Федеральное государственное автономное образовательное учреждение высшего образования «Сибирский федеральный университет»

На правах рукописи

ГУТНИК СЕРГЕЙ ИОСИФОВИЧ

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПНЫХ ПОСЯГАТЕЛЬСТВ В ОТНОШЕНИИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Специальность: 12.00.08 – «уголовное право и криминология; уголовно-исполнительное право»

ДИССЕРТАЦИЯ
на соискание ученой степени кандидата
юридических наук

Научный руководитель:
доктор юридических наук, профессор
Щедрин Н.В.

Красноярск – 2017

ОГЛАВЛЕНИЕ

Введение

Актуальность темы исследования. Процесс глобализации на сегодняшний день является, с одной стороны, важной характеристикой современных общественных отношений, а с другой стороны, создаёт ряд определённых проблем, которые существенно влияют на все сферы жизнедеятельности общества.

Одной из сущностных характеристик глобализации на современном этапе является активное развитие системы информационных отношений, влекущее за собой изменение статуса человека в информационном пространстве и требующее создания особых условий для реализации предоставленных ему естественных и неотчуждаемых прав и свобод. Попадая в поле информационного пространства, человек остаётся человеком с его многообразными общественными и правовыми статусами, хотя и, как указывают некоторые исследователи[1], начинает терять свою идентичность и становится одиноким.

Современные технические средства позволяют собирать и обрабатывать значительные объёмы социально значимых сведений, необходимых для жизнедеятельности человека, общества и государства. Стремительное развитие компьютерной и цифровой техники даёт возможность получать доступ и использовать различные банки данных практически любым субъектам информационных отношений. При этом скорость получения и распространения любого вида информации с каждым днём только увеличивается.

Человек как субъект многих правоотношений является наиболее уязвимым в информационном поле, поскольку реализация его прав и свобод связана с оборотом личной информации о нём – персональных данных. Обладая различным набором сведений о человеке, злоумышленники могут

[1] Семенов Е.Е. Информационная глобализация и её влияние на трансформацию социальных связей в современном мире / Е.Е. Семенов // Вестник Костромского государственного университета им. Н.А. Некрасова. – 2010. - №1 (том 16). С. 133.

использовать их в преступных целях. В связи с этим возникает необходимость обеспечения надлежащего механизма правовой охраны личной информации, которая непосредственно связана с человеком.

Вопросы правового обеспечения безопасности персональных данных в последнее время стали объектом пристального внимания со стороны многих государств, в том числе и России. Об этом говорит многообразие принятых нормативных правовых актов, посвящённых данному вопросу[2], а также научных исследований[3].

Совет Безопасности Российской Федерации в 2016 году констатировал, что информационная безопасность государства подвергается множеству угроз. В частности, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе, в части, затрагивающей неприкосновенность частной жизни, личную и семейную тайну, при обработке персональных данных с использованием информационных технологий[4].

О неуклонном росте различного рода утечек персональной информации, в том числе сопряжённых с преступными посягательствами свидетельствует и статистика. Так, за 2015 год Роскомнадзором в ходе проверок было 1397 нарушений, что на 37% больше, чем в 2014 году[5]. Растёт число зарегистрированных преступных посягательств в отношении персональной информации, а также с её незаконным использованием при совершении различных мошеннических и иных действий[6].

---

[2] Федеральный закон «О персональных данных», «Об информации, информационных технологиях и защите информации», Стратегия развития информационного общества, Доктрина информационной безопасности Российской Федерации, Концепция защиты персональных данных в информационных системах персональных данных оператора связи, Концепция информационной безопасности детей и т.д.

[3] См.: Ершов М.А. Ответственность за посягательства на конфиденциальную информацию по российскому уголовному праву. Автореф. дисс. … канд. юрид. наук. Нижний Новгород, 2010; Терещенко Л.К. Правовой режим информации. Автореферат дисс. … докт. юрид. наук. М., 2011; Петрыкина Н.И. Правовое регулирование оборота персональных данных в России и странах ЕС (сравнительно-правовое исследование): Дисс. … канд. юрид. наук. М., 2007.

[4] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ 05.12.2016 №646) // РГ. 2016. №7144.

[5] Отчёт о деятельности уполномоченного органа по защите прав субъектов персональных данных за 2015 год [Электронный ресурс]: http://rkn.gov.ru/docs/Otchet_ZPD_rus2015.pdf

[6] См., например: Утекшие персональные данные в России всё чаще используются для «кражи личности» [Электронный ресурс]: https://www.infowatch.ru/presscenter/news/7858; В России увеличилось число

Между тем, следует отметить, что преступные посягательства в отношении персональной информации не всегда могут быть правильно квалифицированы правоприменительными органами с позиций уголовного закона вследствие неправильной оценки обстоятельств, непонимания сущности составов соответствующих преступлений, а также во многих случаях нежелания пострадавших субъектов персональных данных заявлять об указанных фактах. Это приводит к искажению данных официального статистического учёта и создаёт трудности при осуществлении деятельности по предупреждению соответствующих правонарушений.

Институт персональных данных в российской правовой системе является относительно новым, вследствие чего возникает множество дискуссионных моментов, затрагивающих вопросы реализации регулирующих его законодательных норм. Нормы уголовного права пока не могут в полной мере учесть специфику института персональных данных, что влечет за собой ошибки и спорные вопросы в правоприменении. По существу, появилась новая группа общественных отношений, охрана которых со стороны уголовного закона должна производиться с учётом определённых особенностей, установленных иными нормами законодательства.

Анализ средств массовой информации показывает, что любые факты преступных посягательств в отношении персональной информации могут вызывать широкий общественный резонанс, что свидетельствует о необходимости повышенной правовой охраны рассматриваемого правового института и совершенствования норм уголовного закона с целью обеспечения безопасности личности и всей системы общественных отношений. Сказанное выше свидетельствует об актуальности проблемы

преступлений с использованием персональных данных [Электронный ресурс]: https://safe-doc.com/v-rossii-uvelichilos-chislo-prestupleniy-s-ispolzovaniem-personalnyh-dannyh; Перешли на личности: в России растёт число краж персональных данных [Электронный ресурс]: https://rg.ru/2017/03/26/v-rossii-vyroslo-chislo-krazh-personalnyh-dannyh.html

совершенствования норм уголовного закона о преступных посягательствах в отношении персональных данных.

Объектом исследования выступает комплекс общественных отношений, связанных с уголовно-правовой охраной персональных данных в современных правовых условиях Российской Федерации.

Предмет исследования составляют нормы действующего законодательства Российской Федерации, дореволюционного российского законодательства, уголовного законодательства России советского периода, регулирующего правоотношения по обеспечению правовой охраны персональных данных, общепризнанные принципы и нормы международного права и международные договоры в области правового регулирования и охраны оборота персональных данных, ведомственные нормативные правовые акты. Кроме того, в предметное поле входят научно-теоретические исследования по теме диссертационного исследования, данные социологических исследований, уголовно-правовой статистики, уголовные дела и материалы об отказе в возбуждении уголовных дел, материалы гражданских и арбитражных судебных дел, материалы дел об административных правонарушениях, публикации по указанной проблематике, электронные ресурсы всемирной информационно-коммуникационной сети «Интернет».

Цель и задачи исследования. Основная цель диссертационного исследования состоит в комплексном анализе института персональных данных с позиций правовой теории мер безопасности в контексте их уголовно-правовой охраны от различных преступных посягательств; совершенствование норм российского уголовного права и норм иных отраслей законодательства.

Для достижения указанной цели ставились следующие **задачи:**

1. Исследовать правовую природу института персональных данных;

2. Изучить эволюцию и закономерности развития норм российского уголовного права, посвящённых охране института персональных данных;
3. Провести анализ норм международного и иностранного права, посвящённых уголовно-правовому регулированию института персональных данных;
4. Рассмотреть особенности правовой охраны персональных данных с позиций правой теории мер безопасности;
5. Осуществить анализ норм уголовного права, посвящённых охране института персональных данных;
6. Исследовать особенности объективных и субъективных признаков преступных посягательств в отношении персональных данных;
7. Выявить проблемы квалификации преступных посягательств в отношении персональных данных на основе анализа научной литературы, судебной и иной правоприменительной практики и разработать меры по совершенствованию данных уголовно-правовых норм.

Методология и методы диссертационного исследования. Методологической основой диссертационного исследования являются общенаучные методы (логический и диалектический методы познания, системный подход, которые использовались в процессе исследования правового содержания института персональных данных); метод классификации (использовался при исследовании и систематизации преступных посягательств в отношении персональных данных); метод анализа и синтеза различных правовых норм; статистический и сравнительно-правовой методы.

Нормативную базу исследования составляют: Конституция Российской Федерации, Уголовный кодекс Российской Федерации, законодательные акты Российской Федерации, регулирующие оборот персональных данных, а также уголовное законодательство,

осуществляющее правовое регулирование охраны персональных данных в зарубежных странах. Значительную часть нормативной базы диссертационного исследования составили документы ООН, Совета Европы, Европейского Союза и других международных и региональных организаций, многосторонние и двухсторонние договоры, в которых содержатся общепризнанные принципы и нормы международного права.

Эмпирическую основу исследования составляет опубликованная судебная практика судов общей юрисдикции Российской Федерации по гражданским делам, связанным с незаконным оборотом персональных данных, делам об административных правонарушениях, а также по уголовным делам о преступных посягательствах в отношении персональных данных, практика Европейского Суда по правам человека, статистические данные. Всего автором диссертационного исследования проанализировано 50 судебных актов по гражданским делам, 30 судебных актов по делам об административных правонарушениях и 105 приговоров по уголовным делам за период с 2012 по 2016 гг.

Степень научной разработанности темы. Институт персональных данных появился в российской правовой науке относительно недавно, однако стал объектом исследований многих правоведов. Терминологическая основа исследования была сформулирована на основе изучения работ по кибернетике, философии, социологии, истории, теории права. Общие вопросы правовой охраны персональной информации исследовались в работах следующих учёных-правоведов: М.Ю. Авдеева, Р.И. Бодрова, И.В. Бондаря, Л.А. Букалеровой, М.В. Бундина, В.В. Гафнер, Р.И. Дремлюги, В.П. Иванского, С.М. Крянина, В.П. Кузьмина, А.В. Кучеренко, Н.А. Лопашенко, М.Н. Малеиной, А.С. Маркевич, А.В. Мнацаканян, Г.П. Новоселова, Е.Ю. Покаместовой, Н.И. Петрыкиной, Я.М. Плошкиной, А.В. Серебренниковой, Л.К. Терещенко, Э.А. Цадыковой, Н.В. Щедрина, В.Н. Щепетильникова.

Вопросы, связанные с уголовно-правовой охраной персональных данных, в том числе вопросы различных видов правовых режимов, под

которые может подпадать данный вид информации, освещались в работах: Р.Р. Гайфутдинова, Д.Ю. Гришмановского, Ю.В. Дубровского, Ю.А. Дунаевой, М.А. Ершова, В.С. Козлова, В.А. Мазурова, О.А. Пальчиковской, С.М. Паршина, Н.И. Пикурова, В.Г. Степанова-Егиянца, А.В. Суслопарова, И.А. Шевченко, И.А. Юрченко и др.

Работы этих авторов внесли значительный вклад в изучение института персональной информации. В то же время, комплексно институт персональных данных в контексте уголовно-правовой охраны не исследовался. Именно поэтому указанная проблематика в силу активного развития информационных технологий, общественных отношений и законодательства не теряет своей актуальности.

Научная новизна диссертации определяется тем, что институт персональных данных впервые в российском правоведении подвергнут комплексному исследованию в качестве объекта уголовно-правовой охраны. Научная новизна конкретизируется в основных **положениях, выносимых на защиту**, которые имеют значение для дальнейшего развития правового регулирования института персональных данных и его уголовно-правовой охраны:

1. Персональные данные – это информация, позволяющая идентифицировать физическое лицо (А), свободный оборот которой создает опасность причинения вреда законным интересам личности (Б), и по поводу которой установлен правовой режим конфиденциальности (В).

А. Под информацией, позволяющей идентифицировать физическое лицо, следует понимать совокупность логически связанных между собой сведений, отражающих в себе свойства и признаки событий, фактов, явлений, объектов окружающей действительности, которые предоставляют возможность познающему субъекту получить осведомлённость об этом физическом лице - ее обладателе.

Б. Не контролируемое обладателем собирание, распространение и использование этих сведений создает опасность нарушения не только его

права на неприкосновенность частной жизни, но и может подвергнуть опасности другие его права (например, право на жизнь, право собственности и т.д.).

В. Указанная информация должна быть объектом охраны, в связи с чем в отношении нее устанавливается правовой режим конфиденциальности, а именно совокупность правил безопасности (специальных запретов и обязанностей), которые ограничивают ее собирание, распространение и использование третьими лицами без согласия самого физического лица (ее обладателя), за исключением случаев, когда обязанность по передаче такой информации установлена федеральным законом.

Согласие обладателя означает его прямое волеизъявление на собирание, распространение и использование персональных данных третьими лицами для целей, которые обусловлены получением такого согласия.

2. Перечень сведений конфиденциального характера, установленный на сегодняшний день не утратившим силу Указом Президента РФ, должен содержаться не в данном подзаконном акте, а в федеральном законе, что будет соответствовать принципу ограничения конституционных прав и свобод человека и гражданина только на основании федерального закона (ч. 3 ст. 55 Конституции РФ).

3. Предлагается внести изменения в п. 7 ст. 2 Федерального закона «Об информации, информационных технологиях и защите информации», изложив его в следующей редакции: «7. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определённой информации требование не передавать такую информацию третьим лицам без согласия её обладателя, за исключением случаев, когда обязанность по передаче такой информации третьим лицам установлена федеральным законом».

4. Уголовно-правовая охрана персональных данных обусловлена режимным характером указанной информации. Охранительное уголовное

правоотношение в отношении персональных данных не может возникнуть, если не нарушено правило безопасности (ограничение или запрет), установленное специальным правовым режимом персональных данных – режимом личной или семейной тайны, режимом коммерческой, банковской, налоговой тайны.

5. Уголовно-правовое значение для целей привлечения виновного лица к уголовной ответственности имеет лишь такой поиск информации, который завершился получением искомых сведений, и именно это следует включать в понятие «собирание». Для целей уголовно-правовой охраны и квалификации преступных посягательств в отношении персональной информации, подпадающей под соответствующий правовой режим безопасности, общественно опасным в процессе незаконного собирания сведений, составляющих личную и семейную тайну, является именно результат такого собирания.

6. Альтернативный признак «распространение» характерен как для посягательств, предусмотренных ст. 137 УК РФ, так и для ст. 183 УК РФ. Поэтому предлагается использовать в диспозиции ст. 183 УК РФ термин «распространение» вместо термина «разглашение». При этом распространение персональных данных для целей привлечения к уголовной ответственности виновных лиц всегда должно сопровождаться незаконным, неправомерным содержанием, то есть в отсутствие согласия лица, являющегося правообладателем данных, а также при отсутствии предусмотренных федеральным законом оснований, при которых распространение персональных данных допускается без согласия правообладателя (субъекта персональных данных).

7. В целях устранения правовой неопределённости при квалификации нарушения неприкосновенности частной жизни, совершённого с использованием своего служебного положения, предлагается изложить диспозицию ч. 2 ст. 137 Уголовного кодекса РФ в следующей

редакции: «2. Те же деяния, совершённые лицом, которому указанные сведения были доверены или стали известны по службе или работе…».

Теоретическая значимость исследования заключается в развитии представлений о персональных данных как об особом виде информации, подлежащем уголовно-правовой охране, а также в развитии правовой теории информационной безопасности с позиций уголовного права. Результаты данного исследования могут стать основой для проведения дальнейших научных исследований в сфере уголовно-правового регулирования уголовно-правовой охраны персональной информации.

Практическая значимость исследования заключается в разработке рекомендаций по совершенствованию информационного и уголовного законодательства, а также практики его применения. Результаты диссертационного исследования могут быть применены при совершенствования норм Уголовного кодекса Российской Федерации и других нормативных правовых актов, в подготовке обзоров судебной практики по уголовным делам, а также разъяснений Пленума Верховного Суда РФ, в деятельности следственных и судебных органов при рассмотрении уголовных дел, связанных с преступными посягательствами в отношении персональных данных. Результаты диссертационного исследования могут быть также использованы в учебном процессе образовательных организаций высшего образования при совершенствовании курсов уголовного и информационного права.

Степень достоверности результатов диссертационного исследования. Выводы, сформулированные в диссертационном исследовании, имеют высокую степень достоверности, что подтверждается следующим:

- в работе были использованы данные, полученные ведущими учёными-правоведами в ходе многолетних научных исследований в области уголовного и информационного права;

- применён широкий комплекс общенаучных и частнонаучных методов познания, которые составляют методологическую базу диссертационного исследования;

- осуществлён сравнительный правовой анализ обширной нормативно-правовой основы, включающей не только российское, но и зарубежное законодательство, а также общепризнанные принципы и нормы международного права, регламентирующие правовую охрану персональных данных;

- произведён анализ судебной и иной правоприменительной практики, сложившейся по поводу привлечения виновных лиц к уголовной ответственности за посягательства в отношении персональных данных.

Апробация и внедрение результатов диссертационного исследования. Основные положения и выводы, сформулированные в диссертации, отражены в 16 публикациях, в том числе три – в научных журналах, входящих в перечень рецензируемых научных изданий, в которых должны быть опубликованы научные результаты диссертаций.

Результаты научных исследований докладывались и обсуждались на ежегодных всероссийских научных конференциях студентов, аспирантов и молодых учёных Юридического института Сибирского федерального университета (2011-2015); на XI Международной научно-практической конференции молодых учёных «Традиции и новации в системе современного российского права (Москва, 2012 г.); IV Международных Макаренковских чтениях «Неомакаренковская педагогика в условиях реформирования уголовно-исполнительной системы и становления ювенальной юстиции: международный и российский опыт» (Красноярск, Канск, 2012 г.); VII Международной научно-практической конференции студентов и аспирантов «Правовое регулирование в условиях модернизации государственности: национальный и международный правовые аспекты» (Казань, 2012 г.); Ежегодной Всероссийской научно-практической конференции «Правовые проблемы укрепления российской государственности» (Томск, 2013);

Всероссийской научно-практической конференции «Проблемы предупреждения и борьбы с преступлениями и иными правонарушениями» (Новосибирск, 2013); Ежегодной Всероссийской научно-практической конференции «Правовые проблемы укрепления российской государственности» (Томск, 2015 г.), IX Международной научной конференции студентов, аспирантов и молодых учёных «Енисейские правовые чтения» (Красноярск, 2015 г.), Днях молодёжной науки «Енисейские правовые чтения» в рамках XII Международной научно-практической конференции студентов, аспирантов и молодых учёных «Проспект Свободный 2016» (Красноярск, 2016).

Результаты диссертационного исследования послужили основой для проведения соответствующих учебных занятий по следующим дисциплинам: «Правоведение» (со студентами инженерно-физических, экономических и строительных специальностей профильных институтов Сибирского федерального университета), «Правовая статистика», «Криминология», «Правовые аспекты мер безопасности», «Противодействие коррупции» (для студентов направления и специальности «Юриспруденция» Юридического института СФУ), «Основы научных исследований» (со студентами специальности «Таможенное дело» Юридического института СФУ), «Основы информационно-аналитической работы» (для студентов направления «Международные отношения» Юридического института СФУ).

Кроме того, результаты диссертационного исследования были использованы автором в процессе разработки лекции-консультации по теме «Персональные данные: изменения законодательства, требования защиты персональных данных, согласие на обработку персональных данных при размещении данных в интернете и базах данных, обезличивание персональных данных, раскрытие данных на государственных сайтах» в рамках программы обучения государственных и муниципальных служащих Красноярского края «Электронное управление. Электронное правительство»

в отделе по подготовке государственных и муниципальных служащих управления и государственной службы губернатора Красноярского края[7].

Структура диссертации определена поставленными автором целями и задачами исследования, логикой последовательного изложения изучаемой проблемы. Работа состоит из введения, двух глав, заключения, списка использованных нормативных актов и литературы.

[7] Красноярский край. Кадровая политика [Электронный ресурс]: http://www.kadry24.krskstate.ru/press/kadrcentr/0/id/22837

Глава 1. Становление и развитие института охраны персональных данных

1.1. Персональные данные как вид конфиденциальной информации: понятие, признаки и правовая характеристика

Информационные правоотношения пронизывают человеческое общество на протяжении длительного периода времени. Однако массив законодательства и правовых норм, регулирующих отношения в этой сфере, становится с каждым годом всё обширнее, несмотря на сравнительно недавнюю регламентацию.

Информация, являясь непременным условием жизни и социальной деятельности людей, предметом их постоянного внимания, существует столько же, сколько существует общество. Она сопровождает любые социальные отношения, определяет решения и действия индивида[8].

Информация становится основополагающим инструментом общественного развития. Входя в гражданский оборот и пронизывая в буквальном смысле все виды общественных отношений, она приобретает серьёзную ценность для общества, что и обусловливает, в свою очередь, потребность в урегулировании информационных правоотношений, а также рост числа соответствующих нормативных актов.

Большинство правовых норм в сфере регулирования информационных правоотношений в Российской Федерации нацелены на обеспечение информационной безопасности участников таких отношений. Это следует, в частности, из Стратегии развития информационного общества в Российской Федерации, пункт 8 Раздела IV которой гласит: «Основным направлением развития Стратегии в области противодействия использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам Российской Федерации является **обеспечение неприкосновенности частной жизни, личной и**

[8] Платон. Аристотель Государства. Законы. Политик. М.: Мысль, 1998. С. 35.

семейной тайны, соблюдение требований по обеспечению безопасности информации ограниченного доступа»[9]. Таким образом, информация ограниченного доступа или конфиденциальная информация, включая персональные данные, становится ключевым объектом обеспечения безопасности в информационной сфере, и обеспечение безопасности именно данного вида информации является залогом безопасности всей системы общественных отношений.

Как указывается в научной литературе, «обеспечение безопасности системы означает сохранение её целостности, упорядоченности, устойчивости, а также способности к самоуправлению и управлению»[10]. Поэтому такое обеспечение безопасности не может происходить без установления различных мер юридической ответственности за нарушение условий, позволяющих обеспечить состояние защищённости информационных процессов. Юридическая ответственность реализуется с учётом специфических методов информационного права при возникновении конфликтных противоправных ситуаций[11]. Из этого следует, что предотвращение угрозы информационной безопасности должно обеспечиваться надлежащими правовыми нормами.

Законодательные акты, раскрывая сущность информационной безопасности, довольно часто оперируют понятиями «конфиденциальная информация», «персональная информация», «персональные данные» «данные личного характера», «тайна». Между тем, отображение сущности института персональных данных невозможно без выработки единого подхода к его пониманию. Однако следует признать, что на сегодняшний день определить единство подходов в понимании института персональных данных ни в правовой доктрине, ни в действующем российском законодательстве не

---

[9] Стратегия развития информационного общества в Российской Федерации (утв. Указом Президента РФ 07.02.2008 №Пр-212) // РГ. 2008. №34.

[10] Концептуально-теоретические основы правового регулирования и применения мер безопасности: монография / Под науч. ред. Н.В. Щедрина; Сиб. фед. ун-т. Красноярск, 2010. С. 14.

[11] Ковалева Н.Н. Информационное право: учебное пособие / Н.Н. Ковалева. М., 2007. С. 138.

представляется возможным, что характерно для многих правовых институтов современной российской правовой системы.

Вопрос о сущности персональных данных как разновидности информации весьма сложен и неоднозначен. Именно поэтому только комплексный анализ подходов относительно изучаемого объекта может сформировать целостную картину о нём. Таким образом, на данном этапе нашей задачей является изучение вопроса о сущности персональных данных с позиций понятий и признаков, породивших данный правовой институт.

1.1.1. Понятие информации

Сущность персональных данных как объекта настоящего исследования не может происходить вне разрыва логических связей, из которых данное понятие происходит.

Принято считать, что первоначальным родовым понятием в этой логической связке должно выступать понятие информации, которое обобщает в себе все последующие виды, в том числе и понятие персональных данных[12]. Не представляется единым и подход к определению понятия «информация», поскольку каждое из изученных определений, так или иначе, содержит в себе лишь отдельные признаки рассматриваемого явления.

Обзор справочно-энциклопедической литературы позволяет сделать вывод, что информация может определяться как сведения, сообщения о чём-либо. Так, Большая Советская Энциклопедия определяет информацию как «осведомление, сообщение о каком-либо событии, о чьей-либо деятельности»[13]. Информацию (от лат. information – разъяснение, изложение, осведомлённость) также определяют как сведения о чём-либо, независимо от формы их представления[14]. Анализ определений из словаря С.И. Ожегова

[12] Здесь сам термин «данные» может быть отождествлён с понятием «информация».
[13] Большая Советская Энциклопедия. В 50 т. / Гл. ред. А.М. Прохоров. – М.: Изд.: Советская Энциклопедия, 1972. Т. 10. С. 249.
[14] Борисов Е.Ф., Петров А.А., Березкина Т.Е. Экономика. М.: Проспект, 2015. С. 30.

позволяет сделать вывод о тождественности понятий «информация» и «сведения», так как информация понимается как «сведения об окружающем мире и протекающих в нем процессах, воспринимаемых человеком или специальным устройством», а «сведения» - как «познания в какой-либо области, известия, сообщения, знания, представление о чём-либо»[15].

В общефилософском понимании информация рассматривается сквозь призму категорий «отражение» и «различие». Категория «отражение» позволяет выявить свойства изучаемого объекта познания, а категория «разнообразие» позволяет отграничить полученные путём изучения свойства одного объекта от свойств другого объекта существующей реальности. Разнообразие сведений, которое существует в отражающем объекте относительно отражаемого, по существу и представляет собой информацию[16].

А.Д. Урсул указывает, что «информация, так же, как и энергия, существует во всех сферах и фрагментах мироздания, является характеристикой всех материальных систем и форм существования материи в мироздании. Информация выступает как отражение разнообразия или разнообразие отражения»[17]. В.Г. Афанасьев констатировал, что информация является результатом отражения многообразия действительности, сообщениями, сведениями о ней[18].

Сегодня в философии встречаются и иные подходы к понятию информации. В частности, вполне очевидной, на наш взгляд, становится позиция, согласно которой понятие «информация» выводится из гносеологии – теории познания – и вступает в соотношение с понятием «знание».

Так, М.А. Петров пишет, что «информация представляется определённой семиотической организацией, системой логически организованных высказываний и предложений, выраженных в языке,

---

[15] Ожегов С.И. Словарь русского языка / С.И. Ожегов. М.: 1989 г. С. 253.
[16] Украинцев Б.С. Информация и отражение // Вопросы философии. 1963. № 2. С. 36.
[17] Урсул А.Д. Информация и глобальные процессы: междисциплинарные исследования // Знание. Понимание. Умение. 2013. №3. С. 27.
[18] Афанасьев В.Г. Социальная информация . М., 1994. С. 12.

зафиксированных в текстах и функционирующих в обществе как продукт человеческой деятельности»[19].

На наш взгляд, данное определение учитывает важное свойство информации – её функционирование исключительно внутри общества, а также то, что информация является следствием человеческой деятельности. Вполне очевидно, что информация вне общества существовать не может, поскольку она создана для передачи, накопления, обмена и использования.

Многие отождествляют информацию со сведениями, позволяющими сделать человека осведомлённым относительно того или иного объекта окружающей действительности. М.А. Ершов связывает понятие информации с признаком ценности, определяя информацию как ц»енные для субъектов правоотношений сведения (сообщения, данные) о лицах, предметах, фактах, событиях, явлениях, процессах независимо от формы их представления»[20].

Между тем, полагаем, что это утверждение не всегда является справедливым. Так, информация не перестаёт быть таковой даже в том случае, если никакой ценности для конкретного субъекта она не принесла. В этом смысле ценность (или полезность) информации не является её сущностным признаком, а несёт в себе лишь качественную составляющую применительно к конкретным жизненным ситуациям. Более того, субъект правоотношений по своему усмотрению определяет, является ли полученная им информация ценной или нет. Основная содержательная цель информации – получение знания об объекте окружающего мира.

С позиций теории кибернетики информацию определяли как объективно существующую субстанцию. В частности, известный идеолог теории кибернетики советского периода Н. Винер утверждал: «Информация – это не энергия и не материя, это обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления

---

[19] Петров М.А. Информационно-знаниевая сущность познавательного процесса // Вестник Иркутского государственного университета. 2010. №26(2).

[20] Ершов М.А. Ответственность за посягательства на конфиденциальную информацию по российскому уголовному праву. Автореф. дисс. … канд. юрид. наук. Нижний Новгород, 2010. С. 32.

к нему наших чувств»[21]. Информация всегда важна для развивающихся систем при принятии управленческого решения, вследствие чего информация может существенно повлиять на явления и события, которые подконтрольны воле и сознанию человека.

В.М. Глушков полагал, что «информация в самом общем её понимании представляет собой меру неоднородности материи и энергии в пространстве и во времени, меру изменений, которыми сопровождаются все протекающие в мире процессы»[22].

Информация - это «специфический атрибут объективного мира (в т.ч. жизнедеятельности личности, общества, государства), создающий условия, необходимые для обеспечения устойчивости и развития систем различной природы»[23]. Отсюда можно сделать вывод, что информация обеспечивает необходимые условия коммуникаций в обществе, что позволяет ему функционировать и активно взаимодействовать между собой его институтам и иным структурным элементам.

Развитие общественных отношений обусловливает необходимость их чёткой правовой регламентации, в том числе и в сфере информационного обмена. Именно поэтому понятие информации должно обеспечиваться надлежащей правовой регламентацией и должно быть закреплено соответствующими правовыми нормами.

Поскольку понятие «информация» рассматривается нами применительно к её правовому значению для целей диссертационного исследования, обратимся к определению информации, которое дано современными правовыми актами. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 №149-ФЗ определяет информацию весьма просто: это сведения (сообщения, данные) независимо от формы их представления. Закон при этом никаким образом не конкретизирует, что понимается под сведениями, а отождествляет

[21] Винер Н. Кибернетика, или Управление и связь в животном и машине. М., 1968. С. 201.
[22] Цит. по: Туманова Л.В., Снытников А.А. Обеспечение и защита права на информацию. М., 2001. С. 9.
[23] Большая энциклопедия: В 62 т. Т. 19. М.: ТЕРРА, 2006. С. 145.

их с сообщениями и данными. Как видим, законодательное определение информации является весьма узким по сравнению с тем, которое приводится с позиций философии и теории кибернетики. Можно сделать однозначный вывод, что под информацией с позиций федерального закона можно понимать достаточно большой перечень данных: это могут быть сведения о субъектах, объектах, факты, события, действия, бездействия, свойства, присущие объектам, явления, - всё то, что позволяет тому или иному лицу получить определённую долю осведомлённости для использования или неиспользования в каких-либо целях.

В юридической науке подходы к определению термина «информация» мало отличаются от законодательного подхода.

Так, В.П. Кузьмин определяет информацию как «сведения об окружающем мире, которые уменьшают существующую в отношении его степень неопределенности, отчуждённые от их создателя и ставшие сообщениями, воспроизводимыми путем передачи субъектами устным, письменным либо другим способом»[24]. В.Г. Степанов-Егиянц понимает под информацией «любые сведения, полученные только определённым путём и пригодные для постоянного хранения, передачи и автоматизированной обработки» [25] . В.В. Гафнер определяет информацию как «сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые воспринимают информационные системы (живые организмы, управляемые машины) в процессе жизнедеятельности и работы»[26]. В.Н. Щепетильников определяет информацию как совокупность знаний, мыслей, объектов материального и духовного мира различной природы, несущих в себе определенную энергию и могущих быть воспринятыми человеком[27].

---

[24] Кузьмин В.П. Понятие и юридическая сущность информации // Информационное право. 2009. №2.
[25] Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ. Автореферат дисс. … канд. юрид. наук. М., 2005. С. 15.
[26] Гафнер В.В. Информационная безопасность: учеб. пособие. Ростов-на-Дону: Феникс, 2010. С. 14.
[27] Щепетильников В.Н. Уголовно-правовая охрана электронной информации: Автореферат дисс. … канд. юрид. наук. Рязань, 2006. С. 9.

Однако всё же некоторые исследователи признают, что законодательное определение является весьма узким и исключает из себя целую группу сущностных признаков информации.

Например, А.В. Суслопаров полагает, что «под информацией понимаются сведения, не имеющие физических характеристик, хранящиеся на материальном носителе и передающиеся посредством сигналов в форме определённого кода»[28]. Подобная позиция представляется нам небесспорной. Информация может существовать, будучи и не зафиксированной на материальном носителе. А учитывая, что человек, который обладает определённой информацией, может рассматриваться источником информации, способным посредством речи и с помощью иных средств передавать её, то наличие признака закреплённости информации только на материальном носителе исключает из себя значительную часть сведений, которые тоже подлежат правовой охране и регламентации и признаются информацией.

И.А. Юрченко отходит от законодательного определения понятия «информация», не отождествляет понятие информации с понятием «сведения», указывая, что «сведения представляют собой некое отношение между информацией и отображаемым ею объектом. Это отношение включает в себя факт, информацию о нём и субъекта, получающего эту информацию»[29].

В свою очередь, С.М. Паршин, соглашаясь с подобной логикой, пишет, что «под информацией следует понимать зафиксированный в материальной или идеальной форме и характеризующий факты окружающей действительности результат её восприятия человеком»[30].

---

[28] Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера: Автореферат дисс. … канд. юрид. наук. Владивосток, 2010. С. 9.
[29] Юрченко И.А. Информация конфиденциального характера как предмет уголовно-правовой охраны: Дисс. … канд. юрид. наук. М., 2000. С. 28.
[30] Паршин С.М. Тайна в уголовном законодательстве (теоретико-прикладное исследование): Дисс. … канд. юрид. наук. Нижний Новгород, 2006. С. 28.

По нашему мнению, вышеуказанная позиция является справедливой, поскольку информационный обмен в обществе происходит сквозь призму субъективного восприятия. Информация может носить определённую эмоциональную окраску, а восприятие той или иной информации разными людьми может происходить по-разному. В силу этого, субъективное восприятие информации во многих случаях может даже приводить к ошибкам в коммуникации.

В литературе высказывается также мнение, согласно которому в информации можно выделить две составляющие – сведения (как содержательная часть информации) и коммуникация (как совокупность действий по сбору и обмену сведениями)[31]. Полагаем, что такой подход оптимальнее всего отражает современное понимание информации, поскольку она сегодня немыслима без содержательной и коммуникативной составляющих, что позволяет эффективно её использовать. Необходимо также учитывать, что коммуникативная составляющая информации характеризует динамики обмена информацией.

Довольно интересной является точка зрения, которую предлагают Т.В. Закупень и С.Ю. Соболь. По мнению авторов, информация может выступать в следующих значениях:

«1. Как определенные сведения, факты, данные о различных процессах и явлениях, протекающих в природе и обществе;

2. Как процесс, то есть сообщение какому-либо субъекту определенных сведений, передача информации;

3. Как оценка, которую человек дает в своем сознании определенным явлениям»[32].

Нам представляется, что понятие информации должно нести в себе определённое сущностное содержание, которое может быть универсально

---

[31] Войниканис Е., Якушев М. Информация. Собственность. Интернет: Традиции и новеллы в современном праве. М.: Волтерс Клувер, 2004. С. 3.

[32] Закупень Т.В., Соболь С.Ю. Информация и её правовое регулирование // Журнал российского права. 2004. № 1. С. 33.

применимым к различного рода ситуациям и общественным отношениям. По существу, без движения информации, без информационного обмена невозможна вообще деятельность любого социально организованного института, как и общества в целом. Данное утверждение справедливо и для правовой системы. Именно поэтому определение понятия «информация» должно содержать в себе несколько сущностных признаков, позволяющих отличить информацию от пустого набора логически не связанных и разрозненных данных, не имеющих отношения к явлениям, фактам и событиям.

Исходя из этого, полагаем, что понятие «информация» соответствует следующим признакам:

1. Это совокупность логически связанных между собой сведений, которые отражают в себе свойства и признаки событий, фактов, явлений, объектов окружающей действительности.
2. Информация способна предоставить человеку возможность получить знания, сделать его осведомлённым относительно событий, фактов, явлений, объектов окружающей действительности, которыми он не обладал на определённый момент времени.
3. Информация всегда существует в социально организованном человеческом обществе как универсальное средство коммуникации и как средство межличностного обмена.
4. Информация может быть подвергнута субъективной обработке со стороны человека, поэтому доля её объективности, соответствия действительности будет в каждом случае зависеть от характера её представления (передачи).
5. Происхождение той или иной информации всегда сопряжено с объективными причинами. Развитие общественных отношений всегда связано с передачей определённой информации. Соответственно, те или иные сведения становятся, на наш взгляд,

информацией с того момента, когда возникли информационные отношения, и те или иные сведения необходимо донести до определенного или неопределенного круга субъектов через акты коммуникации. Кроме того, если степень неопределенности по поводу интересующего объекта возрастает, то информация становится инструментом, позволяющим повысить знания об этом объекте.

Отсюда **информацию** можно определить следующим образом: это совокупность логически связанных между собой сведений, отражающих в себе свойства и признаки событий, фактов, явлений, объектов окружающей действительности, которые посредством коммуникации предоставляют возможность познающему субъекту получить осведомлённость о них.

Безусловно, данное определение не претендует на универсальность и сформулировано для целей исследования. Данное определение, на наш взгляд, можно рассматривать как основу для раскрытия понятия «персональные данные». Следовательно, персональные данные являются разновидностью информации, поскольку позволяют получить заинтересованному лицу осведомлённость о личности конкретного субъекта.

В то же время, персональные данные являются особой разновидностью информации, что проявляется в тесной связи данного понятия с понятием «конфиденциальность информации». Поэтому раскрытие понятия «персональные данные» должно быть осуществлено, в том числе, при помощи анализа понятия «конфиденциальность информации».

1.1.2. Понятие конфиденциальности информации

Европейская Конвенция о защите прав человека и основных свобод от 04.11.1950 в ч. 1 ст. 10 устанавливает, что каждый имеет право свободно

выражать своё мнение. Это право включает свободу придерживаться своего мнения и свободу **получать и распространять информацию**[33].

Свобода информационного обмена и право на получение и распространение информации становится неотъемлемым правом человека в большинстве государств. Так, например, п. 1 ст. 1 и п. 1 ст. 2 Основного закона Федеративной Республики Германия предусмотрено, что каждый имеет право на свободное развитие своей личности в той мере, в какой он не нарушает прав других и не посягает на конституционный строй или нравственный закон; достоинство человека неприкосновенно; уважать и защищать его – обязанность всей системы государственной власти. Этими нормативными положениями, как подчеркнул Конституционный Суд ФРГ в «Решении о переписи населения» 1983 года, гарантируется **право каждого на информационное самоопределение**[34].

Конституция Российской Федерации в ч. 4 ст. 29 закрепляет, что каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Между тем, вполне очевидно, что это право не является абсолютным, поскольку существует множество обстоятельств, при которых свободное движение и обмен информацией могут наносить значительный ущерб государству и обществу в целом. Последствия от свободного движения негативной информации могут быть несоизмеримо велики в мировом информационном пространстве, что, в свою очередь создаёт угрозу стабильности и безопасности мирового сообщества и всей человеческой цивилизации. Именно поэтому свободный обмен информацией может быть ограничен с целью обеспечения безопасности, обеспечения охраны государства и общества в целом. Такое ограничение должно быть обоснованным, достаточным и необходимым.

---

[33] Европейская конвенция о защите прав человека и основных свобод ETS №005 // СЗ РФ. 1998. №20. Ст. 2143.

[34] Grundgesetze fuer die Bundesrepublik Deutschland [Электронный ресурс]: http://www.gesetze-im-internet.de/gg/

Одним из способов ограничения права на свободное получение, использование и распространение информации можно рассматривать установление перечня сведений, распространение которых не может быть свободным, - так называемая **конфиденциальная информация**.

Вопрос о понятии конфиденциальной информации является достаточно спорным, и единства мнений относительно его содержания и признаков в правовой доктрине не существует.

Феномен конфиденциальности (приватности) некоторые зарубежные исследователи связывают с появлением нового понимания системы прав человека, ибо новое право выделилось из права приватности, права на одиночество, на частную сферу, свободную от постороннего вторжения[35]. Таким образом, признавая права и свободы человека высшей ценностью, законодательство многих современных государств исходит из необходимости обеспечения всех условий для полноценного развития личности, в том числе посредством сохранения в тайне некоторых информационных аспектов повседневной жизни человека.

Федеральный закон «Об информации, информатизации и защите информации» от 20.02.1995 №24-ФЗ, утративший на сегодняшний день юридическую силу, определял конфиденциальную информацию следующим образом: «Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации»[36]. Это определение было основой для рассмотрения всех дел, связанных с нарушением режима конфиденциальной информации.

Однако данное понимание конфиденциальной информации в нормативном смысле было слишком узким и не учитывало огромный массив информации, которая по своим признакам также не могла быть свободно

[35] García González A. La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado [Электронный ресурс]: http: //www.juridicas.unam.mx/publica/rev/boletin/cont/120/art/art3.html

[36] Федеральный закон «Об информации, информатизации и защите информации» от 20.02.1995 №24-ФЗ (утратил силу) // СПС КонсультантПлюс.

обмениваемой и распространяемой – информации с ограниченным доступом. Например, в этот перечень, исходя из представленного определения, не могли входить сведения, затрагивающие личную или семейную тайну, которые могли быть и недокументированными, однако, для субъекта представляли сведения закрытого (конфиденциального) характера. Именно поэтому данное законодательное положение неоднократно подвергалось серьёзной критике[37].

Федеральный закон «Об информации, информационных технологиях и защите информации», принятый вместо предыдущего законодательного акта, указанные выше недостатки устранил, закрепив понятие «конфиденциальность информации». В новом законе «конфиденциальность информации» определена как «обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя»[38].

Нетрудно заметить, что в данном случае правовое определение конфиденциальности информации представлено уже не как разновидность информации, а как набор критериев или правовой режим информации, соблюдать который обязан каждый субъект информационных правоотношений в силу указания различных законодательных актов.

Конфиденциальность информации определяется и в других нормативных правовых актах.

Так, Закон Российской Федерации «О средствах массовой информации» в статье 41 устанавливает императивное правило, в соответствии с которым редакция средства массовой информации не вправе разглашать в распространяемых сообщениях и материалах сведения, предоставленные гражданином с условием сохранения их в тайне. Редакция обязана сохранять в тайне источник информации и не вправе называть лицо,

---

[37] См., например: Терещенко Л.К. Правовой режим информации. Автореферат дисс. … докт. юрид. наук. М., 2011. С. 43.

[38] Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 №149-ФЗ // СЗ РФ. 2006. №31 (ч. I). Ст. 3448.

предоставившее сведения с условием неразглашения его имени [39] . Таким образом, закон напрямую устанавливает требование для средств массовой информации об обеспечении конфиденциальности сведений, полученных от физического лица и публикуемых в последующем в официальных источниках. Вполне логично, что ограничение, связанное с сохранением конфиденциальности сведений об источнике информации, установлено федеральным законом и ставит конфиденциальность в зависимость от усмотрения лица, являющегося непосредственным источником информации. Из этого, на наш взгляд, можно сделать вывод, что режим конфиденциальности устанавливается лицом, а закон предоставляет такую правовую возможность в виде правила поведения в отношении средств массовой информации.

Важно понимать, что объём сведений, в отношении которых субъект самостоятельно устанавливает режим конфиденциальности, определяется, исходя из его личных соображений, и в некоторых случаях такое ограничение может носить настолько строгий характер, что обеспечивает закрытость личной информации не только от третьих лиц, не имеющих личных контактов с субъектом, но даже и от его близких родственников или членов семьи.

Например, в последнее время стала весьма актуальной проблема соблюдения конфиденциальности сведений личного характера со стороны владельцев различных мобильных приложений. В частности, житель юга Франции обратился с иском в суд в отношении компании «Uber», являющейся владельцем мобильного сервиса по заказу такси онлайн, после того, как из-за некорректной работы приложения его супруга узнала об измене. Мужчина потребовал от фирмы 48 миллионов долларов компенсации морального вреда. Он вызвал такси с мобильного телефона супруги. Несмотря на то, что он вышел из своего аккаунта на смартфоне жены, ей

[39] Закон Российской Федерации «О средствах массовой информации» от 27.12.1991 №2124-1 // РГ от 08.02.1992. №32.

продолжили приходить уведомления о поездках мужа. В результате из-за полученной информации супружеская пара расторгла брак. Представители «Uber» отказались комментировать случившееся, но указали, что защита персональных данных клиентов является приоритетом компании[40].

В личной практике диссертанта имела место правовая ситуация, связанная с разглашением средством массовой информации конфиденциальных сведений. Корреспондентом одной из районных газет проведена неформальная беседа с председателем Общественной палаты города М., которая являлась инициатором обращения в органы государственной власти с просьбой разобраться в ситуации вокруг градообразующего предприятия, находящегося в стадии банкротства. В неформальной беседе председатель дала согласие на публикацию самого обращения в газете, но дать интервью отказалась, прокомментировав, однако, ситуацию под условием сохранения её имени в тайне, а также сохранения в тайне её мнения. Вопреки положениям ст. 41 Закона РФ «О средствах массовой информации» корреспондент разместил не только текст обращения Общественной палаты в государственные органы, но и комментарии председателя, поместив также в статью её изображение, нарушив, таким образом, условие о сохранении указанной информации в тайне. Председатель Общественной палаты города М. по данному факту вынуждена была обратиться в суд с исковым заявлением в порядке гражданского судопроизводства. Однако в последующем правовой конфликт был разрешён во внесудебном порядке.

Если бы данная ситуация стала предметом рассмотрения гражданского дела в суде общей юрисдикции, то это был бы первый в Красноярском крае случай защиты принципа конфиденциальности информации, переданной физическим лицом средству массовой информации.

---

[40] Француз решил отсудить у Uber 48 миллионов долларов из-за распавшегося брака [Электронный ресурс]: https://lenta.ru/news/2017/02/13/uber/

В статье 3 Федерального закона «О коммерческой тайне» с учётом изменений, внесённых в связи с введением в действие Федерального закона «Об информации, информационных технологиях и защите информации» коммерческая тайна стала определяться как «режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду»[41]. Как видим, режим конфиденциальности стал распространяться и на коммерческую тайну.

Аналогичным образом с режимом конфиденциальности стали связаны понятия «банковская тайна», «налоговая тайна», «служебная тайна», «медицинская тайна» и т.д.

На основании изложенного можно сделать вывод, что конфиденциальность информации применительно к каждой из её разновидностей заключается по своему содержанию в ограничении свободного обмена данной информацией в силу того, что информация, в отношении которой законом устанавливается конфиденциальность, имеет существенное юридическое значение и может влиять на всю систему общественных отношений, а потому должна охраняться специальными правовыми режимами.

Хотя Федеральный закон «Об информации, информационных технологиях и защите информации» содержит определение конфиденциальности информации, тем не менее, в нём отсутствует перечень информации, которая должна быть конфиденциальной. Такой перечень установлен Указом Президента Российской Федерации от 06 марта 1997 №188 «Об утверждении перечня сведений конфиденциального характера»[42].

Среди таких сведений Указ Президента называет следующие:

---

[41] Федеральный закон «О коммерческой тайне» от 29.07.2004 №98-ФЗ // СЗ РФ. 2004. №32. Ст. 3283.

[42] Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 №188 // СЗ РФ. 1997. №10. Ст. 1127.

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
2. Сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с Федеральным законом от 20 августа 2004 г. N 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" и другими нормативными правовыми актами Российской Федерации.
3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).
4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).
6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

По существу установление перечня, содержащего все возможные с позиций действующего законодательства сведения, в отношении которых должна обеспечиваться их конфиденциальность, является шагом вперед. Он устанавливает, что доступ к какой информации не может быть свободным в

силу обстоятельств, установленных законом. Перечень согласуется с ч. 1 ст. 10 Европейской Конвенции о защите прав человека и основных свобод.

Однако Указ Президента по своей юридической силе и иерархической характеристике в системе действующих источников российского права имеет статус подзаконного акта. Это вызывает определённые сомнения относительно того, что ограничение права на доступ к информации установлено подзаконным актом. Ведь в соответствии с ч. 3 ст. 55 Конституции Российской Федерации права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, свободы, здоровья, прав и законных интересов, обеспечения обороны страны и безопасности государства.

Из этого можно сделать вывод, что ограничение права на доступ к информации в виде установления перечня сведений конфиденциального характера не может устанавливаться Указом Президента, а должно быть закреплено в профильном федеральном законе. По нашему мнению, данный перечень должен содержаться в Федеральном законе «Об информации, информационных технологиях и защите информации», поскольку именно в нём устанавливается сущность конфиденциальности информации как правовой категории.

В правовой доктрине термин «конфиденциальная информация» рассматривается учёными-юристами под различными углами зрения. Так, одни утверждают, что конфиденциальная информация является родовым понятием по отношению ко всем видам тайн, которые закреплены в действующем российском законодательстве[43].

М.А. Ершов определяет конфиденциальную информацию следующим образом: «Это ценные для субъектов правоотношений сведения (сообщения, данные) независимо от формы их представления, доверенные узкому кругу

[43] Пелешенко Ю. Кадровик. Трудовое право для кадровика. 2011. №8.

лиц в связи с исполнением определённых обязанностей, и доступ к которым ограничен в соответствии с положениями федеральных законов»[44].

И.А. Шевченко отождествляет понятие конфиденциальной информации с понятием тайны, указывая, при этом, что «конфиденциальная информация не является препятствием для её передачи третьим лицам»[45]. Аналогичной позиции придерживается М.Н. Малеина, указывая, что «конфиденциальность» и «тайна» - понятия синонимичные по отношению к защите персональных данных»[46].

Е.А. Палехова под конфиденциальностью понимает «обязательное для соблюдения субъектом или иным получившим доступ к информации лицом требование не допускать её распространения без согласия субъекта-обладателя информации или наличия иного законного основания»[47].

С.Ю. Головина рассматривает конфиденциальность как «принцип обеспечения защиты информации и гарантии её секретности»[48].

М.В. Бундин определяет конфиденциальную информацию как «информацию ограниченного доступа». Далее, используя пример с персональными данными, он указывает, что «конфиденциальность заключается в нераспространении, а именно в недопущении действий, направленных на передачу и ознакомление с информацией третьими лицами, её опубликование, размещение в открытом доступе»[49].

Анализ вышеприведённых позиций позволяет сделать вывод, что в научной литературе между понятием «конфиденциальная информация» и «конфиденциальность информации» не устанавливается существенная разница. Скорее всего, это связано с тем, что Федеральный закон «Об

---

[44] См.: Ершов М.А. Указ. соч.
[45] Шевченко И.А. Уголовно-правовая охрана неприкосновенности частной жизни: Дис. … канд. юрид. наук. Красноярск, 2006. С. 80.
[46] Малеина М.Н. Право на тайну и неприкосновенность персональных данных // Журнал российского права. 2010. №11.
[47] Палехова Е.И. Конфиденциальная информация и институт персональных данных в банковской деятельности // Предпринимательское право. 2010. №3.
[48] Молодцов М.В., Головина С.Ю. Трудовое право России. М., 2010. С. 197-198.
[49] Бундин М.В. Персональные данные как информация ограниченного доступа // Информационное право. 2009. №1.

информации, информатизации и защите информации» 1995 года, как нами было уже указано выше, содержал понятие «конфиденциальная информация» и определял её только как специально охраняемые документированные сведения. Действующий на сегодняшний день Федеральный закон «Об информации, информационных технологиях и защите информации» 2006 года содержит понятие «конфиденциальность» информации.

Представляется, что между понятиями «конфиденциальная информация» и «конфиденциальность информации» имеется существенное различие. Оно заключается в том, что «конфиденциальная информация» является качественной характеристикой соответствующего вида информации, в отношении которого устанавливается режим конфиденциальности. «Конфиденциальность информации» является правовым режимом информации, который устанавливается на основании федерального закона и заключается в применении ограничений и запретов в отношении свободного обмена конкретным видом информации.

Таким образом, прежний федеральный закон, содержав в себе понятие «конфиденциальная информация», определял разновидность информации и в связи с этим устанавливал, что изначально существует информация, доступ к которой ограничен в силу прямого указания закона. Термин «конфиденциальность», содержащийся в действующем федеральном законе, на наш взгляд, является более удачным, поскольку закрепляет критерии отнесения информации к конфиденциальной, в силу чего доступ к ней может быть ограничен, и она не подлежит несанкционированному разглашению.

К таким критериям относятся, в частности следующие:

1. Наличие субъекта, получившего доступ к определённой информации.
2. Специальное правовое основание, при помощи которого субъект получил доступ к данной информации.
3. Обязательное требование не передавать данную информацию третьим лицам.

4. Передача указанной информации возможна только с согласия её обладателя.

Кроме того, законом предоставляется возможность субъекту самостоятельно определять ту или иную информацию в качестве конфиденциальной.

Между тем, если проанализировать действующие российские законодательные акты в области охраны конфиденциальной информации, то можно сделать вывод, что конфиденциальность в этом смысле не является абсолютной, а потому применение конфиденциальности может быть ограничено в силу специальных оснований, установленных законом.

Так, Федеральный закон «О персональных данных»[50] устанавливает, что, по общему правилу, одним из условий обработки персональных данных является согласие субъекта персональных данных на их обработку (п. 1 ч. 1 ст. 6). В то же время, статья 7 названного Федерального закона закрепляет, что операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законом. Статья 10 в п. 2.1-9 ч. 2 устанавливает перечень оснований, при которых получение согласия субъекта на обработку персональных данных, а, как следствие, обеспечение их конфиденциальности, не требуется. Среди них, в частности, указываются такие, как: необходимость защиты жизни и здоровья субъекта персональных данных; всероссийская перепись населения; необходимость установления или осуществления прав субъекта персональных данных, а равно и в связи с осуществлением правосудия и т.д.

Федеральный закон «О коммерческой тайне» в ч. 1 ст. 6 устанавливает, что обладатель информации, составляющей коммерческую тайну, по мотивированному требованию органа государственной власти, иного государственного органа, органа местного самоуправления предоставляет им

[50] Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ // СЗ РФ. 2006. №31 (ч. I). Ст. 3451.

на безвозмездной основе информацию, составляющую коммерческую тайну. А в соответствии с ч. 3 указанной статьи обладатель информации, составляющей коммерческую тайну, а также органы государственной власти, иные государственные органы, органы местного самоуправления, получившие такую информацию, обязаны предоставить эту информацию по запросу судов, органов предварительного следствия, органов дознания по делам, находящимся в их производстве, в порядке и на основаниях, которые предусмотрены законодательством Российской Федерации[51].

В соответствии со ст. 41 Закона Российской Федерации «О средствах массовой информации» редакция средства массовой информации обязана сохранять в тайне источник информации и не вправе называть лицо, предоставившее сведения с условием неразглашения его имени, за исключением случая, когда соответствующее требование поступило от суда в связи с находящимся в его производстве делом[52].

В свою очередь, Федеральный закон «О банках и банковской деятельности» в ст. 26 устанавливает, что кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, о счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону. Справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией им самим, судам и арбитражным судам (судьям), Счетной палате Российской Федерации, налоговым органам, федеральному органу исполнительной власти в области финансовых рынков, Пенсионному фонду Российской Федерации, Фонду социального

[51] Федеральный закон «О коммерческой тайне» от 29.07.2004 №98-ФЗ // СЗ РФ. 2004. №32. Ст. 3283.
[52] Закон Российской Федерации «О средствах массовой информации» от 27.12.1991 №2124-1 // РГ. 1992. №32.

страхования Российской Федерации и органам принудительного исполнения судебных актов, актов других органов и должностных лиц в случаях, предусмотренных законодательными актами об их деятельности, а при наличии согласия руководителя следственного органа - органам предварительного следствия по делам, находящимся в их производстве. В соответствии с законодательством Российской Федерации справки по операциям и счетам юридических лиц и граждан, осуществляющих предпринимательскую деятельность без образования юридического лица, выдаются кредитной организацией органам внутренних дел при осуществлении ими функций по выявлению, предупреждению и пресечению налоговых преступлений[53].

Таким образом, можно сделать вывод, что определение конфиденциальности информации, содержащееся в Федеральном законе «Об информации…», не является полным. Представляется, что оно должно быть дополнено словами, делающими исключение из общего правила о легальном ограничении конфиденциальности, которое устанавливается соответствующими нормативными правовыми актами. Поэтому редакция п. 7 ст. 2 Федерального закона «Об информации…» может выглядеть следующим образом:

«7. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определённой информации требование не передавать такую информацию третьим лицам без согласия её обладателя, за исключением случаев, когда обязанность по передаче такой информации третьим лицам установлена федеральным законом»

1.1.3. Понятие персональных данных

Термин «персональные данные» существует в российской правовой системе сравнительно недавно. Впервые он был введён Федеральным законом «Об информации, информатизации и защите информации» 1995

[53] Федеральный закон «О банках и банковской деятельности» от 02.12.1990 №395-1 // Ведомости СНД РСФСР. 1990. №27. Ст. 357.

года, который определял его как информацию о гражданах, относил их к конфиденциальной информации и устанавливал правило, в соответствии с которым сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную тайну, семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения, не допускается[54]. При этом из содержания самого закона (например, ч. 1 ст. 11) следовало, что перечень персональных данных должен быть установлен на уровне федерального закона.

Впрочем, такой перечень был установлен, но не законом, а подзаконным актом – Указом Президента РФ от 06 марта 1997 №188, который определял персональные данные как сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность[55].

Как пишет Л.К. Терещенко, «основы правового режима персональных данных, установленные в Федеральном законе «Об информации, информатизации и защите информации», содержали ряд черт, характерных для европейской модели защиты персональных данных. Принципиальным сохранившимся до нашего времени отличием от европейской модели правового регулирования является упор на защиту информации персонального характера в отрыве от защиты прав субъектов персональных данных и их интересов»[56].

В 2005 году Российская Федерация ратифицировала Конвенцию Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных» 1981 года, присоединившись, таким образом, к нормам международного права в сфере защиты персональных данных и взяв на себя, тем самым, обязательство привести своё внутреннее

---

[54] Федеральный закон «Об информации, информатизации и защите информации» (утратил силу) от 20.02.1995 №24-ФЗ // СЗ РФ. 1995. №8. Ст. 609.

[55] Указа Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 №188 // СЗ РФ. 1997. №10. Ст. 1127.

[56] Терещенко Л.К. Правовой режим персональных данных и безопасность личности // Закон. 2013. №6. С. 38.

законодательство к соответствию с этими нормами. Конвенция впервые предусмотрела признанное международным сообществом определение персональных данных: «Персональные данные означают информацию, затрагивающую конкретного или могущего быть идентифицированным лица»[57].

На основании данной Конвенции в 2006 году был принят, а в 2007 году вступил в законную силу Федеральный закон «О персональных данных», который закрепил легальное определение рассматриваемого термина. В п. 1 ст. 3 указанного закона установлено, что под персональными данными понимается любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных) [58] . Ранее, до внесения изменений Федеральным законом от 25.07.2011 №261-ФЗ [59] определение персональных данных включало в себя ещё и примерный перечень сведений, относящихся к персональным данным, а именно: фамилия, имя и отчество, год, месяц и дата места рождения, адрес, семейное и социальное, имущественное положение, образование, профессия, доходы и другая информация. Таким образом, перечень персональных данных считался открытым и не ограничивался определённым набором видов информации о гражданине. Однако такое решение представляется не совсем корректным, поскольку при определении юридически значимого термина необходимо исходить, прежде всего, из его внутреннего содержания и сущностных признаков.

Вероятно, существование такого подхода и вынудило законодателя внести в Федеральный закон изменения, отойдя от определения персональных данных через перечень, ограничившись лишь законодательно закреплёнными критериями отнесения информации к персональным данным.

---

[57] Конвенция Совета Европы «О защите личности в связи с автоматической обработкой персональных данных» // Сборник документов Совета Европы в области защиты прав человека и борьбы с преступностью.- М.: СПАРК, 1998. С. 106 - 114.

[58] Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ // СЗ РФ от 31.07.2006. №31 (1 ч.). Ст. 3451.

[59] Федеральный закон «О внесении изменений в Федеральный закон «О персональных данных» от 25.07.2011 №261-ФЗ // СЗ РФ. 2011. №31. Ст. 4701.

Как видим, институт персональных данных достаточно прочно вошёл в законодательный оборот российской правовой системы, в связи с чем в юридической науке сформировалось множество подходов к понятию персональных данных.

Так, по мнению М.Н. Малеиной, «помимо фамилии, имени и отчества, даты рождения, адреса места жительства, под персональными данными следует понимать, в том числе, сведения о выбираемых читателем книгах, которые собираются в базе библиотеки, использующей электронную форму заказа и читательские билеты со штрих-кодом. Биометрические персональные данные (сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность) включают отпечатки пальцев, результаты анализа ДНК, сетчатку глаза, атавизмы, различные отклонения в развитии и др.»[60].

Некоторые авторы определяют персональные данные как «сведения о фактах, событиях и обстоятельствах частной жизни физического лица, позволяющих его идентифицировать»[61]. Такое мнение основано на том, что не только личные сведения входят в понятие «персональные данные», но и информация о фактах, обстоятельствах, событиях, которые позволяют идентифицировать физическое лицо. Различные события, безусловно, играют большую роль в жизни любого человека, поскольку могут повлиять на его статус, положение, права, обязанности (если речь идет о юридических фактах).

В то же время, события являются, на наш взгляд, не информацией о гражданине, а, скорее, причиной, определяющей возникновение такой информации. Именно поэтому не совсем корректно указывать события как системообразующий признак информации о гражданине. Вероятно, в силу специфики данного института, представляется возможным говорить именно

---

[60] Малеина М.Н. Право на тайну и неприкосновенность персональных данных / М.Н. Малеина // Журнал российского права. 2010. №11 // СПС «Гарант».

[61] Липатов А. Защита персональных данных / А. Липатов // Финансовая газета. Региональный выпуск. – 2009. - №36 // СПС «КонсультантПлюс».

о сведениях и событиях, а не о юридических фактах, которые влекут данные события, поскольку не вся информация, позволяющая идентифицировать физическое лицо, влечёт за собой определенный юридический факт. Между тем, информация о таком событии может представлять достаточную ценность для достижения тем или иным субъектом конкретной цели.

В.Б. Наумов полагает, что «веб-адрес, сведения об установленном программном обеспечении и режиме работы компьютера идентифицируют информационные технологии, а не пользователя, поэтому не относятся к персональным данным. Однако существует вероятность возникновения ситуации, «когда отдельные элементы массивов данных не позволяют идентифицировать пользователя, а вся совокупность обработанных данных дает такую возможность» [62] . Если исходить из формально-логического анализа законодательных норм о персональных данных, то можно прийти к выводу, что под ними понимается только та информация, на основе которой можно идентифицировать личность гражданина, к которому относятся сведения о фактах, признаваемые персональными данными. Следовательно, с данным мнением можно согласиться в той части, что обезличенное представление об установленном программном обеспечении на компьютерном носителе, а также адрес ещё не в полной мере могут позволить идентифицировать личность гражданина, которому всё это принадлежит. А потому действительно вызывает сомнение отнесение данных сведений к персональным данным.

Согласно другой позиции, персональные данные представляют собой информацию (зафиксированную на любом носителе) о конкретном человеке, которая отождествляется или может быть отождествлена с ним[63].

Е.Ю. Покаместова, напрямую не определяя термин «персональные данные», пишет, что «под защитой конфиденциальности персональных данных необходимо понимать особый правовой режим обработки

[62] Наумов В.Б. Право и Интернет: очерки теории и практики. М., 2002. С. 132.
[63] Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право. СПб: Юридический центр Пресс, 2005. С. 244.

информации, относящейся к определённому или определяемому на основе такой информации физическому лицу, включающей сведения о фактах его биографии, нормативных (назывных) данных, национальности, месте жительства, заболеваниях, семейной жизни, привычках, увлечениях, нравственных, политических, сексуальных, религиозных пристрастиях, а также иные сведения, отражающие особенности последнего по отношению к другим людям (обществу)»[64].

Как видим, несмотря на существование достаточно точного по смыслу законодательного определения персональных данных, в доктрине единства мнений по поводу содержания данного понятия не сложилось. Представляется, что справедливые положения присутствуют в каждом из вышеприведённых определений. Именно поэтому при формулировании собственного определения понятия персональных данных мы будем исходить из сущностных признаков, которые содержатся во всех вышеперечисленных подходах.

Итак, не вызывает сомнений тот факт, что персональные данные являются разновидностью **информации**, поскольку представляют собой определённый набор сведений, позволяющий получить осведомлённость о физическом лице. Персональные данные более чем соответствуют признакам информации, так как уменьшают степень неопределенности о конкретном человеке.

Применительно к персональным данным также необходимо выделять признак **относимости** к тому или иному субъекту. В данном случае субъектом всегда должно выступать только физическое лицо. Сложно говорить о персональных данных иных субъектов правоотношений, а именно юридических лиц и публично-правовых образований.

---

[64] Покаместова Е.Ю. К вопросу о персональных данных и их классификации в отечественной правовой системе // Проблемы современной семьи: нравственно-психологические, правовые, социально-экономические аспекты: сборник статей третьей межвузовской научно-практической конференции. Воронеж: МОУ ВЭПИ, 2006. С. 71-76.

В соответствии с положениями главы 76 Гражданского кодекса РФ каждое юридическое лицо имеет средства индивидуализации [65]. Такие средства необходимы для идентификации юридического лица, отграничивающего его от иных субъектов в целях поддержания устойчивости гражданского оборота. Однако невозможно говорить о средствах индивидуализации юридического лица как о его персональных данных. Объяснить это можно тем, что персональные данные тесно связаны с личностью человека. Кроме того, средства индивидуализации необходимы юридическому лицу для осуществления деятельности в рамках только гражданского оборота. Персональные данные применимы в более широком круге общественных отношений, в том числе правоотношений.

Трудно говорить и о наличии персональных данных у публично-правовых образований – они представляют собой публичные, более сильные в правовом поле субъекты, впрочем, как и юридические лица. Гражданин, будучи субъектом, например, административных правоотношений, признаётся подчиняющимся субъектом и является менее защищённым от властных предписаний публичных органов и публично-правовых образований. Исходя из этого, можно сделать вывод, что наименования, идентифицирующие юридические лица и публично-правовые образования, не требуют особой правовой защиты, как того требуют персональные данные гражданина.

В то же время, на наш взгляд, персональные данные физического лица и средства индивидуализации юридических лиц и публично-правовых образований являются весьма схожими по своему содержанию. Так, к средствам индивидуализации юридических лиц в соответствии со ст. 1225 Гражданского кодекса РФ принято относить: фирменное наименование, коммерческое обозначение, товарный знак, знак обслуживания, наименование происхождения товара.

---

[65] Гражданский кодекс Российской Федерации. Часть I // СЗ РФ от 25.12.2006. №52 (1 ч.). Ст. 5496.

Как указывается в научной литературе, «средства индивидуализации юридического лица представляют собой различные способы, позволяющие выделить одно юридическое лицо из множества других»[66]. Действительно, средства индивидуализации являются способом выделения, обособления юридического лица от множества других организаций. Именно средства индивидуализации позволяют идентифицировать юридическое лицо в гражданском обороте.

Более того, Р.И. Бодров полагает, что «категория «средства индивидуализации» распространяет своё действие не только в отношении юридических лиц, но и граждан (физических лиц). При этом, указывается, что гражданско-правовые термины «средства индивидуализации» и «персональные данные» соотносятся между собой как целое и часть, поскольку любые персональные данные официально квалифицируются как информация о физическом лице»[67].

Полагаем, что с подобной позицией следует согласиться. Однако представляется, что общим началом, объединяющим средства индивидуализации юридических лиц и персональных данных является идентификация субъекта правоотношений – физического или юридического лица. Именно идентификация субъекта правоотношений, в конечном итоге, и является причиной существования средств индивидуализации и персональных данных: на основе средств индивидуализации можно выделить юридическое лицо, а на основе персональных данных – идентифицировать гражданина (физическое лицо).

Таким образом, предлагается определить «персональные данные» как разновидность «идентификационных данных», в которые помимо вышеуказанных также включаются «средства индивидуализации юридических лиц».

---

[66] Попова С.И. Средства индивидуализации юридических лиц: вопросы теории и практики // Научный журнал КубГАУ. 2015. №113(09). С. 29.

[67] Бодров Р.И. Гражданско-правовые средства индивидуализации граждан (физических лиц): вопросы теории и практики: Автореферат дисс. … канд. юрид. наук. М., 2016. С. 9.

Бесспорным, на наш взгляд, также является и признак **конфиденциальности** персональных данных, поскольку это вид информации, который не подлежит всеобщему разглашению ввиду возможности распространения сведений о частной жизни лица. Как пишет М.В. Бундин, в соответствии со ст. 3 Федерального закона «О персональных данных» конфиденциальность персональных данных заключается в их нераспространении или недопущении действий, направленных на передачу и ознакомление с персональными данными третьими лицами, их опубликование, размещение в открытом доступе[68].

В то же время, вопрос о содержании конфиденциальности персональных данных не является однозначным. В частности, если законодательно конфиденциальность рассматривается как обязательное требование не допускать распространения персональных данных, то в литературе эта позиция критикуется. В частности, Н.И. Петрыкина указывает, что «конфиденциальность является свойством персональных данных, признаком, переданным им заинтересованными лицами. Обязательство же лица о неразглашении этой информации является следствием этого ее свойства. Персональные данные не становятся конфиденциальными в процессе их оборота, они являются таковыми изначально по своей правовой природе»[69].

На наш взгляд, данная позиция не всегда является справедливой. Персональные данные могут входить в число сведений, на которые распространяется конфиденциальность или, проще говоря, условие о сохранении их в тайне, а также обязательство о нераспространении без согласия лица. Но, в то же время, это зависит от конкретного вида правоотношения, а также объёма персональных данных, которые необходимо запросить. Например, в соответствии с ч. 8 ст. 14 Федерального закона «О

---

[68] Бундин М.В. Персональные данные как информация ограниченного доступа по российскому законодательству // Реклама и право. 2009. №1.

[69] Петрыкина Н.И. Правовое регулирование оборота персональных данных в России и странах ЕС (сравнительно-правовое исследование): Дисс. … канд. юрид. наук. М., 2007. С. 44.

персональных данных» право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе, если обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка; обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными, и т.д.[70].

Безусловно, из любого субъективного права физического лица существуют исключения, обусловленные взаимным сосуществованием людей в социуме и, с правовой позиции, граждан в государстве. Неудивительно, что государство должно заботиться о существовании самого себя как системы, и любые правовые нормы рассматриваются, в первую очередь, как гаранты его укрепления. Таким же образом законодатель действует и в случае с конфиденциальностью персональных данных: согласно ч. 2 ст. 1 Федерального закона №152-ФЗ его действие не распространяется на отношения, возникающие при обработке персональных данных для личных и семейных нужд, для организации хранения, комплектования, учёта и использования содержащих персональные данные документов Архивного фонда РФ и иных архивных документов в соответствии с законодательством РФ об архивном деле; при обработке персональных данных, отнесённых к сведениям, составляющим

[70] Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ // СЗ РФ. 2006. №31 (ч. I). Ст. 3451.

государственную тайну; при предоставлении уполномоченными на то органами информации о деятельности судов. Иными словами, если таковое необходимо для функционирования государства, положения Федерального закона «О персональных данных» не применяются. То же самое подтверждается ч. 2 ст. 10 вышеуказанного закона, в которой перечислены те случаи, когда допускается обработка специальной категории персональных данных, запрещённая по общему правилу. Это данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни. Такая информация может стать объектом обработки в связи с реализацией международных договоров, в соответствии с трудовым законодательством и законодательством о государственной социальной помощи, об обязательных видах страхования и т.д. Таким образом, можно заметить, что конфиденциальность персональных допускается в том случае, когда это не является препятствием для функционирования государственных структур и общества в целом.

Именно поэтому предусмотренные исключения из общего правила о том, что персональные данные в целях обеспечения их конфиденциальности могут обрабатываться только с согласия их субъекта, говорят, скорее о конфиденциальности персональных данных как об их признаке, а не как о свойстве, изначально присущем данному виду информации.

Говоря о признаках персональных данных гражданина, следует заметить, что такая информация должна составлять **сведения о частной жизни**. Личность сегодня охраняется государством всесторонне. Следовательно, если охраняется частная жизнь, в качестве ее элементов должны рассматриваться сведения о частной жизни. В этой связи некоторые авторы выделяют такой признак персональных данных, как отнесение их к **личной информации.**

Как указывает Э.А. Цадыкова, «право на неприкосновенность частной жизни означает неприкосновенность личной информации» [71]. С таким мнением, на наш взгляд, следует согласиться. Любые персональные данные являются сведениями о конкретном человеке. Но не любые сведения о человеке могут помочь его идентифицировать. В частности, существование персональных данных, по большей части, направлено на идентификацию соответствующего субъекта, который выступает в качестве участника множества правоотношений. В то же время, существует большой объём информации, который хотя и относится к идентифицируемому субъекта, но с целью его идентификации может быть никак не связан, а для различных правоотношений может вообще не иметь никакого значения. Так, информация о личной жизни субъекта, его увлечениях может быть и не связана с персональными данными, а является личной информацией, которая может никаким образом не влиять на правовой статус субъекта.

В отношении персональных данных можно выделить другой существенный признак, который красной нитью прослеживается и из положений закона, и из вышеперечисленных подходов к определению персональных данных. Этот признак заключается в **идентифицируемости** человека на основе персональных данных. Установлением содержания данного признака является наиболее проблемным, поскольку единства подходов по этому поводу не существует.

Как пишет А.С. Маркевич, «основная смысловая нагрузка при квалификации информации как персональных данных сводится исключительно к вопросу об идентификации. Информация, по сути, представляет собой установление идентичности (тождества, равнозначности), однако человек не может быть полностью «равен своим персональным данным». Более того, сам человек не может быть

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

идентифицирован только с помощью собственных персональных данных, поскольку он не идентичен ничему, кроме самого себя»[72].

Представляется, что процесс идентификации всегда направлен на установление личности – субъекта персональных данных. Причём способы такой идентификации могут быть весьма разнообразными. В криминалистической теории идентификации указывается, что «идентифицировать объект» - означает установить его тождественность самому себе. При этом «суть процесса идентификации заключается в отождествлении объекта путём взаимного сопоставления объекта и его отображения» [73] . Если исходить из того, что персональные данные представляют собой не что иное, как отражение человека с позиций теории идентификации, то указанная выше позиция А.С. Маркевича не кажется нам верной, поскольку человек становится идентифицируемым субъектом на основе персональных данных. И это вовсе не означает, что человек полностью становится равным своим персональным данным. Персональные данные, в таком случае, выступают всего лишь средством идентификации, а не самой идентификацией. Исходя из этого, мы полагаем, что законодательно установленный признак **идентифицируемости** является неотъемлемым и содержательным для понятия персональных данных.

В правоприменительной практике в последние годы возникает множество проблем, связанных с отнесением к персональным данным на основе признака **идентифицируемости** той или иной информации, которая, с одной стороны, могла бы подпадать под понятие «персональные данные» и подлежать соответствующей правовой охране, но с другой – не квалифицируется правоприменителями как таковая.

Количество обрабатываемых в различных информационных системах персональных данных с каждым годом возрастает. Однако это порождает

---

[72] Маркевич А.С. Организационно-правовая защита персональных данных в служебных и трудовых отношениях. Автореферат дисс. … канд. юрид. наук. Воронеж, 2007.

[73] Волохова О.В., Егоров Н.Н., Жижина М.В. и др. Криминалистика: учебник (под. ред. Е.П. Ищенко). М.: "Проспект", 2011.

проблему соблюдения права на неприкосновенность частной жизни, что напрямую связано с достаточностью персональных данных для идентификации. Например, для оказания государственной услуги по выдаче гражданину выписки из Единого государственного реестра недвижимости оператору совершенно не нужно знать социальное происхождение гражданина, его имущественное положение. Следовательно, объём персональных данных, необходимых для оказания государственной услуги, должен быть ограниченным целью оказания услуги.

Необходимость минимизации состава обрабатываемых государством персональных данных подчёркивается и со стороны органов государственной власти РФ. В частности, Президентом РФ поручено Председателю Правительства РФ обеспечить внесение изменений в федеральные законы, предусматривающие минимизацию состава обрабатываемых персональных данных, необходимых для решения возлагаемых на государственные информационные системы задач[74].

В исследованиях российских юристов на сегодняшний день сформулирована проблема отнесения к персональным данным паспортных данных, а именно серии и номера, в том числе и всех сведений, которые содержатся в паспорте – фамилия, имя и отчество, дата рождения, место рождения, личная подпись, личный код. И проблема даже заключается не в том, что у авторов вызывает сомнение отнесение данных сведений к персональным, а в том, что на их основании невозможно идентифицировать личность, следовательно, они не могут охватываться режимом конфиденциальности и, тем более, тайны.

Если проанализировать Федеральный закон «О гражданстве Российской Федерации»[75], а также Постановление Правительства Российской Федерации «Об утверждении Положения «О паспорте гражданина

[74] Путин поручил Медведеву принять меры для защиты персональных данных россиян [Электронный ресурс]: https://news.mail.ru/politics/29583624/?frommail=1
[75] Федеральный закон «О гражданстве Российской Федерации» от 21.05.2002 №62-ФЗ // СЗ РФ. 2002. №22. Ст. 2031.

Российской Федерации, образца бланка и описания паспорта гражданина Российской Федерации»[76], то можно прийти к выводу, что паспорт является документом, удостоверяющим личность гражданина Российской Федерации на территории Российской Федерации. При этом личность может быть также удостоверена на основании иного документа, содержащего указание на гражданство Российской Федерации. Соответственно, паспорт позволяет идентифицировать личность гражданина Российской Федерации, поскольку он содержит персональные данные.

В литературе и правоприменительной практике существует две противоположные позиции по данному вопросу, использование каждой из которых может серьёзно и существенно влиять на реализацию права гражданина на неприкосновенность частной жизни.

Согласно первой позиции, сведения, указанные в паспорте, независимо от их вида, признаются персональными данными, должны подлежать правовой охране в виде установления режима конфиденциальности в отношении них[77].

Согласно второй позиции, выработанной в правоприменительной практике, паспортные данные (серия и номер паспорта) не являются вообще персональными данными, поскольку не позволяют идентифицировать личность гражданина – владельца паспорта, следовательно, обеспечение режима их конфиденциальности нецелесообразно, как и возможность их правовой защиты от незаконных посягательств.

Так, Постановлением Тринадцатого Арбитражного апелляционного суда от 21.06.2010 года по делу №А56-4788/2010 оставлено без изменения решение Арбитражного суда г. Санкт-Петербурга и Ленинградской области, которым было удовлетворено заявление ОАО «Т*» к Управлению Федеральной службы по надзору в сфере связи, информационных технологий

---

[76] Постановление Правительства РФ от 8 июля 1997 г. N 828 "Об утверждении Положения о паспорте гражданина Российской Федерации, образца бланка и описания паспорта гражданина Российской Федерации" // СЗ РФ. 1997. №28. Ст. 3444.

[77] Ещё раз о персональных данных [Электронный ресурс]: http://old.svobodainfo.org/ru/node/557

и массовых коммуникаций по г. Санкт-Петербургу и Ленинградской области о признании недействительным предписания. Существо спора заключалось в том, что Управлением Роскомнадзора в отношении ОАО «Т*» было вынесено предписание, в соответствии с которым уполномоченный орган установил со стороны поднадзорного субъекта нарушения Федерального закона «О персональных данных» и Постановления Правительства РФ от 15.09.2008 №687. Нарушения заключались в том, что ОАО при осуществлении деятельности по перевозке пассажиров осуществляет обработку персональных данных пассажиров, пользующихся льготными проездными билетами. Следовательно, в соответствии с частью 1 статьи 22 Закона №152-ФЗ Общество обязано направлять в уполномоченный орган по защите прав субъектов персональных данных уведомление об обработке таких данных. Однако такая обязанность не исполнялась.

Рассматривая дело по существу, суд апелляционной инстанции пришёл к выводу, что в соответствии с пунктом 3 данного описания нумерация бланка паспорта состоит из 3 групп цифр. Первые 2 группы, состоящие из 4 цифр, обозначают серию бланка паспорта, третья группа, состоящая из 6 цифр, обозначает номер бланка паспорта.

Таким образом, серия и номер паспорта относятся не к личности гражданина, а к бланку документа, удостоверяющего его личность[78].

Аналогичную позицию выразила судебная коллегия по гражданским делам Московского городского суда по делу №33-6709 по иску Р. К Высшему Арбитражному Суду Российской Федерации и Арбитражному суду города Москвы об обязании изъять паспортные данные заявителя из определений, размещённых Арбитражным судом города Москвы, Высшим Арбитражным Судом Российской Федерации на официальных сайтах www.msk.arbit.ru и kad.arbitr.ru. В обоснование своей позиции суд кассационной инстанции указал: «В обжалуемом судебном решении суд первой инстанции правильно указал, что паспортные данные не отнесены

[78] Картотека арбитражных дел [Электронный ресурс]: http://kad.arbitr.ru

Законом №152-ФЗ к персональным данным. Как следует из п. 4 Положения о паспорте гражданина Российской Федерации в паспорт вносятся следующие сведения о личности гражданина: фамилия, имя, отчество, пол, дата рождения и место рождения. В соответствии с п. 3 данного положения бланк паспорта имеет нумерацию, которая состоит из трёх групп цифр и означает серию бланка паспорта и номер бланка паспорта. Разрешая заявленные требования, суд первой инстанции верно исходил из того, что серия и номер паспорта относятся не к личности гражданина, а к бланку документа, удостоверяющего его личность, и пришёл к выводу о том, что перечисленная информация не может быть отнесена к персональным данным в соответствии с требованиями ФЗ «О персональных данных», а поэтому размещённые в сети Интернет Арбитражным судом города Москвы судебные определения от 10.08.2011 года не содержат сведений о персональных данных Р., опубликование которых запрещено действующим законодательством, и не влечёт нарушение его прав»[79].

Совершенно неожиданная позиция по изучаемой проблеме встретилась нам в практике следственных органов. Так, старшим следователем Следственного отдела по Чкаловскому району г. Екатеринбурга СУ СК РФ по Свердловской области 11.02.2013 было вынесено постановление об отказе в возбуждении уголовного дела по сообщению о совершении преступления, предусмотренного ч. 1 ст. 137 УК РФ по факту разглашения Ф. персональных данных Д. и Т. на основании п. 1 ч. 1 ст. 24 УПК РФ за отсутствием в действиях Ф. состава преступления.

По материалам доследственной проверки в порядке ст. 144 УПК РФ следователем было установлено, что Ф., ранее знакомый Д., осуществив выход в сеть «Интернет», опубликовал на своей странице микроблога в социальной сети «Твиттер» отсканированное изображение её заграничного паспорта гражданина РФ, на котором разборчиво видны серия, номер, дата и

[79] Определение Московского городского суда от 29.02.2012 по делу №33-6709 [Электронный ресурс]: Доступ из справ.-правовой системы «КонсультантПлюс».

место рождения, а также дата выдачи заграничного паспорта с доступом для широкого круга лиц, тем самым, разгласив её персональные данные. В этот же день Ф., осуществив выход в сеть «Интернет», подобным образом разместил также на том же ресурсе отсканированное изображение заграничного паспорта гражданина РФ Т., которое содержало те же самые сведения, что и в случае с Д.

В мотивировочной части Постановления об отказе в возбуждении уголовного дела следователем указано следующее. Статья 137 УК РФ предусматривает ответственность за деяние, выражающееся в незаконном собирании и распространении сведений о частной жизни лица, которые составляют его личную или семейную тайну, без его согласия. К сведениям, образующим личную и семейную тайну лица, относятся субъективно относимые человеком к скрытым от посторонних лиц данные, затрагивающие индивида и его связей в обществе, ранее не разглашавшиеся на публике, а именно сведения, не имеющие общественного значения, а являющиеся доступными исключительно принадлежащему лицу, которые носят как порочный, так и непорочный характер. Таким образом, **к сведениям, составляющим личную и семейную тайну не относятся фамилия, имя, отчество, дата и место рождения, а также паспортные данные**, так как данные сведения являются доступными для широкого круга лиц и значимыми для осуществления лицом своих функций в обществе и не являются доступными исключительно принадлежащему лицу, а используются в повседневной жизни. Своими действиями Ф. не выполнил объективной стороны состава преступления, предусмотренного ч. 1 ст. 137 УК РФ, а именно не собирал и не разглашал сведений, составляющих личную или семейную тайну Д. и Т[80].

В практике существует и позиция, прямо противоположная вышеприведённым и трактующая закон совершенно иным образом. Так,

[80] Данные паспортов Дикушиной и Токарского не являются персональными данными [Электронный ресурс]: http://blog.pravo.ru/blog/6827.html

Определением судебной коллегии по гражданским делам Московского городского суда от 20.06.2011 года по делу №33-16822 оставлено без изменения решение Измайловского районного суда г. Москвы по иску П. к ООО «Лабораторное оборудование» от 18.02.2011 об обязании ответчика удалить с сайта в сети «Интернет» не соответствующие действительности и порочащие его честь, достоинство и деловую репутацию сведения, а также персональные данные, а именно: паспортные данные, адрес места жительства, номера телефонов.

Судом первой инстанции было установлено, что 20.07.2010 года на сайте в сети «Интернет» ООО «Лабораторное оборудование» была размещена информация о том, что П. оказался организатором одного из незаконных «бизнесов», им была организована фирма-однодневка ООО «ТД Лабтех», в результате оперативно-розыскной деятельности, проведённой ОБЭП Восточного округа г. Москвы, незаконная деятельность П. была прекращена, получены все необходимые улики, ведётся следствие. Также были опубликованы данные о месте жительства П. и его **паспортные данные**. Суд, установив факт распространения ответчиком в нарушение требований ст.ст. 3 и 7 Федерального закона «О персональных данных» персональных данных истца: паспортных данных, адреса места жительства, номеров телефонов, - без его согласия, правильно признал, что **нарушение права истца на личную тайну подлежит защите** в соответствии со ст. 150 Гражданского кодекса РФ[81].

В другом, более позднем судебном акте – Определении Верховного Суда РФ от 12.09.2012 №56-АПГ12-13 – суд всё же относит паспортные данные к персональным данным. Так, прокурор Приморского края обратился в суд с заявлением о признании недействующими пунктов 2, 3, 4 постановления Законодательного Собрания Приморского края №79 «О представлении депутатами Законодательного Собрания Приморского края сведений о доходах, об имуществе и обязательствах имущественного

[81] Определение Московского городского суда от 20.06.2011 по делу №33-16822 // СПС «КонсультантПлюс».

характера» в части включения в форму справок о доходах, имуществе и обязательствах имущественного характера депутата Законодательного Собрания Приморского края, супруги (супруга) и несовершеннолетних детей депутата указания адреса места регистрации, документа, удостоверяющего личность (вид документа, серия, номер, кем и когда выдан), номеров домашнего и мобильного телефонов названных лиц, ссылаясь на их противоречие статьям 12.1, 12.5 Федерального закона «О противодействии коррупции» и Федерального закона «О персональных данных». Отменяя решение суда первой инстанции, которым постановлено в удовлетворении заявления прокурора Приморского края отказать, Верховный Суд РФ исходил из следующего. В оспариваемом нормативном правовом акте субъекта РФ в число сведений, представляемых депутатами и членами их семей, о доходах, имуществе и обязательствах имущественного характера включены: адреса места регистрации, документ, удостоверяющий личность (вид документа, серия и номер, кем и когда выдан), номеров домашнего и мобильного телефонов, что не соответствует федеральному законодательству. Обязанность предоставлять сведения о доходах, имуществе и обязательствах имущественного характера действительно предусматривается в отношении указанных лиц Федеральным законом «О противодействии коррупции». Но, в то же время, регламентация порядка предоставления указанных сведений направлена на урегулирование порядка реализации антикоррупционных мер и достижение целей противодействия коррупции, установления правовых и организационных основ предупреждения коррупции и борьбы с ней. Оспариваемый нормативный правовой акт включил в правовое регулирование дополнительные (по сравнению с федеральным регулированием) положения, обязывающие депутатов и членов их семей представлять иные сведения, которые не относятся к числу сведений о доходах, имуществе и обязательствах имущественного характера, а относятся к категории **персональных данных,**

представление которых регламентировано Федеральным законом «О персональных данных»[82].

Разобщённость представленных позиций говорит о том, что данная проблема должна быть решена и не только в правоприменительной практике и на законодательном уровне, в правовой теории. Безусловно, рациональная логика присутствует в каждой из представленных позиций. Однако охрана прав граждан не должна предполагать альтернатив в вынесении юридически значимых решений, которые могут повлиять существенным образом на реализацию гражданами своих прав на конфиденциальность персональных данных.

С одной стороны, законодательство Российской Федерации не содержит норм, закрепляющих правила, на основании которых устанавливается достаточность данных, позволяющих идентифицировать личность. Поэтому логика правоприменителей, не признающих паспортные данные персональными данными, нам вполне понятна.

Достаточность персональных данных для идентификации гражданина сугубо индивидуальна для каждого вида правоотношений, в которых реализация субъективных прав гражданина связана с идентификацией его личности. Например, высшее учебное заведение, принимая абитуриента на программу высшего образования по направлению магистратуры, должно истребовать у соискателя персональные данные, подтверждающие наличие у него высшего образования, поскольку это влияет на возможность гражданина претендовать вообще на поступление в магистратуру. Кроме того, ч. 3 ст. 69 Федерального закона «Об образовании в Российской Федерации» напрямую указывает, что к освоению программы магистратуры допускаются лица, имеющие высшее образование любого уровня[83]. Таким образом, достаточный объём персональных данных в данном случае будет отличаться от минимального.

---

[82] Определение Верховного Суда РФ от 12.09.2012 №56-АПГ12-13 // СПС «КонсультантПлюс».
[83] Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 №273-ФЗ // СЗ РФ. 2012. №53 (ч. I). Ст. 7598.

К аналогичному выводу можно прийти при анализе правоотношений в сфере здравоохранения. Для целей правильного и квалифицированного оказания медицинской помощи лечащий врач должен обладать персональными данными о пациенте, которые раскрывают его хронические заболевания, либо те, которые он уже перенёс и был от них излечён. При недостаточности данных сведений гарантия качественного оказания врачебной помощи полностью отсутствует.

С другой стороны, некоторые правоприменительные органы признают, что серия и номер паспорта в совокупности с фамилией, именем и отчеством, а также датой и местом рождения, датой выдачи паспорта являются достаточной информацией, позволяющей идентифицировать личность владельца паспорта, например, для целей, связанных с его налогообложением[84].

Кроме того, каждый субъект персональных данных имеет свои фамилию, имя и отчество, дату и место рождения, адрес места жительства – минимальный объём персональных данных, позволяющий его идентифицировать в большинстве правоотношений. Государство, подтверждая устойчивую правовую связь с данным субъектом в виде признания гражданства, выдаёт ему паспорт (документ, удостоверяющий его личность) и присваивает ему индивидуальную серию и номер. Наличие у гражданина бланка паспорта с соответствующими серией и номером позволяет сделать однозначный вывод о принадлежности гражданина к гражданству Российской Федерации, вследствие чего серия и номер паспорта в совокупности со всеми остальными персональными данными всё же позволяют идентифицировать личность гражданина. **Таким образом, полагаем, что паспортные данные всё же должны относиться к персональным данным и подлежать правовой охране.**

---

[84] Федеральная налоговая служба [Электронный ресурс]: http://service.nalog.ru:8080/innmy.do;jsessionid=7CEA800DA5F22435CEBE010D1EB36E21

Помимо этого, анализ некоторых правоприменительных актов позволяет сделать вывод, что должностные лица различных правоохранительных органов, как и суды, вынося различные виды юридически значимых решений, не всегда правильно уясняют содержание признаков конфиденциальности и идентифицируемости в отношении конкретных видов персональных данных, что приводят к ошибкам при квалификации действий соответствующих субъектов.

Так, решением Енисейского районного суда Красноярского края в удовлетворении исковых требований К. о признании увольнения незаконным, восстановлении на службе в органах внутренних дел, взыскании денежного довольствия за время вынужденного прогула и компенсации морального вреда отказано. Судом установлено, что К. являлся сотрудником органом внутренних дел, а именно государственным инспектором безопасности дорожного движения. Находясь на службе в органах внутренних дел, К. создал в социальной сети «Вконтакте» сообщество под названием «Е* Criminal». В ходе изучения записей в указанном сообществе было установлено, что администратор данной группы размещал на странице данные о расстановке наружных нарядов сотрудников дорожно-патрульной службы с указанием персональных данных сотрудников, информацию о возбуждённых уголовных делах, происшествиях на территории района, а также различную информацию и комментарии к ней, наносящие ущерб имиджу органов внутренних дел. Как указано в судебном решении, в ходе изучение новостной ленты сообщества выявлены многочисленные нарушения Федерального закона «О персональных данных». В частности, администратором группы размещалась информация о заступлении на службу нарядов ГИБДД с указанием фамилий сотрудников, информация из суточных сводок о происшествиях, имевших место на территории района и о возбуждённых уголовных делах.

При этом на довод истца о том, что имена и фамилии сотрудников ГИБДД, размещённые в сообществе, не могут быть признаны охраняемыми

законом персональными данными, суд в мотивировочной части решения указал следующие доводы: «К персональным данным лица следует относить, прежде всего, его фамилию, имя, отчество, год, месяц, дату и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессию, доходы, а также иную информацию, при которой возможно идентифицировать конкретное лицо. Администратором исследуемой группы размещена информация о совершённом ДТП с указанием фамилий и инициалов его участников, года рождения одного из участников, марки и государственного номера транспортного средства, принадлежащего одному из участников ДТП. Данная информация размещалась в группе несколько раз, что представлено в материалы дела в виде соответствующих скриншотов веб-страниц. Таким образом, факт размещения К. персональных данных участников ДТП и сотрудников органов внутренних дел нашёл своё подтверждение в ходе рассмотрения дела»[85].

Представляется, что в рассматриваемом случае судом не в полной мере дана оценка тому, являются ли разглашённые истцом персональные данные охраняемыми и подпадающими под соответствующий режим конфиденциальности. Исходя из этого, на наш взгляд, вывод суда о том, что истцом был нарушен Федеральный закон «О персональных данных», был сделан преждевременно. В частности, суду логичнее было бы в обоснование своей позиции провести анализ действующих нормативных правовых актов в отношении персональных данных сотрудников полиции, из чего можно было прийти к прямо противоположным выводам. Так, п. 9 ч. 1 ст. 28 Федерального закона «О полиции»[86] устанавливает, что сотрудник полиции имеет право на защиту своих персональных данных. В соответствии с с п. 6

[85] Решение Енисейского районного суда Красноярского края от 24.01.2017 по делу №2-39/2017 [Электронный ресурс]: https://eniseysk--krk.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=283598798&delo_id=1540005&new=0&text_number=1

[86] Федеральный закон «О полиции» от 07.02.2011 №3-ФЗ // СЗ РФ. 2011. №7. Ст. 900.

ч. 2 ст. 39 Федерального закона «О службе в органах внутренних дел»[87] передача персональных данных сотрудника третьей стороне не допускается без согласия сотрудника, выраженного в письменной форме, за исключением случаев, установленных федеральными законами. Однако если обратиться к п. 1 ч. 4 ст. 5 Федерального закона «О полиции», то согласно данной норме при обращении к гражданину сотрудник полиции обязан назвать свои должность, звание, фамилию, предъявить по требованию гражданина служебное удостоверение, после чего сообщить причину и цель обращения. Таким образом, применительно к анализируемой ситуации персональные данные сотрудников ГИБДД, которые были размещены в сообществе в социальной сети, вряд ли можно назвать подпадающими под режим конфиденциальности и соответствующих правовых ограничений.

В отношении иной группы персональных данных, разглашение которых вменялось истцу, являвшемуся сотрудником органов внутренних дел, а именно персональных данных участников ДТП, можно сделать вывод, что неправомерность такого разглашения была установлена вполне достоверно. Так, норма ч. 6 ст. 5 Федерального закона «О полиции» закрепляет, что полученные в результате деятельности полиции сведения о частной жизни гражданина не могут предоставляться кому бы то ни было без добровольного согласия гражданина, за исключением случаев, предусмотренных федеральным законом. Таким образом, по общему правилу, сведения о ДТП, которые так или иначе затрагивают частные интересы участников ДТП, без их личного согласия либо конклюдентных действий не могут свободно разглашаться через социальные сети.

Однако, как видим, в вышеприведённом судебном акте суд не провёл достаточного правового анализа соответствующих норм, ограничившись лишь указанием на то, что персональные данные не могут быть разглашены

[87] Федеральный закон «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» от 30.11.2011 №342-ФЗ // СЗ РФ. 2011. №49 (ч. I). Ст. 7020.

третьими лицами без согласия субъектов персональных данных, хотя существует множество нормативных исключений из данного правила.

Таким образом, отсутствие единообразия в толковании и применении законодательных норм может приводить к неопределённости в правоприменении, что неблагоприятно в последующем сказывается на реализации прав и свобод человека и гражданина, хотя в идеалах правового государства, каким позиционируется в Конституции 1993 года Российская Федерация, такого быть не должно. Именно это и обусловливает формирование единого подхода к пониманию института персональных данных в российском законодательстве.

Итак, мы пришли к выводу, что персональные данные представляют собой такую информацию, в отношении которой установлен запрет на её свободный оборот в информационном пространстве, за исключением случаев, специально предусмотренных законом [88] . Указанный запрет подкрепляется, в свою очередь, наличием в законодательстве норм, предусматривающих меры ответственности за нарушение конфиденциальности персональных данных[89].

Как указывает Р.В. Амелин, «если доступ к информации получает неуполномоченное лицо, происходит утрата конфиденциальности»[90]. В то же время, не все персональные данные имеют ограниченный оборот. Если речь идёт об общедоступных персональных данных, признаки которых установлены ст. 8 Федерального закона «О персональных данных», то на них режим конфиденциальности или ограниченность оборота не распространяется.

Сущностные признаки персональных данных как вида информации, позволяющей идентифицировать личность человека, влияют на их понимание субъектами правоприменения, именно поэтому они должны быть

---

[88] Например, если имела место обработка общедоступных персональных данных или с соблюдением требований к обезличиванию.

[89] См., например, ст. 13.11, ст. 13.14 Кодекса РФ «Об административных правонарушениях».

[90] Амелин Р.В. О возможном решении проблемы неполноты главы 28 УК РФ // Уголовно-исполнительная система: право, экономика, управление. 2009. №5. С. 5.

учтены законодателем при формировании соответствующих норм права, а также влиять на формирование практики применения таких норм.

В ходе анализа законодательства, правовой доктрины и правоприменительной практики мы пришли к следующим выводам относительно исследуемого правового института персональных данных:

1. персональные данные – это информация, которая относится к личности человека;
2. персональные данные всегда относятся к определённому физическому лицу;
3. для персональных данных, как правило, характерен признак конфиденциальности, который зависит от вида правоотношений, а также объёма данных, в которых личность субъекта правоотношения подлежит установлению на основе его персональных данных, следовательно, это информация, в отношении оборота которой могут существовать определенные ограничения и запреты (информация ограниченного доступа);
4. это такая информация, которая составляет сведения о частной жизни или является личной информацией о физическом лице;
5. основным сущностным признаком персональных данных является идентифицируемость субъекта на основе его персональных данных.

С указанных позиций под **персональными данными** следует понимать информацию, которая позволяет идентифицировать физическое лицо и в отношении которой на основе федерального закона может устанавливаться режим её конфиденциальности.

Определив понятие персональных данных и выделив его признаки, перейдём к рассмотрению вопроса о развитии российского и зарубежного законодательства, а также общепризнанных принципов и норм международного права о персональных данных.

1.2. Развитие российского законодательства об уголовно-правовой охране персональных данных

Тенденции развития законодательства об охране персональных данных существенно влияют на содержание самой охраны изучаемого института. Правильное построение принципов охраны способствует эффективному механизму правового регулирования и обеспечения безопасности персональных данных. Именно поэтому изучение вопросов, связанных с тенденциями развития законодательства о персональных данных приобретает актуальное значение в рамках настоящего исследования.

Как указывает О.А. Пальчиковская, «исследование законодательных актов России начала IX – середины XIX вв. свидетельствует о том, что российское уголовное законодательство этого периода, защищая жизнь человека, право собственности и иные блага и интересы, не обеспечивало необходимой защиты частной жизни человека, и, как следствие, её информационного аспекта»[91]. Между тем, это вовсе не означает, что правовые нормы об охране частной жизни вовсе отсутствовали в российском законодательстве. Несмотря на весьма косвенный охват в охране частной жизни, нормы российского права различных исторических периодов развития российского государства, тем не менее, в зачаточном состоянии обеспечивали безопасность частной жизни и сведений, составляющих частную жизнь.

По нашему мнению, историю развития законодательства об охране персональных данных можно условно разделить на несколько этапов, каждый из которых характеризуется своими специфическими особенностями в правовом регулировании вопросов, связанных с охраной персональных данных. Рассмотрим каждый их этапов развития отечественного законодательства об уголовно-правовой охране персональных данных.

---

[91] Пальчиковская О.А. Уголовно-правовая охрана личной и семейной тайны: Дисс. … канд. юрид. наук. М., 2011. С. 59.

Первый этап (начало XVIII в. – первая половина XIX в.). Первые в России законодательные нормы об охране конфиденциальной информации, относящейся к личности человека, можно выделить уже в эпоху Петра I. Так, до начала XVIII века законодательством охранялась тайна исповеди, которая, что вполне логично, включала в себя сведения, составляющие личную и семейную тайну. «Неразглашение тайны исповеди гарантировалось «Духовным Регламентом о праве чина церковного и монашеского», который был составлен в 1719, а подписан Петром I в 1720 году»[92]. Как указывает Гостев И.М., «в 1722 году на основании указа Петра I Феофаном Прокоповичем было составлено Дополнение к указанному документу, в котором были определены условия и порядок разглашения тайны исповеди. Согласно этому документу, под страхом сурового наказания, от духовника требовалось доводить содержание исповеди до сведения церковного начальства в случаях, когда исповедуемый замыслил воровство, измену или же плохо отзывался о государе»[93]. Таким образом, условно можно сделать вывод, что ограничение тайны исповеди допускалось, если это было необходимо для защиты государственных интересов.

Законодательство данного периода, по существу, не закрепляло никаких прав, а утверждало только обязанности, именно поэтому устанавливалась обязанность церковных иерархов раскрывать тайну исповеди (личную и семейную тайну) в целях обеспечения безопасности государства от преступных посягательств. Для этого, по существу, абсолютномонархического периода российской государственности было вполне логичным отсутствие норм, регламентирующих права человека, понятие о которых только начинало зарождаться в трудах европейских просветителей XVIII века. Для данного периода характерно и отсутствие единого кодифицированного законодательного акта, закрепляющего нормы об уголовной ответственности за разглашение или неразглашение различных

[92] Павлов А.С. Курс церковного права. СПб.: Изд-во Лань, 2002. С. 185.
[93] См.: Гостев И.М. Защита коммерческой тайны: история и современность [Электронный ресурс]: http://old.it2b.ru/it2b3.view3.page77.html

видов тайн. Ситуация значительно изменилась с приходом к власти императора Александра II, провозгласившего курс на проведение либеральных реформ в Российской империи, что породило следующий этап в развитии законодательства.

Второй этап (с 1866 по 1917 год – дореволюционный период). В 1845 году в Российской империи было принято Уложение о наказаниях уголовных и исправительных – первый законодательный акт, который упорядочивал нормы об уголовной ответственности на территории России[94]. Оно содержало в себе достаточное количество норм об охране различных объектов и правоотношений, которые представлялись с позиций законодателя наиболее важными. Однако в первоначальном виде Уложение не содержало уголовно-правовых норм об ответственности за посягательство на сведения, которые не подлежали разглашению (по существу – за посягательство на личную и семейную тайну).

В 1866 году в Уложение были внесены изменения, в результате которых, в частности, появились нормы об охране личной тайны и об установлении уголовной ответственности за посягательство на неё. Так, в Уложении появилась статья 1039, которая предусматривала уголовную ответственность за распространение порочащих сведений о частной жизни лиц, которые составляют тайну: «Оглашение в печати о частном или должностном лице, или обществе, или установление такого обстоятельства, которое могло повредить их чести, достоинству и доброму имени»[95]. При этом следует иметь в виду, что ключевым в этой норме было распространение именно порочащих сведений, которые, впрочем, как могли соответствовать действительности, так и не могли. В противном случае, если сведения не соответствовали действительности, то можно было говорить ещё

[94] Уложение о наказаниях уголовных и исправительных 1845 г. (в ред. 1866 и 1885 гг.). Издание четырнадцатое. Издано Н.С. Таганцевым. – СПб: Американская Скоропечатня, Литейный проезд, д. 33. 1909.
[95] Там же.

и о наступлении ответственности за клевету, различные виды которой были закреплены в Уложении в первоначальной редакции от 1845 года.

Безусловно, данная норма весьма косвенно относится к современному пониманию уголовно-правовой охраны персональных данных, однако, по существу, это было первое законодательное правило, которое устанавливало, как указывает О.А. Пальчиковская, «уголовную ответственность за деяние, посягающее на сведения о частной жизни лица, составляющие тайну, в том числе личную или семейную»[96].

В дальнейшем, в Российской империи в качестве дополнения к Уложению о наказаниях уголовных и исправительных был принят Устав о наказаниях, налагаемых мировыми судьями, в котором нормы об охране конфиденциальных сведений получили значительное развитие и продолжение. Так, статья 137 Устава устанавливала уголовную ответственность за разглашение с намерением оскорбить чью-либо честь сведений, «сообщённых втайне», либо указанные сведения должны быть получены путём нарушения тайны переписки (путём вскрытия письма), либо иным «противозаконным образом». Нельзя сказать, что субъект данного преступления был специальным, но, тем не менее, законодатель установил, что ответственность за такое разглашение могло нести лицо, которому сведения были сообщены втайне в силу звания, занятия или профессии, либо иное лицо, которым указанные разглашённые сведения были узнаны незаконным способом[97].

Статья 420 Уложения предусматривала уголовную ответственность за разглашение молвы, для чьей-либо чести оскорбительной. Данное преступление могло быть совершено только специальным субъектом, и его совершение можно было вменять только лицам, совершившим его с использованием служебного положения.

---

[96] Пальчиковская О.А. Уголовно-правовая охрана личной и семейной тайны: Дисс. … канд. юрид. наук. – М., 2011. С. 61.

[97] Устав о наказаниях, налагаемых мировыми судьями [Электронный ресурс]: https://traditio.wiki/Устав_о_наказаниях,_налагаемых_мировыми_судьями

Были и иные статьи, охранявшие личную тайну и тайну переписки, например ст.ст. 1102 и 1104, по которым за разглашение сведений, которые содержались в почтовых отправлениях, к уголовной ответственности привлекались почтовые чиновники, то есть, как и в случае со ст. 420 Уложения, субъект данных преступлений был специальным.

Вопрос об отнесении последних трёх норм к охраняющим личную тайну, в то же время, на наш взгляд, является спорным. Так, А.М. Ершов полагает, что «они охраняли личную тайну и тайну переписки как виды конфиденциальной информации» [98]. По нашему мнению, не стоит так однозначно относить объект охраны данных правовых норм исключительно к личной тайне, поскольку наличие возможности привлекать к ответственности за данные преступления только должностных лиц свидетельствовало, скорее, о цели поддержания правопорядка в чиновничьей среде и склоняет к выводу, что основным охраняемым объектом данного преступления были всё же интересы государственной службы.

В 1903 году в Российской империи был принят новый кодифицированный законодательный акт уголовного права под названием «Уголовное уложение», который закрепил новые нормы об ответственности за преступления, совершаемые различными физическими лицами. Следует заметить, что в нём законодатель более тщательно подошёл к регулированию вопросов, затрагивающих ответственность за преступления с незаконным использованием личной информации. В частности, Уложение содержало главу 28 «Об оскорблении» и главу 29 «Об оглашении тайн».

Так, в ст. 531 Уголовного уложения содержалась норма об уголовной ответственности за опозорение разглашением, хотя бы в отсутствие опозоренного, обстоятельства, его позорящего [99]. Указывалось, что при опозорении должны быть оглашены обстоятельства, позорящие честь того, кого виновное лицо позорит. Кроме того, законодатель устанавливал, что как

[98] Ершов А.М. Ответственность за посягательство на конфиденциальную информацию по российскому уголовному праву: Дисс. … канд. юрид. наук. М., 2010. С. 43.
[99] Уголовное уложеніе 22 марта 1903 года / Издание Н.С. Таганцева. СПб., 1904. С. 718.

обвинение в деянии, так и разглашение обстоятельств, одинаково предполагают, что было рассказано или сообщено о событии, факте или же о ряде таких событий, то есть о чём-либо совершившемся или совершающемся [100] . Таким образом, устанавливалась уголовная ответственность за разглашение сведений, которые, по существу, носили позорящий характер для потерпевшего и представляли для него сведения, не подлежащие разглашению.

В совокупности со ст. 537 Уголовного уложения можно сделать вывод, что ответственность по ст. 531 наступала в случае разглашения не соответствующих действительности сведений, поскольку ст. 537 закрепляла, что разглашение обстоятельства, позорящего честь, не почитается наказуемым опозорением, если обвиняемый докажет, что:

1. разглашённое обстоятельство истинно;
2. он имел достаточное основание считать разглашённое обстоятельство истинным и учинил такое разглашение ради государственной или общественной пользы, или в интересах исполняемой им обязанности, или в интересах защиты личной чести или чести его семьи[101].

Следует также иметь в виду, что данное основание освобождения от уголовной ответственности не являлось абсолютным. Вероятно, в интересах защиты внешней политики Российской империи, а также права на частную жизнь законодатель закрепил в статье 538 положение о том, что обвиняемый в опозорении не может представлять доказательств истинности разглашённого обстоятельства и не может быть освобождён от ответственности, если указанное обстоятельство:

1. Относится к главе иностранного государства, иностранному послу, поверенному в делах или иному дипломатическому агенту такого государства;

[100] Там же. С. 731.
[101] Там же. С. 735.

2. Относится к частной или семейной жизни опозоренного и притом разглашение было учинено в распространённых или публично выставленных произведении печати, письме или изображении или в публичной речи[102].

Мы видим, что охрана частной жизни уголовно-правовым способом, а именно режима её тайны, производилась весьма своеобразно, но, тем не менее, это гарантировало неизбежность наступления ответственности за распространение сведений, которые не могли быть известны широкому кругу лиц, или сведений, в отношении которых лицо вообще установило режим полной приватности (конфиденциальности).

Уголовная ответственность за разглашение сведений, которые составляли тайну и не могли быть разглашены под угрозой наказания, устанавливалась также статьёй 541 Уголовного Уложения. Её диспозиция выглядела следующим образом: «Обязанный по своему званию хранить в тайне доверенное ему сведение, виновный в умышленном оглашении оного, без достойных уважения причин, если притом оглашённое сведение могло причинить имущественный ущерб или опозорить лицо, к коему оно относилось, и виновный не подлежит за сие оглашение наказанию как за оскорбление».

В примечаниях Н.С. Таганцева к Уголовному уложению 1903 года указывается, что оглашение тайн, по общему правилу, не наказуемо; для установления ответственности необходима наличность каких-либо других условий, и к числу таковых относится оскорбительность оглашённых сведений, о коих говорится в ст. 541[103]. Такая позиция представляется нам весьма интересной, поскольку современный уголовный закон по содержанию статьи 137 УК РФ свидетельствует об обратном, и наказуемым является любое незаконное разглашение тайн, которые относятся к частной жизни лица.

---

[102] Там же. С. 736.
[103] Там же. С. 743.

Статья 541 Уголовного Уложения охраняла право на сохранение в тайне сведений, разглашение которых могло причинить имущественный ущерб или опозорить потерпевшего. Таким образом, хотя и косвенно, законодатель всё же гарантировал право на неприкосновенность частной жизни. Преступление заключалось, по существу, в неисполнении обязанности по неразглашению – в разглашении сведений, которые стали известны виновному в силу того, что хранение данных сведений было ему доверено. Отсюда следует, что субъект данного преступления был специальным – лицо, которому сведения стали известны в силу служебных или иных обстоятельств. Статья также напрямую закрепляет, что преступление могло быть совершено только с прямым умыслом.

О.А. Пальчиковская полагает, что «статья 541 в своей диспозиции предусматривала также специальное условие для освобождения от уголовной ответственности за совершение данного деяния - «наличие достойных уважения причин» для разглашения сведения о частной жизни лица, составляющих тайну. Учитывая, что закон не содержал определения обстоятельств, которыми можно было признать «достойными уважения», то можно сделать вывод, что этот признак носил оценочный характер».[104] Нам представляется, что подобное толкование не является бесспорным, поскольку любое разглашение сведений, которые составляют тайну конкретного лица, не является «достойным уважения», за исключением, конечно же, случаев, которые связаны с раскрытием информации в силу прямых служебных обязанностей. На наш взгляд, в данном случае, если речь шла об исполнении лицом своих служебных обязанностей либо в иных случаях, когда такое разглашение было оправданным, то лицо действительно не могло нести уголовную ответственность. Несовершенство данной нормы при её широком толковании могло порождать широкие возможности усмотрения при назначении виновным лицам наказания.

---

[104] Пальчиковская О.А. Уголовно-правовая охрана личной и семейной тайны: Дисс. … канд. юрид. наук. М., 2011. С. 67.

Уголовное Уложение 1903 года продолжало действовать вплоть до Октябрьской революции 1917 года и утратило силу после революционных событий в России.

Третий этап (1917-1960 гг.). Октябрьская Революция 1917 года наложила серьёзный отпечаток на правовую систему Российского государства, поскольку любой законодательный акт обязательно должен был быть направлен на защиту социалистической идеологии, а также на проведение политики по защите интересов однопартийности в условиях последующей Гражданской войны и военного времени.

Первым нормативно-правовым актом, регулирующим правоотношения в сфере привлечения виновных лиц к уголовной ответственности, стал принятый в 1922 году Уголовный кодекс РСФСР. Он полностью соответствовал духу эпохи исторического развития России на данном этапе и защищал исключительно публичные интересы. Неудивительно, что ни в действующем законодательстве этого периода не было понятия «личная тайна», ни в УК не было норм, охраняющих личную тайну. Единственное исключение из данных положений заключается в статье 117, которая содержала норму об уголовной ответственности за разглашение должностным лицом не подлежащих оглашению сведений. Это свидетельствовало о весьма узком объёме правоотношений по обеспечению охраны конфиденциальной информации в данный период, поскольку уголовная ответственность наступала только в отношении специального субъекта – должностного лица. Представляется также, что на практике правоприменитель, скорее всего, использовал данную норму только в случае разглашения сведений, называемых современным языком служебной (или любой другой профессиональной) тайны.

Принятый в 1926 году следующий Уголовный кодекс РСФСР вообще не содержал норм об ответственности за нарушение личной тайны, не говоря уже об охране иных видов тайн. В связи с этим представляется, что охрана

частной жизни не являлась одной из первостепенных задач молодого Советского государства.

Однако ситуация несколько изменилась с принятием 15.02.1929 года Устава почтовой, телеграфной, телефонной и радиосвязи, утверждённого Постановлением Совета народных комиссаров СССР. Этот нормативный акт содержал в статье 6 следующие правила: «Содержание всех видов почтовой, телеграфной и радиотелеграфной корреспонденции составляет тайну корреспондирующих лиц. Служащим связи общего пользования и специального назначения воспрещается нарушать означенную тайну, а также давать посторонним лицам сведения о том, кем и кому корреспонденция подана или кем и от кого получена. За нарушение правил настоящей статьи служащие несут уголовную ответственность в порядке, устанавливаемом законодательством союзных республик»[105]. В то же время, анализ положений Уголовного кодекса РСФСР данного периода позволяет сделать вывод о том, что специальная норма, которая обеспечивала бы указанные выше правила, в законе отсутствовала, что свидетельствовало о правовом пробеле.

Принятая в 1936 году Конституция СССР, закрепившая за собой звание «самой демократичной конституции» [106] впервые за историю Советского государства на законодательном уровне закрепила в ст. 128 неприкосновенность жилища, тайну переписки, телефонных переговоров, почтовых, телеграфных сообщений[107]. Совершенно аналогичное положение в статье 132 закрепляла принятая в 1937 году Конституция (Основной закон) РСФСР 1937 года[108].

Нельзя, однако, утверждать, что в эпоху сталинского режима и вплоть до принятия новой Конституции 1978 года право на неприкосновенность частной жизни было абсолютным и неограниченным, так как политические

---

[105] Постановление СНК СССР от 15.02.1929 «О введении в действие Устава почтовой, телеграфной, телефонной и радиосвязи, утверждённого Постановлением Совета народных комиссаров СССР» // СЗ СССР. 1929. №22. Ст. 193, 194.
[106] Хлевнюк О. В. Хозяин. Сталин и утверждение сталинской диктатуры. М., РОССПЭН, 2012. С. 249.
[107] Конституция СССР от 05.12.1936 // Известия ЦИК СССР и ВЦИК. 1936. №283.
[108] Конституция (Основной закон) РСФСР от 21.01.1037 // Известия ЦИК Союза ССР и ВЦИК. 1937. №20.

события той эпохи свидетельствуют о том, что положения указанных законодательных актов оставались лишь декларативными и не реализуемыми в действительности.

Четвёртый этап (1960 – 1991 гг.). В 1960 году Верховным Советом РСФСР был принят новый Уголовный кодекс, который упорядочил действовавшие нормы об уголовной ответственности на территории России. В первоначальной редакции этот законодательный акт не содержал никаких охранительных норм, которые были бы посвящены персональным данным и вообще праву на неприкосновенность частной жизни. Однако с течением времени и изменением состояния преступности в него регулярно вносились изменения, поскольку в 80-х годах прошлого столетия начались активные экономические и инфраструктурные преобразования во всех сферах жизни Советского государства, что не могло не сказаться на нормах уголовного права. Стремительное развитие рыночных отношений, рост преступности обусловили изменение законодательства данного периода. В связи с этим в УК были введены две нормы об охране персональной информации:

- Ст. 135 – нарушение тайны переписки;

- Ст. 124^{1} – разглашение тайны усыновления.

Кодекс не содержал норм об уголовной ответственности за посягательства на другие виды личной информации, следовательно, иные сведения, которые не подпадали под данные условия уголовно-правовой охраны, не подлежали охране вообще.

Пятый этап (1991 г. - настоящее время). В нынешнем виде правовой институт персональных данных в России начал формироваться относительно недавно. Термин «персональные данные» стал известен российскому законодательству, по существу, только в конце XX века в связи с рыночными преобразованиями в экономике и демократическими реформами в государственно-правовой системе.

Характеризуя современные источники правового регулирования в области персональных данных, нужно отметить, что регулирование осуществляется на основе актов различной юридической силы.

Среди нормативных актов в Российской Федерации наибольшей юридической силой (высшей юридической силой) обладает Конституция РФ. Она, как основной закон государства, содержит в себе некоторые положения, которые, в принципе, относятся и к защите персональных данных.

Принятая в 1993 году, Конституция Российской Федерации закрепила ряд положений об охране основных прав и свобод человека и гражданина, закрепив также положение о том, что человек, его права и свободы являются высшей ценностью. Ст. 23 Конституции РФ содержит базовое положение, согласно которому каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Ст. 24 указывает, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается[109].

Право каждого гражданина на неприкосновенность частной жизни конкретизируется и раскрывается в соответствующих федеральных законах.

Впервые нормы о персональных данных и их защите были затронуты в Федеральном законе «Об информации, информатизации и защите информации» от 20.02.1995 года №24-ФЗ[110], который на сегодняшний день утратил силу в связи с принятием Федерального закона «Об информации, информационных технологиях и защите информации».

По существу, это был первый нормативный правовой акт, на законодательном уровне закреплявший основные понятия и принципы в области информационных охранительных правоотношений. В рассматриваемом законе содержались системообразующие нормы в области

---

[109] Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с поправками от 30.12.2008 №6-ФКЗ, от 30.12.2008 №7-ФКЗ) // Российская газета от 25.12.1993 г. №237.

[110] Федеральный закон "Об информации, информатизации и защите информации" от 20 февраля 1995 г. N 24-ФЗ // Российская газета. 2003. 7 июля.

защиты персональных данных, как и информационных прав и обязанностей субъектов.

Персональные данные в нём были отнесены к информации, носящей конфиденциальный характер. Они использовались как синоним понятия «информация о гражданах». Режим использования и обработки информации о гражданах, согласно закону, был ограниченным. В свою очередь, физические и юридические лица, владеющие информацией о гражданах, получающие и использующие её, несли ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

Подчеркнём, что закон в ст. 11 содержал положение, согласно которому допускалось существование негосударственных организаций и частных лиц по обработке и предоставлению пользователям персональных данных. Согласно п. 4 этой статьи такая деятельность не могла осуществляться без специального разрешения и подлежала обязательному лицензированию.

Закон 1995 года не содержал указание на ответственность за нарушение правил обработки персональных данных (информации о гражданах), что, в свою очередь, ставило под вопрос целесообразность существования нормы об охране персональных данных.

В последующем в соответствии с вышеназванным Федеральным законом был принят Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера»[111], в котором также указывалось, что персональные данные являются охраняемой конфиденциальной информацией с ограниченным доступом. Данный нормативный акт продолжает действовать по сей день.

[111] Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении Перечня сведений конфиденциального характера" // Справочная правовая система "Гарант"

Далее вопросы защиты персональных данных были затронуты в новом, принятом в 2001 году Трудовом кодексе РФ (далее – ТК РФ)[112]. В новом кодексе впервые за многие годы был затронут вопрос о правах и обязанностях сторон трудовых правоотношений при обработке персональных данных работников. В отличие от многих других кодифицированных нормативных правовых актов, в ТК РФ была введена глава 14, которая посвящена защите персональных данных работников. В указанной главе приводится понятие персональных данных, как и понятие «обработка персональных данных» - получение, хранение, комбинирование, передача или любое другое использование. Устанавливаются общие требования при обработке персональных данных и гарантии их защиты, принципы хранения и использования персональных данных работников, права работников в целях обеспечения защиты персональных данных, хранящихся у работодателя. Впервые говорится о том, что лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, привлекаются к дисциплинарной и материальной ответственности, а также к гражданско-правовой, административной и, что немаловажно, к уголовной ответственности.

В целях упорядочения информационных правоотношений и приведения в соответствие правовых норм требованиям российских реалий 27.07.2006 года был принят Федеральный закон «Об информации, информационных технологиях и защите информации» №149-ФЗ. Закон устанавливает, что персональные данные являются информацией ограниченного доступа, а правовое регулирование отношений в области персональных данных осуществляется специальным Федеральным законом.

Часть 8 статьи 9 указанного закона закрепляет, что запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или

[112] Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ // СЗ РФ от 07.01.2002. №1 (ч. 1). Ст. 3.

семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральным законом.

С целью разрешения множества пробелов в правовом регулировании отношений в области защиты персональных данных, а также обеспечения реализации некоторых положений Федерального закона «Об информации…» 27.07.2006 года был принят Федеральный закон №152-ФЗ «О персональных данных», который стал специальным нормативным актом, устанавливающим принципы и правила обеспечения прав на неприкосновенность личных сведений конфиденциального характера. По нашему мнению, принятие данного закона можно считать значительным достижением в области обеспечения защиты персональных данных

Впервые на общезаконодательном межотраслевом уровне (без привязки к конкретной отрасли права) появилась формулировка самого понятия: «персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации 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, другая информация»[113]. Закон №152-ФЗ также разъясняет, что «обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных». Исходя из этих определений, можно отчётливо представить себе, о каких объёмах может идти речь и насколько сложная задача стоит перед государственными и коммерческими структурами, являющимися операторами персональных данных[114].

[113] Следует заметить, что указанное определение содержалось в первоначальной редакции федерального закона «О персональных данных» до принятия соответствующих изменений.
[114] Беловский Н. Персональные данные и их защита // Финансовая газета. Региональный выпуск. 2009. №32.

Чтобы крупнейшие операторы обработки персональных данных в лице государственных органов, организаций, коммерческих структур могли привести в соответствие с новым законодательством свои принципы работы с субъектами персональных данных, новый Федеральный закон предоставлял им отсрочку в выполнении новых требований к порядку обработки, хранения и использования персональных данных.

Информационные системы персональных данных, созданные до дня вступления Закона в силу, должны были быть приведены в соответствие с его требованиями не позднее 1 января 2010 г. То есть к 1 января 2010 г. должен был завершиться переходный период по внесению необходимых изменений в существующие информационные системы персональных данных. Но этот срок был продлен.

29 декабря 2009 г. вступил в силу Федеральный закон от 27.12.2009 № 363-ФЗ «О внесении изменений в статьи 19 и 25 Федерального закона «О персональных данных» (далее - Федеральный закон N 363-ФЗ)[115]. Самое существенное его положение касается сроков приведения в соответствие его требованиям имеющихся информационных систем персональных данных, созданных до 1 января 2010 г. Они должны быть приведены в соответствие с требованиями Федерального закона N 152-ФЗ не позднее 1 января 2011 г. Все операторы, осуществляющие обработку персональных данных, получили законную отсрочку на год[116].

До принятия Федерального закона отечественными организациями проводились исследования общественного мнения о необходимости принятия Закона «О персональных данных», а также отношения к нему. Исследование мнения профессионалов проводилось сотрудниками организации SecurityLab. Исследования проводились в период с 25 октября по 25 ноября 2006 года. В процессе сбора первичных статистических данных

[115] Федеральный закон «О внесении изменений в статьи 19 и 25 Федерального закона «О персональных данных» от 27.12.2009 г. №363-ФЗ // СЗ РФ от 28.12.2009. №52 (1 ч.). Ст. 6439.
[116] Полякова О.Н. Персональные данные: отсрочка на год // Страховые организации: бухгалтерский учет и налогообложение". 2010. №1.

приняли участие 300 респондентов. В результате проведенного анализа были выявлены следующие результаты.

1. Подавляющее большинство специалистов, а именно 94%, убеждено, что России был необходим Федеральный закон «О персональных данных», поскольку они были озабочены беззащитностью приватной информации и постоянными утечками баз данных.
2. Однако 40% опрошенных специалистов не верят в то, что закон сможет работать на практике, поскольку закон содержит недостаточно конкретные требования (как считают 49%), а также причиной является нехватка денег на адекватные системы защиты, по мнению 20%.
3. Подавляющее большинство опрошенных специалистов (79%) считает, что текущие требования закона вполне пригодны для реализации[117].

Конечно, принятие специального нормативного правового акта в области охраны персональных данных имело огромное положительное значение. В то же время, нельзя не отметить определенные минусы принятого закона применительно к вопросам правового регулирования. Несмотря на то, что проблема защиты персональных данных уже давно была поставлена в российской правовой действительности, принятие нового закона само по себе эту задачу не решает. Федеральный закон «О персональных данных» содержит лишь формальные требования к безопасности приватной информации. При этом за соблюдением положений закона должны следить специальные уполномоченные федеральные органы исполнительной власти. Но механизм контроля со стороны уполномоченного органа и эффективный механизм реализации норм о привлечении к ответственности виновных лиц за нарушение правил работы с персональными данными до сих пор не выработан.

Проблемным моментом также является положение ч. 2 ст. 5 Федерального закона «О персональных данных». Согласно этой норме, хранение приватных сведений должно осуществляться не дольше, чем этого

[117]Информационный портал SecurityLab [Электронный ресурс]: http://SecurityLab.ru.

требуют цели их обработки. По достижении цели использования данных они должны быть уничтожены оператором. Это значит, что, например, электронный магазин обязан уничтожать данные своих клиентов после того, как они исполнили свои обязательства перед магазином. Однако если данные на сайте сохранились, но правоотношение уже прекращено, то это является прямым нарушением положений закона. Необходимо при этом учитывать, что в Российской Федерации на сегодняшний день вовсе отсутствует нормативно-правовое регулирование правоотношений, связанных с осуществлением электронной торговли, хотя Государственной Думой и рассматривался проект Федерального закона «Об электронной торговле». Следовательно, сложно говорить о применимости закона к данным отношениям ввиду особенностей купли-продажи товаров через Интернет.

Следует согласиться с мнением А.В. Кучеренко, который указывает, что формирование правовой платформы института персональных данных в России в настоящее время, как представляется, осуществляется по трём основным направлениям.

1. Активно идет процесс создания специализированных правовых актов различной юридической силы, к числу которых следует отнести: ФЗ «О персональных данных», Федеральный закон от 3 декабря 2008 г.№242-ФЗ «О государственной геномной регистрации в Российской Федерации»[118], Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»[119] и другие.
2. Значительно возросли темпы нормотворчества государственных органов исполнительной власти в данной сфере; так, практически каждым федеральным министерством и ведомством были изданы акты, регулирующие обработку персональных данных служащих указанных

[118] Федеральный закон «О государственной геномной регистрации» от 03.12.2008 №242-ФЗ (ред. от 17.12.2009) // СЗ РФ от 08.12.2008. №49. Ст. 5740.
[119] Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных

органов или их оборот в целом. Специальные акты были приняты Федеральной службой безопасности, Минкомсвязи, Федеральным фондом обязательного медицинского страхования, Пенсионный фондом России.

3. Институт персональных данных начинает укрепляться в непрофильных отраслях законодательства – в Трудовом кодексе РФ (в нём нормы о персональных данных были закреплены еще до принятия специального Федерального закона), в Федеральном законе «Об актах гражданского состояния» и во многих иных[120].

Однако, на наш взгляд, вполне очевидно, что это далеко не полный перечень тенденций и направлений дальнейшего реформирования законодательства о персональных данных.

Современные источники нормативно-правового регулирования отношений, связанных с персональными данными, нельзя назвать неизменными. Они непрерывно будут изменяться с развитием информационных технологий. Но следует подчеркнуть, что основные принципы регулирования таких правоотношений останутся неизменными, поскольку они были выработаны наукой и правоприменительной практикой. Значительную роль в формировании современных правовых норм о персональных данных в России сыграли общепризнанные принципы и нормы международного права, которые признаны универсальными и применяются на территориях многих государств мира.

[120] Кучеренко А.В. Этапы и тенденции нормативно-правового регулирования оборота персональных данных в Российской Федерации // Информационное право. 2009. №4. С. 32-36.

1.3. Правовое регулирование отношений по охране персональных данных в международном и иностранном праве

Персональные данные стали объектом нормативно-правовой регламентации сравнительно недавно. Несмотря на это, в мировой нормативно-правовой практике накопилось достаточно много актов, с помощью которых осуществляется правовое регулирование вопросов, связанных с обеспечением безопасности персональных данных.

История создания правовых норм и законодательства о персональных данных свидетельствует о стремительном развитии этих норм, об их появлении, изменении и обновлении, появлении новых принципов в правовом регулировании.

Поскольку ни одно современное государство не может обойтись без международного сотрудничества в области защиты и охраны наиболее важных общественных отношений, а также, поскольку государства стремятся к глобализации, этим объясняется значительная роль международного права и его общепризнанных принципов и норм. Как указывается в правовой доктрине, «современное международное право является общим для всех государств в том смысле, что именно общепризнанные принципы и нормы характеризуют его основное содержание, его социальную и общечеловеческую ценность»[121].

В связи с вышеизложенным, довольно часто неурегулированность тех или иных общественных отношений в национальной правовой системе восполняется за счёт появления общепризнанных принципов и норм международного права, а также международных договоров об охране наиболее важных общественных отношений, имеющих всеобщее значение. Так, государство, подписывая и ратифицируя международный договор, берёт на себя обязательство обеспечить применение таких норм внутри своей

[121] Международное право: учебник / Отв. ред. Г.В. Игнатенко и О.И. Тиунов. 6-е изд., перераб. и доп. М.: Норма: ИНФРА-М, 2013. С. 14.

территории. Данный тезис вполне справедлив и в отношении норм, посвящённых правовой охране персональных данных.

В России нормативное регулирование отношений, связанных с персональными данными, в Советский период развития законодательства отсутствовало. Возможно, это было связано с отсутствием необходимости во всестороннем обеспечении прав и свобод человека и гражданина. Это связано также с отсутствием стремительного развития информационных правоотношений и информационных технологий в целом. Именно поэтому мы видим необходимость в рассмотрении, в первую очередь, международных актов, положивших основу для возникновения в российском праве норм об охране персональных данных.

В международном праве отношения, связанные с обращением персональных данных и обеспечением их безопасности, регулируются достаточно давно. Актуальность и своевременность принятия нормативных правовых актов, регулирующих отношения в области защиты персональных данных, подтверждается зарубежным опытом[122].

Общепризнанные принципы и нормы международного права и международные договоры начали формироваться в послевоенный период, как и международные организации, их аккумулирующие.

Первым международно-правовым актом, сформировавшим нормы об охране права на неприкосновенность частной жизни в Европе, была принятая в 1950 году Европейская Конвенция о защите прав человека и основных свобод, которая закрепила в статье 8 право на уважение частной и семейной жизни. В ней, в частности, указывается, что каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции. Не допускается вмешательство со стороны публичных властей в осуществление этого права, за исключением случая, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка,

[122] Копылов В.А. Информационное право. М.: Юристъ, 2009. С. 392.

экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья и нравственности или защиты прав и свобод других лиц[123]. Содержание указанного права на уважение личной и семейной тайны, по существу, предопределяется и правом на обеспечение безопасности и конфиденциальности персональных данных каждого в специально предусмотренных случаях.

Европейский суд по правам человека во многих своих решениях вполне чётко отвечает на вопрос о связи между правом на уважение личной и семейной тайны и правом на неприкосновенность персональной информации. Именно поэтому, на наш взгляд, Европейскую конвенцию о защите прав человека и основных свобод можно рассматривать как один из международных договоров, непосредственно регулирующих отношения в сфере обеспечения безопасности персональных данных.

Так, в деле Гаскин против Соединённого Королевства (Gaskin v. the United Kingdom) Европейский суд по правам человека в Постановлении от 07.07.1989 (§ 37, Серия А, №160) утверждает, что конфиденциальность общественных архивов, которые содержат персональную информацию о физических лицах, имеет важное значение для получения объективной и достоверной информации, и что такая конфиденциальность может быть также необходима для защиты третьих лиц. Заявитель хотел начать разбирательство против местных властей в связи с тем, что, как он утверждал, когда он был ребенком, с ним плохо обращались в приёмной семье. Он попытался получить доступ к своему делу, которое имелось у местных властей. Власти решили, что информация в деле заявителя должна быть ему предоставлена только в том случае, если иные лица, которые предоставили информацию для этого дела, дадут своё согласие на раскрытие информации. Он пожаловался на то, что отсутствие непосредственного доступа к документам нарушило его право на уважение частной жизни.

---

[123]Европейская конвенция о защите прав человека и основных свобод ETS №005 // СЗ РФ. 1998. №20. Ст. 2143.

Европейский суд усмотрел в действиях Правительства нарушение статьи 8 Европейской конвенции, которая предусматривает, что каждый имеет право на уважение частной и семейной жизни. Суд указал в Постановлении, что заявителю было отказано в доступе к информации, касающейся того периода его детства, когда он находился под опекой государства. Между тем, эта информация является важной для частной жизни заявителя и именно поэтому должна была быть ему предоставлена Правительством Соединённого Королевства. Система, которая ставит возможность доступа к документам в зависимость от согласия лиц, предоставивших информацию, может в принципе рассматриваться как соответствующая обязательствам по ст. 8, учитывая свободу усмотрения государства. При такой системе интересы индивида, стремящегося получить доступ к документам, относящимся к его личной или семейной жизни, должны быть обеспечены, когда предоставившие информацию лица отсутствуют или безосновательно отказываются дать своё согласие. Такая система будет соответствовать принципу пропорциональности только в том случае, если она обеспечивает то, чтобы независимый орган мог принять окончательное решение о том, должен ли быть предоставлен доступ в случаях, когда предоставившие информацию лица не отвечают на запрос или отказываются дать свое согласие. В настоящем деле заявитель не мог воспользоваться подобной процедурой[124]. Вполне очевидно, что в данном деле необходимо было исходить из принципа разумности, поскольку ни одно физическое лицо в мире не может не обладать конфиденциальной информацией о самом себе. В противном случае, необходимость обеспечения конфиденциальности персональных сведений утрачивает всякий смысл.

В другом деле – Аманн против Швейцарии (Amann v.Switzerland) - заявителю, занимавшемуся продажей приборов для эпиляции, поступил телефонный звонок из бывшего советского посольства с заказом на прибор.

[124] Постановление Европейского Суда по правам человека от 07.07.1989 (§37, серия А, №160).

Прокуратура перехватила звонок и попросила службу разведки собрать информацию о заявителе. В данном деле Европейский суд усмотрел нарушение статьи 8 Европейской конвенции, указав, что запись телефонного разговора, а также сбор и хранение информации нарушили право человека на уважение частной жизни, поскольку внутренним законодательством государства-ответчика не были чётко установлены полномочия властей в этой сфере[125].

В деле S. И Марпер против Соединённого Королевства (S. and Marper v. The United Kingdom) заявители были взяты под стражу, а затем им было предъявлено обвинение в совершении преступлений. У них были отобраны следы пальцев рук и образцы ДНК. Все их ходатайства были отклонены, так как в соответствии с законодательством государства-ответчика эти данные о заявителях могли храниться бессрочно. В указанном деле Европейский суд подчеркнул, что закон не устанавливал условия и порядок хранения следов пальцев рук и образцов ДНК, более того, он не предоставлял гарантий, исключающих их неправомерное или нецелевое использование, а также не давал возможности принимать в расчёт индивидуальные обстоятельства каждого конкретного дела. Суд указал в Постановлении (п. 68), что все три категории информации, представленные в указанном деле, имеют статус персональных данных, так как они относятся к установленным лицам. Следовательно, они подлежат особой охране и не могут быть переданы третьим лицам и нарушают право на неприкосновенность частной жизни лица. Поэтому Европейский Суд установил факт нарушения со стороны компетентных органов государства-ответчика положений ст. 8 Европейской Конвенции[126].

Таким образом, можно проследить неоспоримую взаимосвязь между правом на уважение (неприкосновенность) частной жизни, личной и

---

[125] Постановление Европейского суда по правам человека от 16.02.2000 [Электронный ресурс]: http://www.echr.coe.int

[126] Постановление Европейского суда по правам человека от 04.12.2008 [Электронный ресурс]: http://www.echr.coe.int

семейной тайны и обеспечением безопасности персональных данных (персональной информации).

Безусловно, специфический характер правоотношений в сфере оборота персональных данных, а также обеспечения их безопасности не мог не породить специального правового регулирования на международном уровне. В связи с этим, впервые унифицированные международные нормы о персональных данных появились с принятием Конвенции Совета Европы о защите личности в связи с автоматической обработкой персональных данных от 28.01.1981 (ETS №108). В преамбуле конвенции указано, что государства исходят из необходимости усиления гарантий прав и основных свобод каждого человека и в особенности права на неприкосновенность его личной сферы, вызванную все возрастающим перемещением через границы персональных данных, обработанных с применением автоматизированных средств. Государства также подтверждают приверженность свободе информации независимо от границ и необходимость уважения неприкосновенности личной сферы и свободного обмена информацией между народами[127].

Этот международно-правовой акт стал одним из первых нормативных документов, закрепляющих необходимость правовой охраны персональных данных как объекта, наибольшим образом подверженного различным посягательствам. Это исторически первый международный договор, по сути, глобального значения, который содержит юридически обязывающие нормы в области защиты персональных данных[128].

Конвенция устанавливает область своего применения в виде автоматизированных баз персональных данных и автоматической обработки персональных данных в публичном и частном секторе. В Конвенции устанавливаются также основные принципы защиты данных, а именно:

---

[127] Конвенция Совета Европы «О защите физических лиц в отношении автоматизированной обработки данных личного характера (ETS№108) от 28.01.1981 // СПС «КонсультантПлюс».

[128] Ратификация Конвенции Совета Европы: Защита персональных данных будет усилена [Электронный ресурс]: http://www.privacy-journal.ru/journal/2013y/101/article_895.html

получение данных добросовестным и законным способом, их накопление для строго определенных и законных целей, адекватность данных, точность, надлежащая форма.

В Конвенции содержится одно из основных правил: стороны обязуются принимать надлежащие меры для того, чтобы основные принципы защиты данных были реализованы в национальном праве. Это положение является важным ключевым моментом, повлиявшим, на наш взгляд, впоследствии, на появление норм об охране персональных данных в национальных правовых системах государств Совета Европы.

В то же время, поскольку современное международное право базируется на принципе автономии воли и **сотрудничества**[129], то вполне оправдано, что нормы Конвенции предоставляют каждому государству-участнику возможность отступить от установлений Конвенции, когда такое отклонение, предусмотренное национальным законодательством, составляет необходимую меру в демократическом обществе. Среди таких случаев, в частности, можно выделить следующие:

1. При защите безопасности государства, общественной безопасности, денежного обращения государства или при подавлении уголовных правонарушений.
2. При защите лицом, о котором идет речь, прав и свобод других.

Российская Федерация присоединилась к рассматриваемой Конвенции ещё в 2001 году, однако в течение достаточно длительного периода времени не ратифицировала её. Федеральный закон о ратификации Конвенции 1981 года был подписан в 2005 году. Параллельно Правительством Российской Федерации велась большая работа по имплементации норм Конвенции в российское законодательство. И лишь 15 мая 2013 года Российская Федерация завершила процедуру ратификации Конвенции [130], передав

[129] Международное право: учебник / Под ред. Г.В. Игнатенко, О.И. Тиунова. 6-е изд., перераб. и доп. – М.: НОРМА: Инфра-М, 2013. С. 37.
[130] О ратификации Россией Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс]: http://www.coe.mid.ru/doc/avt_obr_PD.htm

ратификационную грамоту на хранение Генеральному секретарю Совета Европы. Конвенция вступила в силу для Российской Федерации с 01 сентября 2013 года.

Принятие Конвенции 1981 года завершило, по существу, процесс внедрения норм международного права о защите персональных данных в российскую правовую систему, значительным образом повлияв на законодательство и нормативные акты в целом.

Российское законодательство об охране персональных данных является, пожалуй, самым «молодым» среди законодательства европейских государств, поскольку вопросы охраны данных личного характера уже давно стали в Европе предметом законодательного регулирования.

Принятие правовых норм об обеспечении безопасности персональных данных во многих странах сопровождалось созданием специальных государственных органов, которые были уполномочены обеспечивать безопасность персональных данных. Государства создали на основе законодательства не зависимые от правительства государственные органы по защите прав субъектов персональных данных во главе с соответствующим омбудсменом – уполномоченным лицом по защите прав. Впервые такой орган был введен в 1919 году в Швеции, за которой последовали и другие страны. Сегодня так называемые «Комиссии по защите данных» или «Data Protection Commission» действую в Австралии, Австрии, Англии, Бельгии, Болгарии, Венгрии, Греции, Италии и т.д.[131]

В 1984 году в **Соединённом Королевстве Великобритании** был принят «Акт о защите данных» (The Data Protection Act). В соответствии с ним, защите подлежат персональные данные, обрабатываемые с помощью компьютерной техники. Вводятся понятия «персональные данные», «регистратор персональных данных», «трибунал». Среди основополагающих начал правового регулирования обеспечения безопасности персональных данных Акт называет обязательную регистрацию деятельности по обработке

[131] Копылов, В.А. Информационное право [Текст]: учебник. 2-е изд., перераб. и доп. М.: Юристъ, 2002.

персональных данных в специальном регистре (Data Protection Registrar) путём заполнения специальной регистрационной формы. Обязательным считается указание объёма персональных данных, которые подлежат обработке и использованию, а также источники, откуда персональные данные были получены. Кроме того, в регистре в обязательном порядке должна быть отражена информация о том, кому из третьих лиц планируется передавать зарегистрированные персональные данные.

Акт также содержит очень важное положение, согласно которому если лицо осуществляет работу с информацией персонального характера и при этом оно не зарегистрировано в Регистре (Registrar), то оно признаётся виновным в нарушении требования обязательной регистрации деятельности по обработке и использованию персональных данных[132].

Рассматривая законодательство о защите персональных данных в других европейских странах, нельзя не остановиться на нормативно-правовом акте **Федеративной Республики Германии** от 20.12.1990 года «О совершенствовании обработки данных и защите информации», который упорядочивает общественные отношения, возникающие в процессе накопления, переработки и использования персонифицированной информации (персональных данных). Данный нормативно-правовой акт по-другому определяет институт персональных данных, нежели это произведено в Конвенции 1981 года. Закон ФРГ определяет персональные данные как совокупность сведений о частной жизни или общественно-политической активности гражданина, прямо или косвенно относящихся к физическому лицу. Необходимо отметить, что любую информацию, которая позволяет идентифицировать физическое лицо, закон относит к персонифицированной информации[133]. Как и во многих странах мира, контроль и надзор за

[132] Data Protection Act 1998 [Электронный ресурс]: http://www.legislation.gov.uk/ukpga/1998/29/contents
[133] Bundesdatenshutzgesetz 20.12.1990 [Электронный ресурс]: http://www.juris.de

соблюдением и исполнением положений данного закона возложен на Федерального уполномоченного по защите персональных данных[134].

Защита персональных данных осуществляется в ФРГ на уровне федерации и на уровне федеральных земель, каждая федеральная земля имеет свой собственный закон «О персональных данных».

Но на этом немецкое законодательство об обеспечении безопасности персональных данных не завершается, так как в 1991 году в ФРГ был принят Закон о документации Штази[135], что было вызвано объединением Германии и вхождением в её состав бывшей Германской Демократической Республики, а также в целях обеспечения безопасности лиц, чьи данные хранились в секретных архивах службы госбезопасности бывшей ГДР[136].

В **Королевстве Испания** вопросы, связанные с защитой персональных данных, регулируются Основным законом о защите данных (Ley Orgánica de Protección de Datos de Carácter Personal или Organic Law of Data Protection – LOPD)[137]. В дополнение к этому закону в Испании было принято Положение о применении Основного закона о защите данных (Real Decreto Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal или Regulation implementing Spanish Organic Law of Data protection)[138].

В соответствии с Основным законом Испании персональные данные определяются как любая информация относительно физических лиц, которые могут быть идентифицированы на её основе. Согласно указанным нормативно-правовым актам любой гражданин Испании вправе возражать против обработки данных, относящихся лично к нему. Кроме того, любой гражданин вправе указать оператору, неправомерно обрабатывающему его

---

[134] Копылов В.А. Указ соч. С. 394.
[135] Ein Service des Bundesministeriums der Justiz in Zusammenarbeit mit der juris GmbH. [Электронный ресурс]: http://www.juris.de.
[136] Горелихина О.А., Шлиньков А.А. Правовая защита персональных данных в Германии // Вопросы экономики и права. 2012. №3. С. 323.
[137] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
[138] Real Decreto 1720/2007, de 21 de diciembre, Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.

данные, на необходимость прекращения такой обработки. В то же время, испанский закон предусматривает, что реализация гражданином такого права возможна до тех пор, пока гражданин не совершит каких-либо незаконных действий или преступлений. При этом, ограничение такого права возможно только в разумных пределах, необходимых для защиты публичных интересов.

Во **Франции** защита персональных данных подвержена законодательному регулированию достаточно давно. С 1978 года во Франции действует Закон «Об обработке данных, файлах данных и индивидуальных свободах» (Loi relative à l'informatique, aux fichiers et aux libertés)[139], который устанавливает не только нормы, регулирующие правоотношения в сфере оборота персональных данных, но и меры ответственности за нарушение установленных правил. Эксперты отмечают, что указанный закон является весьма суровым с позиций установления мер уголовной ответственности за совершение правонарушений, связанных с посягательством на персональные данные. Например, любое нарушение правил сбора и хранения персональных данных оценивается законодателем как наиболее опасное правонарушение в указанных отношениях и наказывается на срок до 5 лет тюремного заключения[140].

В **Китайской Народной Республике** до недавнего времени нормы об охране персональных данных отсутствовали. Но так было до тех пор, пока не было принято несколько важных нормативных актов, регулирующих вопросы обеспечения прав субъектов персональных данных. В частности, в Решении Постоянного комитета Всекитайского собрания народных представителей «Об усилении охраны Интернет-информации» указывается, что безопасность персональных данных является важной обязанностью государства, а обеспечение такой безопасности возможно только

[139] Act №78-17 of 6 january 1978 On information technology, data files and civil liberties [Электронный ресурс]: URL:http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf

[140] См., например: Иванский В.П. Персональные данные как основной объект посягательств на неприкосновенность сферы частной жизни: законодательный опыт в зарубежных странах // Административное право и процесс. 2012. №8. С. 50-56.

посредством контроля за деятельностью Интернет-пользователей[141]. Кроме того, в связи с расширением экономического сотрудничества с различными государствами мира, а также с распространением так называемой электронной торговли (посредством информационно-телекоммуникационных сетей) 25 октября 2013 года Всекитайским Собранием народных представителей был одобрен проект поправок в Закон КНР «О защите прав потребителей», в котором появились специальные положения об охране персональных данных потребителей. В случае если участник предпринимательской деятельности осуществляет сбор данных потребителей, он обязан указать цель, способы и пределы сбора и использования данных, а также получить согласие потребителя. При осуществлении сбора персональных данных участники предпринимательской деятельности обязаны раскрыть правила сбора и использования данных. Сбор и использование персональных данных потребителей не может осуществляться в нарушение законодательства и соглашения потребителя с участником предпринимательской деятельности. Кроме того, на участника предпринимательской деятельности возлагаются обязанности по сохранению конфиденциальности персональных данных потребителей и не вправе раскрывать, изменять, продавать или передавать персональные данные потребителей другим лицам[142].

Несмотря на то, что указанные положения применяются в Китае только для потребительских правоотношений, по существу, они содержат в себе принципы, которые используются во многих международных соглашениях и договорах, регулирующих отношения, связанные с использованием, обработкой и охраной персональных данных.

В **Соединённых Штатах Америки** на сегодняшний день существует два законодательных акта, которые определяют нормативно-правовое

---

[141] Решение ПК ВСНП об охране персональных данных граждан [Электронный ресурс]: http://cnlegal.ru/civil_law/network_information_protection/

[142] Проект изменений в Закон КНР «О защите прав потребителей» [Электронный ресурс]: http://cnlegal.ru/civil_law/consumer_protection_law_amend_draft/

регулирование защиты неприкосновенности частной жизни и персональных данных. Во-первых, это Закон «О защите персональных данных» 1980 г. (Privacy Protection Act)[143], а во-вторых, это Закон «О защите информации при передаче данных по электронному каналу» 1986 г. (Electronic Communications Privacy Act)[144]. Кроме того, существуют ещё несколько актов, регулирующих узкоотраслевые принципы работы с персональными данными. Например, на уровне США, существует Закон о страховании здоровья и возложении ответственности 1996 г. (Health Insurance Portability and Accountability Act)[145], Закон о справедливых и точных кредитных сделках 2003 г. (Fair and Accurate Credit Transaction Act)[146] и Закон о защите детей в сети Интернет (Child Online Privacy Protection Act)[147]. На уровне штатов существует только Закон штата Калифорния о защите частной жизни в сети Интернет (The California Online Privacy Protection Act)[148]. Единый нормативно-правовой акт о защите персональных данных отсутствует. По существу, эти законодательные акты регулируют деятельность государственных органов при обработке персональных данных граждан.

Если проанализировать положения указанных актов, то можно прийти к выводу, что они ориентированы на правовое регулирование в узконаправленных сферах жизнедеятельности, вследствие чего не представляется возможным понять общие принципы обработки и передачи персональных данных и реализации правоотношений, связанных с ними. Можно лишь сформулировать, что все эти нормативные акты исходят из того, что любые персональные данные являются неприкосновенными, и их

---

[143] The Privacy Protection Act of 1980 [Электронный ресурс]: https://epic.org/privacy/ppa/

[144] Electronic communication Privacy Act of 1986 (ECPA), 18 U.S.C. 2510-22 [Электронный ресурс]: https://it.ojp.gov/default.aspx?area=privacy&page=1285

[145] Brian K. Atchinson and Daiel M. Fox The Politics of The Health Insurance Portability and Accountability Act // Health affairs. 1997. Vol. 16. Number 3.

[146] Fair and Accurate Credit Transactions Act of 2003 [Электронный ресурс]: http://www.gpo.gov/fdsys/pkg/PLAW-108publ159/html/PLAW-108publ159.htm

[147] Restriction of access by minors to materials commercially distributed by means of World Wide Web that are harmful to minors [Электронный ресурс]: http://www.law.cornell.edu/uscode/text/47/231

[148] Business and Professions Code Section 22575-22579 [Электронный ресурс]: http://leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579

несанкционированный оборот не допускается, за исключением специально оговоренных случаев.

Персональные данные определяются, как и во многих международных соглашениях, как сведения, на основе которых их субъект может быть опознан, причём не только на основе традиционной информационной формы, но и посредством информации, получаемой через сеть Интернет. Вмешательство в частную жизнь посредством использования персональных данных запрещено под угрозой применения различных мер юридической ответственности. Однако из данного правила существует исключения, которыми, как показывает международная геополитическая ситуация, США активно пользуются. Например, правило о невмешательстве в частную жизнь не распространяется на случаи нарушения законодательства, в том числе уголовного; в случаях, когда такое вмешательство связано с поддержанием национальной безопасности, обороной государства или обеспечением экономической безопасности государства[149].

Существование различных международных организаций, созданных для определённых целей, вносит вклад в развитие правовых норм в мире. Поэтому такое международное объединение, как Европейский Союз, не является исключением в регулировании вопросов, связанных с защитой персональных данных. Так, Директивой Европейского Союза 95/46/ЕС Европейского парламента и Совета от 24.10.1995 г. «О защите прав частных лиц применительно к обработке личных данных и о свободном движении таких данных»[150] установлены многие из ныне действующих принципов охраны персональных данных, которые фактически уже были закреплены в национальных нормах государств-участников Европейского Союза. Среди них можно отметить такие, как: принцип срочности хранения персональных данных, соответствие целям, для которых они собираются и обрабатываются;

[149]Searches and seizures by Government officers and employees in connection with investigation or prosecution of criminal offences [Электронный ресурс]: http://www.law.cornell.edu/uscode/text/42/2000aa

[150] Директива Европейского Союза 95/46/ЕС Европейского парламента и Совета от 24.10.1995 г. «О защите прав частных лиц применительно к обработке личных данных» // Официальный журнал Европейских сообществ от 23.11.1995 г. №L. 281. С. 31. Разд. 1, затрагивающий качество данных. С. 6

для персональных данных, сохраняемых более длительные сроки в исторических и иных целях, должны быть установлены необходимые гарантии обеспечения их защиты.

Необходимо отметить несколько основополагающих начал данной Директивы – гармонизация положения законодательства государств-членов, имеющих целью обеспечить эквивалентный уровень защиты основных прав и свобод, в частности, права на невмешательство в частную жизнь при использовании персональных данных в секторе телекоммуникаций, и обеспечить свободную передачу таких данных, а также телекоммуникационного оборудования и услуг в рамках сообщества[151]. Это свидетельствует о том, что в сфере защиты персональных данных поддерживается принцип соблюдения баланса частных и публичных интересов, поскольку поддержание такого баланса, в свою очередь, может обеспечивать правопорядок в правоотношениях, связанных с персональными данными.

Принятое в разных государствах законодательство, регулирующее охрану персональных данных, мало изменилось со времени его формирования. Впрочем, для российского законодательства это нехарактерно, поскольку оно подвергалось значительным изменениям.

Таким образом, можно прийти к выводу, что принципы регулирования правоотношений в сфере обеспечения безопасности персональных данных, а также охраны права на неприкосновенность частной жизни в законодательстве исследуемых государств во многом совпадают, и это обусловлено глобальным характером проблемы охраны персональных данных, которая наиболее остро возникает в современном мире развития информационных технологий. При этом значительную роль в формировании национального законодательства сыграли общепризнанные принципы и нормы международного права в сфере защиты персональных данных, которые были имплементированы в соответствующие правовые системы.

---

[151] Там же. Ст. 1.

Глава 2. Уголовно-правовой анализ и проблемы применения законодательства об ответственности за преступные посягательства в отношении персональных данных

Меры ответственности в праве довольно часто выступают как правовой инструментарий, позволяющий обеспечить безопасность жизненно важного объекта, причём «важность» такого объекта не подвергается сомнению, поскольку его устранение влечёт или может повлечь за собой серьёзные разрушительные, негативные последствия для всей системы общественных отношений. Именно поэтому некоторые исследователи рассматривают уголовный закон как средство обеспечения безопасности важного для общества объекта охраны. В связи с этим, правильная конструкция соответствующей нормы уголовного закона и правильное её применение в идеале позволят оградить объект от вредоносного преступного посягательства. Но незнание оснований применения такого вида ограничительного воздействия, как меры уголовной ответственности, не может обеспечить соответствующее понимание характера и степени общественной опасности преступного посягательства на объект охраны, а тем более, - понимание введения мер наказания и иных мер уголовно-правового характера.

Что же касается персональных данных, то обоснование их уголовно-правовой охраны в правовой литературе не так однозначно, как представляется правоприменителю, который уже выработал определённый механизм применения уголовного закона для некоторых разновидностей преступных посягательств в отношении персональных данных. Многие из существующих сегодня в практике механизмов имеют спорный и неоднозначный характер. Кроме того, статистика зарегистрированных преступлений показывает, что удельный вес преступлений, связанных с посягательствами на персональные данные за последние годы в России возрос.

Исходя из этого, вопрос, связанный с основаниями введения мер уголовной ответственности за преступные посягательства в отношении персональных данных остаётся первоочередным в уголовно-правовом анализе и выявлении соответствующих проблем.

На наш взгляд, степень понимания проблем криминализации посягательств в отношении персональных данных повышает использование правовой теории мер безопасности, основные положения которой уже более 20 лет назад предложены Н.В. Щедриным[152], и разработаны в рамках его научной школы [153] . Согласно этой теории в процессе становления цивилизации «выкристализовались» базовые ценности, опираясь на которые человечество выиграло в конкуренции с другими живыми существами. Ценности, образующие каркас современного цивилизованного общества, закреплены в международно-правовых документах и действующей Конституции Российской Федерации. Их утрата и разрушение может вернуть человечество в состояние варварства, а затем и дикости, подтверждение чему мы периодически получаем пока, к счастью, в локальных масштабах.

Для охраны системообразующих ценностей человечеством «изобретены» правила безопасности, основу которых составляют специальные ограничения (специальные запреты и обязанности) и определенное сочетание которых образует режим безопасности [154] . В зависимости от значимости объекта охраны правила можно подразделить на правила безопасности, повышенной безопасности и особой безопасности. Соответствующим образом можно классифицировать и режимы безопасности. В трактовке Н.В. Щедрина диспозиции статей Особенной части Уголовного кодекса – это правила особой безопасности, диспозиции

---

[152] См.: Щедрин Н.В. Введение в правовую теорию мер безопасности: Монография / Краснояр. гос. ун-т, 1999. 180 с.; Щедрин Н.В. Меры безопасности как средство предупреждения преступности. Дис. ... докт. юрид. наук: 12.00.08. Красноярск, 2001. 348 с.

[153] См.: Концептуально-теоретические основы правового регулирования и применения мер безопасности: монография / под науч. ред. Н.В. Щедрина ; Сиб. федер. ун-т. Красноярск : СФУ, 2010. 324 с.

[154] Щедрин Н.В. Введение в правовую теорию мер безопасности… С. 103-104.

норм иных охранительных отраслей права – правила повышенной безопасности[155]. «Нарушение правил особой безопасности влечет за собой применение уголовно-правовых санкций»[156].

В контексте правовой теории мер безопасности – персональные данные являются объектом охраны, по поводу которых в разных отраслях права сформулированы правила безопасности, повышенной безопасности и особой безопасности. Иными словами, проблема криминализации посягательств в отношении персональных данных – это проблема формулирования правил особой безопасности, то есть соответствующих диспозиций статей Особенной части Уголовного кодекса.

Возможно, общественной потребности в криминализации нарушения правил обращения с персональными данными не существует, и для их защиты достаточен режим повышенной охраны, предусмотренный другими отраслями права (законодательства). Необходимость уголовно-правовой охраны персональных данных возникает только в случаях, когда на режим повышенной охраны персональных данных «накладываются» режимы особой охраны информации, относящихся к тому или иному виду тайны. Именно эта рабочая гипотеза легла в основу настоящего диссертационного исследования.

2.1. Персональные данные как объект повышенной (правовой) и особой (уголовно-правовой) охраны

2.1.1. Персональные данные как объект повышенной правовой охраны

Информация, позволяющая идентифицировать физическое лицо, довольно часто становится объектом пристального внимания многих лиц. И

---

[155] Щедрин Н.В. Концептуально-теоретические основы правового регулирования и применения мер безопасности // Криминология: вчера, сегодня, завтра. 2013. № 4. С. 26-35.
[156] Щедрин Н.В. Новый Уголовный кодекс России в контексте социального управления // Lex Russica. 2015 № 3. С. 48-63.

это не случайно, потому что человек в течение всей своей жизни может позиционировать себя в общественных связях только при помощи информационного обмена. Такая информация позволяет выделить человека, обособить его от всех остальных, придать ему черты индивидуальности и в некоторых ситуациях позволяет породить определённые виды правоотношений.

Невозможно, однако, утверждать, что оборот такой личной (приватной) информации является неограниченным и может разглашаться повсеместно, причём не только как со стороны субъекта – источника данной информации, но и других лиц. Разглашение той или иной информации может существенным образом навредить человеку и не только в имущественном, социальном, но и в морально-нравственном аспекте его жизнедеятельности. Поэтому ранее, в главе 1 мы утверждали, что конфиденциальность персональных данных позволяет ограничить свободное перемещение данного вида информации в целях обеспечения безопасности указанных сведений. Но необходимо, в то же время, понимать, каковы основания введения подобного рода ограничений, потому что отсутствие соответствующих оснований недопустимо. В противном случае, цель уголовного закона в виде установления круга преступных деяний и мер ответственности за их совершение теряется.

Для понимания оснований правовой охраны проанализируем существующие правовые позиции относительно охраны персональных данных в законодательстве и научной литературе.

С принятием Конституции Российской Федерации 1993 года, которая провозгласила высшей ценностью права и свободы человека и гражданина, в значительной степени изменился подход к пониманию прав человека. Так, в ст. 2 Конституции РФ указывается, что признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства. Конституция РФ закрепляет и другое положение, в соответствии с которым каждому гарантируется право на неприкосновенность частной жизни, личной и

семейной тайны (ст. 23). Таким образом, основной закон Российской Федерации, по существу, устанавливает объекты правовой охраны, без которых действующая система правоотношений не может существовать.

Вместе с тем, существуют различные аспекты жизнедеятельности человека, которые в значительной степени могут быть подвержены опасному воздействию со стороны внешних сил. Причем необходимо учитывать, что разрушение такого объекта может повлечь за собой разрушение действующей системы правоотношений. Как пишет Н.В. Щедрин, если эти объекты уничтожить и разрушить, человечество вернётся к состоянию дикости и поставит себя на грань вымирания. Чтобы общество функционировало как развивающаяся система, необходима защита её сущностных элементов[157]. Это так называемые объекты повышенной охраны. Они определяются как важнейшие свойства (отношения) существующей системы, утратив которые она либо разрушится, либо трансформируется в другую и не сможет достичь поставленной перед ней цели[158].

В качестве объектов повышенной охраны выделяются такие, как жизнь здоровье, честь и достоинство, половая неприкосновенность, собственность и иные конституционные права и свободы человека и гражданина. В целом, можно говорить, что объектами повышенной охраны называются наиболее важные стороны человеческой жизни. К таким важным сторонам, на наш взгляд, следует относить и персональные данные, поддержание конфиденциальности которых обеспечивает, в свою очередь, безопасность другого объекта повышенной охраны – права на неприкосновенность частной жизни.

Любая систематизированная и социально значимая информация может быть использована как во благо, так и во вред человеку. Поэтому

---

[157] Щедрин Н.В. Введение в правовую теорию мер безопасности: монография. Красноярск: Краснояр. гос. ун-т, 1999. С. 72.

[158] Щедрин Н.В. Источник повышенной опасности, объект повышенной охраны и меры безопасности. Красноярск: Юридический институт КрасГУ, 2006. С. 12.

важно понимать, каковы социальные предпосылки повышенной охраны персональных данных.

Персональные данные гражданина, позволяющие идентифицировать его среди большого числа граждан, содержат в себе характеристики, которые могут быть отнесены к личной информации. Так, информация о семейном положении гражданина или информация о месте его работы составляет личную информацию. Данная информация, прежде всего, необходима самому гражданину, чтобы непосредственно распоряжаться своими способностями к самовыражению в современном мире.

Как указывают некоторые исследователи, «каждому гражданину принадлежит изначально право определять объём личной информации, который может быть известен неопределенному кругу лиц» [159] . Соответственно, это право гражданина является производным, от права на неприкосновенность частной жизни. Отсюда также следует, что персональные данные являются необходимым инструментом, с помощью которого человек может реализовать право на неприкосновенность частной жизни, так как способен самостоятельно установить режим конфиденциальности (тайны) в отношении конкретного перечня сведений.

Неприкосновенность частной жизни всячески охраняется законом. Любые посягательства на неприкосновенность частной жизни влекут за собой ответственность, установленную законом. Следовательно, если неприкосновенность частной жизнь рассматривается как объект охраны, то право гражданина самостоятельно определять объём персональных данных, которые не могут быть разглашены, должно входить в содержание неприкосновенности частной жизни.

Персональные данные в своей достаточной совокупности позволяют идентифицировать личность их субъекта, который в процессе своей жизни осуществляет тот или иной вид деятельности, занимая определённое

---

[159] См.: Цадыкова Э.А. Гарантии охраны и защиты персональных данных человека и гражданина // Конституционное и муниципальное право. 2007. №14.

положение в обществе, приобретая деловые и личные связи, социальный и деловой статус. Каждый субъект персональных данных вправе определять достаточный объём данных (сведений, информации), который необходим для его эффективной деятельности в процессе своего становления и развития. Но это вовсе не означает, что все сведения о субъекте могут быть достоянием широкой общественности.

В научной литературе указывается, что «персональные данные – лишь информация, позволяющая идентифицировать личность. Само по себе распространение этих данных не столько наносит ущерб личности, сколько создаёт возможность для причинения ущерба»[160]. С данным мнением можно согласиться, но лишь отчасти, поскольку 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. Разглашение персональных данных существенным образом может нарушить право на неприкосновенность частной жизни и явиться своеобразной «платформой» для совершения иных правонарушений и неправомерных действий.

Профессор М.Н. Малеина, говоря о персональных данных, использует понятие «право на тайну и неприкосновенность персональных данных». Она указывает, что «это субъективное право содержит правомочия требовать от третьих лиц не нарушать тайну персональных данных, предоставить соответствующую информацию (или её часть) другим лицам, определять содержание и судьбу персональных данных, которые в силу тех или иных обстоятельств стали известны третьим лицам, в установленном законом порядке»[161]. Подобного мнения придерживается и А.А. Иванов, указывая, что «персональные данные представляют собой личное неимущественное благо,

---

[160] Авдеев М.Ю. Нормативное содержание права на неприкосновенность частной жизни // Новый юридический журнал. 2013. №1. С. 50.

[161] См.: Малеина М.Н. Право на тайну и неприкосновенность персональных данных // Журнал российского права. 2010. С. 20.

а право на персональные данные – личное неимущественное право. При этом, осуществляя право на персональные данные, его субъект вправе требовать, чтобы с этими данными обращались надлежащим образом – не получали их без согласия правообладателя, а получив - проводили предусмотренные операции с данными в установленном законом порядке»[162].

Представляется, что с таким мнением, следует согласиться, поскольку правовая природа неприкосновенности персональных данных исходит, прежде всего, из содержания права на неприкосновенность частной жизни. Человек самостоятельно определяет перечень сведений, которые не подлежат разглашению, а также перечень сведений, который может быть публично доступен. Следовательно, вопрос о правовой охране персональных данных каждый раз зависит от стремлений самого человека защитить значимую для него информацию о себе путём установления соответствующего режима конфиденциальности персональной информации.

Анализ позиций, высказанных относительно правовой охраны персональных данных, даёт основание сформулировать проблему соответствующего объекта повышенной правовой охраны, поскольку не во всех правоотношениях является понятным, что именно подлежит правовой охране – право на неприкосновенность частной жизни или сами персональные данные.

Так, вышеприведённое мнение Н.М. Малеиной позволяет сделать вывод, что объектом охраны должно быть право на неприкосновенность персональных данных, а не сами персональные данные[163]. С другой стороны, если следовать логике о том, что под правовую охрану могут подпадать наиболее значимые блага и интересы, то сами персональные данные, являясь личным неимущественным благом, также подпадают под правовую охрану.

---

[162] Иванов А.А. Хранение персональных данных за рубежом с точки зрения российского права [Электронный ресурс]: http://zakon.ru/Blogs/xranenie_personalnyx_dannyx_za_rubezhom_s_tochki_zreniya_rossijskogo_prava/16124

[163] См.: Малеина М.Н. Указ. соч.

Э.А. Цадыкова включает персональные данные в понятие личной информации, которая охраняется в составе обеспечения права на неприкосновенность частной жизни, исходя из того, что личная информация может раскрывать отдельные элементы частной жизни человека[164].

М.Ю. Авдеев полагает, что неприкосновенность персональных данных является важнейшей составляющей права на неприкосновенность частной жизни, следовательно, правовой охране подлежит всё это право целиком, а не его отдельные элементы[165].

Представляется, что правовая охрана того или иного объекта обусловливается разрушительным характером соответствующих последствий, которые могут возникнуть в результате причинения вреда такому объекту. Это следует из понятия объекта повышенной охраны: «системы, обладающие свойствами, утрата которых приведёт к причинению существенного и необратимого вреда: разрушению самой системы или утрате функций, для которых она создана и предназначена» [166]. Следовательно, право на неприкосновенность персональных данных в целях повышенной охраны может приобретать самостоятельное значение, то есть охраняться не только в рамках права на неприкосновенность частной жизни в целом. Так, повышенная охрана может быть характерна для персональных данных лица, являющегося свидетелем по уголовному делу, и в связи с этим ему должна быть обеспечена государственная защита в рамках соответствующих мероприятий, установленных федеральным законом [167]. 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

---

[164] Цадыкова Э.А. Конституционное право на неприкосновенность частной жизни: Сравнительно-правовое исследование. Автореферат дисс. … канд. юрид. наук. М., 2007. С. 19.
[165] Авдеев М.Ю. Там же.
[166] Концептуально-теоретические основы правового регулирования и применения мер безопасности: монография / Под науч. ред. Н.В. Щедрина; Сиб. фед. ун-т. Красноярск: СФУ, 2010. С. 16.
[167] Федеральный закон «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» от 20.08.2004 №119-ФЗ // СЗ РФ. 2004. №34. Ст. 3534.

источник информации для эффективного и быстрого отправления правосудия.

Опасность преступных посягательств в отношении персональных данных заключается в том, что нарушается комплекс правоотношений, в которых человек может себя идентифицировать на основании соответствующих персональных данных. Следовательно, нарушение одного права в таком случае влечёт нарушение других неотъемлемых прав, например, права на жизнь.

Так, в Соединённых Штатах Америки имел место случай, иллюстрирующий нарушение других прав посредством нарушения права на неприкосновенность персональных данных. Гражданин, пострадавший от пуль, в перестрелке был тяжело ранен. Впоследствии он попал под программу защиты свидетелей и был помещен полицией в охраняемую палату. Но преступники через Интернет вошли в компьютерную сеть клиники, где он лежал, и, изменив программу стимуляции сердца, убили его [168] . Это произошло в силу доступности персональных данных пострадавшего в различных информационных системах, в том числе социальных сетях, а также несовершенство компьютерной сети клиники, что позволило практически беспрепятственно совершить преступление. Отсутствие и непринятие необходимых мер по защите персональных данных гражданина привело к его смерти. Мы видим в указанном случае, что нарушение права на неприкосновенность персональных данных о свидетеле по уголовному делу привело к нарушению его права на жизнь.

Другой случай, имевший место в России, свидетельствует о том, что в результате преступных посягательств в отношении персональных данных пострадало ещё и право на тайну переписки. Так, К. осуждена за неправомерный доступ к компьютерной информации и нарушение тайны переписки. Было установлено, что К. умышленно, с целью ознакомления с

[168] Криминология: учебник / под общ. ред. А.И. Долговой. 4-е изд., перераб. и доп. М.: Норма: Инфра-М, 2010. С. 835.

конфиденциальной информацией, неоднократно осуществляла неправомерный доступ к охраняемой законом компьютерной информации в локальной сети интернет. Путем обмана пользователей социальной сети «Вконтакте» получила доступ к их личным данным, содержащимся на закрытых от всеобщего обозрения страницах. Она же, с целью нарушения тайны переписки, без согласия потерпевшей В. зарегистрировала страницу в социальной сети «Вконтакте» с указанием персональных данных потерпевшей, в дальнейшем, используя данную страницу, осуществляла личную переписку от ее имени, и знакомилась с содержанием писем, адресованных потерпевшей. По приговору суда К. была осуждена к 10 месяцам 5 дням лишения свободы условно[169].

Сегодня довольно часто опасности подвержены жизнь и здоровье лиц, являющихся представителями государственной власти, персональные данные которых попадают в руки злоумышленников. Так, председательствующему на процессе в Мосгорсуде по делу об убийстве адвоката Станислава Маркелова и журналистки Анастасии Бабуровой судье Александру Замашнюку предоставлена охрана. Причиной этому послужило сообщение представителя государственного обвинения о том, что на форумах националистов в сети Интернет появилась информация, содержащая персональные данные судьи[170]. Учитывая, что указанное уголовное дело получило весьма широкий общественный резонанс и что были установлены лица, причастные к совершению преступления, была получена информация, что персональные данные судьи могут быть использованы в целях совершения в отношении него посягательств на жизнь или здоровье. Именно поэтому было принято решение о взятии судьи под охрану.

Опасность преступных посягательств в отношении персональных данных обусловлена также и тем, что глобальная компьютерная сеть «Интернет» предоставляет не только широкие возможности для поиска,

---

[169] Гендиректор осуждена за переписку «Вконтакте» [Электронный ресурс]: http://pravo.ru/news/view/47465/

[170] Судья по делу об убийстве Маркелова и Бабуровой взят под охрану [Электронный ресурс]: http://www.pravo.ru/news/view/49615/

получения и распространения информации, но и для различного рода злоупотреблений. Как справедливо указывает Р.И. Дремлюга, «сама природа сети Интернет зачастую является благоприятной для совершения преступлений, так как такие её свойства, как глобальность, трансграничность, анонимность пользователей, охват широкой аудитории, распределение основных узлов сети и их взаимозаменяемость, создают преступникам, использующим Интернет, преимущества на всех этапах совершения преступления, а также позволяют эффективно скрываться от правоохранительных органов»[171].

В последние годы Правительство РФ активно переходит на электронный документооборот, а также на оказание государственных услуг в электронном виде. Это затрагивает и правовые нормы, призванные упорядочить различные виды общественных отношений. Так, с 02.01.2017 года вступил в силу Федеральный закон «О государственной регистрации недвижимости» [172] , который закрепил возможность государственной регистрации прав на недвижимое имущество и сделок с ним посредством электронных ресурсов информационно-телекоммуникационной сети «Интернет» с идентификацией гражданина через портал государственных услуг.

Безусловно, с одной стороны, это значительно упрощает процедуру регистрации новых собственников в отношении недвижимого имущества. С другой стороны, такая форма, предусмотренная законом, создаёт серьёзную почву для различных злоупотреблений и преступных посягательств. Сведения о собственниках являются персональными данными, как и информация, идентифицирующая их на портале «Госуслуги». Обладая данной информацией, злоумышленники могут без особых препятствий в установленные законом сроки зарегистрировать имущественные права, пока как предыдущие собственники могут даже об этом и не узнать. Кроме того,

[171] Дремлюга Р.И. Интернет-преступность. Автореферат дисс. … канд. юрид. наук. Владивосток, 2007. С. 8.
[172] Федеральный закон «О государственной регистрации недвижимости» от 13.07.2015 №218-ФЗ // СЗ РФ. 2015. №29. Ст. 4344.

как указывается в средствах массовой информации, имущество в конечном итоге может оказаться у добросовестных приобретателей, истребовать его у которых оказывается проблематичным либо вообще невозможным[173].

Очевидно, что нарушение права на неприкосновенность персональных данных может подвергать опасности другие права, рассматриваемые в качестве объектов повышенной охраны. Таким образом, право на неприкосновенность персональных данных является не чем иным, как объектом повышенной правовой охраны.

С этих позиций, можно сделать вывод, что задача правовых механизмов по регулированию оборота персональных данных должна заключаться в предоставлении надлежащего инструментария для охраны персональных данных. Закон в этом случае должен выработать соответствующие ограничительные механизмы, позволяющие обеспечить безопасность персональных данных, так как их ненадлежащий оборот может привести к нарушению всей действующей системы общественных отношений.

Статус объекта повышенной охраны может подтверждаться и тем, что за различные посягательства на этот объект устанавливаются различные меры юридической ответственности, в том числе уголовной, которая считается наиболее серьёзным видом ответственности по степени карательного воздействия.

2.1.2. Персональные данные как объект уголовно-правовой охраны

Представленные в юридической литературе позиции относительно того, что персональные данные являются объектом уголовно-правовой охраны, весьма неоднозначны.

---

[173] Мошенники легко отберут у вас квартиру [Электронный ресурс]: http://mirnov.ru/ekonomika/nedvizhimost-zhkh/moshenniki-legko-otberut-u-vas-kvartiru.html; Государственная регистрация – не только учёт, но и контроль, и… Ответственность [Электронный ресурс]: http://www.garant.ru/article/649894/

Объект уголовно-правовой охраны довольно часто определяют через понятие охраняемых общественных отношений, которым в результате совершения преступления может быть причинён вред. Это достаточно устоявшаяся в уголовно-правовой доктрине позиция[174]. При этом серьёзных различий между объектом уголовно-правовой охраны и объектом преступления не проводится.

Так, Е.К. Каиржанов полагал, что объект уголовно-правовой охраны и объект преступления по объёму понятий совпадают между собой[175].

Н.И. Коржанский полагает, что различие между указанными понятиями заключается только в наличии или отсутствии преступного посягательства. Объект уголовно-правовой охраны – то общественное отношение, которое поставлено под защиту уголовного закона, но которое преступному изменению не подвергалось. А в отличие от этого, объект преступления – то общественное отношение, которое уже подвергалось преступному изменению[176].

Между тем, в научном сообществе уже сложились прямо противоположные мнения, в соответствии с которыми указанные понятия объекта уголовно-правовой охраны и объекта преступления являются неравнозначными.

Так, Л.Д. Гаухман пишет, что «понятие «объект уголовно-правовой охраны» и «объект преступления» - понятия неодинаковые по своему значению, даже несмотря на то, что в основе их обоих лежит категория «общественные отношения». Первое даёт лишь общее представление о круге общественных отношений, защищаемых уголовным законом, имеет

---

[174] См., например: Пионтковский А. А. Учение о преступлении. М. 1961, С. 132; Таганцев Н.С. Русское уголовное право. Лекции. Часть Общая. В 2-х т. Т. 1. – М., 1994. – С. 29, 31.

[175] Каиржанов Е.К. Интересы трудящихся и уголовный закон. Проблемы объекта преступлений. Алма-Ата, 1973. С. 22.

[176] Коржанский Н.И. Основания и критерии выбора объектов уголовно-правовой охраны. Труды ВСШ МВД СССР, 1976. Вып. 12. С. 116.

общесоциальное значение. Второе имеет уголовно-правовое значение, так как характеризует элемент состава преступления»[177].

В литературе подчёркивается также, что «объект уголовно-правовой охраны возникает с момента вступления в силу уголовного закона, охраняющего общественные отношения, объект же преступления – с момента совершения преступления»[178].

Е.А. Корякина полагает, что «объект уголовно-правовой охраны» и «объект преступления» – нетождественные понятия. Под объектом уголовно-правовой охраны следует понимать не общественные отношения, а блага и интересы, охраняемые уголовным законом. Объект отдельного преступления – блага и интересы, в отношении которых осуществлено преступное посягательство или была создана угроза такого посягательства»[179].

Р.В. Закомолдин указывает, что «объект уголовно-правовой охраны представлен наиболее значимыми общественными отношениями, является первичным по отношению к объекту преступления, поскольку деяние не будет преступным, если оно посягает на объект, который не охраняется уголовным законом. Следовательно, объект уголовно-правовой охраны существует независимо от того, было ли совершено преступное посягательство или нет, в отличие от объекта преступления, который возникает только по факту совершения общественно опасного деяния»[180].

Следует признать тот факт, что объект уголовно-правовой охраны действительно является самостоятельным понятием, отличным по объёму от понятия объекта преступления, поскольку последний относится к виновно совершённому общественно опасному деянию, запрещённому уголовным законом под угрозой наказания. Объект же уголовно-правовой охраны сам по себе подчёркивает повышенную охрану тех или иных общественных

---

[177] Гахуман Л.Д. Квалификация преступлений: закон, теория, практика. М.: АО «Центр ЮрИнфоР», 2001. С. 64.
[178] Уголовное право. Общая часть: учебник / Под ред. А.Н. Тарбагаева. М.: Проспект, 2012. С. 53.
[179] Корякина Е.А. Жизнь человека как объект уголовно-правовой охраны. Автореферат дисс. … канд. юрид. наук. Екатеринбург, 2011. С. 14.
[180] Закомолдин Р.В. Преступные нарушения специальных правил и требований безопасности: монография. Тольятти: Филиал РГСУ в г. Тольятти, 2013. С. 6.

отношений, благ и законных интересов, гарантируя, что государство обеспечит надлежащий правоохранительный механизм, направленный на применение мер ответственности за преступные посягательства на этот объект. Отсюда можно сделать вывод, что понятие объекта уголовно-правовой охраны функционально и генетически связывается с понятием объекта особой охраны, закрепляя законодательную возможность возникновения охранительных правоотношений в случае совершения преступного посягательства.

Следовательно, говоря об уголовно-правовой охране конкретного объекта, необходимо понимать, что речь идёт не об объекте конкретно совершённого общественно опасного деяния, а системе правоотношений, которые подлежат уголовно-правовой охране в силу особой опасности преступных посягательств в отношении них.

Персональные данные, являясь особым видом информации, представляют собой во многих случаях необходимое условие реализации субъектом тех или иных прав и свобод, поскольку субъект, вступая в правоотношение, должен идентифицировать себя, «выделить», «обособить» от всех остальных участников. Поскольку отношения, связанные с установленным законом оборотом персональных данных могут подвергаться серьёзным опасностям, то общественные отношения по обороту персональных данных могут рассматриваться в качестве объекта уголовно-правовой охраны.

Обоснование уголовно-правовой охраны персональных данных не может обойтись и без ответа на вопрос о том, что же в таком случае является объектом соответствующих преступных посягательств. В этой связи довольно интересной представляется позиция Г.П. Новоселова, который полагает, что «в качестве конструктивного признака понятия объекта преступления обычно усматривается одновременно и то, что нарушается преступлением, и то, что подвергается воздействию в процессе его совершения, и то, что изменяется в результате такого воздействия, и то, что

требует своей уголовно-правовой охраны, и, наконец, то, что терпит вред». Однако он указывает, что «каждая из этих характеристик важна по-своему и отображает только отдельную сторону данного явления»[181].

Кроме того, при обосновании того, что же входит в понятие объекта преступления, автор указывает, что «объектом любого преступления выступают люди, которые в одних случаях выступают в качестве отдельных физических лиц, в других – как некоторого рода множество лиц, имеющих или не имеющих статус юридического лица, в-третьих – как социум (общество)»[182].

Представляется, что если человек является объектом преступления, то в этой связи неприкосновенность его персональных данных приобретает серьёзное значение, а наличие уголовно-правовых норм об ответственности даёт основание говорить о том, что правовая охрана персональных данных имеет обособленный, «повышенный» характер. При этом сами персональные данные необходимо, на наш взгляд, рассматривать в некоторых случаях и как предмет преступных посягательств, поскольку с их помощью и осуществляются сами преступные посягательства.

Говоря о современном состоянии уголовно-правовой охраны персональных данных, следует отметить, что на сегодняшний день с момента введения в действие Федерального закона «О персональных данных» правоприменительная практика пошла по пути квалификации преступных посягательств в отношении персональных данных по нескольким статьям Особенной части Уголовного кодекса РФ.

В то же время, ни одна норма Особенной части, из подлежащих применению в подобных случаях при совершении преступлений, не содержит положения, в каком именно контексте следует охранять персональные данные. Это следует из того, что нормы Особенной части об ответственности за преступные посягательства на персональные данные

---

[181] Новоселов Г.П. Учение об объекте преступления. Методологические аспекты. М.: Издательство НОРМА, 2001. С. 44.
[182] Там же. С. 60.

носят бланкетный характер, и в самом уголовном законе не раскрывается, какие категории персональных данных подлежат охране. Кроме того, персональные данные, подпадая под различные правовые режимы безопасности, носят настолько межотраслевой характер, что вопрос об уголовно-правовой охране персональных данных в каждом конкретном случае ставится в зависимость от разновидности персональных данных, их содержания, а также запретов и ограничений, которые в данном конкретном деле были в отношении них установлены.

Между тем, понимание механизма уголовно-правовой охраны, сущности оснований привлечения виновных лиц к уголовной ответственности имеет важное практическое значение, поскольку практика показывает, что правоприменители не всегда руководствуются обоснованной логикой в вопросах квалификации и назначения наказания за соответствующие преступления, посягающие на персональные данные.

Анализ уголовных дел о преступлениях, посягающих на персональные данные, показал, что деяния виновных лиц квалифицируются по нескольким статьям Особенной части УК РФ. Подавляющее большинство из изученных уголовных дел возбуждались и расследовались по ст. 137 УК РФ – нарушение неприкосновенности частной жизни. Кроме того, деяния квалифицировались по ст. 183 (незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну).

Так, приговором мирового судьи Ленинского округа г. Тюмени Г. Был признан виновным в совершении преступления, предусмотренного ч. 1 ст. 137 УК РФ. Судом было установлено, что летом 2013 года Г. После ссоры со своей знакомой создал в социальной сети «Вконтакте» её поддельную страницу, на которой выложил фотографии девушки в обнажённом и полуобнажённом виде. Спустя некоторое время, в той же социальной сети он создал ещё одну страницу от имени девушки, где к её откровенным фото

добавил номера телефонов и статус с предложениями услуг интимного характера[183].

В другом уголовном деле, Ноябрьский городской суд Ямало-Ненецкого автономного округа признал виновным П., бывшего специалиста по обучению отдела розничного рынка фиксированного бизнеса филиала ОАО «Мобильные ТелеСистемы», в совершении преступления, предусмотренного ч. 3 ст. 183 УК РФ. Было установлено, что в декабре 2013 года П. с помощью своего коллеги получил персональные данные абонентов и отправил их со своего электронного адреса на электронный адрес знакомого. За эту услугу сотрудник филиала ОАО «МТС» получил 5000 рублей[184].

В некоторых случаях правоприменительная практика квалифицирует действия по незаконному собиранию или распространению персональных данных, составляющих личную и (или) семейную тайну, по совокупности со ст. 272 УК РФ. Так, в отношении жительницы Калуги В. было возбуждено уголовное дело по ч. 1 ст. 137 и ч. 1 ст. 272 УК РФ, поскольку она в июне 2010 года узнала логин и пароль от личной страницы своего знакомого на сайте «Одноклассники». Используя логин и пароль, В. зашла на его страницу, где ознакомилась со входящими и исходящими сообщениями и, используя сервис сайта «Одноклассники», переслала их копии без согласия мужчины его знакомой. Кроме того, впоследствии В., зайдя на личную страницу потерпевшего, изменила сведения о частной жизни в графе «статус» на его личной странице, а также удалила его фотографию, сведения о друзьях и знакомых[185].

---

[183]В Тюмени осуждён мужчина, который в социальной сети разместил откровенные фото своей бывшей девушки [Электронный ресурс]: http://proctmo.ru/press-center/news/7418/

[184] За продажу персональных данных абонентов МТС осуждён специалист-наставник сотовой компании [Электронный ресурс]: http://pravo.ru/news/view/103838/

[185] Женщину, шпионившую за знакомым в «Одноклассниках», будут судить по 3 статьям УК [Электронный ресурс]: http://pravo.ru/news/view/62062/

При этом нам 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.

В большинстве указанных случаев правоприменительные органы не в полной мере соотносят объект посягательства с реальными последствиями посягательства или направленностью умысла виновного лица на совершение преступления. Поэтому в одних случаях квалификация содеянного происходит по одной из указанных норм Особенной части УК РФ, а в других – по двум нормам. Очевидно, что эта проблема порождена отсутствием единства в понимании сущности объекта охраны, а также оснований такой охраны. Таким образом, возникает необходимость анализа норм выявленных статей Особенной части на предмет объекта уголовно-правовой охраны, который они закрепляют.

Статья 137 УК РФ посвящена охране неприкосновенности частной жизни, что и указывается большинством исследователей как основной непосредственный объект преступления, предусмотренного данной нормой. При этом право на неприкосновенность частной жизни является неотъемлемым и неотчуждаемым, гарантированным Конституцией РФ. В этой связи справедливо высказывание И.Л. Петрухина, в соответствии с которым сложная юридическая ситуация заключается в том, что «потребность в личной жизни лежит за пределами права, но последнее выражает, закрепляет эту потребность и обеспечивает её удовлетворение»[186].

В комментарии к Уголовному кодексу РФ под редакцией А.И. Рарога указывается, что «объектом преступления, предусмотренного ч. 1 ст. 137 УК РФ является конституционное право на неприкосновенность частной жизни»[187]. В комментарии к Уголовному кодексу РФ под редакцией В.Т. Томина и В.В. Сверчкова указывается, что «основным объектом преступного посягательства в данном случае выступают общественные отношения,

[186] Петрухин И.Л. Личная жизнь: пределы вмешательства. М., 1989. С. 7.
[187] Грачева Ю.В., Ермакова Л.Д. и др. Комментарий к Уголовному кодексу РФ / Отв. ред. А.И. Рарог. М.: Проспект, 2011.

складывающиеся по поводу реализации конституционного принципа неприкосновенности частной жизни, личной и семейной тайны, а факультативными объектами могут быть честь, достоинство и доброе имя человека» [188]. В комментарии к Уголовному кодексу РФ под ред. А.В. Бриллиантова авторы обращают внимание, что «общественные отношения, складывающиеся по поводу реализации данного конституционного права, составляют основной объект рассматриваемого состава преступления»[189].

В литературе также высказывается мнение, что объектом данного преступления является общественное отношение, при котором ни одно лицо без волеизъявления другого лица не имеет права вторгаться в его частную жизнь в форме собирания или распространения сведений о нём[190]. В свою очередь, Н.И. Пикуров указывает, что «определение объекта уголовно-правовой охраны, а точнее, границ частной жизни, в данном случае представляет наибольшую сложность»[191].

Некоторые авторы указывают, что «строгого определения частной жизни нет не только в Конституции РФ, но и в международных актах, относящихся к данной сфере. Но даже в отсутствие легальных дефиниций сложно отрицать наличие тесной связи между понятиями «частная жизнь» и «персональные данные»[192].

В то же время, если обратиться к содержанию статьи 137 УК РФ, то можно обнаружить, что право на неприкосновенность частной жизни, которое подлежит в данном случае уголовно-правовой охране, охраняется в контексте личной и семейной тайны. Такая формулировка, в принципе,

---

[188] Комментарий к Уголовному кодексу Российской Федерации / Под ред. В.Т. Томина и В.В. Сверчкова. М.: Юрайт-Издат, 2010. С. 225.

[189] Комментарий к Уголовному кодексу РФ (постатейный) / Под ред. А.В. Бриллиантова. М.: Проспект, 2010. С. 255.

[190] Уголовное право. Особенная часть: учебник / Под ред. И.В. Шишко. М.: Проспект, 2012. С. 108.

[191] Пикуров Н.И. Некоторые вопросы уголовно-правовой охраны частной жизни // Уголовно-правовая охрана личности и её оптимизация: Научно-практическая конференция памяти профессора А.Н. Красикова (20-21 марта 2003 г.) / Под ред. Б.Т. Разгильдиева. Саратов, 2003. С. 74.

[192] 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. 2012. №12. С. 75.

следует из положений ст. 23 Конституции РФ, которая как раз и подразумевает под реализацией права на неприкосновенность частной жизни право определять объём информации, который будет составлять личную и семейную тайну человека.

О понятии «тайна» в литературе ведётся множество споров. Некоторые исследователи указывают, что общеправовое определение понятия тайны в российском законодательстве отсутствует. Связано это с межотраслевым характером института тайны в российской правовой системе. Так, в одной из своих работ А. Кибальник и И. Соломоненко, формулируя определение тайны в уголовном праве, указывают, что применительно к уголовно-правовой охране 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[193].

В.А. Мазуров, выделяя общие признаки различных видов тайн в российском законодательстве, определяет тайну как «охраняемые государством конфиденциальные сведения в области социально-политической, экономической, военной и частной жизни граждан, незаконное получение, разглашение, использование которых создаёт угрозу причинения вреда правам и законным интересам граждан, общества, государства и влечёт за собой ответственность виновных лиц в соответствии с действующим законодательством Российской Федерации»[194].

С.Г. Селезнёва, раскрывая понятие «тайна», указывает, что «тайна предполагает не просто информацию, а её определённое состояние, правовой режим. При этом информация скрывается постольку, поскольку неблагоприятным образом может повлиять на мотивацию поступков, на

[193] Кибальник А., Соломоненко И. Понятие и виды тайны в уголовном праве // Российская юстиция. 2001. №2. С. 53.
[194] Мазуров В.А. Уголовно-правовая защита тайны. Автореферат дисс. … канд. юрид. наук. Барнаул, 2001. - С. 179.

поведение и мнение других субъектов. Защищая эти сведения, мы защищаем, прежде всего себя»[195].

И.В. Бондарь под тайной понимает «представленную в нематериальной форме или на физических носителях и имеющую потенциальную духовно-нравственную, этическую, коммерческую либо иную общественно-значимую ценность информацию, известную или доверенную ограниченному кругу лиц, доступ к которой ограничен действующим федеральным законодательством, в связи с чем её владелец либо иной обладатель принимает необходимые меры к охране её конфиденциальности, разглашение которой влечёт применение мер юридической ответственности»[196].

А.В. Серебренникова справедливо, на наш взгляд, указывает, что «законодатель вполне обоснованно использует понятие «тайна» для разграничения степени конфиденциальности информации, без использования данного термина трудно бы было доказать, в чём заключается общественная опасность действий, если виновное лицо разглашает сведения, которые не являются тайной»[197].

По существу, тайна определяется как информация, совокупность сведений, в отношении которой установлен правовой режим, предполагающий в силу её уязвимости набор ограничений и запретов в целях обеспечения её охраны. Следует согласиться с тем, что тайна – всегда ограничение свободного потока информации, а потому в зависимости от вида охраняемой информации можно вводить в правовой оборот различные виды тайн, в том числе личную и семейную тайну, охране которых посвящена ст. 137 УК РФ. Кроме того, сохранение определённой информации в тайне

---

[195] Селезнёва С.Г. Понятие тайны в уголовном праве // Вестник Челябинского государственного университета. Серия Право. 2013. Вып. 35. №5(296). С. 97.
[196] Бондарь И.В. Тайна по российскому законодательству (проблемы теории и практики). Автореферат дисс. … канд. юрид. наук. Н.Новгород, 2004. С. 74.
[197] Серебренникова А.В. Уголовно-правовое обеспечение конституционных прав и свобод человека и гражданина по законодательству Российской Федерации и Германии. М.: ЛексЭст, 2005. С. 40-52.

подчёркивает её повышенную ценность для субъекта и свидетельствует о том, что это есть не что иное, как нематериальное благо.

Понятия «личная» и «семейная» тайна в юридической науке также определяются по-разному.

Большинство авторов ставят знак тождества между понятиями «неприкосновенность частной жизни» и «личная и семейная тайна», определяя, что неприкосновенность частной жизни зависит от соблюдения режима тайны сведений, которые являются ценными для субъекта, и разглашение которых для него может иметь неотвратимые негативные последствия. Так, И.А. Юрченко определяет, что «информация, относящаяся к тайне, является таковой, в первую очередь, поскольку сам субъект отнёс её к данному виду»[198]. В свою очередь, сам субъект определяет, что такая информация является неприкосновенной.

В.Е. Трофимова указывает, что «под личной тайной следует понимать охраняемые уголовным законом сведения (информация), отражающие особо важные стороны частной жизни лица, который придаёт им конфиденциальный характер. Под семейной тайной следует понимать охраняемые уголовным законом сведения, отражающие особо важные стороны частной жизни нескольких лиц (двух или более), находящихся друг с другом в семейных отношениях, которые придают им конфиденциальный характер»[199].

Пономарева Ю.В. полагает, что «понятия «личная тайна» и «семейная тайна» являются весьма абстрактными в российском законодательстве, что позволяет многим исследователям включать в них совершенно неожиданные содержательные моменты. Например, данные понятия являются смежными с иными понятиями, такими, как «персональные данные», «тайна усыновления», «тайна переписки», «тайна телефонных переговоров». По

---

[198] Юрченко И.А. Нарушение неприкосновенности частной жизни // Чёрные дыры в российском законодательстве (Москва). 2002. С. 75-79.

[199] Трофимова В. Е. Понятие и содержание личной и семейной тайны // Молодой ученый. 2013. №12. С. 682-685.

сути, личная тайна определяется как информация о личной, бытовой, интимной сферах жизни субъекта, в которые включается достаточно широкий и слабо очерченный перечень сведений. Отсутствие чёткого законодательного регулирования указанных понятий свидетельствует о серьёзном правовом пробеле»[200].

Таким образом, личная и семейная тайна по своему содержанию раскрывают право на неприкосновенность частной жизни. Но при этом, на наш взгляд, тайна является не набором сведений, а правовым режимом, устанавливающим совокупность ограничений и запретов в отношении набора сведений. Отсюда очевидна функциональная связь между личной и семейной тайной как правовым режимом ограничения свободного распространения персональных данных и самими персональными данными, в отношении которых этот режим со стороны конкретного субъекта может быть установлен.

О режимном характере личной и семейной тайны, как и любого вида тайны, в том числе, в отношении персональной информации, говорит, в частности, А.А. Ефремов, указывая, что «тайна является не только конфиденциальной информацией, но и правовым режимом информации»[201]. Следовательно, уголовно-правовая охрана персональных данных в контексте применительно к личной и семейной тайне будет зависеть от того, входят ли указанные данные в режим личной и семейной тайны или нет.

Кроме того, «режимный характер правовой охраны» в отношении личной и семейной тайны подтверждается позицией Конституционного Суда РФ, выраженной в Определении от 28.06.2012 №1253-О «Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьёй 137 Уголовного кодекса Российской Федерации»: «Право на неприкосновенность

---

[200] Пономарева Ю.В. Законодательство о тайнах: проблемы и пробелы правового регулирования // Вестник Южно-Уральского государственного университета. Серия «Право». – 2014. – Том 14. №3. С. 111.

[201] Ефремов А.А. Понятие и виды конфиденциальной информации [Электронный ресурс]: http://www.russianlaw.net/law/confidential_data/a90/

частной жизни, личную и семейную тайну означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера… Соответственно, 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»[202].

Уголовно-правовой охране других видов тайны посвящена статья 183 УК РФ. Как указывается в литературе, статья 183 Уголовного кодекса РФ посвящена уголовно-правовой охране охраняемой законом экономически значимой информации, составляющей соответствующий вид тайны – коммерческой, налоговой или банковской. Так, преступление, предусмотренное ст. 183 УК РФ, посягает на сохранность сведений, которые выступают в качестве предмета преступления и в отношении которых существует режим их конфиденциальности[203]. Г.А. Русанов полагает, что «непосредственным объектом преступления, предусмотренного ст. 183 УК РФ, являются общественные отношения, обеспечивающие право на сохранность коммерческой, налоговой и банковской тайны»[204].

Признавая, что решающим в обосновании сущности объекта преступления является всё же сложившаяся система общественных отношений, мы будем исходить из того, что объектом данного преступления действительно являются общественные отношения, но связанные с обеспечением конфиденциальности сведений, составляющих коммерческую, налоговую или банковскую тайну в целях реализации мер безопасности

---

[202] Определение Конституционного Суда РФ «Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьёй 137 Уголовного кодекса Российской Федерации» от 28.06.2012 №1253-О // СПС «КонсультантПлюс».

[203] Уголовное право Российской Федерации. Общая и Особенная части: Учебник / Под ред. А.И. Чучаева. М.: Контракт, Инфра-М, 2013. С. 238.

[204] Русанов Г.А. Преступления в сфере экономической деятельности. Учебное пособие. М.: Проспект, 2014. С. 64.

сложившейся экономической системы. Конфиденциальность указанного вида информации необходима, поскольку это обеспечивает устойчивость делового оборота при осуществлении предпринимательской и иной экономической деятельности, а также безопасность субъектов торгового оборота.

Общественная опасность данного вида посягательства на указанные виды конфиденциальной, охраняемой законом информации вполне очевидна. Б.В. Волженкин писал, что «развитие свободного предпринимательства и связанной с ним конкуренции настоятельно требует правового обеспечения защиты информации, представляющей коммерческую ценность, разглашение которой может причинить вред субъектам экономической деятельности»[205]. Следовательно, информация, подпадающая под понятие коммерческой, налоговой и банковской тайны, является важнейшей составляющей в механизме охраны сложившейся системы экономических правоотношений.

Применительно к ст. 183 УК РФ, персональные данные могут охраняться лишь в том случае, если эти сведения представляют собой коммерческую, налоговую или банковскую тайну, то есть в отношении них установлен режим ограничений и запретов, связанных с тем, что разглашение такой информации может быть экономически небезопасным для хозяйствующего субъекта.

Понятие коммерческой тайны законодательно закреплено в Федеральном законе «О коммерческой тайне», при этом необходимо подчеркнуть, что данный нормативный акт различает между собой понятия «коммерческая тайна» и «информация, составляющая коммерческую тайну. Так, в ст. 3 под коммерческой тайной понимается режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. Информацию,

[205] Волженкин Б.В. Преступления в сфере экономической деятельности по уголовному праву России. М.: Юридический центр Пресс, 2007. С. 461.

составляющую коммерческую тайну, закон определяет следующим образом: «Сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введён режим коммерческой тайны[206].

Как видим, законодатель достаточно подробно описал признаки, по которым ту или иную информацию следует относить к коммерческой тайне. Представляется, что логика законодателя при описании данных понятий вполне очевидна – тайна действительно является правовым режимом, накладывающим определённые ограничения и запреты на свободный доступ такой информации; при определении же понятия информации, составляющей коммерческую тайну, законодатель исходит из признаков, по которым можно обличить данный вид сведений. Таким образом, можно определить, что тайна применительно к коммерческой тайне устанавливает правовой режим, а понятие информации несёт в себе содержательный аспект сведений, которые должны подпадать под режим коммерческой тайны.

В коммерческом обороте персональные данные нередко подпадают под режим коммерческой тайны. В некоторых случаях, совпадение правовых режимов, действующих в отношении той или иной информации, на практике может вызывать определённые проблемы в правоприменении. Так, в целях исполнения Федерального закона «О противодействии коррупции» Правительством РФ был принят соответствующий пакет подзаконных актов, который предусматривал, что ряд должностных лиц компаний с государственным участием (созданных для выполнения задач, поставленных перед Правительством РФ) обязаны (по аналогии с государственными

[206] Федеральный закон «О коммерческой тайне» от 29.07.2004 №98-ФЗ // СЗ РФ. 2004. №32. Ст. 3283.

служащими и лицами, замещающими государственные должности) ежегодно публиковать в открытом доступе сведения об имуществе, а также о доходах и обязательствах имущественного характера [207] . Однако Постановлением Правительства РФ от 25.03.2015 №276[208] в указанный нормативный акт были внесены существенные изменения, и главы двадцати трёх подконтрольных государству акционерных обществ и члены их семей исключены из перечня лиц, обязанных публиковать сведения имущественного характера в открытом доступе. Таким образом, лица, которые по своему правовому статусу, по существу, были приравнены к государственным служащим, перестали нести бремя отчётности перед общественностью. Средства массовой информации связывали такое изменение с тем, что акты Правительства нарушали режим коммерческой тайны в отношении такой информации: «Само наличие государства в качестве акционера не меняет статус компании как коммерческой структуры. При этом, топ-менеджмент госкомпаний обязан предоставлять данные в Правительство РФ, но они являются в том числе коммерческой тайной»[209].

По данному вопросу существуют и другие мнения: «Сравнение с коммерческой тайной некорректно, так как сделать выводы о бизнес-процессах на базе подобной информации нельзя. Скорее, это можно считать персональными данными (с соответствующими правовым режим – прим.), но тогда не понятно, в чём заключается разница между компаниями с госучастием и, например, госкорпорациями, как «Ростех» и ВЭБ»[210].

Представляется, что отнесение той или иной совокупности персональных данных к коммерческой тайне должно быть обоснованным с

---

[207] Постановление Правительства РФ «О представлении гражданами, претендующими на замещение должностей в организациях, созданных для выполнения задач, поставленных перед Правительством Российской Федерации, и работниками, замещающими должности в этих организациях, сведений о доходах, расходах, об имуществе и обязательствах имущественного характера, проверки достоверности и полноты представляемых сведений и соблюдения работниками требований к служебному поведению от 22.07.2013 №613 // СЗ РФ. 2013 №30 (часть II). Ст. 4121.

[208] Постановление Правительства РФ «О внесении изменений в Постановления Правительства РФ от 22.07.2013 №613 и от 18.12.2014 №1405» от 25.03.2015 №276 // СЗ РФ. 2015. №14. Ст. 2122.

[209]Государственная зарплатная тайна [Электронный ресурс]: http://www.vedomosti.ru/newspaper/articles/2015/03/30/gosudarstvennaya-zarplatnaya-taina

[210] Топ-менеджеров сохранили в тайне [Электронный ресурс]: http://kommersant.ru/doc/2698251

позиций обеспечения безопасности наиболее важных охраняемых систем в государстве и с позиций соблюдения баланса частных и публичных интересов. Безусловно, сведения о доходах и расходах, об имуществе и обязательствах имущественного характера в отношении лиц, являющихся работниками или топ-менеджерами компаний с государственным участием, представляют собой персональные данные и, по общему правилу, отнесение их к той или иной разновидности тайны (в том числе и коммерческой) должно определяться самими субъектами. Но статус компании, которая обеспечивает выполнение публичных интересов и финансируется за счёт средств государственного бюджета, обусловливает и специальные меры социальной ответственности в отношении топ-менеджеров и работников данной компании, так как возможные злоупотребления и хищения с их стороны могут угрожать всей системе общественных отношений и интересам государства, а не только отдельно взятой компании. Исходя из этого, запреты и ограничения, которые были установлены в отношении топ-менеджеров компаний с государственным участием, по нашему мнению, были мало связаны с содержанием коммерческой тайны и обеспечивали публичные интересы государства в большей мере, чем в настоящее время.

Анализ уголовных дел с квалификацией преступного деяния по ст. 183 УК РФ, где предметом выступали персональные данные, показал, что чаще всего режим коммерческой тайны в таких случаях нарушается в отношении следующего вида персональных данных:

1. Персональные данные клиентов коммерческих фирм, которые постоянно или временно поддерживают связь с коммерческой организацией и пользуются услугами (работами) данной организации;
2. Персональные данные физических лиц – партнёров коммерческой организации, которые на паритетных или иных началах сотрудничают с организацией.

3. Персональные данные третьих лиц, которые прямо или косвенно могут влиять на конкурентоспособность организации в торговом обороте.

Очевидно, что все эти указанные виды персональных данных обладают для организации важнейшим признаком, позволяющим устанавливать в отношении них режим коммерческой тайны, - они помогают организации периодически или постоянно извлекать прибыль, избегать неоправданных расходов или же получать иную выгоду имущественного характера и именно поэтому являются особо ценными. С другой стороны, персональные данные, подпадающие под режим коммерческой тайны, могут содержать в себе сведения, которые, помимо всего прочего, ещё и составляют личную или семейную тайну.

В литературе высказывается мнение, 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» [211] . Следует констатировать, что судебно-следственная практика восприняла данную позицию, и незаконное отчуждение клиентских баз действительно квалифицируется по ст. 183 УК.

Так, приговором Октябрьского районного суда г. Новосибирска П. и К. были признаны виновными в совершении преступления, предусмотренного ч. 3 ст. 183 УК РФ. Судом было установлено, что у П., исполняющей обязанности руководителя отдела оптовых и розничных продаж, и К., менеджера региональных продаж, работающих в организации ,

[211] 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.

осуществляющей предпринимательскую деятельность по оптовой торговле, возник умысел на незаконное использование клиентской базы организации, в которой они осуществляли свою деятельность. С целью совершения преступления они создали коммерческую организацию, в которой заняли руководящие должности. Для ведения хозяйственных операций ими была установлена на персональный компьютер клиентская база их первоначального места работы, которая была им доверена в связи со служебной деятельностью. Осуществляя деятельность по торговле керамическими изделиями и посудой, П. и К., таким образом, заключали договоры купли-продажи с лицами, являвшимися клиентами организации – их прежнего места работы. Таким образом, П. и К. незаконно воспользовались сведениями, составляющими коммерческую тайну[212].

Кроме того, В.Г. Степанов-Егиянц предлагает относить к персональным данным, подпадающим под режим коммерческой тайны, в том числе и логины и пароли (учётно-регистрационные данные) абонентов организации, необходимые для доступа в интернет, но только в том случае, если они отнесены потерпевшей организацией к коммерческой тайне[213].

Представляется, что любая клиентская база коммерческой организации или индивидуального предпринимателя, содержащая персональные данные лиц, которые пользовались услугами или работами указанных субъектов хозяйственной деятельности, подпадает под режим коммерческой тайны независимо от соблюдения или несоблюдения данным субъектом правил и режима коммерческой тайны. Это связано, в первую очередь, с тем, что такой режим в виде ограничений и запретов устанавливается законом с целью обеспечения безопасности экономической деятельности субъектов, осуществляющих извлечение прибыли. Продажа, передача или иное неправомерное использование клиентской базы

---

[212] Приговор Октябрьского районного суда г. Новосибирска по делу №1-15/11 от 04.07.2011 [Электронный ресурс]: http://www.gcourts.ru/case/6510527

[213] Степанов-Егиянц В.Г. Проблемы разграничения неправомерного доступа к компьютерной информации со смежными составами // Право и кибербезопасность. 2014. №2(5). С. 31.

хозяйствующего субъекта в любом случае влечёт за собой причинение ущерба его интересам, так как «уход» клиентов означает отток капитала, «уход» дохода, удаление возможности получить какую-либо иную выгоду имущественного характера. Таким образом, полагаем, что режим коммерческой тайны в отношении клиентских баз коммерческих организаций распространяется в силу установленных законодательных признаков.

Понятие **банковской тайны**, как и любой иной охраняемой законом тайны, установлен в действующем законодательстве. В частности, статья 26 Федерального закона «О банках и банковской деятельности» устанавливает, что кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону [214]. Режимный характер банковской тайны выражается в системе ограничений и запретов, предусмотренных этой же статьёй федерального закона. Так, установлено, что справки о состоянии счетов физических лиц могут выдаваться, например, органам предварительного следствия по делам, находящимся в их производстве, только при наличии согласия руководителя следственного органа; по запросу суда в рамках рассмотрения гражданского или уголовного дела; в случае проверки в соответствии с Федеральным законом «О противодействии коррупции сведений о доходах, об имуществе и обязательствах имущественного характера указанных категорий граждан и т.д.

Кроме того, о режимности банковской тайны можно судить, исходя из того, что она относится к одному из видов профессиональной тайны,

[214] Федеральный закон «О банках и банковской деятельности» от 02.12.1990 №395-I // Ведомости СНД РСФСР. 1990. №27. Ст. 357.

отнесённой в соответствии с Указом Президента РФ от 06.03.1997 №188 к перечню сведений конфиденциального характера[215].

В литературе также ведутся множественные споры о том, к какому виду конфиденциальной информации следует относить сведения, составляющие банковскую тайну. Так, одни исследователи полагают, что «банковскую тайну необходимо относить к разновидности коммерческой тайны, поскольку это напрямую следует из Указа Президента»[216]. Другие относят банковскую тайну к конфиденциальной информации юридических лиц наряду со служебной и коммерческой тайной[217]. Третьи предлагают считать банковскую тайну в качестве самостоятельной разновидности конфиденциальной информации[218].

По нашему мнению, банковская тайна, вытекая из содержания законодательно установленных ограничений и запретов в отношении конкретного вида информации, обладает специфическим характером, позволяющим говорить о самостоятельном характере режимности данной информации. Такая специфичность связана с тем, что под режим банковской тайны подпадают сведения о банковских счетах, операциях, вкладах, которые не могут свободно распространяться в гражданском обороте в силу социальной значимости этой информации для граждан и организаций. Именно поэтому система ограничений и запретов в отношении указанных сведений позволяет говорить о самостоятельном правовом режиме банковской тайны.

С позиций уголовно-правовой охраны, нарушение режима банковской тайны влечёт установление различных мер юридической ответственности, в

---

[215] Указ Президента РФ от 06.03.1997 №188 «Об утверждении перечня сведений конфиденциального характера» // СЗ РФ. 1997. №10. Ст. 1127.

[216] Гостев И.М. Информационное право: вопросы законодательного регулирования // Технологии и средства связи. 1997. №1. С. 98-102.

[217] Крылов В.В. Информационные преступления – новый криминалистический объект // Российская юстиция. 1997. №4. С. 25-28.

[218] См., например: Лопатин В. Информационная безопасность России. Человек. Общество. Государство. – СПб., 2000. - С. 12; Саврасова В.А. Банковская тайна в системе конфиденциальной информации // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2012. №10(24), часть вторая. С. 158.

том числе и уголовной. На наш взгляд, информацию о банковских счетах и вкладах, а также любую другую информацию банковского характера применительно к гражданину можно отнести к разновидности персональных данных. Соответственно, они будут являться персональными данными, подпадающими под правовой режим банковской тайны и подлежать уголовно-правовой охране по ст. 183 Уголовного кодекса РФ.

Режимный характер банковской тайны, в то же время, в некоторых случаях может создавать правовые препятствия в реализации других важных элементов действующей законности и правопорядка, поскольку с использованием правовых ограничений и запретов на свободное распространение данного вида информации может быть связана невозможность пресечения различного рода мошеннических действий.

В связи с этим высказывается мнение о том, что необходимо смягчить правовой режим ограничений и запретов, установленный банковской тайной, путём введения правовой нормы о возможности обмена банковской информацией при расследовании и пресечении случаев кибермошенничеств с неправомерным использованием персональных данных, входящих в структуру банковской информации. Кроме того, в средствах массовой информации указывается, что на практике обмен банковской информацией фактически уже существует, однако осуществляется незаконно[219].

Полагаем, что при обсуждении целесообразности введения подобной нормы в законодательство Российской Федерации следует исходить из принципа достаточной необходимости для ограничения действия сразу нескольких правовых институтов: с одной стороны, правового режима банковской тайны, а с другой – правового режима конфиденциальности персональных данных. Оба указанных режима в подобных правоотношениях являются объектами повышенной охраны, и их нарушение может повлечь за собой нарушение большего числа правоотношений. Кроме того, факт

[219] ЦБ может пожертвовать банковской тайной [Электронный ресурс]: http://www.vedomosti.ru/finance/articles/2016/02/18/630132-tsb-mozhet-pozhertvovat-bankovskoi-tainoi

мошеннических действий может устанавливаться только правоохранительными органами, так как именно ими и возбуждаются уголовные дела по соответствующей квалификации. Следуя данной логике, представляется, что единственным законным механизмом обеспечить безопасность банковской информации от преступных посягательств в рамках действующих правовых режимов её конфиденциальности будет запрос правоохранительного органа, основанного на судебном решении, в связи с расследуемым уголовным делом, тем более что это положение уже содержится как в норме Федерального закона «О банках и банковской деятельности» (ст. 26), так и в нормах Федерального закона «О персональных данных» (ч. 8 ст. 14).

Кроме того, на сегодняшний день обсуждается иной механизм обеспечения защиты режима банковской тайны и конфиденциальности персональных данных через расширение перечня оснований для истребования соответствующего вида информации[220].

Правоприменительная практика в Российской Федерации, по существу, признаёт, что если персональные данные входили в состав сведений, составляющих банковскую тайну, то в данном случае, в первую очередь, в уголовно-правовом смысле страдают интересы хозяйствующих субъектов.

Так, в г. Сосновый Бор Ленинградской области был вынесен приговор экономисту отдела по работе с физическими лицами банка «Таврический», признанного виновным в совершении преступления, предусмотренного ч. 2 ст. 183 УК РФ. Судом в ходе рассмотрения дела было установлено, что сотрудник банка в силу своего служебного положения имел доступ к конфиденциальной информации, содержащей персональные данные клиентов банка, сведения о состоянии их лицевых счетов, но был обязан обеспечивать закрытость указанной информации. Злоупотребив своим

[220] См., например: Центробанку расширят возможности по истребованию резервных копий клиентских баз [Электронный ресурс]: http://pravo.ru/news/view/126358

служебным положением, в целях взыскания в свою пользу долга с гражданина он получил сведения о состоянии счёта указанного лица и предоставил их в ОМВД России г. Сосновый Бор Ленинградской области[221].

Необходимо понимать, что в рассматриваемом случае пострадал не только так называемый «экономический объект посягательства», но и «интересы личности гражданина», чья информация о банковском счёте была неправомерно использована. На наш взгляд, в подобных случаях персональные данные выступают объединяющей категорией между различными объектами посягательства. С одной стороны, субъект, совершая данное преступление, нарушает законодательство о банках и банковской деятельности, так как произвольное и несанкционированное использование банковской информации о гражданине запрещено законом. С другой стороны, нарушается право гражданина на сохранение в тайне сведений о нём, которые в силу закона не могут свободно распространяться.

В литературе высказывалось мнение, что «банковскую тайну необходимо отнести к разновидности тайны частной жизни»[222]. С этим, по существу, соглашается Д.Ю. Гришмановский, указывая, что «разглашение сведений о клиенте банка, о его банковских операциях и счетах может нарушить право частной жизни»[223]. На наш взгляд, режимом банковской тайны могут охватываться сведения, которые относятся к персональным данным, составляющим, помимо всего прочего, тайну частной жизни. Но это, скорее, исключение, частный случай, чем общее правило. Поэтому уголовно-правовая охрана персональных данных, входящих в состав информации, подпадающей под режим банковской тайны, зависит также от режимности указанной информации – от установленных ограничений и запретов, предусмотренных действующим законодательством.

---

[221] В городе Сосновый Бор Ленинградской области вынесен приговор бывшему служащему банка за разглашение банковской тайны [Электронный ресурс]: http://prokuratura-lenobl.ru/news/lo/6436

[222] Таланпойка В., Шабалин В. Право на тайну // Гражданская защита. 1999. №4. С. 33.

[223] Гришмановский Д.Ю. Банковская тайна и проблемы доступа к ней органов расследования // Антология научной мысли: к 10-летию Российской академии правосудия. Сборник статей. М.: Статут, 2008. С. 193-197.

Наконец, последний вид тайн, который охраняется статьёй 183 УК РФ, - это **налоговая тайна**. В статье 102 Налогового кодекса РФ содержится легальное определение налоговой тайны, под которой понимаются любые полученные налоговым органом, органами внутренних дел, следственными органами, органом государственное внебюджетного фонда и таможенным органом сведения о налогоплательщике, за исключением сведений: являющихся общедоступными, в том числе ставшими такими с согласия их обладателя; об идентификационном номере налогоплательщик; о нарушениях законодательства о налогах и сборах и мерах ответственности за эти нарушения и т.д.[224]. Ограничения и запреты правового характера, которые установлены в отношении сведений, составляющих налоговую тайну, по существу, выражаются в запрете указанным в законе должностным лицам свободно передавать и распространять её. При этом Приказом МНС РФ от 03.03.2003 №БГ-3-28/96 установлен Порядок доступа к конфиденциальной информации налоговых органов. В частности, пунктом 12 предусмотрено, что не допускается предоставление налоговыми органами баз, банков данных, архивов, списков налогоплательщиков и работников налоговых органов, содержащих конфиденциальную информацию, за исключением случаев, предусмотренных федеральным законом[225]. Таким образом, законодатель и правоприменительные органы определяют режим конфиденциальности сведений, составляющих налоговую тайну посредством установления запретительных механизмов в отношении данной информации.

Как и в предыдущих случаях, налоговая тайна представляет собой не что иное, как правовой режим информации. Но вопрос о содержании этого правового режима в научной литературе является дискуссионным.

Так, П.У. Кузнецов относит налоговую тайну к разновидности профессиональной тайны или называет её «специальным условием правового

[224] Налоговый кодекс Российской Федерации. Часть 1 от 31.07.1998 №146-ФЗ (в ред. фед. закона от 04.10.2014) // СЗ РФ. 1998. №31. Ст. 3824.

[225] Приказ МНС РФ «Об утверждении порядка доступа к конфиденциальной информации налоговых органов» от 03.03.2003 №БГ-3-28/96 // Бюллетень нормативных актов федеральных органов исполнительной власти. 2003. №23.

режима профессиональной тайны» [226] . По мнению А.В. Торшина, «в отношении налоговой тайны законодатель определяет не перечень информации или сведений, составляющих налоговую тайну, а так называемые её **конфиденты**, то есть физические лица и организации, которым в силу профессиональной деятельности, по договору или на ином законном основании становятся известными сведения, которые они обязаны сохранять»[227]. Соглашаясь с ним, Е.В. Шеховцева, вместе с тем, полагает, что «при установлении режима налоговой тайны законодатель указывает в качестве её конфидентов не коммерческие организации, а соответствующие государственные органы и их должностные лица, а также привлекаемые ими специалисты и эксперты»[228].

Полагаем, что правовой режим налоговой тайны применительно к охране персональных данных обусловлен содержанием сведений, которые входят в это понятие. Так, сведения о состоянии счетов налогоплательщиков - физических лиц, их задолженности или переплаты по налогам и сборам с указанием идентификационных данных тоже являются персональными данными, сведениями конфиденциального характера, доступ к которым ограничен под режимом налоговой тайны. А поскольку статья 183 УК РФ посвящена, в том числе охране налоговой тайны, то на практике правоприменительные органы используют данную статью при рассмотрении дел, связанных с неправомерным использованием сведений, составляющих налоговую тайну.

В частности, кассационным определением судебной коллегии по уголовным делам Пермского краевого суда по делу №22-4187-2011 квалификация действий осуждённого К. по ч. 3 ст. 183 УК РФ была признана правомерной. Приговором суда первой инстанции было установлено, что К., будучи сотрудником инспекции Федеральной налоговой службы, имея

---

[226] Кузнецов П.У. Основы информационного права. М.: Проспект, 2014. С. 256.

[227] Торшин А.В. Соотношение налоговой тайны с другими режимами защиты конфиденциальной экономической информации // Финансовое право. 2002. №1.

[228] Шеховцева Е.В. Налоговая тайна: правовой режим охраны // Ленинградский юридический журнал. 2013. №1.

допуск к сведениям, составляющим налоговую тайну, и будучи предупреждённым об ответственности за разглашение указанных сведений, за вознаграждение передал сведения о налогоплательщике сотруднику УФСБ, действующему в рамках оперативно-розыскного мероприятия «контрольная закупка». В переданном информационном материале содержались сведения конфиденциального характера, в частности: персональные данные налогоплательщиков, состояние их задолженностей по налогам и сборам, а также лицевые счета[229].

Следует отметить, что по данным ресурса rospravosudie.com количество уголовных дел по ст. 183 УК РФ, связанное с нарушением режима налоговой тайны, а также посредством незаконного использования персональных данных, ничтожно мало по сравнению с числом преступлений, посягавших на режим коммерческой или банковской тайны.

Итак, вышеприведённый анализ показал, что преступные посягательства в отношении персональных данных по своим объектам весьма разнообразны. И это разнообразие проявляется в том, что уголовно-правовая охрана персональных данных по российскому уголовному закону обусловлена правовым режимом, под который до момента совершения соответствующего преступления подпадали персональные данные. Необходимо также отметить, что в этом контексте анализ преступлений, предусмотренных ст.ст. 137 и 183 осуществлён, исходя из сложившейся судебной практики в случае совершения преступных посягательств в отношении персональных данных.

Правовой режим определяется в научной литературе по-разному. Правовой режим определяется как «особый порядок правового регулирования, выражающийся в определённом сочетании юридических средств и создающий желаемое социальное состояние и конкретную степень благоприятности или неблагоприятности для удовлетворения интересов

[229] Кассационное определение Пермского краевого суда от 30.06.2011 по делу №22-4187-2011 [Электронный ресурс]: https://rospravosudie.com/court-permskij-kraevoj-sud-permskij-kraj-s/act-103608751/

субъектов права»[230]. О.С. Родионов понимает под правовым режимом «совокупность юридических средств, устанавливаемых и обеспечиваемых государством в целях урегулирования конкретных общественных отношений путём ограничения одних и стимулирования деятельности отдельных субъектов права»[231].

Совокупность ограничений и запретов (так называемых правил безопасности) Н.В. Щедриным именуется «режимом безопасности». При этом к режимам мер безопасности можно, в частности, отнести: административный надзор за лицами, освобождёнными из мест лишения свободы; профилактический учёт несовершеннолетних правонарушителей; режим гостайны[232].

Полагаем, что следует признать позицию, в соответствии с которой правовой режим обусловливает существование системы мер-дозволений, мер-ограничений и мер-запретов в отношении конкретного вида правоотношений и по поводу конкретного объекта. В нашем случае объектом, в отношении которого применяются эти меры, будут являться персональные данные, которые по своему содержанию представляют собой информацию, подпадающую под специальные режимы ограничений и запретов.

Л.К. Терещенко определяет правовой режим информации как «объектный режим, позволяющий обеспечить комплексность воздействия посредством совокупности регулятивных, охранительных, процессуально-процедурных средств, характеризующих особое сочетание дозволений, запретов и обязываний. При этом указанный правовой режим имеет специфический объект – информацию в её нематериально-правовом смысле»[233]. Кроме того, «различные виды тайн (личной и семейной,

---

[230] Матузов НИ., Малько А.В. Правовые режимы: вопросы теории и практики // Правоведение. 1996. №1.
[231] Родионов О.С. Правовые режимы как важнейший элемент юридической политики // Правоведение. – 1997. - №4. – С. 157.
[232] Щедрин Н.В. Введение в правовую теорию мер безопасности: Монография. Красноярск: Краснояр. гос. ун-т, 1999. С. 102.
[233] Терещенко Л.К. Правовой режим информации. Дисс. … доктора юрид. наук. М., 2011. С. 123.

коммерческой, банковской, налоговой и т.д.), как и конфиденциальность информации, необходимо рассматривать в качестве специальных правовых режимов информации, так как они предусматривают ограничение доступа; запрет на передачу третьим лицам без согласия обладателя информации; возможность, по общему правилу, обладателя информации самостоятельно решать вопрос о сохранении конфиденциальности; производный характер обязанности по сохранению конфиденциальности информации»[234].

Подчеркнём, что тайна является именно правовым режимом, устанавливающим ограничения и запреты в отношении персональных данных, поскольку именно понятие режима подразумевает под собой систему ограничений и запретов.

Актуальность борьбы с преступлениями, которые совершаются с неправомерным использованием персональных данных, с каждым годом возрастает, поскольку в мире идёт непрерывное развитие информационных технологий, и целый комплекс прав личности в связи с этим всё труднее становится обеспечить надлежащей правовой охраной.

Трудности могут возникать при разрешении некоторых конкретных ситуаций, возникающих на практике, и чаще всего это связано с множеством правовых норм, которые могут регулировать один и тот же правовой институт, но совершенно в различных аспектах и с совершенно различными последствиями и правовыми режимами для участников правоотношений.

Проблема отграничения преступлений от иных правонарушений всегда остро формулируется в уголовном праве особенно тогда, когда появляется новый вид общественных отношений, ранее не подпадавших под уголовно-правовую охрану. Но в теории уже достаточно давно выработана позиция, согласно которой главное отличие преступления от иных правонарушений заключается в различной степени общественной опасности данных деяний. При этом общественная опасность признаётся материальным

[234] Там же. С. 323.

признаком преступления, раскрывающим его социальную сущность, которая определяется через:

1. Оценку значимости тех или иных событий;
2. Характера и объёма причинённого вреда объектами уголовно-правовой охраны;
3. Особенностей преступного деяния;
4. Особенностей пола, возраста, должностного положения субъекта[235].

Преступления являются наиболее опасными видами противоправных деяний, которые причиняют вред самым важным видам общественных отношений, являются основополагающими для существования всей системы государства и права. Отсюда бесспорным является положение о том, что административные правонарушения хотя и также обладают определённой общественной опасностью, которую можно оценить как по характеру, так и по степени, тем не менее, они являются менее опасными по сравнению с преступлениями[236].

Как указывает Е.В. Кобзева, «современное российское законодательство создаёт массу коллизионных и пробельных ситуаций, связанных с соотношением преступлений и административных правонарушений. Большая роль в их возникновении принадлежит законодательной технике. Охранительные функции уголовного и административного права не позволяют дать предпочтение какой-либо одной из них в преодолении проблем коллизионного характера. Поэтому такие коллизии необходимо всячески устранять»[237].

---

[235] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Под ред. А.В. Бриллиантова. М.: Проспект, 2015. С. 43.

[236] Лунев А. Е. Административная ответственность за правонарушения. М., 1961. С. 33-35.

[237] Кобзева Е.В. Разграничение преступлений и административных правонарушений: роль законодательной техники // Соотношение преступлений и иных правонарушений: Материалы четвёртой международной научно-практической конференции, посвящённой 250-летию образования Московского гос. ун-та. М.: ЛексЭст, 2005. С. 225.

Нельзя не согласиться с таким мнением, тем более, когда законодатель осуществляет активную работу над проектом нового Кодекса РФ об административных правонарушениях[238].

Правовой охране персональных данных институтом административного права посвящены две статьи действующего Кодекса Российской Федерации об административных правонарушениях, в частности:

1. Статья 13.11 «Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)»;
2. Статья 13.14 «Разглашение информации с ограниченным доступом».

Очевидно, что оба правонарушения связаны с нарушением определённых правил, порядка, предусмотренного действующим профильным информационным законодательством. Но для целей разграничения института административной и уголовной ответственности в отношении посягательства с использованием персональных данных следует проанализировать положения данных норм.

Статья 13.11 КоАП РФ посвящена правовой охране предусмотренного законом порядка оборота персональных данных. При этом данная норма по объективной стороне охватывает широкий спектр альтернативных действий, среди которых: сбор, хранение, использование и распространение информации о гражданах. По существу, данная норма КоАП РФ закрепляет, что установленный порядок оборота персональной информации имеет повышенную ценность для действующей системы общественных отношений и определяет, таким образом, сферу ответственности за его нарушение. Поэтому нарушение правил оборота персональных данных через любой альтернативный признак, регулируемый Федеральным законом «О персональных данных» позволяет привлекать к административной ответственности любое лицо, которое нарушило эти правила. При этом данная норма совершенно не зависит от правового режима персональных

[238] КоАП получил замечания по всем статьям [Электронный ресурс]: http://pravo.ru/court_report/view/125551

данных, правила работы с которыми могут быть потенциально нарушенными.

Статья 13.14 КоАП РФ, в свою очередь, посвящена правовой охране информации с ограниченным доступом и, по существу, предусматривает ответственность за нарушение режима безопасности информации, доступ к которой ограничен федеральным законом. Представляется логичным исключение этой нормой из состава регулирования случаев, когда разглашение такой информации влечёт уголовную ответственность, поскольку это исключает необоснованную двойную юридическую ответственность за одно и то же деяние. Именно это и было сделано законодателем в Федеральном законе «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 07.02.2017 №13-ФЗ, где в качестве разграничивающего признака была добавлена формулировка в ч. 1 ст. 13.11 «если эти действия не содержат уголовно наказуемого деяния»[239].

Можно прийти к выводу, что правовая охрана общественных отношений, складывающихся между субъектами по поводу установленного законом оборота персональных данных, осуществляется ситуационно, с целью охраны информационных правоотношений нежели прав и свобод человека и гражданина.

В то же время, если обратиться к положениям норм Уголовного кодекса РФ об уголовной ответственности за преступные посягательства в отношении персональных данных, то можно обнаружить, что все они осуществляют уголовно-правовую охрану личных прав человека, обеспечиваемых посредством персональных данных, исключительно сквозь призму конкретного информационно-правового режима безопасности, и нарушение такого режима, как правило, связано с нарушением правил работы с персональными данными.

---

[239] Федеральный закон «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» от 07.02.2017 №13-ФЗ // СЗ РФ. 2017. №7. Ст. 1032.

Так, статья 137 УК РФ посвящена уголовно-правовой охране неприкосновенности частной жизни и запрещает под угрозой применения уголовной ответственности незаконное собирание или распространение персональных данных, составляющих личную и семейную тайну, либо распространение таких сведений. Охране подлежит не вся персональная информация, а только та, которая подпадает под правовой режим личной и семейной тайны.

Таким образом, нормы, посвящённые административной и уголовной ответственности за посягательства в отношении персональных данных, существенным образом различаются между собой, так как нормы КоАП РФ устанавливают ответственность за нарушение порядка работы с персональными данными, а нормы УК РФ – за нарушение неприкосновенности персональных данных, подпадающих под соответствующий правовой режим охраны.

В качестве рабочей гипотезы автором изначально выдвигалось предположение о том, что в системе действующих уголовно-правовых норм могли бы появиться специальные нормы, осуществляющие уголовно-правовую охрану персональных данных. Однако в процессе осуществления исследования по данной проблематике указанная гипотеза не получила своего подтверждения в связи со следующим.

Обоснование введения той или иной уголовно-правовой нормы в уголовный закон осуществляется с помощью положений, выдвинутых теорией криминализации. Как указывает А.Д. Антонов, «криминализация, являясь главной составляющей уголовно-правовой политики, представляет собой «объявление общественно опасных деяний преступлением»[240]. Именно теория криминализации вырабатывает основания и принципы появления в уголовном законе новых норм, осуществляющих охрану соответствующих объектов.

[240] Антонов А.Д. Теоретические основы криминализации // Чёрные дыры в российском законодательстве. 2002. №2.

В литературе на сегодняшний день нет единства мнений по поводу того, каким образом осуществляется криминализация соответствующих деяний в качестве преступных. Об этом ведётся множество научных дискуссий.

Так, Н.А. Лопашенко полагает, что «криминализация деяний должна исходить из причин, оснований и принципов. При этом в качестве основания рассматривается существование общественно опасного поведения, которое требует уголовно-правового запрета»[241].

А.И. Коробеев большое внимание уделяет основаниям криминализации, выделяя из них следующие:

«1. Юридико-криминологические основания (степень общественной опасности; распространённость и типичность деяний; динамика деяний с учётом порождающих причин и условий; возможность воздействия на них уголовно-правовыми средствами при отсутствии возможности борьбы иными мерами, а также возможности системы уголовной юстиции);

2. Социально-экономические основания (причиняемый деяниями ущерб; отсутствие негативных последствий уголовно-правового запрета; наличие материальных ресурсов для его реализации);

3. Социально-психологические основания (уровень общественного правосознания и психологии; исторические традиции)»[242].

А.Д. Антонов предлагает аналогичную систему оснований криминализации, однако, представляет несколько иное содержание тех же групп оснований[243].

Полагаем, что следует согласиться с выделением указанных выше нескольких групп оснований криминализации соответствующих деяний, поскольку уголовно-правовая охрана соответствующих отношений должна осуществляться при наличии объективных предпосылок. Криминализация не

---

[241] Лопашенко Н.А. Уголовная политика / Н.А. Лопашенко. М.: Волтерс, 2009. С. 96.

[242] Коробеев А.И. Советская уголовно-правовая политика: проблемы криминализации и пенализации. Владивосток: Изд-во ДВГУ, 1987. С. 69-88.

[243] Антонов А.Д. Теоретические оснований криминализации и декриминализации: Дисс. … канд. юрид. наук. М., 2001. С. 96-110.

может иметь под собой только одно основание, так как преступное деяние наносит ущерб всей системе общественных отношений.

Немаловажным фактором при обосновании криминализации соответствующего деяния является отсутствие её избыточности вследствие введения новой уголовно-правовой нормы в действие, как и достаточность криминализации. «Беспробельность» и «неизбыточность» криминализации называются А.Д. Антоновым «системными принципами криминализации». В качестве примера избыточной криминализации автор приводит содержание ст. 213 УК РФ (на тот момент понятие хулиганства включало в себя нарушение общественного порядка, сопровождающееся уничтожением или повреждением чужого имущества), пока как ч. 1 ст. 167 УК РФ уже предусматривает уголовную ответственность за умышленное уничтожение или повреждение чужого имущества[244].

Если в целях проверки изначально выдвинутой рабочей гипотезы о том, что преступные посягательств в отношении персональных данных нуждаются в криминализации, произвести анализ с позиций теории криминализации, то можно прийти к ряду выводов.

Во-первых, ранее мы уже обосновывали, что посягательства в отношении персональных данных имеют высокую степень общественной опасности, поскольку, с одной стороны, нарушают не только право на неприкосновенность частной жизни, но и ряд других конституционных прав. Во-вторых, в последние годы преступные посягательства в отношении персональных данных только усиливают динамику. Как показывает статистика, всё большее число лиц становятся потерпевшими вследствие похищения их персональных данных, а также жертвами иных преступлений, которые были совершены посредством незаконного использования персональных данных. В-третьих, преступные посягательства в отношении персональных данных наносят серьёзный ущерб не только самим субъектами

[244] Антонов А.Д. Теоретические основы криминализации // Чёрные дыры в российском законодательстве. 2002. №2.

персональных данных, но и всей системе общественных отношений. Кроме того, введение мер уголовно-правового воздействия на преступные посягательства в отношении персональных данных упорядочивает систему общественных отношений по поводу законного их оборота и использования.

В то же время, нами было установлено, что персональные данные могут подпадать под различные правовые режимы конфиденциальности (личной и семейной тайны, коммерческой тайны, банковской тайны, налоговой тайны). Вследствие этого, опасность угрожает только той разновидности персональных данных, которые являются конфиденциальными – сохранение тех или иных сведений в тайне является залогом сохранения системы общественных отношений.

При введении специальной уголовно-правовой охраны преступных посягательств в отношении персональных данных неизбежно возникает избыточность криминализации. Это, в первую очередь, связано с тем, что соответствующие правовые режимы конфиденциальности персональных данных уже подпадают под уголовно-правовое воздействие посредством соответствующих норм Уголовного кодекса РФ (ст. 137, ст. 183).

Кроме того, представляется, что была бы необоснованной и неоправданной криминализация таких посягательств в отношении персональных данных, которые бы не нарушали соответствующего режима их конфиденциальности – выше мы установили, что достаточно большой объём персональных данных может не подпадать под ограниченный доступ в случаях, установленных законом. Между тем, общественная опасность для таких деяний в уголовно-правовом смысле отсутствует, а нарушение правил работы с персональными данными уже является объектом охраны со стороны норм административного права (ст. 13.11 и ст. 13.14).

Таким образом, выделение специальной нормы, посвящённой уголовной ответственности за преступные посягательств в отношении персональных данных с позиций теории криминализации являлось бы

нецелесообразным и говорило бы об избыточности уголовно-правового регулирования.

Правовой режим персональных данных является решающим фактором в обосновании их уголовно-правовой охраны. Ранее мы рассматривали вопрос о том, что режимный характер информационных правоотношений обусловлен, во многом, тем, что законодательство Российской Федерации устанавливает специальные правовые ограничения и запреты в отношении различных видов информации. Следовательно, охранительное уголовное правоотношение (которое принято рассматривать как один из этапов уголовно-правового воздействия [245]) в отношении персональных данных не может возникнуть, если не нарушено правило безопасности (ограничение или запрет), установленное специальным правовым режимом персональных данных – режимом личной или семейной тайны, режимом коммерческой, банковской, налоговой тайны. Это и объясняет тот факт, что уголовно-правовая охрана персональных данных осуществляется в рамках установленных законом режимов тайн.

[245] Чучаев А.И., Фирсова А.П. Уголовно-правовое воздействие: монография. М.: Проспект, 2011. С. 201.

2.2. Признаки объективной стороны и вопросы квалификации преступных посягательств в отношении персональных данных

В науке уголовного права объективная сторона преступления рассматривается как важный элемент состава преступления, отсутствие которого означает и отсутствие состава преступления. При этом, даётся множество определений объективной стороны преступления. Но бесспорным является сущностный признак объективный стороны – это внешняя сторона преступления, выражение преступления «вовне», процесс преступного посягательства.

Объективная сторона преступления представляет собой внешнее проявление преступления в реальной действительности, то есть его физическую сторону[246]. Это система признаков, определяющих уголовно-правовое значение общественно опасного деяния как внешнего события или внешней деятельности субъекта преступления[247]. Объективную сторону преступления определяют также и как совокупность реально существующих обстоятельств, которые характеризуют процесс общественно опасного и противоправного посягательств на охраняемые законом интересы, рассматриваемый с его внешней стороны[248].

Следует признать, что процесс совершения преступления, который характеризуется также и определёнными субъективными признаками, не может быть рассмотрен в отрыве от конкретных обстоятельств дела. Поэтому объективная сторона, как и остальные элементы состава преступления, позволяет определить, какие деяния (в системе с последствиями или без таковых) запрещены уголовным законом, а какие состава преступления не образуют.

Законодательно установленные признаки объективной стороны, которые входят в её содержание, позволяют определить момент окончания

---

[246] Уголовное право. Общая часть: учебник / Под ред. А.Н. Тарбагаева. М.: Проспект, 2014. С. 35.
[247] Уголовное право России. Общая часть / Под ред. А.И. Рарога. М.: Эксмо, 2011. С. 94.
[248] Кудрявцев В.Н. Объективная сторона преступления. М., 1960. С. 9.

преступлений и в связи с этим разделяют преступления на несколько групп по конструкции объективной стороны. Так, по конструкции преступления принято делить на преступления с материальным составом, формальным составом и усечённым составом. Все они различаются между собой, по существу, по моменту окончания преступления, который заложен в диспозиции соответствующей статьи Особенной части Уголовного кодекса РФ.

Как пишет А.Г. Безверхов, «моментом окончания преступления следует считать обозначенный в действующем уголовном законодательстве и устанавливаемый судебной властью предел, с достижением которого уголовно-противоправное деяние становится завершённым (оконченным) преступлением» [249]. Соответственно, уголовный закон устанавливает, что конкретное преступное деяние является общественно опасным либо в связи с наступлением общественно опасных последствий, и тогда оно окончено с момента наступления этих последствий (преступление с материальным составом), либо в связи с тем, что само по себе деяние является общественно опасным, поэтому наступления последствий не требуется, а достаточно только совершить само деяние (преступление с формальным или усечённым составом).

Анализ конструкций составов преступных посягательств в отношении персональных данных показывает, что это преступления с формальным составом, и для их окончания наступление общественно опасных последствий не требуется. Так, преступление, предусмотренное ч. 1 ст. 137 УК РФ, является преступлением с формальным составом и считается оконченным с момента выполнения любого из предусмотренных действий, входящих в его объективную сторону – в данном случае это незаконное собирание или распространение сведений о частной жизни лица и т.д. Преступление, предусмотренное ч. 1 ст. 183 УК РФ, считается оконченным

[249] Безверхов А.Г. О проблеме конструирования составов преступлений по моменту окончания // Вестник Самарской гуманитарной академии. Серия «Право». 2012. №1(11). С. 71.

также с момента совершения общественно опасного деяния, а именно собирания сведений, составляющих соответствующий вид тайны.

Исключение из этого составляют особо квалифицированные составы указанных преступлений. В частности, ч. 3 ст. 137 предусматривает уголовную ответственность за незаконное распространение в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях информации, указывающей на личность несовершеннолетнего потерпевшего, не достигшего шестнадцатилетнего возраста, по уголовному делу, либо информации, содержащей описание полученных им в связи с преступлением физических или нравственных страданий, повлекшее причинение вреда здоровью несовершеннолетнего, или психическое расстройство несовершеннолетнего, или иные тяжкие последствия. В свою очередь, причинение тяжких последствий является обязательным признаком объективной стороны преступления, предусмотренного ч. 4 ст. 183 УК РФ, а ч. 3 указанной статьи предусматривает ответственность за деяния, предусмотренные ч. 1 или ч. 2, причинившие крупный ущерб.

Поскольку рассматриваемые преступные посягательства в отношении персональных данных по конструкции представляют собой преступления с формальным составом, то характеристика преступных деяний, входящих в объективную сторону преступлений, имеет важное значение для их квалификации и индивидуализации в дальнейшем ответственности за их совершение. Поэтому рассмотрим особенности деяний, входящих в объективную сторону преступных посягательств в отношении персональных данных.

Как указывается в учебной литературе, общественно опасное деяние, входящее в объективную сторону, может выражаться в форме действия (активного поведения) или бездействия (пассивного поведения). При этом общественно опасное действие имеет три характерных признака – **физический** (это совокупность определённых и взаимосвязанных между

собой телодвижений), **социальный** (действие является движущей силой совершения преступления, которая причиняет вред и оказывает влияние на соответствующие отношения) и **юридический** (это действие по своей сути является уголовно-противоправным)[250].

Итак, все рассматриваемые преступные посягательства представляют собой по объективной стороне совершение определённых общественно опасных **действий**, предусмотренных диспозициями соответствующих статей Особенной части Уголовного кодекса РФ. Иными словами, преступное посягательство в отношении персональных данных всегда совершается в форме активного человеческого поведения, направленного на достижение преступного результата.

Формы активного человеческого поведения для целей квалификации предусмотрены уголовным законом, и если обобщить их, распределив по разным группам, то можно сделать вывод, что преступные посягательства в отношении персональных данных могут совершаться посредством выполнения следующих действий:

1. Незаконное собирание персональных данных;
2. Незаконное распространение (разглашение) персональных данных;
3. Незаконное использование сведений.

В литературе предлагалось также закрепить в качестве одного из альтернативных признаков преступного посягательства в отношении информации, подпадающей под тот или иной режим конфиденциальности незаконное хранение информации, если оно предполагает дальнейшее использование или распространение сведений, составляющих тайну[251].

Как видим, признаком, объединяющим все рассматриваемые понятия, является их незаконность (неправомерность). Вопрос о незаконном характере применительно к характеризующему признаку объективной стороны

---

[250] Уголовное право. Общая часть / Под ред. А.Н. Тарбагаева. М.: Проспект, 2014. С. 67.
[251] Щепетильников В.Н. Уголовно-правовая охрана электронной информации: Автореферат дисс. … канд. юрид. наук. Рязань, 2006. С. 16.

непосредственно в Уголовном кодексе РФ не раскрывается. Более того, в отношении персональных данных, он может носить специфический характер.

Следует обратить внимание, что любое деяние, входящее в объективную сторону преступного посягательства в отношении персональных данных (собирание, распространение или разглашение, использование) должно обязательно носить неправомерный, незаконный, противоправный характер, поскольку свободный сбор персональных данных или информации как таковой может быть запрещён соответствующим режимом безопасности (конфиденциальности), например, режимом личной и семейной тайны, установленным частным лицом, или режимом банковской тайны, установленным на основании Федерального закона «О банках и банковской деятельности» и т.д. При этом незаконность или неправомерность собирания персональных данных, входящих в тот или иной режим безопасности информации, может быть обусловлена различными правовыми основаниями:

1. Для персональных данных, подпадающих под режим личной и семейной тайны, условием законности (правомерности) собирания, распространения или использования таких данных является наличие согласия лица на собирание его персональных данных (ст. 9 Федерального закона «О персональных данных»). Следует заметить, что, исходя из анализа действующего законодательства о персональных данных, законодательства об информации и информационных технологиях, незаконность сбора сведений презюмируется для каждого факта получения персональных данных о лице, за исключением случаев, если лицо дало своё согласие на сбор персональных данных. При этом Федеральный закон «О персональных данных» устанавливает также случаи, для которых либо требуется обязательное письменное согласие, либо согласие в любой иной форме, позволяющей однозначно определить, что лицо было согласно на сбор персональных данных.

2. Для персональных данных, подпадающих под правовой режим банковской, коммерческой или налоговой тайны – соответствующее положение закона, устанавливающее, что те или иные сведения подпадают под соответствующий режим конфиденциальности. Например, положения налогового законодательства о налоговой тайне, которые устанавливают перечень сведений, подпадающих под режим налоговой тайны.

Режим личной и семейной тайны ограничивает свободный доступ посторонних лиц к персональным данным любого лица, и посторонние лица не вправе собирать эти сведения, за исключением случаев, если это лицо давало в предусмотренном законом порядке согласие на собирание таких сведений, либо собирание сведений предусмотрено законом без согласия лица.

Охрана персональных данных, как и любых сведений, составляющих личную и семейную тайну, может быть обусловлена получением письменного согласия лица на сбор сведений, являющихся его персональными данными. Но письменное согласие может не требоваться в случаях, специально предусмотренных законом. В частности, ст. 10 Федерального закона «О персональных данных» предусматривает, что обработка персональных данных, то есть их обращение в информационном поле может осуществляться без согласия субъекта, например, в случае, если обработка необходима для защиты жизни, здоровья, иных жизненно важных интересов субъектов персональных данных либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия субъекта персональных данных невозможно. Таким образом, незаконность (или неправомерность) собирания, распространения или использования персональных данных применительно к целям их уголовно-правовой охраны обусловлена соответствующими законодательными ограничениями, которые запрещают свободно получать и распространять указанную информацию.

Заметим, что отсутствие согласия лица, чьи персональные данные могут распространяться или иным образом использоваться, может носить бессрочный характер, и ответственность лица наступает независимо от времени, когда персональные данные были неправомерно получены. Об этом свидетельствует и судебная практика.

Так, в г. Кирово-Чепецке направлены в суда материалы уголовного дела по обвинению З. в совершении преступления, предусмотренного ч. 1 ст. 137 УК РФ. По данным следствия, днём 14 августа 2014 года З. со своего компьютера создал учётную запись в социальной сети «Вконтакте» и открыл к ней доступ для остальных пользователей. На этой странице он разместил фотографии своей бывшей одноклассницы, на которых она изображена в обнажённом виде. По словам средств массовой информации, эти снимки были у З. ещё в то время, когда он и его одноклассница учились в школе. Когда 23-летняя девушка увидела свои приватные фотографии в сети интернет, она сразу обратилась в правоохранительные органы, так как не давала своего согласия на размещение указанных фотографий[252].

Получение согласия на обработку персональных данных позволяет смоделировать и предотвратить ситуацию, при которой в результате разглашения персональных данных, во-первых, может пострадать личное нематериальное благо физического лица – а именно право на неприкосновенность частной жизни, личной и семейной тайны; во-вторых, режим конфиденциальности (неразглашения) персональных данных фактически по умолчанию обязывает всех, кто связан с обработкой персональных данных, обеспечивать неприкосновенность таких сведений до тех пор, пока сам субъект не определит, что их конфиденциальность является излишней. Информационное самоопределение физического лица в отношении сведений о нём – важнейшее условие, позволяющее

[252] Пользователя «Вконтакте» судят за публикацию интимных фото бывшей одноклассницы 10-летней давности [Электронный ресурс]: http://pravo.ru/news/view/116028/?utm_source=twitter&utm_medium=cpc&utm_campaign=twitter_share

предотвратить несанкционированное использование данных, в том числе и при совершении преступлений.

Сказанное выше позволяет утверждать, что режим персональных данных, который установлен в отношении них, существенным образом может влиять на квалификацию соответствующих преступных посягательств, поскольку действия, входящие в объективную сторону соответствующих преступлений, должны обладать признаком незаконности (неправомерности). Такой признак может быть предусмотрен соответствующим режимом безопасности, устанавливающим ограничения и запреты на свободное собирание, распространение и использование персональных данных.

Понимание содержания всех действий, входящих в объективную сторону исследуемых преступных посягательств, требует тщательного их анализа. Поэтому остановимся более подробно на каждом из них.

2.2.1. Незаконное собирание персональных данных

Одним из альтернативных признаков, входящих в объективную сторону преступных посягательств в отношении персональных данных, является незаконное собирание сведений.

Содержание данного действия зависит от соответствующего вида преступного посягательства. Однако незаконное собирание сведений имеет черты, общие для всех составов исследуемых преступлений. Так, некоторые исследователи под незаконным собиранием сведений подразумевают «похищение или покупку информации, составляющей личную или семейную тайну другого лица (применительно к составу ст. 137 УК РФ) и похищение документов, приобретение сведений путём подкупа, угрозы любого рода (в том числе, с применением насилия), а также иным незаконным способом (прослушивание телефонных переговоров, неправомерный доступ к компьютерной информации) – применительно к преступлениям,

предусмотренным ст. 183 УК РФ»[253]. В комментарии к Уголовному кодексу РФ под редакцией В.М. Лебедева указывается, что «понятие «собирание» как альтернативный признак объективной стороны преступлений толкуется достаточно широко. Так, собирание сведений может осуществляться любым способом: тайно, открыто, с применением обмана, насилия и т.д. Оно может выражаться в похищении, приобретении, копировании документов или других материальных носителей конфиденциальной информации, в подслушивании, подсматривании, проведении фото- и видеосъёмок, в опросе осведомлённых лиц и т.д.»[254]. Соглашаясь с указанной позицией, отметим, что это не полный перечень действий, подпадающих под понятие «собирание». Под «собиранием», на наш взгляд, следует понимать также систематизацию и накопление полученной информации для использования её в каких-либо целях или без таковых. Таким образом, общим в собирании сведений, безусловно, является совершение активных действий, направленных на достижение преступного результата, и эти действия направлены на получение информации, ограниченной в свободном доступе. В рассматриваемом нами случае речь идёт о действиях, направленных на получение персональных данных, которые не могут свободно распространяться в информационном обороте.

Спорным моментом в правовых исследованиях является вопрос о том, относить ли поиск информации к понятию «собирание» применительно к преступным посягательствам в отношении персональных данных. Мнения различаются не только по содержанию, но и по форме.

Так, Н.А. Лопашенко, рассматривая характеристику объективной стороны преступлений, предусмотренных ст. 183 УК РФ, под собиранием сведений, составляющих коммерческую, налоговую или банковскую тайну,

---

[253] Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. А.И. Рарог. М.: Проспект, 2011.
[254] Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В.М. Лебедев. М.: Юрайт, 2011. С. 305.

понимает, в том числе, «процесс их поиска, обнаружения или накапливания у лица, не допущенного к обладанию соответствующей тайной»[255].

А.А. Каунова, описывая признаки объективной стороны преступлений, предусмотренных ст. 137 УК РФ, указывает, что «под собиранием сведений, составляющих личную или семейную тайну, следует понимать любые действия, направленные на их поиск»[256]. Подобного мнения придерживается и О.А. Пальчиковская, указывая, также, что «собирание сведений о частной жизни лица может приводить к получению информации, а может и не привести к такому результату. Последний случай, по её мнению, необходимо квалифицировать как неоконченное собирание сведений, а именно как покушение на нарушение неприкосновенности частной жизни»[257].

Обратного мнения придерживается М.А. Ершов, указывая, что, «безусловно, собирание сведений представляет собой действия, направленные на получение информации, в том числе и поиск. Но преступление будет считаться оконченным только тогда, когда информация получена. Поэтому поиск имеет лишь промежуточное значение для квалификации объективной стороны рассматриваемого посягательства»[258].

И.А. Шевченко также не соглашается с позицией, в соответствии с которой «поиск сведений является разновидностью незаконного собирания, указывая, что поиск всегда предваряет собирание информации, представляет собой подготовительные действия по поиску источника или носителя информации, сбор которой планируется»[259].

---

[255] Лопашенко Н.А. Преступления в сфере экономики: авторский комментарий к уголовному закону (раздел VIII УК РФ) (постатейный). М.: Волтерс Клувер, 2006.

[256] Каунова А.А. К вопросу о понятии и сущности личной и семейной тайны // Молодой учёный. 2013. №12. С. 645.

[257] Пальчиковская О.А. Уголовно-правовая охрана личной и семейной тайны. Автореф. дисс. … канд. юрид. наук. М., 2011.

[258] Ершов М.А. Ответственность за посягательство на конфиденциальную информацию по российскому уголовному праву (проблемы правоприменения и совершенствования законодательства). Дисс. … канд. юрид. наук. Нижний Новгород, 2010. С. 141.

[259] Шевченко И.А. Уголовно-правовая охрана неприкосновенности частной жизни. Дисс. … канд. юрид. наук. Красноярск, 2005. С. 101.

По нашему мнению, для целей уголовно-правовой охраны и квалификации преступных посягательств на конфиденциальную информацию, в том числе на персональные данные, подпадающие под соответствующий правовой режим безопасности, общественно опасным в процессе незаконного собирания сведений, составляющих личную и семейную тайну, является именно результат такого собирания. Представим себе понятие «собирание» как длящийся во времени процесс. Мы придём к выводу, что он неоднороден по своему составу, для него характерна определённая этапность, и на каждом этапе рассматриваемого процесса могут совершаться совершенно различные задачи. Так, поиск действительно можно рассматривать как первоначальный этап информационного процесса. Но сам процесс поиска является лишь своеобразной отправной точкой, которая может привести либо к получению определённой информации либо к её неполучению в силу множества причин и факторов. Если субъект, осуществлявший поиск информации, в конечном итоге не смог её получить либо он получил информацию, не соответствующую критериям его информационного запроса, цель информационного процесса не достигнута – субъект всё равно не обладает сведениями и данными, которые ему были необходимы. Но если субъекту удалось найти интересующую его информацию, то цель информационного процесса, безусловно, достигнута, и он становится обладателем сведений, которые может использовать для определённых нужд.

На наш взгляд, уголовно-правовое значение для целей привлечения виновного лица к уголовной ответственности имеет лишь такой поиск информации, который завершился получением искомых сведений, и именно это следует включать в понятие «собирание». В случае неполучения информации субъект лишён возможности незаконно использовать полученную персональную информацию по своему усмотрению, так как ею не обладает, а потому не способен её ни распространить, ни продать, ни разгласить в средствах массовой информации, публично

демонстрирующемся произведении и т.д. Сам по себе поиск персональной информации, не приведший к результату в виде получения искомой информации, не может иметь уголовно-правового значения, так как отсутствует критерий общественной опасности подобного деяния – отсутствие информации никаким образом не может причинить вред тому лицу, о ком информация и собиралась.

Например, лицо, имея умысел на незаконное собирание сведений о частной жизни другого лица, устанавливает видеозаписывающее устройство в том месте, где обычно интересующее лицо появляется и проводит место. Однако в течение длительного периода времени интересующее лицо там не появляется, информация и сведения о частной жизни интересующего лица не получены. Следовательно, реального морального вреда потерпевшему лицу причинено не было, а общественная опасность отсутствует, как и состав преступления, так как наблюдающий не получил интересующие сведения, которыми он мог бы воспользоваться в личных целях, в том числе корыстных. В то же время, лицо, устанавливая видеозаписывающее устройство, создаёт угрозу нарушения права на неприкосновенность персональных данных о лице, для наблюдения за которым было установлено указанное устройство. Представляется, что создание условий оконченного преступления в этом случае не образует, хотя это и создаёт опасность совершения преступного посягательства в отношении персональных данных лица, потенциально потерпевшего от преступления.

В литературе также употребляется термин «сбор персональных данных». Так, А.В. Мнацаканян полагает, что в отношении сбора информации в социальных сетях нецелесообразно говорить о целенаправленном сборе данной информации со стороны операторов социальных сетей, поскольку такая информация предоставляется пользователями добровольно. В этой связи следует говорить не о сборе информации, а о доступе к персональным данным, добровольно предоставляемыми пользователями социальных сетей, что не является 11

преступлением [260] . По нашему мнению, персональные данные, как разновидность информации, могут подпадать под различные правовые режимы безопасности, связанные с ограничением доступа к ним, а информация в социальных сетях может размещаться и неправомерно (без согласия субъекта персональных данных). Поэтому операторы социальных сетей всегда осуществляет сбор информации, являющейся персональными данными, но характер доступа к персональным данным с их стороны может быть и ограничен. Отсюда следует, что замена понятия «сбора» («собирание») на понятие «доступ» не во всех подобных случаях является оправданным.

В некоторых случаях персональные данные могут быть получены также путём незаконного прослушивания телефонных переговоров либо путём незаконного проникновения в жилище. В данной ситуации нарушается комплекс конституционных прав. Однако, как справедливо указывает Я.М. Плошкина, «в таком случае проникновение в жилище не является целью преступления, а, скорее, способом его совершения, так как основная цель заключается в получении персональной информации. Поэтому квалификация должна производиться по ст. 137 УК РФ как незаконное собирание информации, составляющей личную или семейную тайну»[261].

В судебной практике случаи, связанные с незаконным собиранием персональных данных без их распространения, встречаются довольно редко. Как правило, незаконное собирание связано с их последующим распространением либо иным неправомерным использованием. Возможно, это как раз и связано с тем, что виновного мало интересует только поиск информации, для него важным является возможность не только получить эту информацию, но и распространить её либо использовать в своих личных целях, например, корыстных или иных.

---

[260] Мнацаканян А.В. Информационная безопасность в Российской Федерации: уголовно-правовые аспекты: Дисс. … канд. юрид. наук. М., 2016. С. 10.

[261] Плошкина Я.М. Уголовная ответственность за незаконное прослушивание телефонных переговоров и аудио- видеонаблюдение за жилищем по законодательству РФ и ФРГ: Автореферат дисс. … канд. юрид. наук. Красноярск, 2005. С. 9.

Так, приговором Менделеевского районного суда Республики Татарстан П. был признан виновным в совершении преступления, предусмотренного ч. 1 ст. 137 УК РФ. В период с января по апрель 2010 года, в неустановленное следствием время, П., находясь у себя дома, обладая познаниями в области информационных технологий, с использованием программного обеспечения «IP Scanner», находясь в глобальной сети Интернет, являющейся средством массовой информации, произвел несанкционированный вход в персональный компьютер своей знакомой и, обнаружив два графических файла с изображением обнаженной потерпевшей, осознавая, что совершает незаконное собирание сведений о её частной жизни, составляющие её личную тайну, без её согласия, нарушая её конституционное право на неприкосновенность частной жизни, произвёл их копирование в свой персональный компьютер[262].

Другой случай, встретившийся автору в судебной практике, имеет более развёрнутый характер по масштабности действий виновных лиц. Приговором Петропавловск-Камчатского городского суда Камчатского края Ш. и Л. Признаны виновными в совершении преступлений, предусмотренных ч. 1 ст. 183, ч. 2 ст. 137, ч. 1 ст. 285 УК РФ. Судом установлено, что Ш., будучи должностным лицом – старшим следователем следственного отдела УФСКН России по Камчатскому краю, осуществляла сбор сведений из банков и учреждений, в которых зарегистрировано имущество нескольких физических лиц, а полученные сведения передавала другом участнику данных деяний – Л. При этом, указанные лица якобы являлись фигурантами уголовных дел, которые находились в производстве непосредственно у Ш. Ш. направляла запросы на указанных лиц в банки и учреждения с целью установления сведений о наличии счетов, банковских пластиковых карт, о движении средств по счетам и спецкартам, об оформленных ценных бумагах, имуществе и транспортных средствах. В

[262] Приговор Менделеевского районного суда Республики Татарстан по делу №№1-16/2014 от 12 февраля 2014 г. [Электронный ресурс]: http://sudact.ru

последующем было установлено, что указанные лица отношений к уголовным делам, находившимся в производстве у Ш., не имели[263].

2.2.2. Незаконное распространение (разглашение) персональных данных

Такой альтернативный признак объективной стороны преступных посягательств в отношении персональных данных, как «распространение», предусматривается в ст. 137 УК РФ. Между тем, в ст. 183 УК РФ используется иной термин – «разглашение». Это самый частый способ совершения преступных посягательств в отношении персональных данных. Более того, обобщение судебной практики показывает, что, как правило, распространение (разглашение) персональных данных является основным этапом информационного преступного процесса, приводящего к преступным результатам в виде нарушения права на неприкосновенность частной жизни или иного правового режима персональных данных.

В толковом словаре С.И. Ожегова под словом «распространить» понимается «сделать доступным, известным для многих»[264]; под словом «разгласить» понимается «рассказав, оповестив, сделать известным; распространить что-либо»[265]. Представляется, что толкование данных слов различается по эмоциональной окраске, так как слово «разглашение» носит более негативную окраску, нежели слово «распространение». «Разглашение» всегда связано с раскрытием чужой (или собственной) тайны, а именно сведений, которые, скорее всего, в силу ряда объективных причин не могут быть разглашены.

Российское законодательство содержит легальные определения обоих понятий. Так, статья 2 Федерального закона «Об информации, информационных технологиях и защите информации» устанавливает, что

---

[263] Кассационное определение Камчатского краевого суда по делу №22-61/2012 [Электронный ресурс]: судебные решения.рф

[264] Словарь Ожегова. Толковый словарь русского языка [Электронный ресурс]: http://www.ozhegov.com/words/29976.shtml

[265] Там же [Электронный ресурс]: http://www.ozhegov.com/words/29208.shtml

распространение информации – действия, направленные на получение информации неопределённым кругом лиц или передачу информации неопределённому кругу лиц [266]. Федеральный закон «О персональных данных» содержит в ст. 3 несколько иное определение понятия «распространение», понимая под ним действия, направленные на раскрытие персональных данных неопределённом кругу лиц[267].

Представляется, что законодатель при определении понятия «распространение» применительно к Федеральному закону «Об информации…» не совсем удачно сформулировал сущностные признаки, по которым можно установить понятие распространения. Признак «получение информации неопределённым кругом лиц», безусловно, является важным, поскольку информации становится известной третьим лицам. Но всё же распространение обладает более деятельностной сущностной характеристикой, то есть представляет собой действия активного субъекта по доведению соответствующего вида информации до неопределённого круга лиц. В этой связи, акты пассивного поведения получателей информации посредством распространения, на наш взгляд, не имеют какого-либо существенного правового значения. Именно поэтому полагаем, что более удачной формулировкой определения понятия «распространение» является та, которая была приведена в Федеральном законе «О персональных данных», так как она предполагает действия, направленные на раскрытие информации, то есть доведение информации до сведения неопределённого круга лиц.

Определение понятия «разглашение» содержится в Федеральном законе «О коммерческой тайне» (а также Налоговом кодексе РФ), хотя это понятие также упоминается и в Федеральном законе «Об информации…». Статья 3 Федерального закона «О коммерческой тайне» устанавливает, что

---

[266] Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 №149-ФЗ // СЗ РФ. 2006. №31 (1 ч.). Ст. 3448.

[267] Федеральный закон «О персональных данных» от 29.07.2006 №152-ФЗ // СЗ РФ. 2006. №31 (1 ч.). Ст. 3451.

под разглашением понимаются действие или бездействие, в результате которых информация, составляющая коммерческую тайну, в любой возможной форме (устной, письменной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору[268]. Как видим, законодательное определение понятия «разглашение» несколько отличается от понятия «распространение», и это отличие прослеживается по нескольким критериям. Во-первых, разглашение, по мнению законодателя, предполагает не только действия, но и бездействие, направленное на доведение до сведения третьих лиц соответствующего вида информации. Во-вторых, в определении понятия «разглашение» конкретизированы способы передачи информации, а именно в устной, письменной форме, в том числе с использованием технических средств, чего нет в определении понятия «распространение». В-третьих, применительно к понятию разглашения законодатель акцентирует внимание на том, что это действия, которые происходят неправомерно, незаконно, то есть вопреки установленному режима ограничения на свободный оборот такой информации, пока как в отношении понятия распространения такого акцента не делается.

Отсюда вполне очевидна логика законодателя о приведении специальных статей Уголовного кодекса РФ, посвящённых охране конкретного вида информации от преступных посягательств, в соответствие с профильным законодательством, регулирующим данные правоотношения. В то же время, представляется, что понятия «распространение» и «разглашение» по своей правовой природе и по содержанию для целей привлечения виновных лиц к установленной уголовной ответственности являются абсолютно идентичными. Это можно продемонстрировать, выделив сущностные признаки, указанные законодателем при определении данных понятий. Так, распространение всегда предполагает совершение

[268] Федеральный закон «О коммерческой тайне» от 29.07.2004 №98-ФЗ // СЗ РФ. 2004. №32. Ст. 3283.

определённых действий, направленных на постановку в известность третьих лиц о той или иной информации (в нашем случае – охраняемых законом персональных данных). То же самое характерно и для разглашения.

Кроме того, способ как распространения, так и разглашения охраняемых законом персональных данных, может быть абсолютно любым и не должен иметь существенного значения для квалификации; он может даже осуществляться посредством глобальной сети Интернет. Главное в этой связи то, что целью как разглашения, так и распространения является раскрытие информации, доведение её до третьих лиц. При этом уголовно наказуемым является только такое разглашение или распространение, которое совершается вопреки установленному правовому режиму персональных данных (режиму личной или семейной тайны, режиму коммерческой, налоговой или банковской тайны).

Отсутствие сущностных различий в указанных понятиях подтверждается также анализом научной литературы, который показывает, что понятия «распространение» и «разглашение» большинством автором между собой отождествляются, хотя и сформулированы по-разному. Так, например, Н.А. Лопашенко под разглашением понимает «передачу сведений хотя бы одному лицу, не допущенному к обладанию тайной, предание сведений огласке» [269] . Ю.В. Гаврилин применительно к преступлению, предусмотренному ст. 137 УК РФ, под распространением сведений о частной жизни лица понимает «сообщение известных виновному сведений третьему лицу (лицам)»[270]. По мнению И.А. Юрченко, «распространение предполагает предание огласке сведений, составляющих тайну, в результате чего они становятся достоянием постороннего лица»[271].

На наш взгляд, более правильным было бы утверждать, что альтернативное действие в объективной стороне соответствующего

---

[269] Лопашенко Н.А. Указ. соч.

[270] Гаврилин Ю.В. Научно-практический комментарий к статье 137 УК РФ «Нарушение неприкосновенности частной жизни» // КонсультантПлюс.

[271] Юрченко И.А. Нарушение неприкосновенности частной жизни // Чёрные дыры в российском законодательстве. 2002.

преступного посягательства должно по правовой природе представлять собой единое понятие и обозначаться однозначно. Поскольку специализированное профильное законодательство в сфере информации использует термин «распространение», а уголовно-правовому регулированию подлежит только незаконное распространение, то различные виды тайн, составляющие соответствующий правовой режим охраняемых законом персональных данных, должны охраняться с позиций установления единого альтернативного признака, входящего в объективную сторону преступных посягательств – «незаконного распространения». Представляется, что это понятие должно применяться не только в отношении преступных посягательств на персональные данные, предусмотренные ст. 137 УК РФ, но и в отношении преступных посягательств, установленных ст. 183 УК РФ. В связи с этим нам предлагается в ст. 183 УК РФ вместо термина «разглашение» использовать термин «распространение». Этот же термин необходимо использовать и в Федеральном законе «О коммерческой тайне», так как это приведёт к единообразному пониманию сущности данного вида преступного посягательства.

В Уголовном кодексе Республики Беларусь схожий состав преступления, аналогичного ст. 183 УК РФ, формулируется совершенно иначе. Во-первых, он именуется как «промышленный шпионаж», а во-вторых, по объективной стороне это преступление представляет собой похищение либо собирание незаконным способом сведений, составляющих коммерческую или банковскую тайну с целью их разглашения либо незаконного использования (ст. 254 Уголовного кодекса Республики Беларусь)[272].

В уголовном законодательстве Украины объективная сторона подобного преступления также сформулирована отлично от российской нормы. Так, ст. 231 Уголовного кодекса Украины предусматривает уголовную ответственность за умышленные действия, направленные на

[272] Уголовный кодекс Республики Беларусь [Электронный ресурс]: http://уголовный-кодекс.бел

получение сведений, составляющих коммерческую или банковскую тайну, с целью разглашения или иного использования этих сведений, а также незаконное использование таких сведений, если это нанесло существенный вред субъекту хозяйственной деятельности[273].

Заслуживает внимания также и то обстоятельство, что во многих случаях преступных посягательств на персональные данные законодатель использует понятие «незаконное распространение». О незаконном распространении нами уже отчасти было сказано. Применительно к незаконному распространению персональных данных, подпадающих под соответствующий режим охраны, следует понимать, по существу, отсутствие согласия правообладателя или субъекта данных на их свободное распространение.

Следует согласиться с мнением, что «позиция законодателя при формулировании альтернативного признака применительно к «разглашению» персональных данных (для целей статьи 183 УК РФ) не в полной мере является последовательной, так как признак «незаконности» указывается только в отношении *распространения* данных и не указывается в отношении *разглашения*»[274]. Между тем, следует отбросить из уголовно-правового поля те случаи, когда распространение персональных данных, подпадающих под соответствующий режим информации, хотя и осуществляется без согласия правообладателя, но, тем не менее, правомерно. Такие случаи приводятся в различных видах законодательных актов Российской Федерации. Например, Федеральный закон «О персональных данных» устанавливает, что операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъектов персональных данных, если иное не предусмотрено федеральным законом. В силу ст. 3 указанного закона распространение входит в понятие обработки данных. Отсюда следует, что в отношении

[273] Уголовный кодекс Украины [Электронный ресурс]: http://pravoved.in.ua/section-kodeks/134-yku.html
[274] Ершов М.А. Указ. соч. С. 143.

распространения данных используются те же нормы закона, что и в отношении обработки. Таким образом, распространение данных может осуществляться и без согласия субъекта персональных данных, если имела место, например, обработка данных для осуществления правосудия, исполнения судебного акта, акта иного органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации «Об исполнительном производстве».

Статья 6 Федерального закона «О персональных данных» предусматривает, что обработка персональных данных допускается в том случае, если осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом. Как мы указали выше, раскрытие сведений о доходах, имуществе и обязательствах имущественного характера государственными и муниципальными служащими – обязанность, установленная соответствующими федеральными законами. В совокупности с этим, статьёй 8 Федерального закона «О противодействии коррупции» устанавливается обязанность государственных, муниципальных служащих, а также лиц, замещающих государственные должности, ежегодно представлять сведения о своих доходах, имуществе и обязательствах имущественного характера по месту службы, и при этом такие сведения без согласия лица размещаются в силу закона на официальных сайтах соответствующего публичного органа в сети Интернет[275].

Судебная практика учитывает вышеуказанные положения. Так, Б. обратился в следственный отдел по г. Соликамску СУ СК РФ по Пермскому краю с заявлением о привлечении к уголовной ответственности сотрудников газеты «Досье 02», в том числе корреспондента Ш. за нарушение неприкосновенности его частной жизни вследствие публикации в газете, содержащей его анкетные данные и, по мнению заявителя,

[275] Федеральный закон «О противодействии коррупции» от 25.12.2008 №273-ФЗ // СЗ РФ. 2008. №52 (ч. 1). Ст. 6228.

фальсифицированную информацию об обстоятельствах преступления. Постановлением следственного органа в возбуждении уголовного дела по признакам составов преступлений по ч. 2 ст. 136 и ч. 2 ст. 137 УК РФ было отказано. Не согласившись с указанным процессуальным решением, гражданин обратился в суд в порядке ст. 125 УПК РФ. Постановлением городского суда в удовлетворении жалобы было отказано. Гражданин обжаловал указанные решения в суд субъекта РФ. Кассационным определением судебной коллегии по уголовным делам Пермского краевого суда по делу №22-9755/2011 постановление суда первой инстанции оставлено без изменения, кассационная жалоба без удовлетворения.

Как указано в кассационном определении, доводы заявителя о незаконной публикации в газете его персональных данных, в том числе фамилии, имени, отчества, места рождения, анкетных данных, а также об искажении обстоятельств преступления, что, по его мнению, влечёт уголовную ответственность сотрудников редакции газеты, несостоятельны в связи со следующим.

Освещение средствами массовой информации судебных процессов законом не запрещено и в полной мере соответствует требованиям п. 1 ст. 6 Конвенции «О защите прав человека и основных свобод» о том, что разбирательство в суде должно быть публичным.

Согласие на публикацию в статье фамилии, имени, отчества осуждённого по вступившему в законную силу приговору суда, вопреки доводам жалобы заявителя, не требуется, поскольку в соответствии с Федеральным законом «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» от 22.12.2009 №262-ФЗ информация по делам, в том числе тексты судебных решений размещаются в сети Интернет и доступны для любого пользователя. Фамилия осуждённого, согласно ч. 5 ст. 15 данного закона, в перечень данных, не подлежащих опубликованию, не входит.

С учётом изложенного, выводы следователя об отсутствии в действиях сотрудников газеты составов преступлений, предусмотренных ч. 2 ст. 136 и ч. 2 ст. 137 УК РФ, предусматривающих уголовную ответственность за нарушение равенства прав и свобод человека и гражданина и нарушение неприкосновенности частной жизни, совершённые с использованием служебного положения, являются правильными[276].

Следует также отметить, что суды, применяя нормы об уголовной ответственности за незаконное распространение или разглашение персональных данных, не всегда видят разницу между распространением и разглашением при составлении судебных актов. Так, приговором Соликамского городского суда Пермского края Р. Была признана виновной в совершении преступления, предусмотренного ч. 2 ст. 137 УК РФ. Р. занимала должность оператора связи ОАО «Уралсвязьинформ», и к ней обратилась П. с целью получения информации о входящих и исходящих звонках и СМС-сообщениях своего супруга Г., а также о его контрабонентах. Р., исполняя договоренность с П, являясь сотрудником учреждения связи, занимая должность оператора связи ОАО «Уралсвязьинформ», понимая, что право на тайну телефонных переговоров и иных сообщений, на неприкосновенность частной жизни граждан Российской Федерации гарантировано ст. 23 Конституции Российской Федерации, действуя умышленно и осознавая, что своими действиями нарушает охраняемое Конституцией Российской Федерации право Г. И его контрабонентов на тайну телефонных переговоров и иных сообщений, а также на тайну их частной жизни, и желая нарушить эти права, вопреки интересам службы, из иной личной заинтересованности, с целью получения информации об абонентах, с которыми происходили входящие и исходящие соединения, состоявшиеся по принадлежащему Г. сотовому телефону, используя программное компьютерное обеспечение ОАО «Уралсвязьинформ», компьютерную технику и печатающее устройство,

[276] Кассационное определение Пермского краевого суда от 06.12.2011 по делу №22-9755/2011 [Электронный ресурс]: судебные решения.рф

доступ к которому она имела в силу занимаемой должности, незаконно, не имея на то соответствующего разрешения, получила в ОАО «Уралсвязьинформ» сведения о состоявшихся телефонных соединениях и СМС-сообщениях с телефона Г.

Продолжая действовать из иной личной заинтересованности и желая выполнить договоренность с П., Р, используя базу данных телефонных сетей, принадлежащую ОАО «Уралсвязьинформ», устанавливала принадлежность номеров телефонов, с которыми в указанный период потерпевший связывался по телефону, выявляла наиболее часто встречающиеся номера, незаконно получала информацию личного характера о владельцах этих номеров. Незаконно получив информацию о соединениях между Г. И его контрабонентами, а также персональные данные указанных контрабонентов, Р., действуя умышленно, сознавая, что своими действиями нарушает охраняемые Конституцией Российской Федерации права граждан на тайну телефонных переговоров и иных сообщений, сведений о частной жизни лиц, составляющих их личную тайну и субъективно относимые гражданами к скрытым от посторонних, в нарушение данного ею письменного обязательства о сохранении в тайне сведений конфиденциального характера, являющегося специальным условием заключённого с ОАО «Уралсвязьинформ» трудового договора, **незаконно получила и разгласила** П. охраняемую Конституцией Российской Федерации и не подлежащую разглашению информацию о телефонных сообщениях и звонках между Г. И его контрабонентами путём передачи указанной информации в отпечатанном и устном виде, а также устно в ходе телефонных переговоров передавала сведения о персональных данных указанных абонентов (фамилия, имя, отчество, год рождения, место регистрации, паспортные данные, а также данные детализации (количество минут соединения, стоимость соединения) телефонных переговоров и номера телефонов контрабонентов) без ведома и согласия этих граждан – абонентов связи, то есть сведения о частной жизни

этих лиц, составляющие их личную тайну, субъективно относимые ими к скрытым от посторонних лиц[277].

Подытожив вышесказанное, отметим, что такие альтернативные признаки объективной стороны преступных посягательств в отношении персональных данных, как «распространение» или «разглашение» для целей привлечения к уголовной ответственности винновых лиц всегда должен сопровождаться незаконным, неправомерным содержанием, то есть в отсутствие согласия лица, являющегося правообладателем данных, а также при отсутствии предусмотренных федеральным законом оснований, при которых распространение или разглашение персональных данных допускается без согласия правообладателя (субъекта персональных данных). В противном случае, состав преступного посягательства в отношении персональных данных в действиях лица будет отсутствовать.

2.2.3. Незаконное использование персональных данных

Незаконное использование данных как разновидность преступного посягательства в отношении охраняемых законом персональных данных указано в качестве альтернативного признака объективной стороны только применительно к статье 183 УК РФ. Часть 2 указанной статьи наряду с разглашением сведений, составляющих коммерческую и иную охраняемую законом тайну (под которую и подпадают те или иные персональные данные), предусматривает также ответственность и за незаконное использование таких сведений. Не вызывает сомнений, что под использованием какого-либо объекта или предмета обычно понимается извлечение из объекта или предмета определённых полезных свойств, исходя из его изначального целевого назначения.

[277] Приговор Соликамского городского суда Пермского края от 16.11.2011 по делу №1-511/11 [Электронный ресурс]: http://sudact.ru

В научной литературе высказываются различные позиции относительно понятия незаконного использования сведений. В частности, Н.А. Лопашенко полагает, что «под использованием сведений, составляющих коммерческую, налоговую или банковскую тайну, следует понимать распоряжение ими любым способом: продажа, обмен указанной информации на различные виды материальных ценностей, применение сведений по прямому назначению – для производства товаров, услуг, корректировки своих действий при заключении договора с субъектом конфиденциальных сведений и т.д.»[278]

По мнению Б.В. Волженкина, «незаконное использование сведений, являющихся чужой тайной, будет иметь место, в частности, при применении этих сведений в экономической (предпринимательской) деятельности без разрешения владельца всеми, кому эта тайна стала известна в связи с профессиональной или служебной деятельностью»[279].

В.И. Гладких и П.Н. Сбирунов указывают, что «использование добытой информации, составляющей коммерческую, налоговую или банковскую тайну, позволяет злоумышленнику, например, повлиять на выбор клиентов, переманить их, усовершенствовать производство или узнать новые для него технологии. И именно в этом заключается общественная опасность незаконного использования данной информации»[280].

А.В. Козлов вообще проблематизирует вопрос, связанный с рассматриваемым альтернативным признаком объективной стороны преступления, предусмотренного ст. 183 УК РФ, указывая, что «незаконное использование сведений, составляющих коммерческую, банковскую или налоговую тайну, для целей дифференциации уголовной ответственности должен рассматриваться отдельно от другого альтернативного признака – разглашения, пока как в настоящий момент оба этих признака содержатся в

---

[278] См.: Лопашенко Н.А. Указ. соч.

[279] Уголовное право России: Часть Особенная: учебник для вузов / Отв. ред. Л.Л. Кругликов. – М.: Волтерс Клувер, 2012. С. 316.

[280] Гладких В.И., Сбирунов П.Н. Особенности квалификации незаконного получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну // Юрист. 2012. №5.

ч. 2 исследуемой нормы УК РФ. Кроме того, он указывает, что общественная опасность незаконного разглашения и незаконного использования значительно различается, так как незаконное разглашение может нанести больший ущерб нежели незаконное использование»[281].

В свою очередь, С.М. Крянин пишет о том, что «не любое незаконное использование коммерческой тайны достигает степени общественной опасности, свойственной преступлению. Он полагает, что уголовная ответственность за незаконное использование соответствующей информации должна наступать только при наличии такого криминообразующего признака объективной стороны преступления, как причинение крупного ущерба»[282].

В.Н. Зайцев, рассматривая альтернативный признак незаконного использования применительно к ст. 183 УК РФ, разделяет мнение С.М. Крянина о меньшей общественной опасности использования, в отличие от разглашения, а также полагает, что «уголовная ответственность за незаконное использование информации, составляющей коммерческую, налоговую или банковскую тайну должна наступать только в том случае, если указанное деяние совершено из корыстной заинтересованности или повлекло по неосторожности разглашение сведений, составляющих соответствующий вид тайны»[283].

Применительно к такому специфичному предмету совершения подобных преступлений, как персональные данные, относительно их незаконного использования в рамках охраны коммерческой, налоговой или банковской тайны какие-либо мнения в литературе отсутствуют. Полагаем, что это связано, по большей части, с тем, что персональные данные всего лишь подпадают под правовой режим соответствующего вида тайн, и именно

---

[281] Козлов А.В. Об устранении преград на пути к дифференциации уголовной ответственности за преступления против коммерческой тайны // Уголовное право: истоки, реалии, переход к устойчивому развитию: материалы VI Российского конгресса уголовного права / Под ред. В.С. Комиссарова. М.: Проспект, 2011. С. 329.

[282] Крянин С.М. Уголовно-правовая охрана секретов производства: Дисс. … канд. юрид. наук. Нижний Новгород: Нижегородская академия МВД России, 2009. С. 115, 160.

[283] Зайцев В.Н. Уголовно-правовая охрана промышленной собственности: Дисс. … канд. юрид. наук. – Нижний Новгород: Нижегородская академия МВД России, 2010. С. 156-157.

поэтому все признаки объективной стороны подобных преступных посягательств рассматриваются вне отрыва от соответствующих составов преступлений. Между тем, как уже отмечалось выше, признак «незаконное использование» характерен только для тех преступных посягательств в отношении персональных данных, которые охраняются в рамках коммерческой, налоговой или банковской тайны.

Применительно к персональным данным, охраняемым правовым режим неприкосновенности частной жизни (личной и семейной тайны) такой альтернативный признак объективной стороны законодателем не выделяется и не используется. На наш взгляд, это можно объяснить характером преступных посягательств, а также охраняемыми правоотношениями, входящими в понятие объектов соответствующих преступлений. Так, анализ практики показывает, что незаконное распространение персональных данных, подпадающих под правовой режим личной и семейной тайны, по существу, является частным случаем использования такой информации в личных целях. Между тем, незаконное использование персональных данных, подпадающих под режим коммерческой, налоговой или банковской тайны, посягает совершенно на другие охраняемые законом интересы и правоотношения, в которых, по большей части, могут пострадать финансовые интересы потерпевших субъектов. Именно поэтому законодатель не выделяет альтернативный признак «незаконное использование» применительно к персональным данным, охраняемым правовым режимом неприкосновенности частной жизни (личной и семейной тайны).

Судебная практика показывает, что альтернативный признак «незаконное использование сведений» во многих уголовных делах о преступлениях, предусмотренных ч. 2 ст. 183 УК РФ, имеет самостоятельное значение, не связанное с незаконным разглашением соответствующего вида конфиденциальной информации. И при этом если обобщить случаи, которые квалифицируются судами как незаконное использование информации,

составляющей коммерческую, налоговую или банковскую тайну, то можно прийти к выводу о том, что большинство осуждённых за незаконное использование сведений действительно совершали это деяние исключительно из корыстной заинтересованности. Данное обстоятельство, на наш взгляд, является вполне объяснимым с позиций криминологии, так как ответственность по ч. 2 или 3 ст. 183 УК РФ за незаконное использование информации, составляющей коммерческую, налоговую или банковскую тайну, наступает лишь в том случае, если оно было совершено лицом, которому эта информация была доверена или стала известна по работе. Лицо, обладая соответствующими сведениями, может полностью осознавать, что сведения, составляющие тайну и находящиеся в его распоряжении могут негативно повлиять на субъекта-обладателя этого вида тайны, но, в то же время, обогатить это лицо. Поэтому виновному не нужно каким-либо образом устранять препятствия в получении конфиденциальной информации, достаточно эту информацию применить для достижения преступной цели.

Так, приговором Сосновоборского городского суда Ленинградской области от 12.12.2014 г. По делу №1-155/2014 Н. был признан виновным в совершении преступлений, предусмотренных ч. 3 и 4 ст. 158 и ч. 3 ст. 183 УК РФ. Судом установлено, что Н., являясь сотрудником Северо-Западного Банка, назначенным на должность клиентского менеджера операционного офиса Сосновоборского отделения, согласно должностной инструкции являясь лицом, допущенным к конфиденциальной информации об операциях, счетах и вкладах клиентов банка и обязанным обеспечивать сохранность банковской тайны, коммерческой тайны и сведений, содержащих персональные данные, связанных как с деятельностью Банка, так и с его клиентами, незаконно использовал сведения, ставшие ему известными в связи с выполнением трудовых обязанностей. А именно в дневное рабочее время, обладая информацией, составляющей банковскую тайну, о наличии счёта, открытого на имя физического лица, и наличии на нём денежных средств в сумме более 1 200 000 рублей, собственноручно

выполнил подпись от имени клиента банка в расходном кассовом ордере и совершил операцию выдачи части вклада наличными деньгами, из которых часть перечислил на обезличенный металлический счёт, открытый им от имени клиента банка, а остальные средства перечислил на свой личный счёт, открытый в том же банке. Действия виновного были квалифицированы как незаконное использование сведений, составляющих банковскую тайну[284].

Как видим, целью незаконного использования сведений, составляющих коммерческую, налоговую или банковскую тайну, по большей части является получение выгод имущественного характера для виновного. Но при этом существенное значение для квалификации соответствующих деяний имеет то обстоятельство, что норма части 2 ст. 183 УК РФ сконструирована как формальный состав, то есть для наличия в действиях виновного оконченного состава преступления не требуется наступления каких-либо последствий, а достаточно совершить действие, связанное с незаконным использованием. Между тем, ч. 3 ст. 183 УК РФ, с одной стороны, предусматривает ответственность за незаконное использование, повлекшее за собой причинение ущерба, либо же если незаконное использование было совершено из корыстной заинтересованности. На наш взгляд, законодатель сконструировал нормы подобным образом, исходя из принципа нормативной экономии. Но здесь, скорее, следует согласиться с мнением А.В. Козлова о том, что данный способ криминализации не обеспечивает дифференциацию уголовной ответственности за совершение подобных деяний. Возможно, поэтому не совсем понятна логика законодателя при формулировании нормы части 3 ст. 183 УК РФ, которая, по сути, приравнивает друг к другу два совершенно разных по общественной опасности деяния – использование сведений, повлекшее причинение крупного ущерба, и использование сведений из корыстной заинтересованности. При этом последнее вовсе не означает, что корыстная

[284] Приговор Сосновоборского городского суда Ленинградской области от 12.12.2014 по делу №1-155/2014 [Электронный ресурс]: http://sudact.ru

заинтересованность всегда должна приводить к преступному результату в виде хищения. Это подтверждается и судебной практикой.

Так, приговором Нижневартовского городского суда Ханты-Мансийского автономного округа – Югры от 21.10.2014 по делу №1-991/2014 К. был признан виновным в совершении преступлений по ч. 3 ст. 30, п. «в» ч. 3 ст. 158 и ч. 3 ст. 183 УК РФ. Как было установлено судом, К., работая консультантом по банковским продуктам ОАО «Сбербанк России», выполнял должностные обязанности по оказанию помощи клиентам в поиске информации, проведению транзакций и пользованию банкоматами, информационно-платёжными терминалами, а также автоматизированной системой «Сбербанк Онл@йн». В день совершения преступления, находясь на своём рабочем месте, К., исполняя свои служебные обязанности, при обслуживании клиента П. получил его идентификатор пользователя и пароли, которыми впоследствии незаконно воспользовался и пытался похитить сумму 311 232 руб. 79 коп., находящуюся на лицевом счёте П. Имея идентификатор пользователя П. и его пароли доступа к управлению счётом сервиса «Сбербанк Онл@йн», К. совершил перевод суммы с этого счёта в размере 1 232 руб. на карту Maestro социальная на имя П., а впоследствии сумму 1 547 руб. на виртуальный лицевой счёт в Yandex Money (Яндекс деньги), принадлежащий К. В дальнейшем К. совершил ещё хищения на сумму более 19 000, но не довёл свой преступный умысел на хищение всей суммы по не зависящим от него причинам, так как о незаконном переводе денежных средств стало известно руководству подразделения ОАО «Сбербанк России»[285].

Таким образом, мы видим, что альтернативный признак объективной стороны «незаконное использование» применяется законодателем только по отношению к тем персональным данным, которые охраняются в рамках правового режима коммерческой, налоговой или банковской тайны.

---

[285] Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югры от 21.10.2014 г. По делу №1-991/2014 [Электронный ресурс]: http://sudact.ru

2.2.4. Проблемы квалификации преступных посягательств в отношении персональных данных

Как и в отношении любых иных видов преступных посягательств, в правоприменительной практике довольно часто возникают проблемы, связанные с квалификацией преступных посягательств в отношении персональных данных. Такие проблемы связаны со многими причинами, в частности: несовершенством законодательных конструкций составов преступных посягательств, отсутствием понимания у правоприменителя мотивов и содержания тех или иных бланкетных законодательных норм, устанавливающих специальное нормативно-правовое регулирование института персональных данных и т.д.

Анализ судебной и иной правоприменительной практики позволяет судить о том, что проблемы квалификации, которые будут проанализированы ниже, должны быть решены не только на правоприменительном, но и на законодательном уровне.

Итак, можно прийти к выводу, что преступные посягательства в отношении персональных данных чаще всего порождают проблемы в квалификации на практике относительно данных, подпадающих под правовой режим личной и семейной тайны. И, по большей части, проблемы вызваны отсутствием единообразия в применения мер ответственности за преступления против личности и компьютерные преступления, если соответствующие персональные данные содержались на компьютерном носителе.

Первая проблема, возникающая при квалификации преступных посягательств в отношении персональных данных, заключается в противоречии между применением нормы статьи 272 УК РФ, устанавливающей ответственность за неправомерный доступ к компьютерной информации, и применением нормы статьи 137 УК РФ. Так,

анализ судебной практики показал, что имеют место приговоры, в которых суды по-разному применяют в этой части уголовный закон. В этой связи наглядно демонстрируют данный тезис следующие судебные акты.

Приговором Менделеевского районного суда Республики Татарстан от 12.02.2014 по делу №1-16/2014 П. был признан виновным в совершении преступления, предусмотренного ч. 1 ст. 137 УК РФ. Как установлено органами предварительного следствия и судом, П. в период с января по апрель 2010 года в не установленное следствием время, находясь у себя дома, обладая познаниями в области информационных технологий, с использованием специального программного обеспечения, находясь в глобальной сети Интернет, произвёл несанкционированный вход в персональный компьютер потерпевшей и, обнаружив два графических файла с её обнажённым изображением, осознавая, что совершает незаконное собирание сведений о частной жизни потерпевшей, составляющих её личную тайну, без её согласия, нарушая её конституционные права на неприкосновенность частной жизни, произвёл их копирование в свой персональный компьютер. Далее, в не установленное следствием время П., находясь в сети Интернет, являясь участником группы «Mendeleevsk anonymous gossips» в социальной сети «Вконтакте», осознавая общественную опасность своих действий и предвидя неизбежность наступления общественно опасных последствий в виде нарушения конституционных прав потерпевшей на неприкосновенность частной жизни и желая их наступления, действуя с прямым умыслом из личной заинтересованности, направил в личное сообщение администратору указанной группы ранее добытые незаконным путём графические файлы с изображением обнажённой потерпевшей, которые были размещены на странице группы «Mendeleevsk anonymous gossips», чем совершил незаконное распространение сведений о частной жизни потерпевшей, составляющих её личную тайну, без согласия

потерпевшей[286]. Суд квалифицировал действия виновного только по ч. 1 ст. 137 УК РФ.

В другом деле квалификация действий виновного была осуществлена иначе. Приговором Октябрьского районного суда г. Архангельска от 20.01.2012 г. по делу №1-14/2012 Б. был признан виновным в совершении преступлений, предусмотренных ч. 1 ст. 137 и ч. 1 ст. 272 УК РФ. Судом установлено, что Б., находясь в жилище О., просматривая личные вещи О. в тайне от нее, обнаружил компакт-диск с записанными на нём личными фотографиями последней, на которых О. была запечатлена в нижнем белье, а также частично обнаженной, которые являются сведениями о частной жизни последней, составляющими ее личную тайну, после чего, он, умышленно, с целью незаконного собирания сведений о частной жизни О., составляющих ее личную тайну, и нарушение тем самым ее права на тайну частной жизни для дальнейшего использования и просмотра данных фотографий, присвоил указанный компакт-диск себе не получив на это согласие О. и действуя в тайне от неё [287] . Как видим, в аналогичном предыдущему случае квалификация осуществлена по совокупности двух преступлений с применением статьи 137 и статьи 272 УК РФ.

Между тем, подобные разночтения в процессе применения уголовного закона совершенно недопустимы, поскольку нарушают единообразие в судебной практике, а также могут существенным образом влиять на реализацию принципа законности в уголовном праве. В литературе существует достаточно однозначная позиция по поводу квалификации таких случаев, но, как видим, мало применяется на практике. В частности, Ю.В. Гаврилин пишет о том, что «в тех случаях, когда неправомерный доступ к компьютерной информации выступает способом совершения другого умышленного преступления, а электронно-вычислительная техника

[286] Приговор Менделеевского районного суда Республики Татарстан от 12.02.2014 по делу №1-16/2014 [Электронный ресурс]: http://sudact.ru
[287] Приговор Октябрьского районного суда г. Архангельска от 20.01.2012 по делу №1-14/2012 [Электронный ресурс]: http://sudact.ru

используется как орудие для достижения преступной цели, содеянное должно быть квалифицировано по совокупности преступлений» [288] . Аналогичной позиции придерживается И.А. Юрченко, указывая, что если собирание сведений о частной жизни осуществляется путём неправомерного доступа к компьютерной информации, то уголовная ответственность за данное деяние должна наступать по совокупности ст. 137 и ст. 272 УК РФ[289]. Р.Р. Гайфутдинов указывает, что «неправомерные действия лиц, посягающих на персональные данные, могут охраняться статьёй 272 УК РФ только в том случае, если они подвергается электронно-цифровой обработке посредством компьютерных глобальных сетей. Подобного рода преступные деяния будут являться двухобъектным посягательством. При уголовно-правовой оценке действия лица будут образовывать разнообъектную идеальную совокупность преступлений, квалифицируемых соответственно по ст. 137 и ст. 272 УК РФ. Субъект осуществляет посягательство, с одной стороны, на отношения по поводу обеспечения целостности и сохранности компьютерной информации, а с другой – на конституционные права неприкосновенности частной жизни, личной и семейной тайны»[290].

При формировании собственной позиции по данному вопросу, хотелось бы, в первую очередь, обратить внимание, что нормы статей 137 и 272 УК РФ действительно охраняют различные правоотношения, блага и интересы, которые хотя и пересекаются между собой, но, тем не менее, охватывают различные стороны общественных отношений и связей. И если статья 137 УК РФ направлена, в первую очередь, на охрану персональных данных, подпадающих под правовой режим конфиденциальности личной или семейной тайны (неприкосновенности частной жизни), и это является сущностным, содержательным признаком данных правоотношений, то статья 272 УК РФ направлена на поддержание общественной безопасности в сфере

[288] Гаврилин Ю.В. Научно-практический комментарий к статье 272 УК РФ // СПС «КонсультантПлюс».
[289] Юрченко И.А. Указ. соч.
[290] Гайфутдинов Р.Р. Уголовно-правовая характеристика посягательства на персональные данные, обрабатываемые в автоматизированных системах // Учёные записки Казанского университета. Серия: Гуманитарные науки. 2014. №4. Том 156. С. 159.

оборота компьютерной информации, применительно к чему персональные данные охраняются не в содержательном, а в формальном аспекте – только в случае, если они имеют форму компьютерной информации.

Данное утверждение может породить, в то же время, позицию, в соответствии с которой невозможно обусловливать общественную опасность и образование совокупности преступлений в том или ином деянии содержанием, а также и формой предмета преступного посягательства. Однако представляется, что если лицо осуществляет неправомерный сбор или распространение персональных данных какого-либо субъекта, и эта информация получена им посредством неправомерного доступа к компьютерной технике или компьютерной сети, то действительно имеет место идеальная совокупность преступлений: с одной стороны, лицо, имея умысел на неправомерное получение персональных данных или их неправомерное распространение, нарушает право на неприкосновенность частной жизни; с другой стороны, общественная опасность деяния повышается, если персональные данные были получены посредством неправомерного доступа к компьютерной информации, так как нарушение норм законодательства, охраняющих правоотношения по обороту компьютерной информации, приобретает в данном случае самостоятельное значение.

Кроме того, «квалификация по идеальной совокупности преступлений в теории квалификации преступлений (в теории уголовного права) имеет место именно тогда, когда начавшись одним и тем же действием, преступление затем как бы «расщепляется»: одной действие приводит к двум разным последствиям, не охватываемым одной статьёй Особенной части Уголовного кодекса; страдают две различные группы общественных отношений, два объекта преступного посягательства. В итоге имеют место быть не одно, а два преступления»[291].

[291] Кудрявцев В.Н. Общая теория квалификации преступлений. М.: Юридическая литература, 1972. С. 288.

Таким образом, полагаем, что вопрос о квалификации преступных посягательств в отношении персональных данных посредством неправомерного доступа к компьютерной информации должен быть разрешён в пользу совокупности двух норм – статьи 137 и статьи 272 УК РФ.

На практике также возникают и иные проблемы, связанные с квалификацией преступных посягательств в отношении персональных данных, так как этот институт достаточно новый для российского законодательства и ещё более новый для целей применения уголовного закона. Следующей проблемой является квалификация такого посягательства в отношении персональных данных, как создание ложных страниц – аккаунтов в различных социальных сетях от имени третьих лиц, случаи которого в последнее время серьёзно участились, хотя малая доля из данных видов посягательств в отношении персональных данных входит в официальную статистическую отчётность правоохранительных органов ввиду высокой латентности рассматриваемого вида преступлений.

Действующая судебная практика исходит из того, что создание ложных страниц в социальных сетях посредством незаконного использования персональных данных третьих лиц является формой нарушения неприкосновенности частной жизни, ответственность за которое предусмотрена ст. 137 УК РФ.

Так, приговором Октябрьского районного суда г. Белгорода Б. был признан виновным в совершении преступлений, предусмотренных ч. 1 ст. 137, ч. 1 ст. 273 и ч. 2 ст. 129 УК РФ. Судом было установлено, что Б., используя персональный компьютер, подключённый к информационно-телекоммуникационной сети «Интернет», незаконно используя вредоносную программу, которая является техническим средством подбора персональных идентификаторов пользователя почтовой системы (паролей), с целью негласного получения информации относительно Л., являющейся пользователем социального Интернет-ресурса «Мой мир@mail.ru», действуя из личных неприязненных отношений к ней, подобрал индивидуальный

пароль, используемый потерпевшей, после чего без согласия и ведома Л. Получил доступ к персональным данным последней и произвёл несанкционированное копирование информации с персональной страницы пользователя социального Интернет-ресурса «Мой мир@mail.ru».

Он же, продолжая свою преступную деятельность, умышленно, из личных неприязненных отношений, с целью подорвать репутацию Л., желая унизить её честь и достоинство, для публичной демонстрации, без водома и согласия последней, разместил на открытом для свободного доступа Интернет-ресурсе «www.vkontakte.ru» (Вконтакте), на персональной странице, незаконно созданной им от имени потерпевшей сведения о частной жизни потерпевшей, составляющие её личную и семейную тайну, а именно её фотографию, сведения о фамилии, имени, месте рождения, семейном положении, о месте учёбы, а также разместил заведомо ложную информацию об интимных предпочтениях потерпевшей[292].

К сожалению, в приговоре не описывается, была ли страница потерпевшей обеспечена настройками приватности, пока как данный момент для целей квалификации деяния Б. по ч. 1 ст. 137 УК РФ имеет, на наш взгляд, ключевое значение.

На сегодняшний день многие социальные сети, устанавливая собственную политику конфиденциальности для пользователей, которые задействуют тот или иной Интернет-ресурс в личных целях, закрепляют возможность пользователя самостоятельно устанавливать режим конфиденциальности его персональных данных, определять объём данных, которые должны быть скрыты от третьих лиц, либо объём данных, являющихся общедоступными. А поскольку право на неприкосновенность частной жизни реализуется лицом самостоятельно, по своему усмотрению, то, исходя из этого, правовой режим персональных данных, которые

[292] Приговор Октябрьского районного суда г. Белгорода от 18.08.2010 [Электронный ресурс]: https://rospravosudie.com/court-oktyabrskij-rajonnyj-sud-g-belgoroda-belgorodskaya-oblast-s/act-102866635/

размещаются в социальных сетях, зависит, в первую очередь, от настроек конфиденциальности, установленных пользователем социальной сети.

На наш взгляд, уголовно-правовой охране должны подлежать только те персональные данные, в отношении которых пользователь установил специальные настройки конфиденциальности. В этой связи невозможно разделить позицию, в соответствии с которой уголовное дело возбуждается за незаконное распространение общедоступных персональных данных, видных абсолютно всем пользователям социальной сети. Именно поэтому орган предварительного расследования и суд, которые разрешают дела о преступных посягательствах в отношении персональных данных, должны доподлинно установить, входили ли персональные данные потерпевшего в состав информации, составляющей его личную или семейную тайну, так как общественная опасность преступных посягательств в отношении персональных данных складывается именно из нарушения права человека на тайну, неприкосновенность информации о нём, которая не может быть разглашена третьим лицам или стать достоянием широкого круга людей.

В рассмотренном примере из судебной практики нельзя признать то обстоятельство, что такие сведения, как фамилия и имя потерпевшей являются персональными данными, входящими в режим личной или семейной тайны, поскольку это всего лишь информация родового характера, которая позволяет идентифицировать субъекта персональных данных, но далеко не во всех случаях. Но если эти данные соединить с изображением потерпевшей, то вероятность её идентификации повышается.

В главе 1 мы уже высказывали позицию, в соответствии с которой не по любой категории персональных данных физическое лицо может быть идентифицировано. Всё зависит от конкретных обстоятельств и условий, при которых данная информация о человеке передаётся или устанавливается. Следовательно, для целей уголовно-правовой охраны имеет значение только такой объём персональных данных, который должен отвечать одновременно двум условиям:

1. Объёма персональных данных достаточно, чтобы их субъект мог быть достоверно идентифицирован;
2. Указанный объём персональных данных должен подпадать под соответствующий правовой режим конфиденциальности.

Если хотя бы одно из данных условий отсутствует, то, на наш взгляд, уголовная ответственность лица в таком случае исключается.

В связи с этим, рассмотрим ситуацию, которая теоретически могла бы возникнуть в правоприменительной практике, но пока диссертанту не встретилась: лицо создаёт ложную страницу-аккаунт в социальной сети, но путём копирования общедоступных персональных данных пользователя социальной сети, а именно его изображения, а также фамилии и имени, даты рождения. Юридический анализ данной ситуации с позиций Федерального закона «О персональных данных» позволяет сделать вывод, что на основе данной совокупности имеется достаточно высокая доля вероятности идентификации личности, являющейся субъектом персональных данных. Однако если имело место копирование общедоступных данных, в отношении которых режим конфиденциальности в настройках социальной сети отсутствовал, возникает вопрос, имело ли место незаконное собирание или распространение персональных данных, подпадающих под соответствующий правовой режим конфиденциальности?

Представляется, что ответ на данный вопрос должен исходить из критериев и признаков деяний, входящих в объективную сторону соответствующего преступного посягательства в отношении персональных данных.

Так, ч. 1 ст. 137 УК РФ, как было нами уже рассмотрено выше, устанавливает ответственность за незаконное собирание или распространение сведений о частной жизни, лица, составляющих его личную или семейную тайну, без его согласия. Отсюда следует, что объективная сторона преступления считается выполненной, если сведения, которые были собраны или распространены, по форме входили в состав личной или

семейной тайны, а также, если субъект персональных данных не давал в этом случае своего согласия на их собирание или распространение. Применительно к социальным сетям, на наш взгляд, первый критерий как раз является не чем иным, как реализацией права на установление режима конфиденциальности персональных данных. Таким образом, уголовная ответственность должна наступать только в том случае, если субъект персональных данных установил настройки конфиденциальности. Но если эти настройки не были установлены, то критерий режима тайны не соблюдён.

С другой стороны, если рассмотреть иное описание альтернативных признаков объективной стороны преступления, предусмотренного ч. 1 ст. 137 УК РФ, то можно заметить, что криминообразующим признаком является также и распространение персональных данных в средствах массовой информации, публичном выступлении или публично демонстрирующемся произведении. Не так давно изменённое информационное законодательство фактически приравняло социальные сети к средствам массовой информации, а судебная практика достаточно давно исходит из этого принципа, хотя и не по уголовным делам о преступных посягательствах в отношении персональных данных.

Так, с 01 августа 2014 года в Российской Федерации вступил в силу Федеральный закон от 05.05.2014 №97-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей»[293], который установил, что авторы Интернет-ресурсов (сайтов, блогов, социальных сетей) с аудиторией свыше трёх тысяч пользователей в сутки обязан

[293] Федеральный закон «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей» от 05.05.2014 №97-ФЗ // Российская газета. 2014. №6373.

регистрироваться в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также претерпевать целый ряд ограничений, больше характерных для средств массовой информации. Фактически социальные сети и иные Интернет-ресурсы, отвечающие данным условиям, стали подпадать под признаки средств массовой информации, что, впрочем, на наш взгляд, не в полной мере обосновано.

Популярность пользователя социальных сетей отнюдь не превращает его в средство массовой информации, так как эта информация может и не нести в себе какой-либо социальной значимой нагрузки. Именно поэтому законодатель преждевременно приравнял всех Интернет-пользователей, имеющих определённое число подписчиков к средствам массовой информации.

Итак, анализ объективных признаков преступных посягательств в отношении персональных данных позволяет говорить о том, что правоприменителем ещё не в полной мере усвоен институт персональных данных в профильном информационном законодательстве для целей применения уголовного закона, поэтому имеются перспективы дальнейшего совершенствования законодательства и судебной практики.

2.3. Субъективные признаки преступных посягательств на персональные данные

Совершённое лицом общественно опасное деяние, признаваемое на основании уголовного закона преступным, является таковым не только в силу характера и степени общественной опасности и объективных признаков, которые нормативно установлены, но и на основании субъективных признаков, позволяющих идентифицировать лицо, совершившее преступление, и его отношение к совершаемому (совершённому) преступному деянию.

Субъективные признаки преступления характеризуют собой однородную группу юридически значимых признаков, которые характеризуют преступление с какой-то одной стороны. Традиционно в науке уголовного права субъективные признаки рассматривают сквозь призму их характеристики как элементов состава преступления. Как правило, субъективные признаки конкретизируются посредством характеристики субъекта преступления и субъективной стороны преступления [294] . Субъективные признаки, наряду с объективными, являются основанием уголовной ответственности за совершение преступления, а также влияют на квалификацию содеянного. Именно поэтому их установление имеет решающее значение при определении оснований уголовной ответственности, в том числе и за преступные посягательства на персональные данные.

2.3.1. Особенности субъекта преступных посягательств на персональные данные

Субъектом преступления по российскому уголовному закону признаётся лицо, виновно совершившее общественно опасное деяние,

[294] См.: Уголовное право. Общая часть / Отв.ред. А.Н. Тарбагаев. М.: Проспект, 2014. С. 65; Уголовное право России. Общая часть / Под ред. А.И. Рарога. М.: Эксмо, 2011. С. 73.

запрещённое уголовным законом, которое способно нести за это деяние установленную уголовную ответственность. При этом способность лица нести уголовную ответственность за общественно опасное деяние, признаваемое преступным, подчиняется нескольким признакам, которые относятся к признакам так называемого «общего субъекта преступления» - вменяемого физического лица, достигшего возраста, установленного Уголовным законом. Необходимо также учитывать, что субъект преступления может конкретизироваться в соответствующих статьях Особенной части Уголовного кодекса РФ и может существенно отличаться от признаков общего субъекта, становясь специальным субъектом.

Под специальным субъектом преступления в наиболее общем виде принято понимать «вменяемое физическое лицо, достигшее возраста уголовной ответственности и обладающее на момент совершения преступления специфическими чертами и признаками, закреплёнными в соответствующей статье Особенной части Уголовного кодекса РФ. Уголовная ответственность таких лиц может наступить только при наличии у лица, совершившего преступление, указанных в статье Особенной части Уголовного кодекса РФ признаков»[295]. Следовательно, специальный субъект характеризует общественно опасное деяние как преступное только в совокупности с другими обстоятельствами, характеризующими субъекта, которые устанавливаются по уголовному делу. Например, это специальный социальный статус субъекта, его принадлежность к той или иной профессии или сфере деятельности, полу, возрасту и т.д.

Если проанализировать нормы Уголовного кодекса РФ об ответственности за преступные посягательства на персональные данные, то можно прийти к выводу, что для них характерно наличие как общего, так и специального субъекта преступления.

---

[295] Тарасова Ю.В. Специальный субъект преступления и его значение в уголовном праве. Дисс. … канд. юрид. наук. М., 2006. С. 11.

Так, общим субъектом, то есть вменяемым физическим лицом, достигшим возраста шестнадцати лет, можно охарактеризовать преступления, предусмотренные ч. 1 и ч. 3 ст. 137, ч. 1, ч. 3 и ч. 4 ст. 183 УК РФ. Для других же (ч. 2 ст. 137, ч. 2 ст. 183 УК РФ) характерно наличие специального субъекта преступления. При этом необходимо учесть, что специальный характер субъекта преступления раскрывается применительно к каждому виду преступного посягательства на персональные данные по-разному. Рассмотрим признаки специального субъекта в указанных преступлениях.

Итак, часть 2 статьи 137 УК РФ содержит признак специального субъекта, а именно «совершение преступления лицом с использование своего служебного положения». Специальный характер субъекта данного преступления обусловлен его социальным статусом, а именно занятостью по определённой службе или трудовой функции, вследствие чего персональные данные становятся ему известны.

Часть 2 статьи 183 УК РФ, в свою очередь, в качестве признаков специального субъекта предусматривает нахождение предмета преступления у субъекта в силу того, что он был ему доверен или стал известен по службе: «Незаконное разглашение или использование сведений, составляющих коммерческую, налоговую или банковскую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе»[296].

Таким образом, можно сделать вывод, что признаки специального субъекта в указанных видах преступных посягательств на персональные данные совпадают в части доступа к указанному виду информации по роду деятельности в связи с исполнением субъектом своих служебных или трудовых обязанностей, хотя и формулировка данного признака специального субъекта в рассматриваемых нормах отличается. В то же время, очевидно, что указанные признаки не совпадают с признаками

[296] Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ // СЗ РФ. 1996. №25. Ст. 2954.

должностного лица, указанными в примечании к статье 285 УК РФ. Кроме того, этот признак определяет лишь род деятельности субъекта преступления, подчёркивая повышенную общественную опасность неправомерного преступного посягательства на персональные данные, подпадающие под соответствующий правовой режим антикриминальной безопасности.

Между тем, в научной литературе существует множество позиций относительно содержания понятия «использование лицом своего служебного положения», поскольку оно носит определённую долю оценочного характера и раскрывается применительно к конкретным ситуациям.

Так, В.В. Романова полагает, что «в общеуголовном смысле понятие «использование своего служебного положения» может раскрываться посредством толкования нескольких понятий: служебное положение, использование служебного положения, субъект использования служебного положения. При этом служебное положение раскрывается для конкретного субъекта в зависимости от содержания его служебной деятельности – выполнения определённых профессиональных функций; использование субъектом своего служебного положения – выполнение функций с целью, связанной с достижением преступного результата; под лицами, использующими своё служебное положение, следует понимать должностных лиц, государственных и муниципальных служащих, а также служащих в целом, которые в широком смысле осуществляют свою профессиональную деятельность»[297].

По мнению Рясова А.В., «под совершением преступления с использованием служебного положения следует понимать совершение преступного деяния лицом, осуществляющим функции представителя власти или выполняющим управленческие функции в государственном органе, органе местного самоуправления, государственном или муниципальном

[297] Романова В.В. Специальный субъект общеуголовных преступлений, совершаемых с использованием служебного положения // Криминалистъ. 2011. №1(8). С. 30-33.

учреждении, государственной корпорации, коммерческой или иной организации, путём злоупотребления или превышения своих служебных полномочий. Таким образом, субъект преступления, совершаемого с использованием служебного положения, безусловно, является специальным. В таком случае, субъекта преступлений, совершаемых с использованием служебного положения, необходимо разделять на три группы: первая – лица, выполняющие организационно-распорядительные или административно-хозяйственные функции в государственных органах, органах, органах местного самоуправления, государственных и муниципальных учреждениях и т.д.; вторая – лица, выполняющие указанные функции в коммерческих и иных организациях; третья – лица, осуществляющие функции представителей власти»[298].

Л.В. Иногамова-Хегай и С.С. Черебредов полагают, что «понятие «использование служебного положения» как признак субъекта любого преступления свидетельствует о повышенной общественной опасности таких преступлений, поскольку, даже оставаясь рядовым служащим, последний, находясь в системе служебной иерархии, имеет, как правило, возможность оказать содействие, каким-либо образом повлиять на ход того или иного процесса, на который не могут повлиять иные лица, не являющиеся служащими данной организации. Таким образом, субъект преступлений, совершаемых с использованием служебного положения, необходимо понимать широко и не только в контексте должностных лиц, но и в контексте осуществления любой служебной деятельности»[299].

В.В. Сверчков применительно к рассматриваемым видам преступлений трактует использование служебного положения как «признак субъекта достаточно широко, указывая, что использование лицом своего служебного положения предполагает реализацию данным лицом для

---

[298] Рясов А.В. Признак «использование служебного положения» и его уголовно-правовая оценка по уголовному законодательству России. Дисс. … канд. юрид. наук. – Ростов-на-Дону, 2010. С. 135.

[299] Иногамова-Хегай Л.В., Черебедов С.С. Квалификация преступлений, совершённых с использованием служебного положения / Л.В. Иногамова-Хегай, С.С. Черебедов. // Уголовное право. 2008. №4. С. 29.

облегчения совершения преступления предоставленных по службе полномочий, а равно использование своего профессионального статуса»[300].

Н.А. Егорова указывает, что «наличие в Уголовном кодексе РФ такого квалифицирующего признака, как совершение деяния лицом с использованием своего служебного положения, позволяет считать специальным субъектом преступления служащего, независимо от вида службы, в том числе и не наделённого управленческими полномочиями»[301].

Аналогично предыдущей позиции, А.Г. Чирков предлагает понимать под субъектом преступлений, совершаемых с использованием служебного положения служащего, понятие которого необходимо трактовать широко, потому что использование служебного положения не должно ограничиваться только сферой государственного или муниципального управления. Речь должна идти также и об осуществлении лицом какой-либо деятельности во всех сферах общественной жизни. Определяющим признаком здесь должно выступать выполнение лицом своих полномочий, а также то, каким образом эти полномочия исполняются[302].

И.П. Галыгина считает, что «под использованием служебного положения следует понимать такие действия лица, которые непосредственно вытекали из его полномочий и являлись осуществлением прав и обязанностей, которыми наделялось это лицо в связи с занимаемой должностью, то есть составляющими его служебную компетенцию. При этом лицо осуществляет свою служебную деятельность и обладает статусом служащего»[303].

По нашему мнению, признак субъекта «совершение преступления лицом с использование служебного положения» должен быть конкретизирован в каждом конкретном случае преступного поведения.

---

[300] Сверчков В.В. Уголовное право. Общая и Особенная части: учебное пособие. М., 2009. С. 393.
[301] Егорова Н.А. Служащий как специальный субъект преступления в уголовном праве России // Уголовное право. 2004. №2. С. 26.
[302] Чирков А.П. Служащий как субъект преступлений, совершаемых с использованием служебного положения // Вестник Балтийского федерального университета им. И. Канта. 2010. №9. С. 25.
[303] Галыгина И.П. Нарушение неприкосновенности частной жизни, совершённое лицом с использованием своего служебного положения // Вестник Кемеровского государственного университета. 2010. №1. С. 125.

Данное понятие будет несправедливо ограничивать только сферой исполнения функций должностного лица, лица, исполняющего управленческие функции в коммерческой или иной организации, или лица, выполняющего функции представителя власти. Здесь необходимо исходить из содержания его служебной деятельности, а также влияния его возможностей в связи со службой на совершение преступного деяния.

Служащий, обладая определённый набором функций и обязанностей, может совершать не только преступления против интересов службы, но и общеуголовные преступления, для которых в Особенной части предусмотрен соответствующий квалифицирующий признак. В таких случаях не интересы службы являются самоцелью совершаемых преступлений, а достижение иных преступных результатов, в том числе, например, получение каких-либо выгод имущественного характера. Поэтому не только должностное лицо, обладающее властными или управленческими полномочиями способно совершить преступление с использованием служебного положения. Для должностных преступлений, в которых специальным субъектом является сугубо должностное лицо, использование служебного положения является априорным признаком. Совершение же иных преступлений с использованием служебного положения необходимо, на наш взгляд, толковать шире и включать иных лиц, подпадающих под категорию «служащие», но с тем лишь ограничением, что использование такого инструмента, как служба позволило достичь преступного результата.

Возвращаясь к преступным посягательствам в отношении персональных данных, ещё раз подчеркнём, что субъект ч. 2 ст. 137 и ч. 2 ст. 183 УК РФ является специальным. Соответственно, говоря о данных видах преступных посягательств на персональные данные, следует отметить, что совершение данных преступлений с использованием служебного положения имеет весьма широкое распространение, и, как показывает судебная практика, нарушение различными служащими различных режимов

конфиденциальности персональных данных с определённой мотивацией приводит к совершению данных преступлений.

Нарушение неприкосновенности частной жизни (которое мы рассматриваем как вид преступного посягательства на персональные данные), совершённое лицом с использованием служебного положения, можно охарактеризовать по субъекту как преступление, которое, безусловно, совершается служащим, причём не только государственного органа, органа местного самоуправления, учреждения, но и служащим коммерческой или иной организации. Это подтверждает и судебная практика.

Так, Калининским районным судом г. Тюмени Ф. был признан виновным в совершении преступления, предусмотренного ч. 2 ст. 137 УК РФ. Как было установлено судом, Ф. работал программистом первой категории сектора разработки программ ОАО «Тюменский расчётно-информационный центр». 17 октября 2012 года на своём рабочем месте, используя компьютерное программное обеспечение УМИС «Биллинг-2007», он незаконно скопировал составляющие личную тайну сведения о серии, номере, дате, месте выдачи паспорта и свидетельстве о рождении, а также адресе регистрации по месту жительства шестнадцатилетней девушки. В дальнейшем программист в социальной сети «Вконтакте» продемонстрировал потерпевшей указанные сведения. Как отмечает прокуратура, всё это он делал с елью «запугать девушку»[304].

Таким образом, мы видим, что совершение преступного посягательства в отношении персональных данных лицом с использованием своего служебного положения действительно квалифицируется как таковое без привязки только к государственной или муниципальной службе, но и к любому другому виду трудовой деятельности, в том числе и в коммерческих и иных организациях. И, как справедливо отмечает И.П. Галыгина, «данный признак субъекта должен пониматься не только в ключе использования

[304] Осуждён программист, демонстрировавший похищенные личные данные в соцсети «Вконтакте» [Электронный ресурс]: http://pravo.ru/news/view/82556/

лицом преимуществ, которыми оно обладает в силу занимаемой должности, но и использование возможностей и преимуществ, которыми оно обладает также и в силу выполнения тех или иных обязательств по договору, выполнения профессиональных функций, вне зависимости от места осуществления указанных обязанностей»[305].

При характеристике специального субъекта преступления, предусмотренного ч. 2 ст. 183 УК РФ, мы указали, что его «специальность» определяется наличием такого признака, как осведомлённость информацией в силу службы или работы. Но следует оговориться, что ч. 2 ст. 183 УК РФ предусматривает и другой признак специального субъекта, а именно «осведомлённость информацией лицом, которому она была доверена».

Слово «доверие», как следует из толкового словаря русского языка С.И. Ожегова и Н.Ю. Шведовой, означает уверенность в чьей-либо добросовестности, искренности, в правильности чего-либо[306]. В психологии под «доверием» принято понимать открытые, положительные взаимоотношения между людьми, содержащие уверенность в порядочности и доброжелательности другого человека, с которым доверяющий находится в тех или иных отношениях[307].

Анализ правовой литературы относительно признака «доверия информации» применительно к субъекту преступления, предусмотренного ч. 2 ст. 183 УК РФ показывает, что признак «доверие» в рассматриваемом случае фактически конкретизирует содержание правоотношения о том, каким образом информация, подпадающая под правовой режим банковской, налоговой или коммерческой тайны, появляется у субъекта преступления.

Так, например, указывается, что лицами, которым вменяется совершение преступления, предусмотренного ч. 2 ст. 183 УК РФ, являются

---

[305] Галыгина И.П. Указ. соч. С. 126.

[306] Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений / Российская академия наук. Институт русского языка им. В. В. Виноградова. 4-е изд., дополненное. М.: Азбуковник, 1999. 944 с.

[307] А. Б. Купрейченко, С. П. Табхарова «Критерии доверия и недоверия личности другим людям» // Психологический журнал. 2007. № 2. С. 55-67.

лица, обладающие информацией в силу того, что она была им доверена или стала известна по службе. При этом буквальное толкование данного высказывания означает, что доверие информации должно обязательно быть с привязкой к служебной или трудовой деятельности. Кроме того, к числу таких лиц следует относить служащих государственных органов (налоговых, внутренних дел, прокуратуры, суда, таможни), работников кредитных и иных коммерческих организаций, нотариусов и адвокатов[308].

По мнению Н.А. Лопашенко, «специальный характер субъекта преступления, предусмотренного ч. 2 ст. 183 УК РФ, объясняется тем, что он на законном основании допущен к обладанию коммерческой, налоговой или банковской тайной (руководители коммерческой или иной организации, банкиры, работники налоговых органов, правоохранительных, таможенных и иных органов)»[309].

Как считает Ю.В. Дубровский, «применительно к субъекту преступления, предусмотренного ч. 2 ст. 183 УК РФ, конфиденциальная информация должна быть доверена специальному субъекту лишь на формально-юридических основаниях. К их числу необходимо относить: трудовой договор, должностные обязанности и инструкции (как обязывающий документ), гражданско-правовой договор (договор подряда, договор поставки, договор возмездного оказания услуг и т.п.). Основания такого рода основываются на нормативных установлениях более высокого уровня – нормах федерального законодательства, регламентирующих особые условия и основания охраны коммерческой, налоговой и банковской тайны. Поэтому для реализации уголовно-правовых отношений необходимо установить наличие соответствующих обязательств, зафиксированных в письменной форме»[310].

---

[308] Уголовное право России. Части Общая и Особенная. 2-е изд. / Под ред. А.В. Бриллиантова. М.: Проспект, 2014. С. 223.

[309] Лопашенко Н.А. Преступления в сфере экономики: авторский комментарий к уголовному закону (раздел VIII УК РФ). – М.: Волтерс Клувер, 2006. С. 459.

[310] Дубровский Ю.В. Коммерческая, налоговая и банковская тайна: уголовно-правовой и криминологический аспекты. Дисс. … канд. юрид. наук. М., 2005. С. 16.

Вполне очевидно, что субъект преступления, предусмотренного ч. 2 ст. 183 УК РФ, является специальным. Его специальный характер однозначно обусловлен тем, что законодатель считает более опасным совершение преступления с использованием служебного положения. Правда, в отличие от ст. 137 УК РФ, специальный характер субъекта указанного преступления формулируется несколько иначе и более конкретно. Если в ч. 2 ст. 137 УК РФ указано, что нарушение неприкосновенности частной жизни совершается лицом с использованием служебного положения, то в ч. 2 ст. 183 УК РФ – лицом, которому информация была доверена или стала известна по службе или работе.

На наш взгляд, следует согласиться с позицией, что посягательство на персональные данные применительно к ч. 2 ст. 183 УК РФ при характеристике специального субъекта необходимо производить с привязкой к служебной деятельности, а также совместно с признаком наличия специального юридического основания, по которому информация стала известна лицу – трудовой договор, должностная инструкция, гражданско-правовой договор и т.д. Только в таком случае можно вести речь о том, что информация действительно находилась в ведении субъекта преступления, а он имел реальную возможность ею незаконно воспользоваться.

Содержащая более подробное описание такого признака субъекта преступления, как использование служебного положения, ч. 2 ст. 183 УК по своей формулировке представляется нам более удачной, чем та, которая содержится в ч. 2 ст. 137 УК РФ, поскольку практически устраняет правовую неопределённость в вопросе субъектного состава при решении вопроса о квалификации действий виннового лица. Так, выше мы описывали дискуссию, которая возникает в литературе по поводу субъекта преступления, предусмотренного ч. 2 ст. 137 УК РФ. Для устранения всех неясностей в вопросе применения данной нормы полагаем, что следует предложить новую редакцию диспозиции ч. 2 ст. 137 УК РФ:

«**Статья 137**. 2. Те же деяния, совершённые лицом, которому указанные сведения были доверены или стали известны по службе или работе…».

2.3.2. Особенности субъективной стороны преступных посягательств на персональные данные

Традиционно под субъективной стороной преступления в теории уголовного права принято понимать «психическую деятельность лица, непосредственно связанную с совершением преступления, то есть связанную с выполнением объективной стороны преступления»[311]. Известна также и дискуссия учёных относительно соотношения субъективной стороны преступления с виной, которую некоторые по своему содержанию отождествляют с субъективной стороной преступления, указывая также, что в содержание вины входит ещё мотив и цель[312]. Другие же, напротив, говорят о том, что субъективная сторона преступления является частью законодательной категории вины, которая как раз и выступает общим основанием уголовной ответственности[313]. Наиболее же распространённой позицией в последнее время является та, в соответствии с которой вина является главным элементом (ядром) субъективной стороны, выражая психическое отношение лица к совершённому преступному деянию, пока как мотив и цель являются лишь факультативными элементами субъективной стороны преступления, вводя которые в отдельные статьи Особенной части Уголовного кодекса РФ, законодатель подчёркивает либо повышенную, либо уменьшенную общественную опасность совершённого деяния[314].

---

[311] Дагель П. С., Котов Д. П. Субъективная сторона преступления и ее установление. Воронеж, 1974. С. 41.
[312] См.: Там же. С. 49-51.
[313] См.: Злобин Г.А. Виновное вменение в историческом аспекте // Уголовное право в борьбе с преступностью. М., 1981. С. 23; Демидов Ю.А. Социальная ценность и оценка в уголовном праве. М., 1975. С. 114.
[314] Уголовное право. Общая часть: Учебник / Под ред. А.Н. Тарбагаева. М.: Проспект, 2014. С. 65.

Мы, в свою очередь, будем придерживаться последней позиции, поскольку субъективная сторона преступления является конструктивным элементом состава преступления, при отсутствии которого то или иное деяние отнести к преступному не представляется возможным. И понятие субъективной стороны, как и любых других элементов состава преступления, является комплексным и содержит ряд признаков, характеризующих психическую деятельность лица, совершающего преступление. Следовательно, вина является главным элементом субъективной стороны преступления, выражая психическое отношение лица к совершённому деянию, что во всех случаях квалификации преступлений является неотъемлемым элементом, подлежащим установлению.

Уголовный закон в статье 24, по существу, закрепляет две формы вины, указывая, что виновным в преступлении признаётся лицо, совершившее деяние умышленно или по неосторожности. И при этом деяние, совершённое только по неосторожности, признаётся преступлением лишь в том случае, когда это специально предусмотрено соответствующей статьёй Особенной части УК РФ. Таким образом, закрепляя формы вины, уголовный закон, тем не менее, не даёт легального определения понятия вины. В то же время, закон раскрывает, какие преступные деяния следует относить к деяниям, совершённым с умышленной или неосторожной формой вины.

Как указывается в научной литературе, «сознание и воля применительно к характеристике вины являются элементами психической деятельности человека. Находясь в тесном взаимодействии, интеллектуальные и волевые процессы не могут противопоставляться друг другу, а всякая интеллектуальная деятельность включает в себя и волевые моменты. Предметное содержание каждого из этих элементов определяется конкретным составом преступления»[315]. Следовательно, каждая форма вины для целей привлечения лица к уголовной ответственности отличается от

[315] Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. А.И. Рарог. М.: Проспект, 2011. С. 39.

другой по интеллектуальному и волевому моменту, что и определяет содержание конкретной формы вины в том или ином преступлении. Именно поэтому существует разделение конкретных форм вины на самостоятельные виды, которые могут приобретать самостоятельное значение в рамках отдельных составов преступлений. Такое самостоятельно значение может выразиться в последующем в индивидуализации наказания за совершённое преступное посягательство, которое привело к определённым опасным преступным последствиям.

Если проанализировать статьи уголовного закона, посвящённые уголовной ответственности за преступные посягательства в отношении персональных данных, то можно обнаружить, что большая часть из них совершается с умышленной формой вины. При этом прямой умысел характерен для ч. 2 и 3 ст. 137 и ч. 1 – 4 ст. 183 УК РФ. Однако можно обнаружить некоторую разобщённость мнений в литературе относительно формы вины преступления, предусмотренного ч. 1 ст. 137 УК РФ. Расхождение может наблюдаться также в отношении мнений относительно субъективной стороны всех преступлений, предусмотренных ст. 137 УК РФ.

Большинство авторов исходят из того, что «преступления, предусмотренные ст. 137 УК РФ, могут совершаться только с прямым умыслом. При этом лицо осознаёт, что собирает сведения о частной жизни или распространяет такие сведения без согласия потерпевшего и желает так поступить. Кроме того, совершая подобные действия, лицо осознаёт, что причиняет вред конституционно закреплённому и охраняемому праву на неприкосновенность частной жизни, личной и семейной тайны»[316].

Некоторые же полагают, что преступления, предусмотренные ст. 137 УК РФ, могут совершаться как с прямым, так и с косвенным умыслом. Виновный осознаёт, что незаконно и без согласия заинтересованного лица собирает или распространяет сведения, составляющие личную или семейную

[316] См.: Уголовное право. Общая и Особенная части: учебник / Под общей ред. М.П. Журавлёва и С.И. Никулина. М.: Норма, 2008. С. 197; Уголовное право. Особенная часть: учебник / Отв. ред. И.Я. Козаченко, Г.П. Новосёлов. М.: Норма, 2008. С. 93.

тайну, предвидит возможность причинения своими действиями вреда правам и законным интересам, и желает причинить такой вред (прямой умысел), сознательно его допускает либо относится к нему безразлично (косвенный умысел)[317].

Рассмотрим конструкцию субъективной стороны преступления, предусмотренного ч. 1 ст. 137 УК РФ. Данная норма не содержит специального указания на то, что это преступление может быть совершено по неосторожности. Следовательно, преступление предполагает только умышленную форму вины. Вопрос о форме умышленной вины в рассматриваемом преступлении зависит от содержания интеллектуального и волевого момента совершаемых преступлений.

Так, ч. 2 ст. 25 УК РФ предусмотрено, что преступление признаётся совершённым с прямым умыслом, если лицо осознавало общественную опасность своих действий (или бездействия), предвидело возможность или неизбежность наступления общественно опасных последствий и желало их наступления. Таким образом, преступление, совершённое с прямым умыслом, имеет место быть в том случае, если лицо обладает специальной целью по достижению преступного результата. Интеллектуальный момент данного вида умысла связан с осознанием противоправности деяния, а также предвидения возможности или неизбежности наступления общественно опасных последствий. Волевой же момент является ключевым при разграничении прямого умысла с косвенным и применительно к прямому умыслу заключается в желании наступления общественно опасных последствий. В косвенном же умысле лицо имеет определённую основную цель и совершает конкретные действия по достижению этой цели.

Как пишет И.А. Шевченко, «в процессе совершения преступления у лица может возникнуть предвидение наступления не только основного результата как цели совершения преступления, но и дополнительного,

---

[317] См.: Уголовное право России. Особенная часть. Учебник / Под ред. В.П. Ревина. М.: ЗАО Юстицинформ, 2010. С. 69;

побочного. Поэтому лицо, стремясь достичь основной результат, предвидит наступление побочного результата, не желает его наступления, так как перед ним стоит иная основная цель, но сознательно допускает его наступление или относится к нему безразлично. Злоумышленник в большинстве случае будет стремиться к достижению материальной выгоды, собиранию и распространению компрометирующей потерпевшего информации, удовлетворению личных интересов и т.д., но вероятность того, что он будет желать именно нарушить право потерпевшего, очень мала. Поэтому, по мнению автора, большинство фактов данного преступного поведения совершается именно с косвенным, а не с прямым умыслом»[318].

В то же время, на наш взгляд, применительно к преступлению, предусмотренному ч. 1 ст. 137 УК РФ, в большинстве случаев совершения такого преступления возникновения предвидения наступления какого-либо побочного последствия (преступного результата) со стороны субъекта не прослеживается, поскольку субъект, совершая это преступное деяние, всегда имеет заранее определённый мотив – корыстную или иную личную заинтересованность. Более того, применительно к преступлению, связанному с посягательством на персональные данные, эти мотивы ещё более конкретизируются, поскольку корыстная или иная личная заинтересованность прослеживаются в стремлении лица получить определённые результаты посредством разглашения конфиденциальных сведений, хотя мотивы и не указываются в диспозиции как обязательные признаки субъективной стороны преступления. Кроме того, субъект, безусловно, осознаёт, что, совершая данное преступление, он посягает на неприкосновенность частной жизни лица, чьи персональные данные он неправомерно разглашает, и этим обусловлена, в том числе, общественная опасность преступления. Также анализ преступлений, совершаемых с незаконным оборотом персональных данных и квалифицируемых по ст. 137

[318] Шевченко И.А. Уголовно-правовая охрана неприкосновенности частной жизни. Дисс. … канд. юрид. наук. Красноярск, 2005. С. 125.

УК РФ, показывает, что в последнее время мотив данных преступлений, по большей части, не связан с получением какой-либо материальной выгоды, а, скорее, связан с местью, с возможностью причинить моральный вред, нарушив, таким образом, личное неимущественное право лица, чьи персональные данные незаконно разглашаются[319].

Таким образом, мы можем сделать вывод, что при анализе субъективной стороны преступления, предусмотренного ч. 1 ст. 137 УК РФ, впрочем, как и всех остальных преступлений, предусмотренных указанной статьёй, совершение преступления всегда обусловлено заранее определённой и конкретной целью по достижению преступного результата. Именно поэтому нам представляется, что данные виды преступлений могут совершаться только с прямым умыслом.

Анализ встречающихся в научной литературе мнений относительно субъективной стороны преступлений, предусмотренных ст. 183 УК РФ, показал, что учёные единодушны относительно формы вины, с которой совершается это деяние[320]. В то же время, в отличие от всех остальных рассматриваемых преступлений, деяние, предусмотренное ч. 3 ст. 183 УК РФ напрямую указывается законодателем как совершаемое из корыстной заинтересованности, что подчёркивает обязательное установление мотива совершаемого преступления с целью установления всей его субъективной стороны.

Следует отметить, что все преступные посягательства на персональные данные, по какой бы норме они ни квалифицировались, имеют одну существенную особенность субъективной стороны, которая позволяет отделить их от иных преступных посягательств, подпадающих под действие данных уголовно-правовых норм.

---

[319] См., например: Осуждён интернет-пользователь, опубликовавший сделанную им интимную фотосессию без согласия модели [Электронный ресурс]: http://pravo.ru/news/view/116343; Молодой человек осуждён за страницу «Вконтакте» с изображениями обнажённой девушки своего приятеля [Электронный ресурс]: http://pravo.ru/news/view/115358/

[320] См.: Лопашенко Н.А. Преступления в сфере экономики: авторский комментарий к уголовному закону (раздел VIII УК РФ). М.: Волтерс Клувер, 2006. С. 458. Кочои С.М. Уголовное право. Общая и Особенная части. М.: Волтерс Клувер, 2009. С. 226.

Выше мы пришли к выводу о том, что данные посягательства всегда совершаются только с прямым умыслом, что исключает их совершение с косвенным умыслом. Следовательно, по интеллектуальному и волевому моменту эти преступления характеризуются осознанием противоправности такого посягательства на персональные данные, предвидением наступления общественно опасных последствий (которые, впрочем, в большинстве составов рассматриваемых преступлений значения для квалификации не имеют) и желанием их наступления. На наш взгляд, преступные посягательства в отношении персональных данных отличает то обстоятельство, что направленность умысла на совершение данного преступления всегда сопровождается осознанием субъектом того, что происходит посягательство на конфиденциальную информацию. И если в случае нарушения неприкосновенности частной жизни субъект может и не осознавать, что персональные данные, которые стали ему по какой-либо причине известны, могут подпадать под режим охраняемой законом личной или семейной тайны, то в случае незаконного получения и разглашения профессиональной тайны субъекту о конфиденциальности указанных сведений доподлинно известно, так как выше мы установили, что направленность умысла по этому преступлению обусловлена желанием субъекта причинить материальный ущерб.

В то же время, признак прямого умысла при квалификации действий виновного по ст. 137 УК РФ усиливается, если потерпевший попросил виновного не раскрывать указанную информацию, то есть формально не только не дал своего согласия на разглашение конфиденциальных персональных данных, но и наложил запрет на их разглашение и свободное распространение. В случае же квалификации действий по ст. 183 УК РФ конфиденциальность указанных сведений презюмируется, потому что режим ограничений и запретов в отношении незаконно собираемых и распространяемых субъектом сведений устанавливается на основании закона либо хозяйствующим субъектом.

Следовательно, преступное поведение и направленность умысла субъекта преступления в отношении преступных посягательств на персональные данные тесно связаны с обладанием указанной информацией и осознанием её значимости для потерпевшего, а также неправомерностью её собирания либо распространения.

Итак, проведённый анализ объективных и субъективных признаков преступных посягательств в отношении персональных данных показал, что в действующей российской правовой системе институт персональных данных постепенно осваивается законодателем, формируется определённое представление о справедливом применении законодательства об уголовной ответственности за нарушение неприкосновенности персональных данных. Однако законодателем также создано множество пробелов и проблемных моментов для правоприменения, так как не во всех случаях должна наступать уголовная ответственность за нарушение неприкосновенности персональных данных.

Заключение

Результаты диссертационного исследования показали, что проблема совершенствования уголовного закона в части регулирования уголовной ответственности за преступные посягательства в отношении персональных данных на сегодняшний день приобретает существенное значение. Связано это, главным образом, с тем, что преступные посягательства в отношении персональных данных имеют повышенную социальную опасность, существенным образом нарушают естественные и неотчуждаемые права и свободы человека и гражданина, а также могут вызывать широкий общественный резонанс. Кроме того, число зарегистрированных преступных посягательств в указанной сфере ежегодно стабильно повышается, несмотря на активные меры, предпринимаемые правоохранительными органами, по их предупреждению.

Основной целью настоящего исследования было проведение комплексного анализа института персональных данных в контексте их уголовно-правовой охраны от различных преступных посягательств, а также с позиций правовой теории мер безопасности, совершенствование норм российского уголовного права и иных отраслей законодательства.

Итоги исследования. Желая достичь указанной цели, по результатам проведённого исследования мы пришли к ряду важнейших выводов, выработке различных рекомендаций и основных перспектив проведения дальнейших научных исследований в указанной предметной области.

Содержание охраняемых общественных отношений невозможно без уяснения понятия информации, а также её признаков, в связи с чем автором проанализированы существующие в доктрине и законодательстве определения и выделяемые признаки понятия «информация». Определено, что информация соответствует ряду сущностных признаков, что отличает её от иных смежных понятий. При этом среди таких признаков необходимо выделять следующие характеристики:

1. Информация представляет собой набор логически связанных между собой сведений относительно объекта, представляющего определённый интерес.
2. Данный набор сведений отражает в себе свойства и признаки событий, фактов, явлений, объектов окружающей действительности.
3. Информация способна предоставить человеку возможность получить знания, сделать его осведомлённым относительно событий, фактов, явлений, объектов окружающей действительности, которыми он не обладал на определённый момент времени до получения этих сведений.
4. Информация всегда существует в социально организованном человеческом обществе как универсальное средство коммуникации и как средство межличностного обмена.
5. Информация может быть подвергнута субъективной обработке со стороны человека, поэтому доля её объективности, соответствия действительности будет в каждом случае зависеть от характера её представления (передачи).
6. Происхождение той или иной информации всегда сопряжено с объективными причинами. Развитие общественных отношений всегда связано с передачей определённой информации. Соответственно, те или иные сведения становятся, на наш взгляд, информацией с того момента, когда возникли информационные отношения, и те или иные сведения необходимо донести до определенного или неопределенного круга субъектов. Кроме того, если степень неопределенности по поводу интересующего объекта возрастает, то информация становится инструментом, позволяющим повысить знания об этом объекте.

Автором дано собственное определение информации, которое учитывает все выделенные выше сущностные характеристики. Таким

образом, **информация** определяется следующим образом: это набор логически связанных между собой сведений, отражающий в себе свойства и признаки событий, фактов, явлений, объектов окружающей действительности, который предоставляет возможность познающему субъекту получить осведомлённость о событии, факте, явлении, объекте с целью дальнейшего использования.

Обоснована позиция, в соответствии с которой персональные данные в свете правовой теории мер безопасности являются объектом повышенной охраны, поскольку их ненадлежащий оборот, связанный в том числе с совершением преступных посягательств, может существенным образом оказать вредоносное воздействие на всю систему общественных отношений. В связи этим, задачей государства является создание надлежащего правового инструментария для охраны персональной информации, в том числе от преступных посягательств.

Автором сделан вывод о том, что уголовно-правовая охрана персональных данных осуществляется в соответствии с правовым режимом их конфиденциальности применительно к каждому конкретному случаю.

Кроме того, уголовно-правовой охране должны подлежать только те персональные данные, в отношении которых установлен соответствующий режим их конфиденциальности. Поэтому при расследовании соответствующих уголовных дел задачей органа предварительного расследования является установление содержания конфиденциальности персональных данных, в отношении которых было осуществлено преступное посягательство. В частности, состав преступления будет в любом случае отсутствовать в отношении тех распространенных данных, которые являлись общедоступными или в отношении которых субъект персональных данных не устанавливал режим конфиденциальности.

Рекомендации.

1. В процессе знакомства с различными свойствами информации автором выявлено, что перечень сведений конфиденциального характера на

сегодняшний день продолжает содержаться в Указе Президента РФ, который по своему статусу имеет юридическую силу подзаконного акта. Между тем, установление перечня сведений конфиденциального характера является своеобразным ограничением или установлением специальных режимов безопасности, под которые может подпадать та или иная информация. Установление соответствующего режима конфиденциальности информации само по себе является ограничением конституционного права каждого человека на свободный поиск и распространение информации, в связи с чем не может быть предусмотрено подзаконным актом. В силу ч. 3 ст. 55 Конституции Российской Федерации указанный перечень сведений конфиденциального характера должен быть перенесён в Федеральный закон «Об информации, информационных технологиях и защите информации», поскольку права и свободы человека и гражданина могут быть ограничены только на основании федерального закона.

2. Автором сделан вывод о том, что определение конфиденциальности информации, содержащееся в Федеральном законе «Об информации, информационных технологиях и защите информации» не является полным, так как не отражает в достаточной мере правовую сущность указанного понятия. С учётом принципов правовой охраны информационных правоотношений, заложенных в российском законодательстве, во многих случаях соответствующий режим конфиденциальности может предусматривать множество исключений из установленных режимом правил безопасности. Поэтому автор считает необходимым предложить иную редакцию п. 2 ст. 7 Федерального закона, которая устанавливает, что конфиденциальность информации распространяется на все случаи в отношении конкретного вида информации, за исключением тех, когда обязанность по раскрытию информации предусмотрена федеральным законом.

3. Автором проанализирован термин «персональные данные», и установлено, что определение указанного термина в законе подвергалось

корректировке. Так, в первоначальной редакции законодатель указывал открытый перечень сведений, которые можно было бы отнести к персональным данным. Впоследствии данный перечень из определения был изъят, но оставлены только сущностные признаки, на основании которых ту или иную информацию можно было отнести к персональным данным.

Между тем, учитывая, что персональные данные всегда подпадают под тот или иной режим конфиденциальности, то определение данного термина автором в этой части дополнено указанием на признак конфиденциальности, установленной законом.

4. По мнению автора, понятие «собирание персональных данных», как и понятие «распространение» или «разглашение персональных данных» следует толковать единообразно. Так, уголовно-правовое значение для целей привлечения виновного лица к уголовной ответственности имеет лишь такой поиск информации, который завершился получением искомых сведений. Именно это и должно составлять содержание понятия «собирание персональных данных», поскольку результат такого собирания обладает признаком общественной опасности. В свою очередь, «распространение» или «разглашение» приобретают уголовно-правовое значение в том случае, если осуществлены в отсутствие согласия лица, являющегося правообладателем данных, а также при отсутствии предусмотренных федеральным законом оснований, при которых распространение или разглашение персональных данных допускается без согласия правообладателя (субъекта персональных данных).

5. Автором установлено, что преступные посягательства в отношении персональных данных могут совершаться специальным субъектом. Однако не во всех нормах, посвящённых охране персональных данных, подпадающих под соответствующий правовой режим конфиденциальности, имеется корректная формулировка указанного признака. В связи с этим, предложено изменить формулировку ч. 2 ст. 137 УК РФ, конкретизировав

категорию специального субъекта, совершающего нарушение неприкосновенности частной жизни.

Дальнейшее развитие законодательства о персональных данных, как и развитие уголовного закона, будет являться результатом совершенствования правовых норм, а также следствием разрешения проблем, возникающих в правоприменительной практике.

Библиографический список

Международные правовые акты

1. Директива Европейского Союза 95/46/ЕС Европейского парламента и Совета от 24.10.1995 г. «О защите прав частных лиц применительно к обработке личных данных» // Официальный журнал Европейских сообществ от 23.11.1995 г. №L. 281. С. 31. Разд. 1, затрагивающий качество данных.
2. Европейская конвенция о защите прав человека и основных свобод ETS №005 // СЗ РФ. 1998. №20. Ст. 2143.
3. Конвенция Совета Европы «О защите личности в связи с автоматической обработкой персональных данных» // Сборник документов Совета Европы в области защиты прав человека и борьбы с преступностью.- М.: СПАРК, 1998. С. 106 - 114.

Нормативно-правовые акты

4. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ 05.12.2016 №646) // РГ. 2016. №7144.
5. Закон Российской Федерации «О средствах массовой информации» от 27.12.1991 №2124-1 // РГ от 08.02.1992. №32.
6. Стратегия развития информационного общества в Российской Федерации (утв. Указом Президента РФ 07.02.2008 №Пр-212) // РГ. 2008. №34.
7. Определение Конституционного Суда РФ «Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьёй 137 Уголовного кодекса Российской Федерации» от 28.06.2012 №1253-О // СПС «КонсультантПлюс».

8. Федеральный закон «Об информации, информационных технологиях и защите информации» от 27.07.2006 №149-ФЗ // СЗ РФ. 2006. №31 (ч. I). Ст. 3448.
9. Федеральный закон «О коммерческой тайне» от 29.07.2004 №98-ФЗ // СЗ РФ. 2004. №32. Ст. 3283.
10. Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 06.03.1997 №188 // СЗ РФ. 1997. №10. Ст. 1127.
11. Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ // СЗ РФ. 2006. №31 (ч. I). Ст. 3451.
12. Федеральный закон «О коммерческой тайне» от 29.07.2004 №98-ФЗ // СЗ РФ. 2004. №32. Ст. 3283.
13. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 №395-1 // Ведомости СНД РСФСР. 1990. №27. Ст. 357.
14. Федеральный закон «О внесении изменений в Федеральный закон «О персональных данных» от 25.07.2011 №261-ФЗ // СЗ РФ. 2011. №31. Ст. 4701.
15. Федеральный закон «О гражданстве Российской Федерации» от 21.05.2002 №62-ФЗ // СЗ РФ. 2002. №22. Ст. 2031.
16. Постановление Правительства РФ от 8 июля 1997 г. N 828 "Об утверждении Положения о паспорте гражданина Российской Федерации, образца бланка и описания паспорта гражданина Российской Федерации" // СЗ РФ. 1997. №28. Ст. 3444.
17. Гражданский кодекс Российской Федерации. Часть I // СЗ РФ от 25.12.2006. №52 (1 ч.). Ст. 5496.
18. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 №273-ФЗ // СЗ РФ. 2012. №53 (ч. I). Ст. 7598.
19. Федеральный закон «О полиции» от 07.02.2011 №3-ФЗ // СЗ РФ. 2011. №7. Ст. 900.

20. Федеральный закон «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации» от 30.11.2011 №342-ФЗ // СЗ РФ. 2011. №49 (ч. I). Ст. 7020.
21. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с поправками от 30.12.2008 №6-ФКЗ, от 30.12.2008 №7-ФКЗ) // Российская газета от 25.12.1993 г. №237.
22. Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ // СЗ РФ.2002. №1 (ч. 1). Ст. 3.
23. Федеральный закон «О внесении изменений в статьи 19 и 25 Федерального закона «О персональных данных» от 27.12.2009 г. №363-ФЗ // СЗ РФ.2009. №52 (1 ч.). Ст. 6439.
24. Федеральный закон «О государственной геномной регистрации» от 03.12.2008 №242-ФЗ (ред. от 17.12.2009) // СЗ РФ.2008. №49. Ст. 5740.
25. Федеральный закон «О государственной регистрации недвижимости» от 13.07.2015 №218-ФЗ // СЗ РФ. 2015. №29. Ст. 4344.
26. Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 №1119 // СЗ РФ. 2012. №45. Ст. 6257.
27. Федеральный закон «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства» от 20.08.2004 №119-ФЗ // СЗ РФ. 2004. №34. Ст. 3534.
28. Постановление Правительства РФ «О представлении гражданами, претендующими на замещение должностей в организациях, созданных для выполнения задач, поставленных перед Правительством Российской Федерации, и работниками, замещающими должности в этих организациях, сведений о доходах, расходах, об имуществе и обязательствах имущественного характера, проверки достоверности и полноты представляемых сведений и соблюдения работниками

требований к служебному поведению от 22.07.2013 №613 // СЗ РФ. 2013. №30 (часть II). Ст. 4121.

29. Постановление Правительства РФ «О внесении изменений в Постановления Правительства РФ от 22.07.2013 №613 и от 18.12.2014 №1405» от 25.03.2015 №276 // СЗ РФ. 2015. №14. Ст. 2122.
30. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 №395-I // Ведомости СНД РСФСР. 1990. №27. Ст. 357.
31. Налоговый кодекс Российской Федерации. Часть 1 от 31.07.1998 №146-ФЗ // СЗ РФ. 1998. №31. Ст. 3824.
32. Приказ МНС РФ «Об утверждении порядка доступа к конфиденциальной информации налоговых органов» от 03.03.2003 №БГ-3-28/96 // Бюллетень нормативных актов федеральных органов исполнительной власти. 2003. №23.
33. Решение ПК ВСНП об охране персональных данных граждан [Электронный ресурс]: http://cnlegal.ru/civil_law/network_information_protection/
34. Постановление Европейского Суда по правам человека от 07.07.1989 (§37, серия А, №160) [Электронный ресурс]: http://www.echr.coe.int
35. Постановление Европейского суда по правам человека от 16.02.2000 [Электронный ресурс]: http://www.echr.coe.int
36. Постановление Европейского суда по правам человека от 04.12.2008 [Электронный ресурс]: http://www.echr.coe.int
37. Федеральный закон «О противодействии коррупции» от 25.12.2008 №273-ФЗ // СЗ РФ. 2008. №52 (ч. 1). Ст. 6228.
38. Федеральный закон «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей» от 05.05.2014 №97-ФЗ // Российская газета. 2014. №6373.

39. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ // СЗ РФ. 1996. №25. Ст. 2954.
40. Уголовный кодекс Республики Беларусь [Электронный ресурс]: http://уголовный-кодекс.бел
41. Уголовный кодекс Украины [Электронный ресурс]: http://pravoved.in.ua/section-kodeks/134-yku.html

Диссертации и авторефераты

42. Антонов А.Д. Теоретические основания криминализации и декриминализации: Дисс. … канд. юрид. наук. М., 2001. 182 с.
43. Бодров Р.И. Гражданско-правовые средства индивидуализации граждан (физических лиц): вопросы теории и практики: Дисс. … канд. юрид. наук. М., 2016. 173 с.
44. Бондарь И.В. Тайна по российскому законодательству (проблемы теории и практики). Автореферат дисс. … канд. юрид. наук. Н.Новгород, 2004. 203 с.
45. Дремлюга Р.И. Интернет-преступность. Автореферат дисс. … канд. юрид. наук. Владивосток, 2007. 26 с.
46. Дубровский Ю.В. Коммерческая, налоговая и банковская тайна: уголовно-правовой и криминологический аспекты. Дисс. … канд. юрид. наук. М., 2005. 237 с.
47. Ершов М.А. Ответственность за посягательства на конфиденциальную информацию по российскому уголовному праву. Автореф. дисс. … канд. юрид. наук. Нижний Новгород, 2010. 30 с.
48. Ершов А.М. Ответственность за посягательство на конфиденциальную информацию по российскому уголовному праву: Дисс. … канд. юрид. наук. М., 2010. 237 с.
49. Зайцев В.Н. Уголовно-правовая охрана промышленной собственности: Дисс. … канд. юрид. наук. Нижний Новгород: Нижегородская академия МВД России, 2010. 197 с.

50. Корякина Е.А. Жизнь человека как объект уголовно-правовой охраны. Автореферат дисс. … канд. юрид. наук. Екатеринбург, 2011. 22 с.
51. Крянин С.М. Уголовно-правовая охрана секретов производства: Дисс. … канд. юрид. наук. Нижний Новгород: Нижегородская академия МВД России, 2009. 180 с.
52. Мазуров В.А. Уголовно-правовая защита тайны. Автореферат дисс. … канд. юрид. наук. Барнаул, 2001. 29 с.
53. Маркевич А.С. Организационно-правовая защита персональных данных в служебных и трудовых отношениях. Автореферат дисс. … канд. юрид. наук. Воронеж, 2007. 170 с.
54. Мнацаканян А.В. Информационная безопасность в Российской Федерации: уголовно-правовые аспекты: Дисс. … канд. юрид. наук. М., 2016. 216 с.
55. Пальчиковская О.А. Уголовно-правовая охрана личной и семейной тайны: Дисс. … канд. юрид. наук. М., 2011. 206 с.
56. Паршин С.М. Тайна в уголовном законодательстве (теоретико-прикладное исследование): Дисс. … канд. юрид. наук. Нижний Новгород, 2006. 207 с.
57. Петрыкина Н.И. Правовое регулирование оборота персональных данных в России и странах ЕС (сравнительно-правовое исследование): Дисс. … канд. юрид. наук. М., 2007. 173 с.
58. Плошкина Я.М. Уголовная ответственность за незаконное прослушивание телефонных переговоров и аудио- видеонаблюдение за жилищем по законодательству РФ и ФРГ: Автореферат дисс. … канд. юрид. наук. Красноярск, 2005. 190 с.
59. Рясов А.В. Признак «использование служебного положения» и его уголовно-правовая оценка по уголовному законодательству России. Дисс. … канд. юрид. наук. Ростов-на-Дону, 2010. 212 с.

60. Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: Дисс. … канд. юрид. наук. М., 2005. 168 с.
61. Степанов-Егиянц В.Г.Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект): Дисс. … докт. юрид. наук. М., 2016. 389 с.
62. Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера: Автореферат дисс. … канд. юрид. наук. Владивосток, 2010. 24 с.
63. Тарасова Ю.В. Специальный субъект преступления и его значение в уголовном праве. Дисс. … канд. юрид. наук. М., 2006. 195 с.
64. Терещенко Л.К. Правовой режим информации. Автореферат дисс. … докт. юрид. наук. М., 2011. 54 с.
65. Цадыкова Э.А. Конституционное право на неприкосновенность частной жизни: Сравнительно-правовое исследование. Автореферат дисс. … канд. юрид. наук. М., 2007. 24 с.
66. Шевченко И.А. Уголовно-правовая охрана неприкосновенности частной жизни: Дис. … канд. юрид. наук. Красноярск, 2006. 196 с.
67. Щедрин Н.В. Меры безопасности как средство предупреждения преступности. Дис. ... докт. юрид. наук. Красноярск, 2001. 348 с.
68. Щепетильников В.Н. Уголовно-правовая охрана электронной информации: Автореферат дисс. … канд. юрид. наук. Рязань, 2006. 20 с.
69. Юрченко И.А. Информация конфиденциального характера как предмет уголовно-правовой охраны: Дисс. … канд. юрид. наук. М., 2000. 205 с.

Литература

70. Авдеев М.Ю. Нормативное содержание права на неприкосновенность частной жизни // Новый юридический журнал. 2013. №1. С. 49-54.
71. Антонов А.Д. Теоретические основы криминализации / А.Д. Антонов // Чёрные дыры в российском законодательстве. 2002. №2. С. 80-113.
72. Амелин Р.В. О возможном решении проблемы неполноты главы 28 УК РФ // Уголовно-исполнительная система: право, экономика, управление. 2009. №5. С. 5-6.
73. Афанасьев В.Г. Социальная информация / В.Г. Афанасьев. М., 1994. 200 с.
74. Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право. СПб: Юридический центр Пресс, 2005. 789 с.
75. Безверхов А.Г. О проблеме конструирования составов преступлений по моменту окончания // Вестник Самарской гуманитарной академии. Серия «Право». 2012. №1(11). С. 70-78.
76. Беловский Н. Персональные данные и их защита // Финансовая газета. Региональный выпуск. 2009. №32. С. 24-26.
77. Большая Советская Энциклопедия. В 50 т. / Гл. ред. А.М. Прохоров. – М.: Изд.: Советская Энциклопедия, 1972. Т. 10. 592 с.
78. Большая энциклопедия: В 62 т. Т. 19. М.: ТЕРРА, 2006. 592 с.
79. Борисов Е.Ф., Петров А.А., Березкина Т.Е. Экономика. М.: Проспект, 2015. 272 с.
80. Бундин М.В. Персональные данные как информация ограниченного доступа // Информационное право. 2009. №1. С. 10-14.
81. В городе Сосновый Бор Ленинградской области вынесен приговор бывшему служащему банка за разглашение банковской тайны [Электронный ресурс]: http://prokuratura-lenobl.ru/news/lo/6436
82. В России увеличилось число преступлений с использованием персональных данных [Электронный ресурс]: https://safe-doc.com/v-rossii-uvelichilos-chislo-prestupleniy-s-ispolzovaniem-personalnyh-dannyh

83. В Тюмени осуждён мужчина, который в социальной сети разместил откровенные фото своей бывшей девушки [Электронный ресурс]: http://proctmo.ru/press-center/news/7418/
84. Винер Н. Кибернетика, или Управление и связь в животном и машине. М., 1968. 344 с.
85. 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. 2012. №12. С. 74-80.
86. Войниканис Е., Якушев М. Информация. Собственность. Интернет: Традиции и новеллы в современном праве. М.: Волтерс Клувер, 2004. 176 с.
87. Волженкин Б.В. Преступления в сфере экономической деятельности по уголовному праву России / Б.В. Волженкин. – М.: Юридический центр Пресс, 2007. 765 с.
88. Волохова О.В., Егоров Н.Н., Жижина М.В. и др. Криминалистика: учебник (под. ред. Е.П. Ищенко). - М.: «Проспект», 2011. 504 с.
89. Гаврилин Ю.В. Научно-практический комментарий к статье 272 УК РФ // СПС «КонсультантПлюс».
90. Гайфутдинов Р.Р. Уголовно-правовая характеристика посягательства на персональные данные, обрабатываемые в автоматизированных системах // Учёные записки Казанского университета. Серия: Гуманитарные науки. 2014. №4. Том 156. С. 158-164.
91. Галыгина И.П. Нарушение неприкосновенности частной жизни, совершённое лицом с использованием своего служебного положения // Вестник Кемеровского государственного университета. – 2010. - №1. - С. 125-129.
92. Гаухман Л.Д. Квалификация преступлений: закон, теория, практика. М.: АО «Центр ЮрИнфоР», 2001. – 316 с.

93. Гафнер В.В. Информационная безопасность: учеб. пособие. Ростов-на-Дону: Феникс, 2010. 324 с.
94. Гендиректор осуждена за переписку «Вконтакте» [Электронный ресурс]: http://pravo.ru/news/view/47465/
95. Гладких В.И., Сбирунов П.Н. Особенности квалификации незаконного получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну // Юрист. 2012. №5. С. 36-41.
96. Горелихина О.А., Шлиньков А.А. Правовая защита персональных данных в Германии // Вопросы экономики и права. 2012. №3. С. 322-326.
97. Гостев И.М. Защита коммерческой тайны: история и современность [Электронный ресурс]: http://old.it2b.ru/it2b3.view3.page77.html
98. Гостев И.М. Информационное право: вопросы законодательного регулирования // Технологии и средства связи. 1997. №1. С. 98-102.
99. Государственная зарплатная тайна [Электронный ресурс]: http://www.vedomosti.ru/newspaper/articles/2015/03/30/gosudarstvennaya-zarplatnaya-taina
100. Государственная регистрация – не только учёт, но и контроль, и… Ответственность [Электронный ресурс]: http://www.garant.ru/article/649894/
101. Грачева Ю.В., Ермакова Л.Д. и др. Комментарий к Уголовному кодексу РФ / Отв. ред. А.И. Рарог. – М.: Проспект, 2011. 820 с.
102. Гришмановский Д.Ю. Банковская тайна и проблемы доступа к ней органов расследования // Антология научной мысли: к 10-летию Российской академии правосудия. Сборник статей. – М.: Статут, 2008. – С. 193-197.
103. Дагель П. С., Котов Д. П. Субъективная сторона преступления и ее установление. Воронеж, 1974. 243 с.

104. Данные паспортов Дикушиной и Токарского не являются персональными данными [Электронный ресурс]: http://blog.pravo.ru/blog/6827.html

105. Демидов Ю.А. Социальная ценность и оценка в уголовном праве. – М., 1975. 182 с.

106. Егорова Н.А. Служащий как специальный субъект преступления в уголовном праве России // Уголовное право. 2004. №2. С. 26-28.

107. 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. 118-121.

108. Ефремов А.А. Понятие и виды конфиденциальной информации [Электронный ресурс]: http://www.russianlaw.net/law/confidential_data/a90

109. Ещё раз о персональных данных [Электронный ресурс]: http://old.svobodainfo.org/ru/node/557

110. Женщину, шпионившую за знакомым в «Одноклассниках», будут судить по 3 статьям УК [Электронный ресурс]: http://pravo.ru/news/view/62062

111. За продажу персональных данных абонентов МТС осуждён специалист-наставник сотовой компании [Электронный ресурс]: http://pravo.ru/news/view/103838

112. Закомолдин Р.В. Преступные нарушения специальных правил и требований безопасности: монография. – Тольятти: Филиал РГСУ в г. Тольятти, 2013. 168 с.

113. Закупень Т.В., Соболь С.Ю. Информация и её правовое регулирование // Журнал российского права. 2004. № 1. С. 14-27.

114. Злобин Г.А. Виновное вменение в историческом аспекте // Уголовное право в борьбе с преступностью. М., 1981. С. 22-34.

115. Иванов А.А. Хранение персональных данных за рубежом с точки зрения российского права [Электронный ресурс]: http://zakon.ru/Blogs/xranenie_personalnyx_dannyx_za_rubezhom_s_tochki_zreniya_rossijskogo_prava/16124

116. Иванский В.П. Персональные данные как основной объект посягательств на неприкосновенность сферы частной жизни: законодательный опыт в зарубежных странах // Административное право и процесс. 2012. №8. С. 50-56.

117. Иногамова-Хегай Л.В., Черебедов С.В. Квалификация преступлений, совершённых с использованием служебного положения // Уголовное право. 2008. №4. С. 27-29.

118. Интернет-ресурс «Википедия» [Электронный ресурс]: http://wikipedia.com.

119. Информационный портал SecurityLab [Электронный ресурс]: http://SecurityLab.ru.

120. Каиржанов Е.К. Интересы трудящихся и уголовный закон. Проблемы объекта преступлений. Алма-Ата, 1973. 160 с.

121. Картотека арбитражный дел «Электронное правосудие» [Электронный ресурс]: http://kad.arbitr.ru

122. Каунова А.А. К вопросу о понятии и сущности личной и семейной тайны // Молодой учёный. 2013. №12. С. 644-646.

123. Кибальник А., Соломоненко И. Понятие и виды тайны в уголовном праве // Российская юстиция. 2001. №2. С. 53-55.

124. КоАП получил замечания по всем статьям [Электронный ресурс]: http://pravo.ru/court_report/view/125551

125. Кобзева Е.В. Разграничение преступлений и административных правонарушений: роль законодательной техники // Соотношение преступлений и иных правонарушений: Материалы четвёртой международной научно-практической конференции, посвящённой 250-

летию образования Московского гос. ун-та. М.: ЛексЭст, 2005. С. 225-228.

126. Козлов А.В. Об устранении преград на пути к дифференциации уголовной ответственности за преступления против коммерческой тайны // Уголовное право: истоки, реалии, переход к устойчивому развитию: материалы VI Российского конгресса уголовного права / Под ред. В.С. Комиссарова. М.: Проспект, 2011. С. 329-333.

127. Комментарий к Уголовному кодексу РФ (постатейный) / Под ред. А.В. Бриллиантова. М.: Проспект, 2010. 1392 с.

128. Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. В.М. Лебедев. М.: Юрайт, 2011. 1069 с.

129. Комментарий к Уголовному кодексу Российской Федерации / Под ред. В.Т. Томина и В.В. Сверчкова. М.: Юрайт-Издат, 2010. 334 с.

130. Концептуально-теоретические основы правового регулирования и применения мер безопасности: монография / под науч. ред. Н.В. Щедрина; Сиб. федер. ун-т. Красноярск : СФУ, 2010. 324 с.

131. Копылов В.А. Информационное право. М.: Юристъ, 2009. С. 392.

132. Ковалева Н.Н. Информационное право: учебное пособие. М., 2007. 360 с.

133. Конституция СССР от 05.12.1936 (утратила силу) [Электронный ресурс]: http://www.hist.msu.ru/ER/Etext/cnst1936.htm

134. Конституция (Основной закон) РСФСР от 21.01.1937 [Электронный ресурс]: http://base.garant.ru/185481

135. Коржанский Н.И. Основания и критерии выбора объектов уголовно-правовой охраны // Труды ВСШ МВД СССР. 1976. Вып. 12.

136. Коробеев А.И. Советская уголовно-правовая политика: проблемы криминализации и пенализации. Владивосток: Изд-во ДВГУ, 1987. 267 с.

137. Кочои С.М. Уголовное право. Общая и Особенная части. М.: Волтерс Клувер, 2009. 496 с.

138. Красноярский край. Кадровая политика [Электронный ресурс]: http://www.kadry24.krskstate.ru/press/kadrcentr/0/id/22837

139. Криминология: учебник / Под общ. ред. А.И. Долговой. 4-е изд., перераб. и доп. М.: Норма: Инфра-М, 2010. 1008 с.

140. Крылов В.В. Информационные преступления – новый криминалистический объект // Российская юстиция. 1997. №4. С. 25-28.

141. Кудрявцев В.Н. Общая теория квалификации преступлений. – М.: Юридическая литература, 1972. 352 с.

142. Кудрявцев В.Н. Объективная сторона преступления. М., 1960. 244 с.

143. Кузнецов П.У. Основы информационного права. М.: Проспект, 2014. 312 с.

144. Кузьмин В.П. Понятие и юридическая сущность информации // Информационное право. 2009. №2. С. 4-8.

145. Купрейченко А.Б., Табхарова С.П. «Критерии доверия и недоверия личности другим людям» // Психологический журнал. — 2007. № 2. С. 55-67.

146. Кучеренко А.В. Этапы и тенденции нормативно-правового регулирования оборота персональных данных в Российской Федерации // Информационное право. 2009. №4. С. 32-36.

147. Липатов А. Защита персональных данных // Финансовая газета. Региональный выпуск. 2009. №36.

148. Лопашенко Н.А. Преступления в сфере экономики: авторский комментарий к уголовному закону (раздел VIII УК РФ). М.: Волтерс Клувер, 2006. 720 с.

149. Лопашенко Н.А. Уголовная политика. М.: Волтерс, 2009. 579 с.

150. Лопатин В. Информационная безопасность России. Человек. Общество. Государство. СПб., 2000. 139 с.

151. Лунев А. Е. Административная ответственность за правонарушения. М., 1961. 186 с.

152. Малеина М.Н. Право на тайну и неприкосновенность персональных данных // Журнал российского права. 2010. №11. С. 18-28.

153. Матузов Н.И., Малько А.В. Правовые режимы: вопросы теории и практики / Правоведение. 1996. №1. С. 16-29.

154. Молодой человек осуждён за страницу «Вконтакте» изображениями обнажённой девушки своего приятеля [Электронный ресурс]: http://pravo.ru/news/view/115358

155. Молодцов М.В., Головина С.Ю. Трудовое право России. М., 2010. 704 с.

156. Мошенники легко отберут у вас квартиру [Электронный ресурс]: http://mirnov.ru/ekonomika/nedvizhimost-zhkh/moshenniki-legko-otberut-u-vas-kvartiru.html

157. Наумов В.Б. Право и Интернет: очерки теории и практики. М., 2002. 432 с.

158. Новоселов Г.П. Учение об объекте преступления. Методологические аспекты. М.: Издательство НОРМА, 2001. 208 с.

159. О ратификации Россией Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс]: http://www.coe.mid.ru/doc/avt_obr_PD.htm

160. Осуждён интернет-пользователь, опубликовавший сделанную им интимную фотосессию без согласия модели [Электронный ресурс]: http://pravo.ru/news/view/116343

161. Осуждён программист, демонстрировавший похищенные личные данные в соцсети «Вконтакте» [Электронный ресурс]: http://pravo.ru/news/view/82556/

162. Отчёт о деятельности уполномоченного органа по защите прав субъектов персональных данных за 2015 год [Электронный ресурс]: http://rkn.gov.ru/docs/Otchet_ZPD_rus2015.pdf

163. Палехова Е.И. Конфиденциальная информация и институт персональных данных в банковской деятельности // Предпринимательское право. 2010. №3. С. 40-45.

164. Павлов А.С. Курс церковного права. СПб.: Изд-во Лань, 2002. 384 с.

165. Перешли на личности: в России растёт число краж персональных данных [Электронный ресурс]: https://rg.ru/2017/03/26/v-rossii-vyroslo-chislo-krazh-personalnyh-dannyh.html

166. Петров М.А. Информационно-знаниевая сущность познавательного процесса // Вестник Иркутского государственного университета. 2010. №26(2).

167. Петрухин И.Л. Личная жизнь: пределы вмешательства. М., 1989. 192 с.

168. Пикуров Н.И. Некоторые вопросы уголовно-правовой охраны частной жизни // Уголовно-правовая охрана личности и её оптимизация: Научно-практическая конференция памяти профессора А.Н. Красикова (20-21 марта 2003 г.) / Под ред. Б.Т. Разгильдиева. Саратов, 2003. С. 72.

169. Пионтковский А. А. Учение о преступлении. М., 1961. 666 с.

170. Платон. Аристотель Государства. Законы. Политик. – М.: Мысль, 1998. – С. 35.

171. Покаместова Е.Ю. К вопросу о персональных данных и их классификации в отечественной правовой системе // Проблемы современной семьи: нравственно-психологические, правовые, социально-экономические аспекты: сборник статей третьей межвузовской научно-практической конференции. – Воронеж: МОУ ВЭПИ, 2006. – С. 71-76.

172. Пользователя «Вконтакте» судят за публикацию интимных фото бывшей одноклассницы 10-летней давности [Электронный ресурс]:

http://pravo.ru/news/view/116028/?utm_source=twitter&utm_medium=cpc&utm_campaign=twitter_share

173. Полякова О.Н. Персональные данные: отсрочка на год // Страховые организации: бухгалтерский учет и налогообложение. 2010. №1.

174. Пономарева Ю.В. Законодательство о тайнах: проблемы и пробелы правового регулирования // Вестник Южно-Уральского государственного университета. Серия «Право». 2014. Том 14. №3. С. 110-113.

175. Попова С.И., Шульга А.К. Средства индивидуализации юридических лиц: вопросы теории и практики // Научный журнал КубГАУ. 2015. №113(09). С. 1-11.

176. Постановление СНК СССР от 15.02.1929 «О введении в действие Устава почтовой, телеграфной, телефонной и радиосвязи, утверждённого Постановлением Совета народных комиссаров СССР» [Электронный ресурс]: http://www.lawrussia.ru/authority/body_1933.htm

177. Проект изменений в Закон КНР «О защите прав потребителей» [Электронный ресурс]: http://cnlegal.ru/civil_law/consumer_protection_law_amend_draft

178. Ратификация Конвенции Совета Европы: Защита персональных данных будет усилена [Электронный ресурс]: http://www.privacy-journal.ru/journal/2013y/101/article_895.html

179. Родионов О.С. Правовые режимы как важнейший элемент юридической политики // Правоведение. 1997. №4. С. 157-158.

180. Романова В.В. Специальный субъект общеуголовных преступлений, совершаемых с использованием служебного положения // Криминалистъ. 2011. №1(8). С. 30-33.

181. Русанов Г.А. Преступления в сфере экономической деятельности. Учебное пособие. М.: Проспект, 2014. 264 с.

182. Саврасова В.А. Банковская тайна в системе конфиденциальной информации // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2012. №10(24), часть вторая. С. 156-159.

183. Сверчков В.В. Уголовное право. Общая и Особенная части: учебное пособие. М., 2009. 704 с.

184. Селезнёва С.Г. Понятие тайны в уголовном праве // Вестник Челябинского государственного университета. Серия Право. 2013. Вып. 35. №5(296). С. 95-98.

185. Семенов Е.Е. Информационная глобализация и её влияние на трансформацию социальных связей в современном мире // Вестник Костромского государственного университета им. Н.А. Некрасова. 2010. №1 (том 16). С. 130-134.

186. Серебренникова А.В. Уголовно-правовое обеспечение права на неприкосновенность частной жизни, тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений по законодательству Германии // Иностранное право. Сборник научных статей и сообщений. М.: МАКС-Пресс, 2005. Вып. 5. С. 40-52.

187. Степанов-Егиянц В.Г. Проблемы разграничения неправомерного доступа к компьютерной информации со смежными составами // Право и кибербезопасность. 2014. №2(5). С. 27-32.

188. Судья по делу об убийстве Маркелова и Бабуровой взят под охрану [Электронный ресурс]: http://www.pravo.ru/news/view/49615/

189. Таганцев Н.С. Русское уголовное право. Лекции. Часть Общая. В 2-х т. Т. 1. М., 1994. 823 с.

190. Талонпойка В., Шабалин В. Право на тайну // Гражданская защита. 1999. №4.

191. Терещенко Л.К. Правовой режим персональных данных и безопасность личности // Закон. 2013. №6. С. 36-43.

192. Топ-менеджеров сохранили в тайне [Электронный ресурс]: http://kommersant.ru/doc/2698251

193. Торшин А.В. Соотношение налоговой тайны с другими режимами защиты конфиденциальной экономической информации // Финансовое право. 2002. №1. С. 45-49.

194. Трофимова В. Е. Понятие и содержание личной и семейной тайны // Молодой ученый. 2013. №12. С. 682-685.

195. Туманова Л.В., Снытников А.А. Обеспечение и защита права на информацию. М., 2001. 344 с.

196. Уголовное право России. Общая часть / Под ред. А.И. Рарога. М.: Эксмо, 2011. 496 с.

197. Уголовное право. Общая часть: учебник / Под ред. А.Н. Тарбагаева. М.: Проспект, 2012. 448 с.

198. Уголовное право Российской Федерации. Общая и Особенная части: Учебник / Под ред. А.И. Чучаева. М.: Контракт, Инфра-М, 2013. 704 с.

199. Уголовное право. Особенная часть: учебник / Под ред. И.В. Шишко. М.: Проспект, 2012. 752 с.

200. Уголовное право России: Часть Особенная: учебник для вузов / Отв. ред. Л.Л. Кругликов. М.: Волтерс Клувер, 2012. 839 с.

201. Уголовное право России. Части Общая и Особенная. 2-е изд. / Под ред. А.В. Бриллиантова. М.: Проспект, 2014. 1184 с.

202. Уголовное право. Общая и Особенная части: учебник / Под общей ред. М.П. Журавлёва и С.И. Никулина. М.: Норма, 2008. 816 с.

203. Уголовное право России. Особенная часть. Учебник / Под ред. В.П. Ревина. – М.: ЗАО Юстицинформ, 2010. 392 с.

204. Уголовное право. Особенная часть: учебник / Отв. ред. И.Я. Козаченко, Г.П. Новосёлов. – М.: Норма, 2008. 1008 с.

205. Уголовное уложеніе 22 марта 1903 года / Издание Н.С. Таганцева. – СПб., 1904. 1125 с.

206. Украинцев Б.С. Информация и отражение // Вопросы философии. 1963. № 2. С. 26-41.

207. Уложение о наказаниях уголовных и исправительных 1845 г. (в ред. 1866 и 1885 гг.). Издание четырнадцатое. Издано Н.С. Таганцевым. СПб: Американская Скоропечатня, 1909.

208. Урсул А.Д. Информация и глобальные процессы: междисциплинарные исследования // Знание. Понимание. Умение. 2013. №3. С. 26-33.

209. Устав о наказаниях, налагаемых мировыми судьями [Электронный ресурс]: https://traditio.wiki/Устав_о_наказаниях,_налагаемых_мировыми_судьями

210. Утекшие персональные данные в России всё чаще используются для «кражи личности» [Электронный ресурс]: https://www.infowatch.ru/presscenter/news/7858

211. Федеральный закон «Об информации, информатизации и защите информации» (утратил силу) от 20.02.1995 №24-ФЗ [Электронный ресурс]: http://base.garant.ru/10103678

212. Француз решил отсудить у Uber 48 миллионов долларов из-за распавшегося брака [Электронный ресурс]: https://lenta.ru/news/2017/02/13/uber/

213. Хлевнюк О. В. Хозяин. Сталин и утверждение сталинской диктатуры. М., РОССПЭН, 2012. 478 с.

214. Цадыкова Э.А. Гарантии охраны и защиты персональных данных человека и гражданина // Конституционное и муниципальное право. 2007. №14. С. 15-18.

215. ЦБ может пожертвовать банковской тайной [Электронный ресурс]: http://www.vedomosti.ru/finance/articles/2016/02/18/630132-tsb-mozhet-pozhertvovat-bankovskoi-tainoi

216. Центробанку расширят возможности по истребованию резервных копий клиентских баз [Электронный ресурс]: http://pravo.ru/news/view/126358

217. Чирков А.П. Служащий как субъект преступлений, совершаемых с использованием служебного положения // Вестник Балтийского федерального университета им. И. Канта. 2010. №9. С. 23-25.

218. Чучаев А.И., Фирсова А.П. Уголовно-правовое воздействие: монография. М.: Проспект, 2011. 320 с.

219. Шеховцева Е.В. Налоговая тайна: правовой режим охраны // Ленинградский юридический журнал. 2013. №1. С. 38-42.

220. Щедрин Н.В. Введение в правовую теорию мер безопасности: монография. Красноярск: Краснояр. гос. ун-т, 1999. 180 с.

221. Щедрин Н.В. Источник повышенной опасности, объект повышенной охраны и меры безопасности / Краснояр. гос. ун-т; Н.В. Щедрин. – Красноярск: Юридический институт КрасГУ, 2006.

222. Щедрин Н.В. Концептуально-теоретические основы правового регулирования и применения мер безопасности // Криминология: вчера, сегодня, завтра. 2013. № 4. С. 26-35.

223. Щедрин Н.В. Новый Уголовный кодекс России в контексте социального управления // Lex Russica. 2015. № 3. С. 48-63.

224. Юрченко И.А. Нарушение неприкосновенности частной жизни / И.А. Юрченко // Чёрные дыры в российском законодательстве. 2002. С. 75-79.

225. Act №78-17 of 6 january 1978 On information technology, data files and civil liberties [Электронный ресурс]: http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf

226. Brian K. Atchinson and Daiel M. Fox The Politics of The Health Insurance Portability and Accountability Act // Health affairs. 1997. Vol. 16. Number 3.

227. Bundesdatenshutzgesetz 20.12.1990 [Электронный ресурс]: http://www.juris.de

228. Business and Professions Code Section 22575-22579 [Электронный ресурс]: http://leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579

229. Data Protection Act 1998 [Электронный ресурс]: http://www.legislation.gov.uk/ukpga/1998/29/contents

230. Ein Service des Bundesministeriums der Justiz in Zusammenarbeit mit der juris GmbH. [Электронный ресурс]: http://www.juris.de

231. Electronic communication Privacy Act of 1986 (ECPA), 18 U.S.C. 2510-22 [Электронный ресурс]: https://it.ojp.gov/default.aspx?area=privacy&page=1285

232. Fair and Accurate Credit Transactions Act of 2003 [Электронный ресурс]: http://www.gpo.gov/fdsys/pkg/PLAW-108publ159/html/PLAW-108publ159.htm

233. García González A. La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado [Электронный ресурс]: http: //www.juridicas.unam.mx/publica/rev/boletin/cont/120/art/art3.htm

234. Grundgesetze fuer die Bundesrepublik Deutschland [Электронный ресурс]: http://www.gesetze-im-internet.de/gg/

235. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal [Электронный ресурс]: https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750

236. Real Decreto 1720/2007, de 21 de diciembre, Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal [Электронный ресурс]: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

237. Restriction of access by minors to materials commercially distributed by means of World Wide Web that are harmful to minors [Электронный ресурс]: http://www.law.cornell.edu/uscode/text/47/231

238. Searches and seizures by Government officers and employees in connection with investigation or prosecution of criminal offences [Электронный ресурс]: http://www.law.cornell.edu/uscode/text/42/2000aa

239. The Privacy Protection Act of 1980 [Электронный ресурс]: https://epic.org/privacy/ppa/

Судебная практика

240. Определение Московского городского суда от 29.02.2012 по делу №33-6709 [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

241. Определение Московского городского суда от 20.06.2011 по делу №33-16822 // СПС «КонсультантПлюс».

242. Определение Верховного Суда РФ от 12.09.2012 №56-АПГ12-13 // СПС «КонсультантПлюс».

243. Решение Енисейского районного суда Красноярского края от 24.01.2017 по делу №2-39/2017 [Электронный ресурс]: https://eniseysk--krk.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=283598798&delo_id=1540005&new=0&text_number=1

244. Приговор Октябрьского районного суда г. Новосибирска по делу №1-15/11 от 04.07.2011 [Электронный ресурс]: http://www.gcourts.ru/case/6510527

245. Кассационное определение Пермского краевого суда от 30.06.2011 по делу №22-4187-2011 [Электронный ресурс]: https://rospravosudie.com/court-permskij-kraevoj-sud-permskij-kraj-s/act-103608751/

246. Приговор №1-16/2014 от 12 февраля 2014 г. [Электронный ресурс]: http://sudact.ru

247. Кассационное определение Камчатского краевого суда по делу №22-61/2012 [Электронный ресурс]: судебные решения.рф

248. Кассационное определение Пермского краевого суда от 06.12.2011 по делу №22-9755/2011 [Электронный ресурс]: судебные решения.рф

249. Приговор Соликамского городского суда Пермского края от 16.11.2011 по делу №1-511/11 [Электронный ресурс]: http://sudact.ru

250. Приговор Сосновоборского городского суда Ленинградской области от 12.12.2014 по делу №1-155/2014 [Электронный ресурс]: http://sudact.ru

251. Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югры от 21.10.2014 г. По делу №1-991/2014 [Электронный ресурс]: http://sudact.ru

252. Приговор Менделеевского районного суда Республики Татарстан от 12.02.2014 по делу №1-16/2014 [Электронный ресурс]: http://sudact.ru

253. Приговор Октябрьского районного суда г. Архангельска от 20.01.2012 по делу №1-14/2012 [Электронный ресурс]: http://sudact.ru

254. Приговор Октябрьского районного суда г. Белгорода от 18.08.2010 [Электронный ресурс]: https://rospravosudie.com/court-oktyabrskij-rajonnyj-sud-g-belgoroda-belgorodskaya-oblast-s/act-102866635