. *Жарова, А.К.* Источники понятий «персональные данные» и частная жизнь лица в российском праве [Текст] / А.К. Жарова, В.М. Елин // Вестник Академии права и управления. – 2017. – № 1 (46). – С. 69–78.

140. *Злобин, Г.А.* Основания и принципы уголовно-правового запрета [Текст] / Г.А. Злобин // Советское государство и право. – 1980. – № 1. – С. 70–76.

141. *Иванов, И.С.* Правовые признаки государственной информационной системы [Текст] / И.С. Иванов // Вестник Воронежского государственного университета. Серия: Право. – 2020. – № 2 (41). – С. 179–187.

142. *Ильютович, Д.А.* Юридическое содержание права гражданина на изображение [Текст] / Д.А. Ильютович // Правовая информатика. – 2015. – № 3. – С. 47–52.

143. *Калятин, В.О.* Персональные данные в Интернете [Текст] / В.О. Калятин // Журнал российского права. – 2002. – № 5. – С. 79–86.

144. *Камалова, Г.Г.* О способе отнесения сведений к информации ограниченного доступа [Текст] / Г.Г. Камалова // Вестник Удмуртского университета. Серия «Экономика и право». – 2015. – № 2. – С. 107–111.

145. *Камалова, Г.Г.* Уголовная ответственность за нарушение режима конфиденциальности в российском и зарубежном законодательстве [Текст] / Г.Г. Камалова // Вестник Томского государственного университета. Право. – 2021. – № 40. – С. 32–48.

146. *Капинус, О.С.* Безопасность персональных данных как один из важнейших объектов конституционно-правовой охраны [Текст] / О.С. Капинус // Вестник Университета прокуратуры Российской Федерации. – 2018. – № 6 (68). – С. 10–15.

147. *Карелин, Д.В.* Уголовно-правовая охрана генетических данных человека: к постановке проблемы [Текст] / Д.В. Карелин, Д.М. Мацепуро,

Ф. Селита // Вестник Томского государственного университета. Право. – 2018. – № 29. – С. 79–90.

148. *Климович, Е.В.* О сущности понятия «персональные данные» как конфиденциальной информации особой категории [Текст] / Е.В. Климович // Международные юридические чтения: матер. ежегод. междунар. науч.-практ. конф. (14 апреля 2005 г.). – Омск: Изд-во Омск. юрид. ин-та, 2005. Ч. 2. – С. 21–30.

149. *Козороиз, Н.Л.* Законодательство защищает информацию [Текст] / Н.Л Козороиз // Право в вооруженных силах. – 2013. – № 9. – С. 107–111.

150. *Конев, Д.А.* Цифровые технологии и биометрические данные: постановка проблемы [Текст] / Д.А. Конев // Пробелы в российском законодательстве. – 2021. – Т. 14, № 4. С. 290–295.

151. *Кротов, А.В.* Опыт обработки персональных данных работника в компании [Текст] / А.В. Кротов // Информационное право. – 2007. – № 2. – С. 21–25.

152. *Крылова, Н.Е.* Незаконные разглашение или использование сведений, составляющих коммерческую тайну: проблемы правоприменения [Текст] / Н.Е. Крылова, Б.М. Леонтьев // Вестник Московского университета. Серия 11: Право. – 2017. – № 3. – С. 3–15.

153. *Кудрявцев, В.Н.* Криминализация: оптимальные модели [Текст] / В.Н. Кудрявцев // Уголовное право в борьбе с преступностью. – М.: Изд-во ИГиП АН СССР, 1981. – С. 3–10.

154. *Кузьмин, Ю.А.* Кража персональных данных (криминологический аспект) [Текст] / Ю.А. Кузьмин // Oeconomia et Jus. – 2020. – № 3. – С. 48–57.

155. *Куприна, Е.* Тайна. Обзор нормативных актов [Текст] / Е. Куприна // Закон. – 1998. – № 2. – С. 83–103.

156. *Латыпова, Э.Ю.* Некоторые аспекты уголовной ответственности за деяния, посягающие на неприкосновенность частной жизни [Текст] / Э.Ю. Латыпова // Oeconomia et Jus. – 2019. – № 2. – С. 35–45.

157. *Лушников, А.М.* Защита персональных данных работника: сравнительно-правовой комментарий главы 14 Трудового кодекса Российской Федерации [Текст] / А.М. Лушников // Трудовое право. – 2009. – № 9. – С. 93–101; № 10. – С. 77–82.

158. *Макаров, А.В.* Персональные данные как объект преступных посягательств на неприкосновенность частной жизни: законодательный опыт в России и зарубежных странах [Текст] / А.В. Макаров, Е.С. Вологдина // Российский следователь. – 2019. – № 5. – С. 71–75.

159. *Малеина, М.Н.* Право на тайну и неприкосновенность персональных данных [Текст] / М. Н. Малеина // Журнал российского права. – 2010. – № 11. – С. 18–28.

160. *Мачковский, Л.Г.* Ответственность за нарушение неприкосновенности частной жизни в уголовном законодательстве России и зарубежных стран [Текст] / Л.Г. Мачковский // Известия высших учебных заведений. Правоведение. – 2003. – № 5 (250). – С. 147–161.

161. *Минбалеев, А.В.* Проблемные вопросы понятия и сущности персональных данных [Текст] / А.В. Минбалеев // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 2 (4). – С. 4–9.

162. *Минзов, А.С.* Безопасность персональных данных: новый взгляд на старую проблему [Текст] / А.С. Минзов, А.Ю. Невский, О.Р. Баронов // Вопросы кибербезопасности. – 2022. – № 4 (50). – С. 2–12.

163. *Мираев, А.Г.* Понятие персональных данных в Российской Федерации и Европейском союзе [Текст] / А.Г. Мираев // Юридическая наука. – 2019. – № 5. – С. 76–82.

164. *Михайлова, И.А.* Персональные данные и их правовая охрана: некоторые проблемы теории и практики [Текст] / И.А. Михайлова // Законы России: опыт, анализ, практика: правовой журнал. – 2017. – № 10. – С. 11–18.

165. *Наумов, В.Б.* Персональные данные в соцсетях и социальных медиа: правовые проблемы защиты и использования [Текст] / В.Б. Наумов, Н.В. Панова, Т.В. Лебедева // Закон. – 2012. – № 5. – С. 119–125.

166. *Наумов, В.Б.* Понятие персональных данных: интерпретация в условиях развития информационно-телекоммуникационных технологий [Текст] / В.Б. Наумов, В.В. Архипов // Российский юридический журнал. – 2016. – № 2. – С. 186–196.

167. *Несмелов, П.В.* К вопросу о конфиденциальной информации в административном праве [Текст] / П.В. Несмелов // Полицейская деятельность. – 2012. – № 4. – С. 60–65.

168. *Никитин, Е.Л.* К вопросу о правовой природе персональных данных работника [Текст] / Е.Л. Никитин, А.А. Тимошенко // Журнал российского права. – 2006. – № 7. – С. 43–52.

169. *Новиков, В.* Понятие частной жизни и уголовно-правовая охрана ее неприкосновенности [Текст] / В. Новиков // Уголовное право. – 2011. – № 1. – С. 43–49.

170. *Новиков, В.А.* Уголовная ответственность за нарушение неприкосновенности частной жизни по законодательству Российской Федерации и Республики Казахстан [Текст] / В.А. Новиков // Вестник Института законодательства и правовой информации Республики Казахстан. – 2015. – № 3 (39). – С. 145–149.

171. *Нуркаева, Т.Н.* Нарушение неприкосновенности частной жизни: вопросы толкования и совершенствования законодательства [Текст] / Т.Н. Нуркаева, И.Р. Диваева // Вестник ВЭГУ. – 2015. – № 1(75). – С. 45–56.

172. *Ображиев, К.В.* Уголовно-правовые нормы с двойной превенцией: понятие, сущность и виды [Текст] / К.В. Ображиев, А.С. Шуйский // Законы России: опыт, анализ, практика. – 2009. – № 12. – С. 116–122.

173. *Озерова, А.С.* О необходимости изменения подхода к понятию «информация» в законодательстве и судебной практике» [Текст] / А.С. Озерова // Правоведение. – 2019. – № 1. – С. 137–156.

174. *Озерова, А.С.* Социальная обусловленность уголовно-правовой охраны персональных данных: опыт некоторых зарубежных стран [Текст] / А.С. Озерова // Правовое государство: теория и практика. – 2022. – № 1. – С. 163–168.

175. *Павлинов, А.А.* Уголовная ответственность за нарушение неприкосновенности частной жизни [Текст] / А.А. Павлинов // Пробелы в российском законодательстве. – 2013. – № 6. – С. 187–191.

176. *Павлюков, В.В.* Правовая и практическая возможность объединения данных в информационно-поисковых системах МВД РФ с информацией из сети Интернет [Текст] / В.В. Павлюков // Вестник Костромского государственного университета. – 2016. – № 3. – С. 226–229.

177. *Пашаев, С.Ю.* Проблемы обеспечения права на личную и семейную тайну в Российской Федерации: теоретико-правовой аспект [Текст] / С.Ю. Пашаев // Современное право. – 2010. – № 10. – С. 21–24.

178. *Перова, Н.А.* Ограничения свободы слова в целях предотвращения разглашения личной и государственной тайны в праве США и Великобритании [Текст] / Н.А. Перова // Право и управление. XXI век. – 2012. – № 1. – С. 93–99.

179. *Петрыкина, Н.И.* К вопросу о конфиденциальности персональных данных [Текст] / Н.И. Петрыкина // Законы России: опыт, анализ, практика. – 2007. – № 6. – С. 115–122.

180. *Пикуров, Н.И.* Проблемы квалификации преступных посягательств на частную жизнь: теория и судебная практика [Текст] / Н.И. Пикуров // Уголовное право. – 2019. – № 2. – С. 51–58.

181. *Пилипенко, С.Г.* К вопросу о реализации права на защиту персональных данных при их обработке в электронной форме [Текст] / С.Г. Пилипенко, А.С. Федосин // Пробелы в российском законодательстве. Юридический журнал. – 2009. – № 3. – С. 213–215.

182. *Пилипенко, С.Г., Федосин А.С.* К вопросу о защите права на неприкосновенность частной жизни при обработке персональных данных [Текст] / С.Г. Пилипенко, А.С. Федосин // Актуальные проблемы современного государства и права: матер. всерос. науч.-практ. конференции (Саранск, 22-23 мая 2008 г.). – М., 2009. – С. 69–75.

183. *Платонова, Н.И.* Современный подход к пониманию персональных данных [Текст] / Н.И. Платонова // Право и современные государства. – 2017. – № 5. – С. 9–16.

184. *Проскурякова, М.И.* Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе [Текст] / М.И. Проскурякова // Сравнительное конституционное обозрение. – 2016. – № 6. – С. 84–98.

185. *Проскурякова, М.И.* Конституционно-правовые рамки защиты персональных данных в России [Текст] / М.И. Проскурякова // Вестник Санкт-Петербургского университета. Право. – 2016. – № 2. – С. 12–27.

186. *Рагимханова Д.А.* Правовой режим общедоступной информации [Текст] / Д.А. Рагимханова, М.А. Аливердиева // Вестник Дагестанского государственного университета. Серия 3: Общественные науки. – 2013. – № 2. – С. 57–61.

187. *Радова, М.А.* Профессиональная тайна в системе уголовно-процессуальных гарантий защиты сведений о частной жизни лица [Текст] / М.А. Радова // Криминалистика: вчера, сегодня, завтра. – 2023. – № 2 (26). – С. 141–150.

188. *Радова, М.А.* Соотношение сведений о частной жизни человека и его персональных данных в уголовном процессе России [Текст] / М.А. Радова // Научный вестник Орловского юридического института МВД России имени В.В. Лукьянова. – 2022. – № 4 (93). – С. 157–165.

189. *Рузанова, В.Д.* Проблемы соотношения защиты права на неприкосновенность частной жизни и права на защиту персональных данных [Текст] / В.Д. Рузанова // Законы России: опыт, анализ, практика. – 2019. – № 9. – С. 17–22.

190. *Русскевич, Е.А.* О некоторых аспектах квалификации соучастия в преступлениях в сфере компьютерной информации [Текст] / Е.А. Русскевич // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2019. – № 3 (57). – С. 30–34.

191. *Русскевич, Е.А.* О квалификации преступлений в сфере компьютерной информации, совершаемых с использованием служебного положения [Текст] / Е.А. Русскевич // Российское правосудие. – 2019. – № 2. – С. 35–41.

192. *Русскевич, Е.А.* Кризис и палингенезис (перерождение) уголовного права в условиях цифровизации [Текст] / Е.А. Русскевич, А.П. Дмитренко, Н.Г. Кадников // Вестник Санкт-Петербургского университета. Право. – 2022. – Т. 13, № 3. – С. 585–598.

193. *Русскевич, Е.А.* Цифровые аналоги официальных документов как предмет преступления: постановка проблемы [Текст] / Е.А. Русскевич, К.Б. Чернова // Вестник Московского университета МВД России. – 2022. – № 3. – С. 231–235.

194. *Русскевич, Е.А.* Квалификация неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации [Текст] / Е.А. Русскевич, И.Г. Чекунов // Уголовное право. – 2022. – № 5 (141). – С. 26–35.

195. *Русскевич, Е.А.* Персональные данные в механизме уголовно-правовой охраны [Текст] / Е.А. Русскевич // Известия Юго-Западного государственного университета. Серия: История и право. – 2023. – Т. 13, № 5. – С. 75-86.

196. *Рязанова, Е.Н.* Ответственность за распространение персональных данных как способ противодействия правонарушениям в сфере информационно-коммуникационных технологий [Текст] / Е.Н. Рязанова // Вестник Санкт-Петербургского университета МВД России. – 2022. – 3 (95). – С. 118–123.

197. *Савинцева, М.И.* Конституционно-правовые основы защиты персональной информации в Японии [Текст] / М.И. Савинцева // Конституционное и муниципальное право. – 2006. – № 9. – С. 39–43.

198. *Сапранкова, Т.Ю.* Особенности регламентации уголовной ответственности за нарушение неприкосновенности частной жизни в законодательстве зарубежных стран [Текст] / Т.Ю. Сапранкова // Проблемы экономики и юридической практики. – 2016. – № 4. – С. 124–127.

199. *Симонова, Е.В.* Определение понятия персональных данных в Российской Федерации [Текст] / Е.В. Симонова // Молодой ученый. – 2017. – № 10. – С. 323–326.

200. *Сергиенко, Л.А.* Правовая защита персональных данных. Цели и принципы правового регулирования [Текст] / Л.А. Сергиенко // Проблемы информатизации. – 1995. – № 1. – С. 37–42.

201. *Серебренникова, А.В.* Преступления против личности по уголовному кодексу княжества Лихтенштейна: общая характеристика [Текст] / А.В. Серебренникова, А.А. Трефилов // Lex Russica. – 2016. – № 12 (121). – С. 113–124.

202. *Серебряков, К.Д.* Некоторые проблемы реализации механизма правовой защиты персональных данных в социальной сети «Вконтакте» [Текст] / К.Д. Серебряков // Вопросы российской юстиции. – 2022. – № 21. – С. 685–695.

203. *Солдатова, В.И.* Защита персональных данных в условиях применения цифровых технологий [Текст] / В.И. Солдатова // Lex Russica. – 2020. – № 2 (159). – С. 33–43.

204. *Соловьев, В.С.* Порноместь: сущность явления и проблемы его уголовно-правовой оценки // Уголовное право. – 2017. – № 6. – С. 60–64.

205. *Соловьев, В.С.* Преступность в социальных сетях интернета (криминологическое исследование по материалам судебной практики) [Текст] // Всероссийский криминологический журнал. – 2018. – Т. 10, № 1. – С. 60–72.

206. *Соловьев, В.С.* Мошеннические действия в социальном сегменте сети интернет (криминологическое исследование по результатам интернет-опроса пользователей) [Текст] // Известия Юго-Западного государственного университета. Серия: История и право. – 2018. – Т. 8, № 3 (28). – С. 100–108.

207. *Соловьев, В.С.* Криминологическая типология механизмов совершения преступлений с использованием информационно-телекоммуникационных технологий [Текст] // Вестник Краснодарского университета МВД России. – 2021. – № 4 (54). – С. 50–57.

208. *Соловьев, В.С.* Основные направления развития криминологической науки и практики предупреждения преступлений в условиях цифровизации общества [Текст] / В.С. Соловьев, А.Л. Осипенко // Всероссийский криминологический журнал. – 2021. – Т. 15, № 6. – С. 681–691.

209. *Стяжкина, С.А.* Информация как объект уголовно-правовой охраны: понятие, признаки, виды [Текст] / С.А. Стяжкина // Вестник Удмуртского университета. Экономика и право. – 2015. – № 2. – С. 157–161.

210. *Стяжкина, С.А.* Уголовно-правовая охрана частной жизни лица [Текст] / С.А. Стяжкина // Вестник Удмуртского университета. Экономика и право. – 2019. – № 29. – С. 538–544.

211. *Судакова, О.В.* Личные неимущественные права, направленные на обеспечение неприкосновенности и тайны личной жизни граждан [Текст] / О.В. Судакова // Балтийский гуманитарный журнал. – 2020. – № 1 (30). – С. 381–384.

212. *Сысенко, А.Р., Белова, К.С., Горденко, А.С.* Особенности расследования неправомерного доступа к компьютерной информации (ст. 272 УК РФ) [Текст] // Криминалистика: вчера, сегодня, завтра. – 2022. – № 4 (24). – С. 183–188.

213. *Талапина, Э.В.* Правовая защита персональных данных во Франции [Текст] / Э.В. Талапина // Право. – 2012. – № 4. – С. 152–162.

214. *Терещенко, А.К.* К вопросу о правовом режиме информации [Текст] / А.К. Терещенко // Информационное право. – 2008. – № 1. – С. 20–27.

215. *Тюрина, Е.Н.* Интегрированные банки данных и сетевые каналы связи как особенный объект правоотношений, возникающих в деятельности органов внутренних дел [Текст] / Е.Н. Тюрина // Труды Академии управления МВД России. – 2012. – № 2 (22). – С. 126–128.

216. *Унукович, А.С.* Меры предупреждения преступлений, совершаемых с использованием информационно-телекоммуникационных технологий в отношении граждан [Текст] // Научный вестник Омской академии МВД России. – 2023. – Т. 29, № 2 (89). – С. 98–102.

217. *Фефелов, П.А.* Критерии установления уголовной наказуемости деяний [Текст] / П.А. Фефелов // Советское государство и право. – 1970. – № 11. – С. 101–105.

218. *Филатова, М.А.* Персональные данные как предмет преступного посягательства журнал [Текст] / М.А. Филатова // Уголовное право. – 2021. – № 11. – С. 35–43.

219. *Халиулина, Э.Т.* Преступления, совершаемые с использованием персональных данных: характеристика состояния [Текст] / Э.Т. Халиулина, А.С. Журавлева // Военное право. – 2021. – № 2 (66). – С. 289–294.

220. *Хохлова, Е.В.* О признаках персональных данных как предмете и средстве совершения преступлений [Текст] / Е.В. Хохлова // Уголовная политика и культура противодействия преступности: матер. междунар. науч.-практ. конф. (30 сент. 2022 г.) / ред. кол.: А.Л. Осипенко (отв. ред.) [и др.]. – Краснодар: Изд-во Краснодар. ун-та МВД России, 2022. – С. 425–427.

221. *Хохлова, Е.В.* Об уголовной ответственности за нарушение неприкосновенности персональных данных человека в странах бывшего СССР [Текст] / Е.В. Хохлова // Вестник Российской правовой академии. – 2022. – № 3 (1). – С. 90–97.

222. *Хохлова, Е.В.* Уголовно-правовая охрана персональных данных в зарубежных странах [Текст] / Е.В. Хохлова // Известия Юго-Западного государственного университета. Серия: История и право. – 2022. – Т. 12, № 4. – С. 62–78.

223. *Хохлова, Е.В.* К вопросу о защите изображения человека как персональных данных (на основе судебной практики по ст. 137 УК РФ) [Текст] / Е.В. Хохлова // Вестник Воронежского института МВД России. – 2023. – № 3. – С. 300–304.

224. *Хохлова, Е.В.* Социальная обусловленность уголовной ответственности за преступления, связанные с персональными данными [Текст] / Е.В. Хохлова // Вестник Тверского государственного университета. Серия: Право. – 2022. – № 3(71). – С. 141–148.

225. *Цадыкова, Э.А.* Гарантии охраны и защиты персональных данных человека и гражданина [Текст] / Э.А. Цадыкова // Конституционное и муниципальное право. – 2007. – № 14. – С. 15–19.

226. *Циулина, Н.Е.* Формирование и развитие правовой категории «персональные данные» [Текст] / Н.Е. Циулина // Вестник УрФО. Безопасность в информационной сфере. – 2013. – №. 1. – С. 47–52.

227. *Чукреев, В.А.* Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны [Текст] / В.А. Чукреев // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2022. – № 3 (91). – С. 107–116.

228. *Шутова, А.А.* Социальная обусловленность существования норм об уголовной ответственности за посягательства на персональные данные [Текст] / А.А. Шутова // Вестник Нижегородской академии МВД России. – 2015. – № 4 (32). – С. 332–335.

229. *Энгельгардт, А.А.* Оценка преступлений как продолжаемого деяния или множественности (на примере преступлений в сфере компьютерной информации) [Текст] / А.А. Энгельгардт // Право и политика. – 2014. – № 12 (180). – С. 1860–1864.

Диссертации и авторефераты диссертаций

230. *Белгородцева, Н.Г.* Теоретико-правовые аспекты защиты персональных данных: автореф. дис. ... канд. юрид. наук [Текст] / Н.Г Белгородцева. – М., 2012. – 25 с.

231. *Бондарь, И.В.* Тайна по российскому законодательству (проблемы теории и практики): автореф. дис. … канд. юрид. наук [Текст] / И.В. Бондарь. – Н. Новгород, 2004. – 27 с.

232. *Бундин, М.В.* Персональные данные в системе информации ограниченного доступа: дис. ... канд. юрид. наук [Текст] / М.В. Бундин. – М., 2017. – 218 с.

233. *Вельдер, И.А.* Система правовой защиты персональных данных в Европейском союзе: дис. ... канд. юрид. наук [Текст] / И.А. Вельдер. – Казань, 2006. – 165 с.

234. *Иванский, В.П.* Теоретические проблемы правовой защиты частной жизни в связи с использованием информационных технологий: дис. … канд. юрид. наук [Текст] / В.П. Иванский. – М., 1998. – 274 с.

235. *Говенко, Ю.А*. Уголовно-правовая охрана тайны частного характера: автореф. дис... канд. юрид. наук [Текст] / Ю.А. Говенко. – Краснодар, 2010. – 26 с.

236. *Гутник, С.И.* Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: дис. … канд. юрид. наук [Текст] / С.И. Гутник. – Красноярск, 2017. – 241 с.

237. *Ефремова, М.А.* Уголовно-правовая охрана информационной безопасности: дис. ... докт. юрид. наук [Текст] / М.А. Ефремова. – М., 2017. – 427 с.

238. *Жигалов, А.Ф.* Коммерческая и банковская тайна в коммерческом и уголовном законодательстве: дис. … канд. юрид. наук [Текст] / А.Ф. Жигалов. – Н. Новгород, 2000. – 257 с.

239. *Кучеренко, А.В.* Правовое регулирование персональных данных в Российской Федерации: автореф. дис. ... канд. юрид. наук [Текст] / А.В. Кучеренко. – Челябинск, 2010. – 22 с.

240. *Мазуров, В.А.* Уголовно-правовая защита тайны: дис. ... канд. юрид. наук [Текст] / В.А. Мазуров. – Томск, 2001. – 198 с.

241. *Мартышин, М.Ю.* Государственная тайна как объект конституционно-правового регулирования: дис. … канд. юрид. наук [Текст] / М.Ю. Мартышин. – М., 2009. – 192 с.

242. *Миндрова, Е.А.* Коллизия права граждан на доступ к информации и права на неприкосновенность частной жизни в условиях информационного общества: автореф. дис. ... канд. юрид. наук [Текст] / Е.А. Миндрова. – М., 2007. – 31 с.

243. *Паршин, С.М.* Тайна в уголовном законодательстве (теоретико-прикладное исследование): дис. ... канд. юрид. наук. – Н. Новгород, 2006. – 207 с.

244. *Пашаев, С.Ю.* Конституционно-правовое регулирование личной и семейной тайны в Российской Федерации: автореф. дис. ... канд. юрид. наук [Текст] / С.Ю. Пашаев. – М., 2010. – 25 с.

245. *Просветова, О.Б.* Защита персональных данных: дис. … канд. юрид. наук [Текст] / О.Б. Просветова. – М., 2005. – 193 с.

246. *Проскурякова, М.И.* Защита персональных данных в праве России и Германии: конституционно-правовой аспект: автореф. дис. ... канд. юрид. наук [Текст] / М.И. Проскурякова. – СПб., 2017. – 26 с.

247. *Русскевич, Е.А.* Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: дис. ... д-ра юрид. наук [Текст] / Е.А. Русскевич. – М., 2021. – 521 с.

248. *Савинцева, М.И.* Конституционно-правовые проблемы регулирования информационных отношений в Японии история и современность: автореф. дис. … канд. юрид. наук [Текст] / М.И. Савинцева. – М., 2007. – 26 с.

249. *Телина, Ю.С.* Конституционное право гражданина на неприкосновенность частной жизни, личную и семейную тайну при обработке персональных данных в России и зарубежных странах: дис. ... канд. юрид. наук [Текст] / Ю.С. Телина. – М., 2016. – 267 с.

250. *Федосин, А.С.* Защита конституционного права человека и гражданина на неприкосновенность частной жизни при автоматизированной обработке персональных данных в Российской Федерации: автореф. дис. ... канд. юрид. наук [Текст] / А.С. Федосин. – Саранск, 2009. – 27 с.

251. *Хуаде, А.Х.* Уголовно-правовая характеристика нарушения неприкосновенности частной жизни: автореф. дис... канд. юрид. наук [Текст] / А.Х. Хуаде. – Краснодар, 2015. – 20 с.

252. *Цадыкова, Э.А.* Конституционное право на неприкосновенность частной жизни: сравнительно-правовое исследование: автореф. дис. … канд. юрид. наук [Текст] / Э.А. Цадыкова. – М., 2007. – 23 с.

253. *Числин, В.П.* Уголовно-правовые меры защиты информации от неправомерного доступа: дис. ... канд. юрид. наук [Текст] / В.П. Числин. – М., 2004. – 134 с.

254. *Шевченко, И.А.* Уголовно-правовая охрана неприкосновенности частной жизни: дис. … канд. юрид. наук [Текст] / И.А. Шевченко. – Красноярск, 2006. – 196 с.

255. *Шутова, А.А.* Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности: теоретический и прикладной аспекты: дис. ... канд. юрид. наук [Текст] / А.А. Шутова. – Н. Новгород, 2017. – 264 с.

256. *Юрченко, И.А.* Информация как предмет уголовно-правовой охраны: дис. ... канд. юрид. наук [Текст] / И.А. Юрченко. – М., 2000. – 205 с.

Материалы правоприменительной практики

257. По делу о проверке конституционности статьи 265 УК РФ в связи с жалобой гражданина А.А. Шевякова: постановление Конституционного Суда РФ от 25.04.2001 № 6-П [Текст] // Рос. газета. – 2001. – 15 июня.

258. Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом «б» части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации»: определение Конституционного Суда РФ от 09.06.2005 № 248-О [Электронный ресурс]. Доступ из справ.-прав. системы «КонсультантПлюс».

259. По делу о проверке конституционности положений частей 2 и 4 ст. 20, ч. 6 ст. 144, п. 3 ч. 1 ст. 145, ч. 3 ст. 318, частей 1 и 2 ст. 319 УПК РФ в связи с запросами Законодательного собрания Республики Карелия и Октябрьского районного суда города Мурманска: постановление Конституционного Суда РФ

от 27.06.2005 № 7-П [Электронный ресурс]. Доступ из справ.-прав. системы «КонсультантПлюс».

260. Об отказе в принятии к рассмотрению жалобы гражданина Глушкова Николая Петровича на нарушение его конституционных прав статьями 3, 5, 6 и 9 Федерального закона «Об информации, информационных технологиях и о защите информации» и статьями 8 и 9 Федерального закона «О персональных данных»: определение Конституционного Суда РФ от 29.01.2009 № 3-О-О [Электронный ресурс]. Доступ из справ.-прав. системы «КонсультантПлюс».

261. Об отказе в принятии к рассмотрению жалобы гражданина Усенко Дмитрия Николаевича на нарушение его конституционных прав положениями статьи 8 Федерального закона «Об оперативно-розыскной деятельности»: определение Конституционного Суда РФ от 26.01.2010 № 158-О-О [Электронный ресурс]. Доступ из справ.-прав. системы «КонсультантПлюс».

262. Об отказе в принятии к рассмотрению жалобы гражданина Богородицкого Сергея Николаевича на нарушение его конституционных прав статьей 5 Закона Российской Федерации «О милиции»: определение Конституционного Суда РФ от 27.05.2010 № 644-О-О [Электронный ресурс]. Доступ из справ.-прав. системы «КонсультантПлюс».

263. Об отказе в принятии к рассмотрению жалобы гражданина Багадурова Магомеда Магомедовича на нарушение его конституционных прав подпунктом 1 пункта 3 статьи 6 Федерального закона «Об адвокатской деятельности и адвокатуре в РФ» статьей 10 Федерального закона «О персональных данных» и частью второй статьи 57 ГПК Российской Федерации»: определение Конституционного Суда РФ от 29.09.2011 № 1063-О-О [Электронный ресурс]. Доступ из справ.-прав. системы «КонсультантПлюс».

264. Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации: определение Конституционного Суда РФ от 28.06.2012 № 1253-О [Электронный ресурс]. Доступ из справ.-прав. системы «Гарант».

265. Об отказе в принятии к рассмотрению жалобы гражданина Кудрякова Антона Васильевича на нарушение его конституционных прав положением части 1 статьи 25.1 Кодекса Российской Федерации об административных правонарушениях: определение Конституционного Суда РФ от 23.04.2015 № 1075-О [Электронный ресурс]. Доступ из справ.-прав. системы «КонсультантПлюс».

266. По делу о проверке конституционности положений пункта 6 статьи 2 и пункта 7 статьи 32 Федерального закона «О некоммерческих организациях», части шестой статьи 29 Федерального закона «Об общественных объединениях» и части 1 статьи 19.34 Кодекса РФ об административных правонарушениях в связи с жалобами Уполномоченного по правам человека в Российской Федерации, фонда «Костромской центр поддержки общественных инициатив», граждан Л.Г. Кузьминой, С.М. Смиренского и В.П. Юкечева постановление Конституционного Суда РФ от 08.04.2014 № 10-П [Текст] // Вестник Конституционного Суда РФ. – 2014. – № 4.

267. По делу о проверке конституционности пункта 8 части 1 статьи 6 Федерального закона «О персональных данных» в связи с жалобой общества с ограниченной ответственностью «МедРейтинг»: постановление Конституционного Суда РФ от 25.05.2021 № 22-П [Текст] // Рос. газета. – 2021. – 8 июня.

268. О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138^1, 139, 144^1, 145, 145^1 Уголовного кодекса Российской Федерации)»: постановление Пленума Верховного Суда РФ от 25.12.2018 № 46 [Текст] // Бюллетень Верховного Суда РФ. – 2019. – № 2.

269. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 [Текст] // Рос. газета. – 2022. – 28 дек.

270. Определение Верховного Суда РФ от 29.01.2018 № 305-КГ17-21291 по делу № А40-5250/2017 [Электронный ресурс]. Доступ из справ.-прав. системы «Гарант».

271. Апелляционное определение Судебной коллегии по гражданским делам Московского городского суда от 30.03.2012 по делу № 11-2538 [Электронный ресурс] // Доступ из справ.-прав. системы «Гарант».

272. Апелляционное определение Нижегородского областного суда от 11.10.2016 по делу № 33-12355/2016 [Электронный ресурс]. – URL: https://www.audar-info.ru/na/article/view/type_id/7/doc_id/26195/ (дата обращения: 04.02.2023).

273. Кассационное определение Седьмого кассационного суда общей юрисдикции от 10.06.2020 № 77-889/2020 [Электронный ресурс]. Доступ из справ.-прав. системы «КонсультантПлюс».

274. Постановление Девятого арбитражного апелляционного суда от 27.07.2017 № 09АП-31744/2017 по делу № А40-5250 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/arbitral/doc/ADkm2q8j8irQ/ (дата обращения: 04.11.2022).

275. Постановление Арбитражного суда Московского округа от 09.11.2017 № Ф05-16382/17 по делу № А40-5250 [Электронный ресурс]. Доступ из справ.-прав. системы «Гарант».

276. Приговор Кировского районного суда г. Ростова-на-Дону от 10.06.2011 по делу № 1-223 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://rospravosudie.com/court-kirovskij-rajonnyj-sud-g-rostova-na-donu-rostovskaya-oblast-s/act-102576386/ (дата обращения: 04.02.2023).

277. Приговор Центрального районного суда г. Новосибирска от 07.12.2012 по делу № 1-566/2012 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/mdwYfSwTqVYB/?page=2&regular-court=&regular (дата обращения: 04.02.2023).

278. Приговор Искитимского районного суда Новосибирской области от 01.12.2016 по делу № 1-627/2016 [Электронный ресурс] // Судебные

и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/IKwb4kGNFudC/?regular-txt=приговор+бубело&regular-case_doc=&regular (дата обращения: 04.02.2023).

279. Приговор Дзержинского районного суда г. Новосибирска от 02.10.2017 по делу № 1-389/2017 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/kN7MkWMrBlUK/?regular-txt=Необутова+приговор&regular-case_doc=&regular (дата обращения: 09.05.2023).

280. Приговор Пролетарского районного суда г. Саранска от 24.05.2018 по делу № 1-78/2018 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/1rMRLV1XcP1/?page=6&regular (дата обращения: 04.02.2023).

281. Приговор Серпуховского городского суда Московской области от 14.01.2019 по делу № 1-27/2019 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/XikJ89Z5aBJ0/?page=5&regular (дата обращения: 04.02.2023).

282. Приговор Октябрьского районного суда г. Ростова-на-Дону от 22.04.2019 по делу № 1-306/2019 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/MEIPEhOnVY5T/?regular (дата обращения: 10.04.2023).

283. Приговор Мокшанского районного суда Пензенской области от 28.06.2019 по делу № 1-36/2019 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/OVzzuMQ72gHB/?page=4&regular (дата обращения: 10.04.2023).

284. Приговор Тбилисского районного суда Краснодарского края от 11.07.2019 по делу № 1-125/2019 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/gGB9phbVHUg0/?regular (дата обращения: 08.02.2023).

285. Приговор Чебаркульского городского суда Челябинской области от 26.12.2019 по делу № 1-349/2019 [Электронный ресурс] // Судебные

и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/i8uMeLpvrKQh/?page=2&regular-court=&regular-date_from=&regular (дата обращения: 09.05.2023).

286. Приговор Октябрьского районного суда г. Ростова-на-Дону от 04.02.2020 по делу № 1-119/2020 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/Mieif03BN1b4/?regular-(дата обращения: 10.04.2023).

287. Приговор Фрунзенского районного суда г. Владимира от 18.05.2020 по делу № 1-77/2020 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/JFXOOMXHQdQx/?regular (дата обращения: 04.02.2023).

288. Приговор Жуковского районного суда Брянской области от 21.05.2020 по делу № 1-127/2019 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/Jir03EOSNHgb/?regular (дата обращения: 04.02.2023).

289. Постановление Пролетарского районного суда г. Саранска от 11.09.2019 по делу № 1-288/2019 о применении судебного штрафа [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/l4O9LJQ90WHR/?page=3&regular (дата обращения: 04.02.2023).

290. Решение Арзамасского городского суда Нижегородской области от 14.06.2016 по делу № 2-2307/2016 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/regular/doc/YTC0pcVgf4o8/ (дата обращения: 04.02.2023).

291. Решение Арбитражного суда г. Москвы от 05.05.2017 по делу № А40-5250/17-144-51 [Электронный ресурс] // Судебные и нормативные и акты РФ. – URL: https://sudact.ru/arbitral/doc/YLVZ7F3cAwU0/ (дата обращения: 15.12.2022).

292. Решение Гагаринского районного суда г. Москвы от 30.08.2017 по делу № 2-3908/2017 [Электронный ресурс]. – URL: https://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/e42670fa-d3d3-4b0d-8e94-45ad1fe78753 (дата обращения: 17.08.2022).

Интернет-ресурсы

293. Актуальные киберугрозы: итоги 2022 года [Электронный ресурс] // Ptsecurity. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения: 09.04.2023).

294. Брат за брата. В Саратове осудили и отправили в колонию невиновного [Электронный ресурс] // Аргументы и факты. – URL: https://aif.ru/society/law/brat_za_brata_v_saratove_osudili_i_otpravili_v_koloniyu_nevinovnogo (дата обращения: 17.08.2022).

295. Бывшую сотрудницу МТС признали виновной в продаже информации о звонках абонентов [Электронный ресурс] // Новости Новосибирска. – URL: https://novosibirsk-news.net/other/2018/04/19/77809.html (дата обращения: 04.02.2023).

296. В Нидерландах отменили закон о хранении данных пользователей телефона и интернета [Электронный ресурс] // Официальный сервер Международной Организации Труда. – URL: https://www.kommersant.ru/doc/2685042 (дата обращения: 09.08.2022).

297. В Петрозаводске вынесен приговор по уголовному делу о мошенничестве в составе организованной группы [Электронный ресурс] // Прокуратура Республики Карелия. – URL: https://epp.genproc.gov.ru/web/proc_10/mass-media/news?item=62606760 (дата обращения: 09.04.2023).

298. В России резко участились кражи персональных данных – число похищенных записей превысило население страны [Электронный ресурс] // Infowatch. – URL: https://www.infowatch.ru/analytics/analitika/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda (дата обращения: 09.01.2023).

299. В России будут судить продавцов персональных данных в даркнете [Электронный ресурс] // Про Пермь. – URL: https://properm.ru/news/2023-02-12/v-rossii-budut-sudit-prodavtsov-personalnyh-dannyh-v-darknete-2683588 (дата обращения: 09.04.2023).

300. В Самаре экс-полицейским вынесли приговор за слив базы МВД [Электронный ресурс] // РИА Новости. – URL: https://ria.ru/20220622/prigovor-1797366783.html (дата обращения: 09.04.2023).

301. В Сети появились данные клиентов сервиса по заказу билетов Туту.ру [Электронный ресурс] // РБК. – URL: https://www.rbc.ru/technology_and_media/02/07/2022/62c058429a7947e0e7f75aff (дата обращения: 27.08.2022).

302. В Сеть утекли данные о 12 млн заемщиков микрокредитных организаций [Электронный ресурс] // Известия. – URL: iz.ru/1005868/2020-04-29/v-set-utekli-dannye-o-12-mln-zaemshchikov-mikrokreditnykh-organizatcii (дата обращения: 17.08.2022).

303. В Тюмени перед судом предстанет сотрудник полиции по обвинению в незаконном распространении информации в отношении местного жителя [Электронный ресурс] // Прокуратура Тюменской области. – URL: https://epp.genproc.gov.ru/web/proc_72/mass-media/news?item=74056760 (дата обращения: 10.04.2023).

304. В Челябинской области будут судить полицейского за слив данных из базы МВД [Электронный ресурс] // Комсомольская правда. Челябинск. – URL: https://www.chel.kp.ru/online/news/4713959/ (дата обращения: 04.02.2023).

305. Ведомости: «Фейковые» аккаунты в соцсетях нарушают закон о персональных данных [Электронный ресурс] // Роскомнадзор. – URL: https://rkn.gov.ru/press/publications/news29215.htm (дата обращения: 15.12.2022).

306. Во Владивостоке возбуждено уголовное дело по факту получения взятки и неправомерного доступа к компьютерной информации [Электронный ресурс] // Следственное управление Следственного комитета РФ по Приморскому краю. – URL: https://primorsky.sledcom.ru/news/item/1671004/ (дата обращения: 04.02.2023).

307. Возбуждено уголовное дело по факту незаконного копирования информации из баз данных оператора сотовой связи [Электронный ресурс] // Генеральная прокуратура РФ. – URL: https://epp.genproc.gov.ru/web/proc_40/mass-media/news?item=61325179 (дата обращения: 09.05.2023).

308. Вынесен приговор по делу о подкупе сотрудника МВД для слежки за оппонентами в судебном споре [Электронный ресурс] // Legal.report. – URL: https://legal.report/vynesen-prigovor-po-delu-o-podkupe-sotrudnika-mvd-dlya-slezhki-za-opponentami-v-sudebnom-spore/ (дата обращения: 07.12.2022).

309. «Гемотест» оштрафовали на 60 тыс. руб. за утечку персональных данных [Электронный ресурс] // Коммерсантъ. – URL: https://www.kommersant.ru/doc/5480244 (дата обращения: 17.08.2022).

310. Данные пользователей «Почты России» попали в интернет [Электронный ресурс] // Коммерсантъ. – URL: https://www.kommersant.ru/doc/5490311 (дата обращения: 09.08.2022).

311. Емельянников М.Ю. Судебное решение: соцсети и сайты объявлений в России теперь незаконны? [Электронный ресурс] // Emeliyannikov.blogspot. – URL: https://emeliyannikov.blogspot.com/2017/12/blog-post.html (дата обращения 26.12.2022).

312. Ефремов А.А. Понятие и виды конфиденциальной информации [Электронный ресурс] // Russianlaw. – URL: http://www.russianlaw.net/law/doc/a90.htm (дата обращения: 12.10.2023).

313. Жителю Краснодарского края предъявлено обвинение в совершении киберпреступлений [Электронный ресурс] // Следственный комитет РФ. – URL: https://zmsut.sledcom.ru/news/item/1417513 (дата обращения: 17.08.2022).

314. «Закон работает, и это – факт»: Роскомнадзор защитил 90 млн человек от кражи персональных данных [Электронный ресурс] // Inforeactor. – URL: http://inforeactor.ru/98875-zakon-rabotaet-i-eto-fakt-roskomnadzor-zashchitil-90-mlnchelovek-ot-krazhi-personalnyh-dannyh (дата обращения: 17.08.2022).

315. Законопроект № 502113-8 «О внесении изменений в Уголовный кодекс Российской Федерации» [Электронный ресурс] // Официальный сайт Государственной Думы РФ. – URL: https://sozd.duma.gov.ru/bill/502113-8 (дата обращения: 04.02.2023).

316. Итоги работы с обращениями граждан в Роскомнадзоре в 2021 году [Электронный ресурс] // Роскомнадзор. – URL: https://rkn.gov.ru/treatments/p436/ (дата обращения: 17.08.2022).

317. Как мошенники получают наши персональные данные из банков? Объяснил эксперт [Электронный ресурс] // Аргументы и факты. – URL: ttps://aif.ru/money/mymoney/kak_moshenniki_poluchayut_nashi_personalnye_dannye_iz_bankov_obyasnil_ekspert (дата обращения: 17.03.2023).

318. Клиенты алкомаркета «утекли» в Сеть [Электронный ресурс] // Коммерсантъ. – URL: https://www.kommersant.ru/doc/4234529 (дата обращения: 17.08.2022).

319. МВД России накрыло группировку, продававшую персональные данные. Среди участников есть пермяки [Электронный ресурс] // 59.ru. – URL: https://59.ru/text/incidents/2022/02/22/70461209/ (дата обращения: 09.04.2023).

320. Московский бизнесмен пришел получать паспорт и узнал, что давно сидит в тюрьме [Электронный ресурс] // Московский комсомолец. – URL: https://www.mk.ru/social/2015/02/08/moskovskiy-biznesmen-prishel-poluchat-pasport-i-uznal-chto-davno-sidit-v-tyurme.html (дата обращения: 01.09.2022).

321. Мужчина представился полиции чужим именем. Наказан невиновный [Электронный ресурс] // Четвертая власть. – URL: https://www.4vsar.ru/news/82285.html (дата обращения: 01.09.2022).

322. Наказали невиновного. В Смоленске нарушитель представился полицейским чужим именем [Электронный ресурс] // Смоленские новости. – URL: https://smoldaily.ru/nakazali-nevino(дата обращения: 01.09.2022).

323. Небензя задал вопрос о реакции ООН на внесение данных детей в «Миротворец» [Электронный ресурс] // РИА Новости. – URL: https://ria.ru/20221206/deti-1836811096.html (дата обращения: 08.12.2022).

324. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств [Электронный ресурс] // ЦБ РФ. – URL: https://cbr.ru/analytics/ib/review_4q_2022/ (дата обращения: 01.09.2022).

325. Обращения в сфере персональных данных [Электронный ресурс] // Роскомнадзор. – URL: https://26.rkn.gov.ru/p8926/p10713/ (дата обращения: 15.12.2022).

326. Орешин Е. Дело ВКонтакте VS Дабл об использовании общедоступных данных пользователей [Электронный ресурс] // Закон. ру. – URL: https://zakon.ru/blog/2018/6/15/delo_vkontakte_vs_dabl_ob_ispolzovanii_obschedostupnyh_dannyh_polzovatelej_poziciya_dabl_v_sude_po_i/ (дата обращения 26.12.2022).

327. Переписка и геоданные россиян могли утекать зарубежным мошенникам [Электронный ресурс] // Известия. – URL:https://iz.ru/1385527/2022-08-26/perepiska-i-geodannye-rossiian-mogli-utekat-zarubezhnym-moshennikam (дата обращения: 17.08.2022).

328. Персональные данные в интернете: угроза утечки и как с ней бороться [Электронный ресурс] // ВЦИОМ. – URL: https://wciom.ru/analytical-reviews/analiticheskii-obzor/personalnye-dannye-v-internete-ugroza-utechki-i-kak-s-nei-borotsja (дата обращения: 17.08.2022).

329. Персональные данные 700 тыс. сотрудников РЖД утекли в Сеть [Электронный ресурс] // РБК. – URL: https://www.rbc.ru/society/27/08/2019/5d65020c9a79473ae12bdea1? (дата обращения: 27.08.2022).

330. Персональные сданные: как будут отслеживать продавцов незаконных баз [Электронный ресурс] // Известия. – URL: https://iz.ru/1262783/valerii-kodachigov/personalnye-sdannye-kak-budut-otslezhivat-prodavtcov-nezakonnykh-baz (дата обращения: 09.04.2023).

331. Персональные данные клиентов МФО выставили на продажу в интернете [Электронный ресурс] // РБК. – URL: https://www.rbc.ru/finances/06/02/2020/5e3971cc9a79472fd1048e1a (дата обращения: 09.04.2023).

332. Персональные данные общего пользования [Электронный ресурс] // Комсомольская правда. – URL: https://www.msk.kp.ru/daily/26333/3217332/ (дата обращения: 09.04.2023).

333. Подведены итоги работы Роскомнадзора в 2021 году по защите прав и интересов граждан в сфере персональных данных [Электронный ресурс] //

Роскомнадзор. – URL: https://rkn.gov.ru/news/rsoc/news74048.htm?print=1&utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения: 17.08.2022).

334. Потерял телефон – отдавай миллион [Электронный ресурс] // Финансовая культура. – URL: https:// fincult.info/rake/poteryal-telefon-otdavay-million (дата обращения 02.02.2023).

335. Почему россияне боятся расстаться с персональными данными, и кому они готовы их доверить. Исследование Sostav и OMI [Электронный ресурс] // Sostav. – URL: https://www.sostav.ru/publication/pochemu-rossiyane-boyatsya-rasstatsya-s-personalnymi-dannymi-i-komu-oni-gotovy-ikh-doverit-issledovanie-sostav-i-omi-38865.html (дата обращения: 03.11.2022).

336. Почти полмиллиона логинов и паролей от аккаунтов на Ozon попали в открытый доступ [Электронный ресурс] // Коммерсантъ. – URL: https://www.kommersant.ru/doc/4026663 (дата обращения: 17.08.2022).

337. «Придешь на суд – будет плохо». Как запугивают и подкупают присяжных в России [Электронный ресурс] // Lenta.ru. – URL: https://lenta.ru/articles/2021/06/24/prisazhnie/ (дата обращения: 17.08.2022).

338. Прокуратура Волгоградской области утвердила обвинительное заключение по уголовному делу о мошенничестве при получении кредитов для оплаты туристических путевок [Электронный ресурс] // Прокуратура Волгоградской области. – URL: https://epp.genproc.gov.ru/web/proc_34/mass-media/news?item=56232080 (дата обращения: 09.04.2023).

339. Рассмотрено уголовное дело в отношении бывших сотрудников полиции, которые продавали персональные данные граждан [Электронный ресурс] // Прокуратура Нижегородской области. – URL: https://epp.genproc.gov.ru/web/proc_52/mass-media/news/archive?item=46470953 (дата обращения: 09.02.2023).

340. Реестр операторов, осуществляющих обработку персональных данных (по состоянию на 05.03.2023) [Электронный ресурс] // Росреестр. – URL: https://pd.rkn.gov.ru/operators-registry/operators-list/ (дата обращения: 04.02.2023).

341. *Рожкова, М.А.* «Общедоступная информация», «открытые данные» и «персональные данные, разрешенные субъектом для распространения» – что это такое и как они между собой связаны? [Электронный ресурс] // Закон.ру. – URL: https://zakon.ru/blog/2021/1/13/obschedostupnaya_informaciya_otkrytye_dannye_i_personalnye_dannye_razreshennye_subektom_dlya_raspros (дата обращения: 04.02.2023).

342. *Рожкова, М.А.* Являются ли персональные данные действительно конфиденциальными, или как соотносятся категории «персональные данные» и «тайны» (взгляд цивилиста) [Электронный ресурс] // Закон.ру. – URL: https://zakon.ru/blog/2019/3/18/yavlyayutsya_personalnye_dannye_dejstvitelno_konfidencia1 (дата обращения: 25.12.2022).

343. *Рожкова, М.А.* Персональные данные: можно ли относить их к имуществу? (взгляд цивилиста) [Электронный ресурс] // Закон.ру. – URL: https://zakon.ru/blog/2019/02/28/personalnye_dannye_mozhno_li_otnosit_ih_k_imuschestvu_vzglyad_civilista (дата обращения: 25.12.2022).

344. РКН начал расследование утечки базы данных водителей Москвы и Подмосковья [Электронный ресурс] // РБК. – URL: https://www.rbc.ru/technology_and_media/25/10/2021/6175eeb89a794778b01c0189 (дата обращения: 27.08.2022).

345. РКН составил протокол на «Яндекс.Еду» после утечки данных курьеров [Электронный ресурс] // Коммерсантъ. – URL: https://www.kommersant.ru/doc/5458856 (дата обращения: 17.08.2022).

346. Роскомнадзор направил запрос лоукостеру «Победа» из-за возможной утечки персональных данных сотрудников [Электронный ресурс] // Рамблер. – URL: https://travel.rambler.ru/news/47996286/?utm_content=travel_media&utm_medium=read_more&utm_source=copylink (дата обращения: 23.08.2022).

347. Роскомнадзор составил протокол на «Ростелеком» за утечки данных [Электронный ресурс] // РБК. – URL: https://www.rbc.ru/technology_and_media/22/07/2022/62da01319a794734d858b656 (дата обращения: 17.08.2022).

348. Роскомнадзор проверит «Ленту» после утечки личных данных россиян [Электронный ресурс] // РБК. – URL: https://www.rbc.ru/business/03/02/2020/5e380bf19a794791dbe68722 (дата обращения: 17.08.2022).

349. Роскомнадзор запросил у СДЭК информацию об утечке данных клиентов [Электронный ресурс] // РИА Новости. – URL: https://ria.ru/20220715/sdek-1802778865.html?utm_source=yxnews& (дата обращения: 17.08.2022).

350. Россияне испугались кражи личных данных и перешли на VPN [Электронный ресурс] // News. – URL: https://news.mail.ru/society/49789704/ (дата обращения: 11.09.2022).

351. Россияне стали чаще жаловаться на незаконное использование их персональных данных [Электронный ресурс] // Ведомости. – URL: https://www.vedomosti.ru/technology/articles/2019/07/22/807016-rossiyane-personalnih (дата обращения: 17.08.2022).

352. Сбер оценивает ущерб от перевыпуска скомпрометированных в России карт в 4,5 млрд рублей [Электронный ресурс] // Газета.ru. – URL: https://www.gazeta.ru/business/news/2022/06/16/17944346.shtml (дата обращения: 17.08.2022).

353. Сбербанк: с начала военной операции на Украине были украдены данные 65 млн россиян [Электронный ресурс] // Коммерсантъ. – URL: https://www.kommersant.ru/doc/5413181 (дата обращения: 17.08.2022).

354. СК возбудил уголовное дело после утечки данных пользователей «Яндекс.Еды» [Электронный ресурс] // РБК. – URL: https://www.rbc.ru/society/06/08/2022/62ed82249a79476795ab9b0e (дата обращения: 17.08.2022).

355. Сливы общества: IT-компании заявили об утечке данных бизнес-школы «Сколково» [Электронный ресурс] // Известия. – URL: https://iz.ru/1336396/ivan-chernousov-natalia-ilina/slivy-obshchestva-it-kompanii-zaiavili-ob-utec (дата обращения: 25.08.2022).

356. СМИ: база данных о ВИЧ-инфицированных и наркозависимых доступна для продажи [Электронный ресурс] // Газета. ru. – URL: https://www.gazeta.ru/tech/news/2016/09/12/n_9103151.shtml (дата обращения: 09.04.2023).

357. СМИ: «Вымпелком» допустил крупнейшую утечку данных за весь 2021 год [Электронный ресурс] // Daily Storm. – URL: https://news.myseldon.com/ru/news/index/258751819 (дата обращения: 17.08.2022).

358. СМИ узнали об утечке базы данных 1,3 млн российских клиентов Hyundai [Электронный ресурс] // РБК. – URL: https://www.rbc.ru/technology_and_media/11/01/2021/5ffbf4af9a79476933c5f164 (дата обращения: 27.08.2022).

359. С начала 2022 года в открытый доступ попало не менее 40 баз данных россиян [Электронный ресурс] // Коммерсантъ. – URL: https://www.kommersant.ru/doc/5504156 (дата обращения: 09.04.2023).

360. Сотрудники Альфа-банка продавали персональные данные клиентов. Их гонорар больше штрафа за разглашение банковской тайны [Электронный ресурс] // Cnews. – URL: https://zoom.cnews.ru/news/item/511675 (дата обращения: 09.04.2023).

361. СПИД пустили в народ. Базы данных по ВИЧ-инфицированным Тольятти и областным наркоманам открыто продаются [Электронный ресурс] // Новости Самары. – URL: https://www.samru.ru/society/novosti_samara/21998.html (дата обращения: 09.04.2023).

362. Судье по делу об убийстве адвоката Маркелова предоставили охрану [Электронный ресурс] // РИА Новости. – URL: https://ria.ru/20110304/342145271.html (дата обращения: 17.08.2022).

363. Утечки возьмут в оборот [Электронный ресурс] // Коммерсантъ. – URL: https://www.kommersant.ru/doc/5379590 (дата обращения: 09.04.2023).

364. *Филатова, М.А.* Уголовно-правовая охрана персональных данных [Электронный ресурс]. – URL: https://www.youtube.com/watch?v=mGyIkYEYn2Y&t=5714s (дата обращения: 10.05.2022).

365. Фонд защиты сданных [Электронный ресурс] // Коммерсантъ. – URL: https://www.kommersant.ru/doc/5515449 (дата обращения: 09.04.2023).

366. ФСБ РФ разоблачила сливавших иностранцам данные о военнослужащих [Электронный ресурс] // Известия. – URL: https://iz.ru/1352429/

2022-06-20/fsb-rf-razoblachila-slivavshikh-inostrantcam-dannye-o-voennosluzhashchikh (дата обращения: 23.08.2022).

367. Хакеры продают сканы паспортов 1,5 млн россиян, украденных у компании Oriflame: эксперт рассказал, что грозит жертвам [Электронный ресурс] // Комсомольская правда. – URL: https://www.kp.ru/daily/28321/4464204/ (дата обращения: 28.11.2022).

368. Чеченские следователи запрашивают данные на русских солдат [Электронный ресурс] // Комсомольская правда. – URL: https://www.kp.ru/daily/25707/907381/ (дата обращения: 24.08.2022).

369. Эксперт Новикова: Более 1,5 млрд записей с персональными данными попали в сеть в 2022 году [Электронный ресурс] // Рос. газета. – URL: https://rg.ru/2022/12/08/bolee-15-mlrd-zapisej-s-personalnymi-dannymi-popali-v-set-v-2022-godu.html (дата обращения: 09.12.2022).

370. «Яндекс» сообщил об утечке данных 5 тыс. почтовых ящиков [Электронный ресурс] // РБК. – URL:https://www.rbc.ru/technology_and_media/12/02/2021/602645dc9a79472c62786d55 (дата обращения: 27.08.2022).

371. Delivery Club оштрафовали на 80 тыс. руб. за утечку персональных данных [Электронный ресурс] // Коммерсантъ. – URL: https://www.kommersant.ru/doc/5515445 (дата обращения: 17.08.2022).

372. Group-IB: объём попавших в сеть персональных данных россиян в 2022 году вырос в 40 раз [Электронный ресурс] // Хабр. – URL: https://habr.com/ru/news/t/712488/ (дата обращения: 17.03.2023).

373. CyberCube: глобальный ущерб, связанный с киберпреступностью, к 2025 году достигнет 10,5 трлн. долларов [Электронный ресурс] // Cisoclub. – URL: https://cisoclub.ru/cybercube-globalnyj-ushherb-svyazannyj-s-kiberprestupnostyu-k-2025-godu-dostignet-105-trln-dollarov/ (дата обращения: 17.03.2023).

374. SuperJob отрицает утечку данных 5 млн пользователей [Электронный ресурс] // Коммерсантъ. – URL: https://www.kommersant.ru/doc/4390414 (дата обращения: 17.08.2022).

ПРИЛОЖЕНИЯ

Приложение 1.

Проект постановления Пленума Верховного Суда РФ «О внесении дополнений в постановление Пленума Верховного Суда Российской Федерации от 25 октября 2018 года № 46 "О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138[1], 139, 144[1], 145, 145[1] Уголовного кодекса Российской Федерации)"»

ПЛЕНУМ ВЕРХОВНОГО СУДА РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

№ __

г. Москва «___» _____ г.

О ВНЕСЕНИИ ДОПОЛНЕНИЙ В ПОСТАНОВЛЕНИЕ ПЛЕНУМА ВЕРХОВНОГО СУДА РОССИЙСКОЙ ФЕДЕРАЦИИ ОТ 25 ОКТЯБРЯ 2018 ГОДА № 46 "О НЕКОТОРЫХ ВОПРОСАХ СУДЕБНОЙ ПРАКТИКИ ПО ДЕЛАМ О ПРЕСТУПЛЕНИЯХ ПРОТИВ КОНСТИТУЦИОННЫХ ПРАВ И СВОБОД ЧЕЛОВЕКА И ГРАЖДАНИНА (СТАТЬИ 137, 138, 138[1], 139, 144[1], 145, 145[1] УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ)"

В связи с возникающими в судебной практике вопросами Пленум Верховного Суда Российской Федерации, руководствуясь статьей 126 Конституции Российской Федерации, статьями 2 и 5 Федерального конституционного закона от 5 февраля 2014 года № 3-ФКЗ «О Верховном Суде Российской Федерации», постановляет внести дополнения в постановление Пленума Верховного Суда Российской Федерации от 25 октября 2018 года № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138[1], 139, 144[1], 145, 145[1] Уголовного кодекса Российской Федерации)»:

1) дополнить пунктом 3.1 следующего содержания:

«3.1. Обратить внимание судов на то, что под персональными данными следует понимать зафиксированную с помощью материального носителя или в нематериальной (идеальной) форме информацию (сведения) о физическом лице (субъекте персональных данных), охраняемую в режиме конфиденциальности (ограниченного доступа), на основании которой может быть осуществлена его однозначная идентификация.

Не подлежит уголовной ответственности собирание или распространение чужих персональных данных, сделанных общедоступными самим их владельцем, в том числе путем размещения в сети «Интернет» (публичный профиль в социальной сети, на сайтах, форумах и иных онлайн ресурсах). В этом случае согласие на собирание, хранение, систематизацию и распространение общедоступных персональных данных презюмируется. В иных обстоятельствах при отсутствии общедоступности персональных данных согласие их субъекта должно быть конкретным, информированным и сознательным и в любой подтверждающей его наличие форме.

Судам необходимо иметь в виду, что установление обладателем персональных данных порядка обращения с ними (ограничение доступа, режим конфиденциальности с закрытым доступом) свидетельствует о желании контролировать и самостоятельно определять степень их открытости. Любое деяние, направленное на получение персональных данных, находящихся в режиме приватности, следует признавать совершенным против или помимо воли их владельца и квалифицировать как посягательство в отношении неприкосновенности чужих персональных данных.

Разъяснить судам, что при незаконном копировании и передаче персональных данных из информационных систем правоохранительных органов должностным лицом содеянное следует квалифицировать по части 3 статьи 272 УК РФ как неправомерный доступ к компьютерной информации с использованием своего служебного положения. В частности, как использование служебного положения должны квалифицироваться действия виновного, которые

не вызывались служебной необходимостью (отсутствовали обязательные условия или основания для их совершения) и противоречили целям и задачам службы, для достижения которых должностное лицо правоохранительного органа было наделено соответствующими служебными полномочиями (доступ к информационной системе персональных данных с получением персонального логина и пароля). Суду надлежит выяснять и указывать в приговоре, какими именно ведомственными документами (должностные инструкции, иные локальные нормативные акты) установлены права и обязанности обвиняемого в копировании и передаче персональных данных должностного лица, злоупотребление какими из этих прав и обязанностей вменяется ему в вину со ссылкой на конкретные нормы (статью, часть, пункт).

Наличие у виновного официального доступа к информационной системе персональных данных (собственный логин и пароль) не исключает возможности его осуждения по статье 272 УК РФ, поскольку им совершены незаконные действия, связанные с неправомерным доступом к персональным данным, имевшие целью их копирование и последующую передачу третьим лицам вопреки интересам службы. Если использование должностным лицом своих служебных полномочий выразилось в незаконном копировании персональных данных, когда фактически произошло их незаконное распространение, содеянное дополнительно не подлежит квалификации по статье 137 УК РФ или статье 138 УК РФ.

Получение должностным лицом незаконного вознаграждения за копирование и передачу персональных данных из ведомственных информационных систем надлежит квалифицировать как получение взятки по статье 290 УК РФ. Совершение должностным лицом указанных действий за взятку образует самостоятельный состав преступления, однако не охватывается объективной стороной преступлений, предусмотренных статьей 290 УК РФ. В таких случаях содеянное взяткополучателем подлежит квалификации по совокупности преступлений как получение взятки за незаконные действия

по службе и по части третьей статьи 272 УК РФ как неправомерный доступ к компьютерной информации с использованием служебного положения.

Действия лица, имевшего на законных основаниях доступ к компьютерной информации в результате выполняемой работы (трудовой, гражданско-правовой договор), надлежит квалифицировать по статье 272 УК РФ, если установлено, что им совершен неправомерный доступ к компьютерной информации в специализированной системе (служебных программах и информационно-поисковых базах данных), с целью копирования и передачи (распространения) персональных данных клиентов (абонентов). Неправомерным следует признавать доступ к компьютерной информации для получения и (или) использования персональных данных без согласия их обладателя виновным, не наделенным необходимыми для этого полномочиями (отсутствие специального (авторизованного) доступа) либо в нарушение установленного нормативными правовыми актами его условий и порядка независимо от формы такого доступа. Осуществление указанными лицами технических функций (администраторы баз данных, инженеры, специалисты, служащие банков, офисов продаж операторов мобильной связи) при наличии к тому оснований не исключает уголовную ответственность по части 3 статьи 272 УК РФ за использование своего служебного положения. Решая вопрос о квалификации содеянного по статье 272 УК РФ, суду надлежит установить, осуществляло ли лицо неправомерный доступ к персональным данным вопреки специальному режиму защиты сведений, составляющих персональные данные, а также коммерческую, служебную, личную, семейную или иную тайну, а также возложена ли на это лицо обязанность соблюдать указанные правила. При установлении обязанности соблюдения лицом конфиденциальности такой информации и предупреждении об ответственности за разглашение в целях обеспечения ее неприкосновенности в соответствии с локальными нормативными актами коммерческой или иной организации (трудовой договор, должностные инструкции, порядок обращения с информацией ограниченного доступа, обязательство о неразглашении информации ограниченного доступа, в том числе составляющей коммерческую,

налоговую, служебную тайны, тайну персональных данных), содеянное следует дополнительно квалифицировать по статье 183 УК РФ.

Действия лица квалифицируются по статье 274^1 УК РФ, если судом установлено, что информационная система (база данных) правоохранительных органов, кредитно-финансового учреждения, мобильного оператора и других государственных или коммерческих учреждений и организаций относится к объекту критической информационной инфраструктуры и включена в Реестр значимых объектов критической информационной инфраструктуры (статья 8 федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»). В ином случае действия лица при наличии на то оснований квалифицируются по статье 272 УК РФ».

Приложение 2.

Анкета для экспертов и результаты их опроса

Респонденты: 250 экспертов – судей, прокуроров, следователей и оперативных сотрудников. Опрос проведён в 2020-2023 гг. в г. Москве, г. Санкт-Петербурге, Курской, Московской, Нижегородской, Пензенской, Саратовской, Тамбовской областях и Краснодарском крае в целях подготовки научных и практических рекомендаций по предупреждению преступлений с персональными данными.

Вопрос № 1. Насколько актуальна в настоящее время проблема преступлений, связанных с персональными данными (то есть *совершаемых в отношении персональных данных и (или) с их использованием*)?

Варианты ответов	**Результаты анкетирования**
1. Актуальность несомненна, поскольку количество таких преступлений за последние годы значительно возросло	150 (60%)
2. Один из самых динамично развивающихся и организованных видов современной преступности	80 (32%)
3. Масштабы распространенности этих преступлений невысоки	15 (6%)
4. Ваш вариант: *«есть и более важные проблемы»; «в реальности таких фактов гораздо больше»; «ввиду высокой латентности сложно дать оценку ее фактическому уровню» и др.*	5 (2%)

Вопрос № 2. Какие преступления (по материалам уголовных дел) совершаются в отношении персональных данных или с их использованием?

Варианты ответов	**Результаты анкетирования**
1. Преступления против собственности	110 (44 %)
2. Преступления против конституционных прав и свобод человека и гражданина	60 (24 %)
3. Преступления в сфере компьютерной информации	30 (12%)
4. Должностные преступления	20 (8%)
5. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну	25 (10%)
6. Незаконное образование (создание, реорганизация) юридического лица	3 (1,2%)
7. Ваш вариант: *«преступления против жизни и здоровья».*	2 (0,8%)

Вопрос № 3. Укажите *качественные* характеристики преступлений с персональными данными:

Варианты ответов	**Результаты анкетирования**
1. Совершаются преступниками-одиночками	65 (26%)
2. Совершаются группой лиц по предварительному сговору	80 (32%)
3. Совершаются организованной группой с обязательным распределением ролей	95 (38%)
4. Совершаются преступным сообществом (преступной организацией)	3 (1,2%)
5. Являются разновидностью транснациональной организованной преступности	7 (2,8%)
6. Ваш вариант	–

Вопрос № 4. Дайте оценку латентности преступлений с персональными данными:

Варианты ответов	**Результаты анкетирования**
1. Гиперлатентность (75–100 %)	115 (46%)
2. Латентность (50–74 %)	40 (16%)
3. Латентность (25–49 %)	60 (24%)
4. Латентность (до 24 %)	30 (12%)
5. Ваш вариант: *«до 30 % возбужденных дел остаются нераскрытыми; «количество жертв, данные которых были украдены, а впоследствии использованы для совершения против них различных посягательств, насчитывает сотни тысяч»* и др.	5 (2%)

Вопрос № 5. Предполагаете ли Вы дальнейший значительный рост преступлений с персональными данными?

Варианты ответов	**Результаты анкетирования**
1. Да	180 (72%)
2. Нет	70 (28%)
3. Ваш вариант	–

Вопрос № 6. Чем объясняется небольшое количество приговоров за преступления с персональными данными?

Варианты ответов	**Результаты анкетирования**
1. Трудностью выявления (раскрываемости) ввиду специфического способа совершения преступлений	80 (32%)

(с использованием сети Интернет и иных информационных технологий)	
2. Несовершенством законодательной конструкции диспозиции ст. 137 УК РФ, при котором правоприменитель неверно толкует понятия частной жизни и персональных данных	85 (34%)
3. Бланкетностью диспозиций ст. 137, 183, 272, 274[1] УК РФ, требующих обращения к другим нормативным актам	39 (15,6%)
4. Правоохранительные органы усилили противодействие указанным преступлениям	7 (2,8%)
5. Потерпевшие не сообщают о подобных фактах в правоохранительные органы	19 (7,6%)
6. Злоумышленники научились успешно скрывать совершение указанных преступлений	17 (6,8%)
7. Ваш вариант: *«сложностью доказывания этих преступлений», «низкая квалификация следователей»; «эти нормы нуждаются в новой редакции», «неочевидным характером совершения этого преступления» и др.*	3 (1,2%)

Вопрос № 7. Чем обусловлена разная квалификация преступлений с персональными данными, совершенных при аналогичных обстоятельствах?

Варианты ответов	**Результаты анкетирования**
1. Нечетко сформулированными и схожими дифференцирующими признаками, не позволяющими разграничивать ст. 137 УК РФ с иными составами преступлений, связанных с персональными данными	30 (12%)
2. Сложностью уголовно-правовой оценки и отграничения понятий «персональные данные», «частная жизнь», «личная тайна», «семейная тайна»	135 (54%)
3. Трудностью толкования категории «общедоступность» применительно к персональным данным, размещаемым в социальных сетях, иных открытых Интернет-ресурсах	84 (33,6%%)
4. Отсутствием разъяснений вопросов квалификации преступлений, связанных с персональными данными, в специальном постановлении Пленума Верховного Суда РФ, а потому отсутствием единообразной судебной практики	1 (0,4%)
5. Ваш вариант	–

Вопрос № 8. Как Вы считаете, понятия «частная жизнь» и «персональные данные», используемые в диспозиции статьи 137 «Нарушение неприкосновенности частной жизни» УК РФ, являются синонимами?

Варианты ответов	**Результаты анкетирования**
1. Являются	50 (20%)
2. Нет, это разные, несовпадающие понятия	200 (80%)
3. Ваш вариант	–

Вопрос № 9. Как следует квалифицировать действия должностного лица правоохранительного органа, совершившего копирование и передачу третьим лицам персональных данных из ведомственных информационно-поисковых систем (базы данных) за денежное вознаграждение?

Варианты ответов	**Результаты анкетирования**
1. По ст. 137 и ст. 272 УК РФ	34 (13,6%)
2. По ст. 272 УК РФ	28 (11,2%)
3. По ст. 272 и ст. 290 УК РФ	188 (75,2%)
4. Ваш вариант	–

Вопрос № 10. Как следует квалифицировать действия должностного лица правоохранительного органа, совершившего копирование и передачу третьим лицам персональных данных из ведомственных информационно-поисковых систем (базы данных) по иным мотивам?

Варианты ответов	**Результаты анкетирования**
1. По ст. 137 и 272 УК РФ	56 (22,4%)
2. По ст. 286 УК РФ	34 (13,6%)
3. По ст. 272 УК РФ	132 (52,8%)
4. По ст. 272 и 286 УК РФ	28 (11,2%)
5. Ваш вариант	–

Вопрос № 11. Как следует квалифицировать действия сотрудников финансово-кредитных учреждений, операторов мобильной связи, совершивших неправомерный доступ с копированием из служебных информационно-поисковых систем (баз данных) персональных данных и передачей их третьим лицам?

Варианты ответов	**Результаты анкетирования**
1. По ст. 137 и 272 УК РФ	20 (8%)
2. По ст. 272 УК РФ	50 (20%)
3. По ст. 183 и 272 УК РФ	180 (72%)
4. Ваш вариант	–

Вопрос № 12. Существует ли необходимость в самостоятельной криминализации незаконного оборота персональных данных для охраны их неприкосновенности (*проектируемая статья 137*[1] *УК РФ*)?

Варианты ответов	**Результаты анкетирования**
1. Да, поскольку эти действия общественно опасны именно в отношении персональных данных	110 (44%)
2. Да, поскольку не всегда персональные данные и частная жизнь означают одно и то же	90 (36%)
3. Да, поскольку административная ответственность неэффективна	15 (6%)
4. Нет, достаточно ст. 137 УК РФ и иных уголовно-правовых средств	20 (8%)
5. Ваш вариант: *«да, в связи с огромным ростом таких преступлений»; «да, чтобы самостоятельно осуществлять уголовное преследование с выявлением и регистрацией таких фактов, привлечением всех соучастников к ответственности»; «да, для отражения самостоятельной статистики по ним»; «да, надо отделить частную жизнь от персональных данных»; «это решит проблему точной квалификации» и др.*	15 (6%)

Вопрос № 13. Какие незаконные действия с персональными данными должны быть уголовно наказуемыми (*проектируемая статья 137*[1] *УК РФ*)?

Варианты ответов	**Результаты анкетирования**
1. Собирание или распространение персональных данных	15 (6%)
2. Собирание персональных данных в целях совершения преступлений	110 (44%)
3. Распространение персональных данных при причинении существенного вреда правам и законным интересам граждан или организаций либо охраняемым законом интересам общества или государства	125 (50%)
4. Ваш вариант	–

Вопрос № 14. Поддерживаете ли Вы предложение о криминализации деяний, совершаемых в отношении информационно-поисковых систем с персональными данными (баз данных) как квалифицирующего признака (*проектируемая статья 137*[1] *УК РФ*)?

Варианты	**Результаты**

ответов	анкетирования
1. Да, это будет способствовать профилактике этих и других преступлений, совершаемых против граждан, собственности и др.	105 (42%)
2. Да, поскольку информационные базы данных часто подвергаются криминальному воздействию (взлом, похищение) в целях последующей продажи	120 (48%)
3. Нет	25 (10%)
4. Ваш вариант	–

Вопрос № 15. Какие признаки незаконного оборота персональных данных для охраны их неприкосновенности (*проектируемая статья 137*[1] *УК РФ*) следует признать квалифицирующими и особо квалифицирующими:

Варианты ответов	**Результаты анкетирования**
1. Организованную группу	120 (48%)
2. Группу лиц по предварительному сговору	70 (28%)
3. С использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»	58 (23,2%)
4. Ваш вариант: *«с причинением крупного ущерба»; «наступление тяжких последствий»; «в отношении двух или более лиц» и др.*	2 (0,8%)
	–

Вопрос № 16. Какое законодательное решение в целях предупреждения других преступлений, совершаемых с использованием персональных данных, представляется более эффективным?

Варианты ответов	**Результаты анкетирования**
1. Наделение диспозиций соответствующих уголовно-правовых норм квалифицирующим признаком «с использованием персональных данных»	60 (24%)
2. Введение нового отягчающего обстоятельства «с использованием персональных данных» в ст. 63 УК РФ	190 (76%)
3. Ваш вариант	–