ПРЕДИСЛОВИЕ

Суд — носитель судебной власти, реализующий ее посредством соответствующего судопроизводства (конституционного, уголовного, гражданского, административного). Осуществление правосудия по уголовным делам предполагает необходимость правильного и единообразного понимания и применения уголовного закона при разрешении уголовных дел. Для выполнения этой задачи Верховный Суд РФ реализует одно из своих полномочий, предусмотренных Конституцией РФ, в частности статьей 126 — дает разъяснения по вопросам судебной практики. В состав Верховного Суда РФ в числе прочих подразделений входит Пленум Верховного Суда РФ, который, в соответствии с п. 1 ч. 3 Федерального конституционного закона от 5 февраля 2014 г. № 3-ФКЗ «О Верховном Суде Российской Федерации» рассматривает материалы анализа и обобщения судебной практики и дает судам разъяснения по вопросам судебной практики в целях обеспечения единообразного применения законодательства.

Название настоящей книги может вызвать вопрос — для чего нужны комментарии к разъяснениям, которые содержатся в постановлениях Пленума. Ответ достаточно прост. В постановлениях

Пленума разъясняются положения, непосредственно связанные с применением конкретных норм материального и процессуального права, тогда как комментарии к отдельным постановлениям Пленума, содержащиеся в данном сборнике, детализируют их применение в практической деятельности.

ПОСТАНОВЛЕНИЕ
ПЛЕНУМА ВЕРХОВНОГО СУДА РФ
от 15 декабря 2022 г. № 37

«О НЕКОТОРЫХ ВОПРОСАХ СУДЕБНОЙ ПРАКТИКИ ПО УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, А ТАКЖЕ ИНЫХ ПРЕСТУПЛЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ, ВКЛЮЧАЯ СЕТЬ «ИНТЕРНЕТ»

В связи с вопросами, возникающими у судов, и в целях обеспечения единообразного применения ими законодательства об уголовной ответственности за преступления в сфере компьютерной информации, предусмотренные статьями 272, 273, 274 и 274.1 Уголовного кодекса Российской Федерации, а также за иные преступления, совершенные с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», Пленум Верховного Суда Российской Федерации, руководствуясь статьей 126 Конституции Российской Федерации, статьями 2 и 5 Федерального конституционного закона от 5 февраля 2014 года № 3-ФКЗ «О Верховном Суде Российской Федерации», постановляет дать судам следующие разъяснения.

По делам о преступлениях в сфере компьютерной информации

1. Обратить внимание судов на необходимость при рассмотрении уголовных дел о преступлениях, пред-

усмотренных статьями 272, 273, 274 и 274.1 Уголовного кодекса Российской Федерации (далее также — УК РФ), руководствоваться положениями федеральных законов, которые регламентируют вопросы создания, распространения, передачи, защиты информации и применения информационных технологий, в частности федеральных законов от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 26 июня 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и других федеральных законов, подзаконных актов, технических регламентов, а также ратифицированных Российской Федерацией международных договоров и соглашений, посвященных указанным вопросам и борьбе с преступлениями в сфере компьютерной информации, в частности Соглашения о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (заключено в городе Душанбе 28 сентября 2018 года).

2. Судам следует учитывать, что исходя из пункта 1 примечаний к статье 272 УК РФ под компьютерной информацией понимаются любые сведения (сообщения, данные), представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи. Такие сведения могут находиться в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах (далее — компьютерные устройства) либо на любых внешних электронных носителях (дисках, в том числе

жестких дисках — накопителях, флеш-картах и т.п.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи.

При этом к числу компьютерных устройств могут быть отнесены любые электронные устройства, способные выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов (персональные компьютеры, включая ноутбуки и планшеты, мобильные телефоны, смартфоны, а также иные электронные устройства, в том числе физические объекты, оснащенные встроенными вычислительными устройствами, средствами и технологиями для сбора и передачи информации, взаимодействия друг с другом или внешней средой без участия человека), произведенные или переделанные промышленным либо кустарным способом.

3. По смыслу части 1 статьи 272 УК РФ в качестве охраняемой законом компьютерной информации рассматривается как информация, для которой законом установлен специальный режим правовой защиты, ограничен доступ, установлены условия отнесения ее к сведениям, составляющим государственную, коммерческую, служебную, личную, семейную или иную тайну (в том числе персональные данные), установлена обязательность соблюдения конфиденциальности такой информации и ответственность за ее разглашение, так и информация, для которой обладателем информации установлены средства защиты, направленные на обеспечение ее целостности и (или) доступности.

4. В статьях главы 28 Уголовного кодекса Российской Федерации следует понимать:

— под компьютерной программой, с учетом положений статьи 1261 Гражданского кодекса Российской Федерации, — представленную в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения;

— под уничтожением компьютерной информации — приведение такой информации полностью или в части в непригодное для использования состояние с целью утраты возможности ее восстановления, независимо от того, имеется ли фактически такая возможность и была ли она впоследствии восстановлена;

— под блокированием компьютерной информации — воздействие на саму информацию, средства доступа к ней или источник ее хранения, в результате которого становится невозможным в течение определенного времени или постоянно надлежащее ее использование, осуществление операций над информацией полностью или в требуемом режиме (искусственное затруднение или ограничение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением);

— под модификацией компьютерной информации — внесение в нее любых изменений, включая изменение ее свойств, например целостности или достоверности;

— под копированием компьютерной информации — перенос имеющейся информации на другой электронный носитель при сохранении неизменной первоначальной информации либо ее воспроизведение в материальной форме (в том числе отправка по электронной почте, распечатывание на принтере, фотографирование, переписывание от руки и т.п.);

— под нейтрализацией средств защиты компьютерной информации — воздействие, в частности, на технические, криптографические и другие средства, предназначенные для защиты компьютерной информации от несанкционированного доступа к ней, а также воздействие на средства контроля эффективности защиты информации (технические средства и программы, предназначенные для проверки средств защиты компьютерной информации, например, осуществляющие мониторинг работы антивирусных программ) с целью утраты ими функций по защите компьютерной информации или контролю эффективности такой защиты.

5. Применительно к статье 272 УК РФ неправомерным доступом к компьютерной информации является получение или использование такой информации без согласия обладателя информации лицом, не наделенным необходимыми для этого полномочиями, либо в нарушение установленного нормативными правовыми актами порядка независимо от формы такого доступа (путем проникновения к источнику хранения информации в компьютерном устройстве, принадлежащем другому лицу, непосредственно либо путем удаленного доступа).

6. Обратить внимание судов на то, что преступления, предусмотренные статьями 272 и 274 УК РФ, признаются оконченными, когда указанные соответственно в части 1 статьи 272 УК РФ или в части 1 статьи 274 УК РФ деяния повлекли наступление общественно опасных последствий (одного или нескольких) в виде уничтожения, блокирования, модификации либо копирования такой информации, а по статье 274 УК РФ также в виде причинения крупного ущерба.

С учетом этого в ходе рассмотрения каждого дела о преступлении, предусмотренном статьями 272 и 274 УК РФ, подлежат установлению не только совершение неправомерного доступа к компьютерной информации или нарушение соответствующих правил, но и общественно опасные последствия, возможность наступления которых охватывалась умыслом лица, осуществившего такой доступ или допустившего нарушение правил, а также наличие причинной связи между данными действиями и наступившими последствиями. Об отсутствии такой связи может свидетельствовать, в частности, наступление указанных последствий в результате технических неисправностей компьютерных устройств или ошибок при функционировании компьютерных программ.

В случае, когда наступление одних общественно опасных последствий повлекло наступление других (например, модификация информации в виде изменения пароля к учетной записи повлекла блокирование информации — ограничение доступа пользователя к этой записи), все такие последствия должны быть указаны в приговоре.

7. Преступление, предусмотренное статьей 272 УК РФ, считается оконченным с момента наступления хотя бы одного из последствий, указанных в части 1 данной статьи, независимо от длительности неправомерного доступа, причин, по которым он прекратился, а также объема информации, которая была скопирована, модифицирована, блокирована или уничтожена.

Если лицо, намереваясь осуществить уничтожение, блокирование, модификацию или копирование охраняемой законом компьютерной информации, выполнило все действия, необходимые для неправомерного доступа к компьютерной информации, либо осуществило такой доступ, однако ни одно из последствий, предусмотренных частью 1 статьи 272 УК РФ, не наступило по независящим от него обстоятельствам (например, в результате срабатывания автоматизированных средств защиты информации или действий лиц, осуществляющих ее защиту), такие действия следует квалифицировать как покушение на совершение данного преступления.

8. В статье 273 УК РФ к иной компьютерной информации, заведомо предназначенной для несанкционированных блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты, могут быть отнесены любые сведения, которые, не являясь в совокупности компьютерной программой, позволяют обеспечить достижение целей, перечисленных в части 1 статьи 273 УК РФ, например ключи доступа, позволяющие нейтрализовать защиту компьютерной информации, элементы

кодов компьютерных программ, способных скрытно уничтожать и копировать информацию.

Уголовную ответственность по статье 273 УК РФ влекут действия по созданию, распространению или использованию только вредоносных компьютерных программ либо иной компьютерной информации, то есть заведомо для лица, совершающего указанные действия, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

9. Судам следует иметь в виду, что объективная сторона преступления, предусмотренного статьей 273 УК РФ, состоит в выполнении одного или нескольких перечисленных в ней действий.

Создание вредоносных компьютерных программ или иной вредоносной компьютерной информации представляет собой деятельность, направленную на разработку, подготовку программ (в том числе путем внесения изменений в существующие программы) или иной компьютерной информации, предназначенных для несанкционированного доступа, то есть совершаемого без согласия обладателя информации, лицом, не наделенным необходимыми для такого доступа полномочиями, либо в нарушение установленного нормативными правовыми актами порядка уничтожения, блокирования, модифицирования, копирования компьютерной информации или нейтрализации средств ее защиты.

10. Для квалификации действий лица по части 1 статьи 273 УК РФ как оконченного преступления до-

статочно установить создание части (фрагмента) кода вредоносной компьютерной программы, позволяющего осуществить неправомерный доступ к компьютерной информации. В таком случае, если еще не было завершено создание вредоносной компьютерной программы, действия лица подлежат квалификации как создание иной вредоносной компьютерной информации.

11. Распространение вредоносных компьютерных программ или иной вредоносной компьютерной информации состоит в предоставлении доступа к ним конкретным лицам или неопределенному кругу лиц любым способом, включая продажу, рассылку, передачу копии на электронном носителе либо с использованием сети «Интернет», размещение на серверах, предназначенных для удаленного обмена файлами.

Под использованием вредоносных компьютерных программ или иной вредоносной компьютерной информации судам следует понимать действия, состоящие в их применении, в результате которого происходит умышленное уничтожение, блокирование, модификация, копирование компьютерной информации или нейтрализация средств ее защиты.

Если действия виновного лица содержат в себе элементы как распространения, так и использования вредоносной компьютерной программы или иной вредоносной компьютерной информации, оба эти действия должны быть указаны в приговоре.

Следует иметь в виду, что не образует состава преступления использование такой программы или информации лицом на принадлежащих ему компью-

терных устройствах либо с согласия собственника компьютерного устройства, не преследующее цели неправомерного доступа к охраняемой законом компьютерной информации и не повлекшее несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты (например, в образовательных целях либо в ходе тестирования компьютерных систем для проверки уязвимости средств защиты компьютерной информации, к которым у данного лица имеется правомерный доступ), равно как и создание подобных программ для указанных целей.

12. При квалификации действий лица по статье 274 УК РФ судам необходимо установить, какие именно правила из перечисленных в части 1 данной статьи были нарушены, а также возложена ли на это лицо обязанность соблюдать указанные правила.

Данные правила могут быть установлены федеральными законами и подзаконными нормативными правовыми актами, а также инструкциями или иными локальными нормативными актами организаций, если они приняты в развитие указанных законов и подзаконных актов, не противоречат им и не изменяют их содержание. Обязанность соблюдения правил, установленных локальным нормативным актом, должна быть доведена до сведения лица, которому вменяется совершение соответствующего преступления (например, при подписании трудового договора, соглашения на использование сетей или оборудования либо отдельного акта ознакомления с такими правилами).

13. Действия лица квалифицируются по части 1 статьи 274.1 УК РФ, если установлено, что компьютерные программы или иная компьютерная информация предназначены для незаконного воздействия именно на критическую информационную инфраструктуру Российской Федерации, определение понятия которой содержится в статье 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В ином случае действия лица при наличии на то оснований могут быть квалифицированы по статье 273 УК РФ.

При этом следует учитывать, что использование вредоносных компьютерных программ для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (в том числе в случае, когда осуществляется распространение этих программ на объекты критической информационной инфраструктуры исключительно для их последующего использования) полностью охватывается частью 2 статьи 274.1 УК РФ и дополнительной квалификации по статье 273 УК РФ не требует.

14. Под тяжкими последствиями как квалифицирующим признаком в статьях 272–274.1 УК РФ следует понимать, в частности, длительную приостановку или нарушение работы предприятия, учреждения или организации, получение доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу лиц, причинение по неосторожности смерти, тяжкого вреда здоровью хотя бы одному человеку и т.п.

В случае, когда подсудимому вменяется признак создания угрозы наступления тяжких последствий, должна быть установлена реальность такой угрозы.

15. Судам следует иметь в виду, что, когда вредоносная компьютерная программа использовалась для осуществления неправомерного доступа к компьютерной информации и это повлекло наступление последствий, предусмотренных частью 1 статьи 272 УК РФ, действия лица подлежат квалификации по совокупности преступлений, предусмотренных соответствующими частями статей 272 и 273 УК РФ.

16. Если действия, предусмотренные статьями 272–274.1 УК РФ, выступали способом совершения иных преступлений (например, модификация охраняемой законом компьютерной информации производилась с целью нарушения авторских или смежных прав, нарушения неприкосновенности частной жизни, тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений либо неправомерный доступ к ней осуществлялся с целью совершения кражи или мошенничества), они подлежат квалификации по совокупности с преступлениями, предусмотренными соответствующими статьями Уголовного кодекса Российской Федерации. В частности, мошенничество в сфере компьютерной информации (статья 159.6 УК РФ), совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статьям 272, 273 или 274.1 УК РФ.

По делам о преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

17. Под информационно-телекоммуникационной сетью в соответствующих статьях Особенной части Уголовного кодекса Российской Федерации понимается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Для целей уголовного законодательства понятия электронных и информационно-телекоммуникационных сетей не разграничиваются. При этом следует иметь в виду, что сеть «Интернет» является одним из их видов.

Для признания наличия в действиях подсудимого признака совершения преступления с использованием электронных или информационно-телекоммуникационных сетей не имеют значения количество компьютерных устройств, входящих в такую технологическую систему, подключение к ней ограниченного количества пользователей или неопределенного круга лиц, а также другие ее характеристики. Таковыми могут признаваться, в частности, сети операторов связи, локальные сети организаций, домашние локальные сети, а также любые иные сети, предоставляющие возможность двум или более пользователям с помощью любых компьютерных устройств осуществлять проводной или беспроводной доступ к информации, расположенной на компьютерных устройствах, подключенных к данной сети, либо обмен информацией

(передачу сообщений) между компьютерными устройствами.

18. При квалификации действий, совершенных с использованием сети «Интернет», судам следует иметь в виду, что под сайтом в сети «Интернет» понимается совокупность программ для компьютерных устройств и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством сети «Интернет» по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать такие сайты. Страница сайта в сети «Интернет» (далее также — интернет-страница) — часть сайта, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети «Интернет».

19. При определении места совершения преступлений с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», и, соответственно, территориальной подсудности уголовного дела судам необходимо учитывать, что доступ к данной сети может осуществляться с помощью различных компьютерных устройств, в том числе переносных (мобильных). Местом совершения такого преступления является место совершения лицом действий, входящих в объективную сторону состава преступления (например, при публичных призывах к осуществлению экстремистской деятельности — территория, на которой лицом использовалось компьютерное устройство для направления другому лицу электронного сообщения, содержащего такие призывы, независимо от места нахождения другого

лица, или использовалось компьютерное устройство для размещения в сети «Интернет» информации, содержащей призывы к осуществлению экстремистской деятельности).

20. Преступление квалифицируется как совершенное с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», независимо от стадии совершения преступления, если для выполнения хотя бы одного из умышленных действий, создающих условия для совершения соответствующего преступления или входящих в его объективную сторону, лицо использовало такие сети.

В частности, по признаку, предусмотренному пунктом «б» части 2 статьи 228.1 УК РФ, при незаконном сбыте наркотических средств квалифицируются действия лица, которое с использованием сети «Интернет» подыскивает источник незаконного приобретения наркотических средств с целью последующего сбыта или соучастников незаконной деятельности по сбыту наркотических средств, а равно размещает информацию для приобретателей наркотических средств.

По указанному признаку квалифицируется и совершенное в соучастии преступление, если связь между соучастниками в ходе подготовки и совершения преступления обеспечивалась с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» (например, при незаконном сбыте наркотических средств обеспечивалась связь между лицом, осуществляющим закладку наркотических средств в тайники, и лицом, передавшим ему в этих целях наркотические средства).

21. Доступ к электронным или информационно-телекоммуникационным сетям, в том числе сети «Интернет», может осуществляться с различных компьютерных устройств, технологически предназначенных для этого, с использованием программ, имеющих разнообразные функции (браузеров, программ, предназначенных для обмена сообщениями, — мессенджеров, специальных приложений социальных сетей, онлайн-игр, других программ и приложений).

При квалификации действий лиц как совершенных с использованием данных сетей необходимо установить, какие именно компьютерные устройства и программы использовались и какие действия совершены с их помощью.

22. Судам следует иметь в виду особенности квалификации отдельных действий, предусмотренных статьями 242 и 242.1 УК РФ, в случаях, когда они совершаются с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

В частности, под распространением порнографических материалов в данных статьях понимается незаконное предоставление конкретным лицам либо неопределенному кругу лиц возможности их использования. Оно может совершаться путем направления в личном сообщении конкретному лицу (по электронной почте либо с использованием социальных сетей, мессенджеров или иных приложений), рассылки определенному или неопределенному кругу лиц (например, в чат в мессенджере), размещения на личных страницах и на страницах групп пользователей, в том числе в социальных

сетях и мессенджерах, ссылки для загрузки (скачивания) файлов порнографического содержания.

Публичная демонстрация с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», заключается в открытом показе порнографических материалов либо в предоставлении неограниченному числу лиц возможности просмотра таких материалов, однако без возможности самостоятельного их использования (путем сохранения на своем компьютерном устройстве, размещения на интернет-страницах от своего имени и т.п.). Как публичная демонстрация подлежат квалификации действия, совершенные в прямом эфире (в частности, на сайтах, позволяющих пользователям производить потоковое вещание, — стриминговых сервисах), а также состоящие в размещении запрещенной законом информации (материалов, сведений) на личных страницах и на страницах групп пользователей (в социальных сетях или на интернет-страницах).

Рекламирование порнографических материалов или предметов представляет собой распространение любым способом, в любой форме и с использованием любых средств информации, адресованной неопределенному кругу лиц и направленной на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке. Для квалификации действий лица как рекламирования таких материалов или предметов с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет», они могут выражаться в любой форме (например, рассылка

сообщений в социальных сетях, мессенджерах или по электронной почте, размещение на личной странице социальных сетей), но должны быть направлены на достижение перечисленных целей.

При квалификации действий лица, связанных с распространением, публичной демонстрацией или рекламированием порнографических материалов с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет», не имеет значения факт нахождения таких материалов в свободном доступе на момент совершения указанных деяний.

23. Обратить внимание судов на то, что при квалификации преступлений, совершаемых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», должно быть установлено, что лицо осуществляло такие деяния умышленно, осознавало содержание и общественную опасность соответствующих действий, включая характер распространяемой, рекламируемой или демонстрируемой информации, предоставление доступа к ней широкому кругу лиц, а также должны быть установлены другие обстоятельства, имеющие значение для юридической оценки содеянного.

24. При возникновении в ходе рассмотрения уголовных дел о преступлениях, предусмотренных статьями 272, 273, 274 и 274.1 УК РФ, об иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», сомнений в том, относится ли, например, та или иная информация к компьютерной

либо является ли технологическая система, использованная лицом при совершении преступления, электронной или информационно-телекоммуникационной сетью, а также для разъяснения технических терминов и других сложных вопросов, требующих специальных знаний, рекомендовать судьям привлекать к участию в судебном разбирательстве соответствующих специалистов.

КОММЕНТАРИЙ

Постановление Пленума Верховного Суда Российской Федерации принял постановление от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»[1], которое содержит разъяснения, направленные на обеспечение единообразного применения судами законодательства об уголовной ответственности за преступления, предусмотренные как статьями 272, 273, 274 и 274.1,

[1] См.: Постановление Пленума Верховного Суда Российской Федерации 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» // Официальный сайт Верховного Суда РФ: URL: http://www.vsrf.ru/ (дата обращения: 28.12.2022).

так и другими статьями Особенной части Уголовного кодекса Российской Федерации об ответственности за преступления, совершаемые с использованием указанных сетей.

Отметим, что ранее вопросы судебной практики по делам о преступлениях в сфере компьютерной информации на уровне постановления Пленума Верховного Суда Российской Федерации не разъяснялись. Между тем ряд вопросов реализации уголовной ответственности за иные преступления, совершаемые с использованием электронных или информационно-телекоммуникационных сетей, прежде всего касающиеся их квалификации, был разъяснен в отдельных постановлениях Пленума Верховного Суда Российской Федерации[1], а также являлся предметом рассмотрения Судебной коллегии по уголовным делам Верховного Суда Российской Федерации.

Согласно данным Судебного департамента при Верховном Суде Российской Федерации[2] за престу-

[1] См., напр.: постановления Пленума Верховного Суда Российской Федерации от 28 июня 2011 г. № 11 (ред. от 28.10.2021) «О судебной практике по уголовным делам о преступлениях экстремистской направленности»; от 9 февраля 2012 г. № 1 (ред. от 03.11.2016) «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // Официальный сайт Верховного Суда РФ: URL: http://www.vsrf.ru/ (дата обращения: 28.12.2022).

[2] См.: Сайт Судебного департамента при Верховном Суде Российской Федерации: URL: http://www.cdep.ru/ (дата обращения: 28.12.2022).

пления в сфере компьютерной информации, статьи об ответственности за которые входят в главу 28 УК РФ, в 2019 г. было осуждено 165 лиц, в 2020 г. — 137 лиц, а в 2021 г. — уже 225 лиц. Относительно небольшое число осужденных за такие преступления обусловлено рядом обстоятельств, включая сложности, возникающие в ходе их выявления, квалификации и доказывания.

По делам о преступлениях, совершенных с использованием электронных и информационно-телекоммуникационных сетей, включая сеть «Интернет», статистические данные были предоставлены судами в рамках обобщения соответствующей практики. Так, в 2019 г. с вменением данного признака было осуждено 6041 лицо, в 2020 г. — 5696 лиц и в 2021 г. — 6726 лиц. При этом около 80% из них осуждено за преступления, состоящие в незаконном обороте наркотических средств, психотропных веществ или их аналогов (части 2–5 ст. 228.1 УК РФ). Также большую долю преступлений, совершенных с использованием указанных сетей, составляют уголовно наказуемые деяния, связанные с незаконным оборотом порнографии (более 80% таковых осуществляются с использованием сети «Интернет»). В связи с этим, а также с учетом вопросов, поступивших из судов, отдельные пункты постановления Пленума посвящены разъяснению особенностей применения судами названного признака при рассмотрении уголовных дел о преступлениях, связанных с незаконным оборотом наркотиков и порнографии, совершенных с исполь-

зованием электронных или информационно-телекоммуникационных сетей.

Содержание постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 структурно поделено на два раздела, первый из которых включает разъяснения, касающиеся преступлений в сфере компьютерной информации, а второй — разъяснения относительно иных преступлений, совершенных с использованием электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет». При этом разъяснения о применения ст. 274.2 УК РФ, введенной Федеральным законом от 14 июля 2022 г. № 260-ФЗ[1], вследствие отсутствия соответствующей судебной практики в постановлении Пленума не приводятся.

В п. 1 постановления Пленума с учетом бланкетного содержания статей 272, 273, 274 и 274.1 УК РФ внимание судов обращено на необходимость при рассмотрении уголовных дел о преступлениях в сфере компьютерной информации руководствоваться положениями не только уголовного, но и иного федерального законодательства Российской Федерации, регламентирующего порядок осуществления создания, распространения, передачи, защиты информации и применения информационных технологий,

[1] См.: Федеральный закон от 14 июля 2022 г. № 260-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» // Собрание законодательства РФ. 2022. № 29 (ч. II), ст. 5227.

в том числе федеральных законов от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1] и от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[2], подзаконных актов, государственных стандартов, а также ратифицированных Российской Федерацией международных договоров и соглашений в данной области, в частности Соглашения о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий 2018 г.[3]

В п. 2 постановления Пленума раскрывается понятие компьютерной информации. При этом Пленум Верховного Суда РФ, основываясь на содержания п. 1 примечаний к ст. 272 УК РФ, придерживается подхода к пониманию такой информации

---

[1] См.: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 29.12.2022) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 09.01.2023) // Официальный интернет-портал правовой информации http://pravo.gov.ru (дата обращения: 29.12.2022).

[2] См.: Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства РФ. 2017. № 31 (ч. I), ст. 4736.

[3] См.: Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (заключено в г. Минске 01.06.2001) // Бюллетень международных договоров. 2009. № 6. С. 12–17.

в широком смысле, согласно которому к ней относятся любые сведения (сообщения, данные), представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи. Одновременно уточняется, что такие данные могут находиться в запоминающем устройстве электронно-вычислительных машин и других компьютерных устройствах, внешних носителях в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи.

В этом же пункте постановления Пленума дано определение компьютерного устройства, понятие которого является общим для всех статей главы 28 УК РФ. Это понятие также трактуется в широком смысле — как любое электронное устройство, способное выполнять функции по приему, обработке, хранению и передаче информации, закодированной в форме электрических сигналов, независимо от способа его изготовления.

В п. 3 постановления Пленума содержится определение охраняемой законом компьютерной информации, ответственность за неправомерный доступ к которой предусмотрена в ст. 272 УК РФ. В объем этого понятия входит не только информация, для которой законом установлен специальный режим правовой защиты, ограничен доступ либо установлены условия отнесения ее к сведениям, составляющим тайну (в том числе персональные данные), но и информация, для которой правообладателем установлены средства ее защиты, направленные на обеспечение ее целостности и (или) доступности.

С учетом этого по уголовным делам о таких преступлениях необходимо устанавливать, что посягательство осуществлено именно в отношении охраняемой законом компьютерной информации, а также указывать в процессуальных решениях, в связи с чем те или иные сведения относятся к такой информации.

Так, кассационным определением были признаны обоснованными выводы судов первой и апелляционной инстанций относительно совершения С. неправомерного доступа к компьютерной информации, повлекшего модификацию компьютерной информации (ч. 1 ст. 272 УК РФ), выразившегося в изменении сведений о страховом полисе в электронной базе данных страховой компании, содержащей коммерческую тайну и персональные данные клиентов, совершенного после прекращения осужденной трудовых отношений и с использованием чужой учетной записи. При этом решение о том, что такая информация охраняется законом, принято судами на основании положений федеральных законов «О персональных данных» и «О коммерческой тайне», а также локальных нормативных актов[1].

Иные понятия, содержащиеся в статьях главы 28 УК РФ, определены в п. 4 постановления Пленума. Здесь на основе положений законодательства, подзаконных нормативных актов, сложившейся судебной практики и мнений специалистов в области

[1] См.: Кассационное определение Седьмого кассационного суда общей юрисдикции от 26 мая 2022 г. № 77–2372/2022 // СПС «КонсультантПлюс».

информационной безопасности раскрыты понятия компьютерной программы, последствий преступных действий в виде уничтожения, блокирования, модификации, копирования компьютерной информации, а также нейтрализации средств ее защиты.

Понятие неправомерного доступа к охраняемой законом компьютерной информации, образующего общественно опасное деяние, наказуемое по ст. 272 УК РФ, раскрыто в п. 5 постановления Пленума как получение или использование такой информации без согласия обладателя информации лицом, не наделенным необходимыми для этого полномочиями, либо в нарушение установленного нормативными правовыми актами порядка независимо от формы такого доступа (путем проникновения к источнику хранения информации в компьютерном устройстве, принадлежащем другому лицу, непосредственно либо путем удаленного доступа). Это разъяснение имеет большое значение для формирования единообразной практики применения ст. 272 УК РФ, поскольку непосредственно в ней, а равно в других нормах уголовного и иного законодательства определение неправомерного доступа к указанной информации не содержится. При этом Пленум Верховного Суда РФ учитывает положения пунктов 5 и 6 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации», согласно которым обладателем информации признается лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации,

определяемой по каким-либо признакам, а доступом к информации — возможность ее получения и использования.

В п. 6 постановления Пленума подчеркивается материальная конструкция составов преступлений, предусмотренных статьями 272 и 274 УК РФ, признаваемых юридически оконченными, когда неправомерный доступ к охраняемой законом компьютерной информации либо нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям повлекли наступление одного или нескольких общественно опасных последствий в виде уничтожения, блокирования, модификации или копирования такой информации (ст. 272 и ст. 274 УК РФ), либо причинения крупного ущерба (ст. 274 УК РФ). Одновременно обращается внимание на необходимость установления по делам о таких преступлениях не только фактических обстоятельств совершения соответствующего общественно опасного деяния и причинения общественно опасных последствий, но еще и наличие причинной связи между деянием и наступившими последствиями. В качестве примера отсутствия причинной связи приводится ситуация, когда указанные последствия наступают в результате технических неисправностей компьютерных устройств или ошибок при функционировании компьютерных программ.

Пленум Верховного Суда РФ также обращает внимание на случаи причинения преступлением в сфере компьютерной информации двух или более общественно опасных последствий, когда одно последствие выступает причиной наступления другого последствия, в частности, когда модификация информации в виде изменения пароля к учетной записи привело к ограничению доступа пользователя к этой записи, то есть к блокированию информации. При этом в приговоре необходимо отразить все последствия, наступившие в результате совершения соответствующего преступления.

Разъяснения, касающиеся определения момента окончания преступления, предусмотренного ст. 272 УК РФ, конкретизированы в п. 7 постановления Пленума, где указано, что этот момент связан с наступлением хотя бы одного из общественно опасных последствий в виде уничтожения, блокирования, модификации или копирования такой информации, причем длительность неправомерного доступа, причины его прекращения либо объем скопированной, модифицированной, заблокированной или уничтоженной информации не влияют на квалификацию содеянного как оконченного преступления. Также указаны условия привлечения к ответственности за покушение на данное преступление, заключающиеся в выполнении лицом всех действий, необходимых для неправомерного доступа к охраняемой законом компьютерной информации, а равно осуществление такого доступа, если эти действия совершены с намерением уничтожить, заблокировать, модифициро-

вать или скопировать такую информацию, если ни одно из таких последствий не наступило по не зависящим от него обстоятельствам, например, в результате срабатывания автоматизированной защиты или действий лиц по обеспечению защиты информации.

Следовательно, при недоказанности наступления хотя бы одного из последствий, указанных в диспозиции ч. 1 ст. 272 УК РФ, либо умысла на его причинение в результате неправомерного доступа к охраняемой законом компьютерной информации состав данного преступления, в том числе покушения на его совершение, отсутствует.

Например, суд апелляционной инстанции посчитал обоснованным оправдание и исключение из обвинения К. указания на совершение преступления, предусмотренного ч. 1 ст. 272 УК ПФ, поскольку доводы обвинения о том, что К. на правах владельца персональной страницы в социальной сети «ВКонтакте» изменила регистрационные данные (логин и пароль доступа) персональной страницы потерпевшей и тем самым блокировала ей доступ к персональной странице пользователя, не были подтверждены представленными стороной обвинения доказательствами, при этом из материалов дела, в том числе ответа ООО «ВКонтакте», следует, что сведения о каком-либо изменении пароля от указанной страницы в соответствующий период времени отсутствуют[1].

[1] См.: Апелляционное определение судебной коллегии по уголовным делам Кемеровского областного суда от 23 июля 2019 г. по делу № 22–2864/2019.

В п. 8 постановления Пленума раскрыто понятие иной компьютерной информации, создание, использование или распространение которой в ст. 273 УК РФ приравнивается к совершению аналогичных действий с компьютерными программами, заведомо предназначенными для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты. Иная компьютерная информация, имеющая такое же вредоносное назначение, может включать различные сведения, хотя и образующие компьютерную программу, но позволяющие причинить указанные последствия (например, элементы кодов компьютерных программ, способных скрытно уничтожать или копировать информацию).

При характеристике объективной стороны этого преступления в п. 9 постановления Пленума разъяснено, что она может выражаться в одном или нескольких действиях, указанных в диспозиции ч. 1 ст. 273 УК РФ, в том числе в создании лицом вредоносных компьютерных программ или иной вредоносной компьютерной информации, под которым понимается деятельность, направленная на разработку, подготовку программ, включая внесение изменений в уже существующие программы, или иной компьютерной информации, предназначенных для несанкционированного доступа к компьютерной информации, ее уничтожения, блокирования или модификации, а равно нейтрализация средств ее защиты.

В п. 10 постановления Пленума дано важное разъяснение относительно определения момента окон-

чания преступления, предусмотренного ч. 1 ст. 273 УК РФ, совершаемого в форме создания вредоносных программ или иной вредоносной компьютерной информации. Данное преступление признается оконченным уже при создании хотя бы фрагмента кода вредоносной компьютерной программы, посредством которого может быть осуществлен неправомерный доступ к компьютерной информации. В данном случае соответствующая часть программы рассматривается в качестве иной вредоносной компьютерной информации, создание которой квалифицируется как оконченное преступление, предусмотренное ст. 273 УК РФ.

Содержание других общественно опасных действий, предусмотренных ст. 273 УК РФ, заключающихся в распространении вредоносных компьютерных программ или иной вредоносной компьютерной информации, раскрыто в п. 11 постановления Пленума. Сущность распространения вредоносных компьютерных программ или иной вредоносной компьютерной информации состоит в предоставлении доступа к ним как определенным лицам, так и широкому, неопределенному кругу лиц посредством использования различных способов, типичными примерами которых являются продажа, рассылка, передача копий на электронных носителях или с использованием сети «Интернет», размещение на серверах для удаленного обмена файлами. Использование же вредоносных компьютерных программ или иной вредоносной компьютерной информации предполагает осуществление с ними

любых умышленных действий по их применению, в результате которого могут наступить последствия в виде уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализация средств ее защиты.

В случаях, когда при совершении данного преступления лицо полностью или частично осуществило одно или несколько действий, предусмотренных в диспозиции ч. 1 ст. 273 УК РФ, все такие действия должны быть указаны в приговоре, поскольку это позволяет оценить степень общественной опасности содеянного.

Пленум Верховного Суда РФ также обращает внимание на случаи создания вредоносных программ или иной вредоносной компьютерной информации, не обладающие общественной опасностью и, как следствие, не образующие состава преступления, предусмотренного ст. 273 УК РФ, в частности, когда такие действия осуществляются лицом на собственном компьютере или хотя и на чужом компьютерном устройстве, но с согласия его собственника, и не связаны с несанкционированным доступом к охраняемой законом компьютерной информации, а также с наступлением указанных последствий. Например, такие правомерные действия могут преследовать образовательные цели, выполняться для тестирования компьютерных устройств или проверки их уязвимости.

Если вредоносные компьютерные программы или иная вредоносная компьютерная информация предназначены для незаконного воздействия на критиче-

скую информационную инфраструктуру Российской Федерации, определяемую в п. 6 ст. 2 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации», создание, распространение и (или) использование таких программ или информации, как указано в п. 13 постановления Пленума, охватывается ст. 274.1 УК РФ, при этом дополнительная квалификация содеянного по ст. 273 УК РФ не требуется. Если же вредоносная компьютерная программа была использована для неправомерного доступа к охраняемой законом компьютерной информации, и это повлекло ее уничтожение, блокирование, модификацию или копирование, действия лица подлежат квалификации по совокупности преступлений, предусмотренных соответствующими частями статей 272 и 273 УК РФ (п. 15 постановления Пленума).

В п. 12 постановления Пленума даны разъяснения относительно особенностей применения ст. 274 УК РФ об ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Данная уголовно-правовая норма отличается многоуровневой бланкетностью, поскольку соответствующие правила могут быть закреплены как в федеральных законах, так и в подзаконных нормативных правовых актах, а также в принятых в их развитие и не противоречащих им инструкциях и иных локальных нормативных актах определенных организаций. Поэтому при ее применении необходимо выяснить, какие именно

правила были нарушены и была ли возложена на конкретное лицо обязанность по их соблюдению, причем такая обязанность в части соблюдения правил, закрепленных в локальном нормативном акте, должна быть доведена до сведения соответствующего лица, в том числе при подписании трудового договора, соглашения на использование сетей или оборудования либо отдельного акта ознакомления с такими правилами.

Один из наиболее сложных вопросов практики применения статей 274–274.1 УК РФ раскрыт в п. 13 постановления Пленума, посвященном понятию тяжких последствий, наступление или создание угрозы наступления которых закреплено в качестве квалифицирующего признака данных преступлений. Понятие тяжких последствий является оценочным, в связи с чем Пленум Верховного Суда РФ привел отдельные примеры наличия в содеянном такого признака, ориентирующие на понимание его содержания: длительная приостановка или нарушение работы предприятия, учреждения или организации, получение доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу лиц, причинение по неосторожности смерти, тяжкого вреда здоровью хотя бы одному человеку и т.п.

Если лицу инкриминируется совершение соответствующего преступления при наличии квалифицирующего признака, состоящего в создании угрозы наступления тяжких последствий, по делу необходимо установить реальность данной угрозы.

В п. 16 постановления Пленума учтена типичная практическая ситуация, когда действия, наказуемые по статьям 272–274.1 УК РФ, выступают способами совершения других преступлений, в том числе нарушения авторских или смежных прав, нарушения неприкосновенности частной жизни, тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, а равно хищений в форме кражи или мошенничества. В таких случаях содеянное квалифицируется по совокупности преступлений, предусмотренных соответствующими статьями Уголовного кодекса Российской Федерации, например, по ст. 272 и ст. 159.6 УК РФ – как осуществление неправомерного доступа к охраняемой законом компьютерной информации и мошенничество в сфере такой информации. Аналогичное правило квалификации данных преступлений содержится в п. 20 постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате»[1].

Отметим, что совершение лицом нескольких преступлений, посягающих не только на охраняемую законом компьютерную информацию, но и на другие объекты, является типичным для данной категории уголовных дел. Как правило, совокупность таких пре-

[1] См.: Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 (ред. от 15.12.2022) «О судебной практике по делам о мошенничестве, присвоении и растрате» // Официальный сайт Верховного Суда РФ: URL: http://www.vsrf.ru/ (дата обращения: 28.12.2022).

ступлений наблюдается в случаях, когда виновные лица действовали на основе корыстных побуждений.

Например, К. была признана виновной, в частности, в совершении преступлений, предусмотренных ч. 3 ст. 272 УК РФ (3 преступления), ч. 3 ст. 183 (5 преступлений), ч. 4 ст. 159 УК РФ (2 преступления). Установлено, что К., являясь руководящим работником банка, действуя умышленно, из корыстной заинтересованности и используя свое служебное положение, совершила неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее модификацию, использовала сведения, составляющие банковскую тайну, без согласия их владельцев и путем обмана похитила денежные средства в сумме более 13 млн руб. с банковских счетов, открытых на имя клиентов банка[1].

Во втором разделе постановления Пленума содержатся разъяснения по вопросам судебной практики, касающимся иных преступлений, совершаемых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». При этом в пунктах 17, 18 и 19 постановления Пленума даны разъяснения общего характера, касающиеся понятий информационно-телекоммуникационной сети, сайта в сети «Интернет» и страницы та-

[1] См.: Апелляционное определение Брянского областного суда от 15 октября 2021 г. по делу № 1–2/2021; определение Первого кассационного суда общей юрисдикции от 26 октября 2022 г. № 77–4904/2022 // СПС «КонсультантПлюс».

кого сайта, а также особенностей места совершения данных преступлений.

Так, определение информационно-телекоммуникационной сети основано на положениях п. 4 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации», при этом такой сетью признается технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Одновременно уточняется, что для целей уголовного законодательства понятия электронных и информационно-телекоммуникационных сетей, видом которых является сеть «Интернет», не разграничиваются, при этом в объем общего понятия таких сетей входят, в частности, сети операторов связи, локальные сети организаций, домашние локальные сети, а также любые иные сети, предоставляющие возможность двум или более пользователям с помощью различных компьютерных устройств осуществлять проводной или беспроводной доступ к информации, расположенной на компьютерных устройствах, подключенных к данной сети, либо обмен информацией (передачу сообщений) между такими устройствами.

На квалификацию преступления по признаку его совершения использованием электронных или информационно-телекоммуникационных сетей не влияют количество компьютерных устройств, входящих в указанную технологическую систему, подключение к ней определенного (ограниченного) числа пользо-

вателей или неопределенного круга лиц, равно как и другие ее характеристики.

При раскрытии понятий сайта в сети «Интернет» и его страницы в п. 18 постановления Пленума использованы положения п. 13 и п. 14 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации».

В п. 19 постановления Пленума дано важное разъяснение относительно территориальной подсудности уголовного дела, зависящей от определения места совершения преступления, объективная сторона которого включала использование электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет». Им признается то место, где лицом были выполнены действия, входящие в объективную сторону соответствующего состава преступления.

Пленум Верховного Суда РФ обращает внимание на то, что доступ к сети «Интернет» либо иной информационно-телекоммуникационной или электронной сети может осуществляться с помощью различных компьютерных устройств, в том числе переносных (мобильных), поэтому важно определить то место, в котором находилось лицо, использовавшее соответствующее устройство для совершения преступления, например, место, где лицо пользовалось компьютером для размещения в сети публичных призывов к осуществлению экстремистской деятельности вне зависимости от места нахождения других лиц, воспринимающих такую информацию.

Кроме того, как разъяснено в п. 21 постановления Пленума, при совершении преступления могут применяться различные компьютерные устройства, а равно программы, имеющие разнообразные функции, например браузеры, мессенджеры, специальные приложения социальных сетей, в связи с чем при квалификации содеянного по признаку использования соответствующих сетей необходимо установить, какие именно компьютерные устройства и программы были задействованы и какие действия совершены с их помощью.

В п. 20 постановления Пленума содержатся разъяснения, имеющие большое значение для формирования практики по уголовным делам о преступлениях, совершаемых с использованием указанных сетей. При этом общим является разъяснение, согласно которому преступление квалифицируется как совершенное с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет», независимо от стадии его совершения, если для выполнения хотя бы одного из умышленных действий, создающих условия для совершения соответствующего преступления или входящих в его объективную сторону, лицо использовало такие сети. То есть квалификация с учетом данного признака осуществляется в случаях, когда электронная или информационно-телекоммуникационная сеть использовалась виновными лицами как на стадиях покушения или оконченного преступления, так и в процессе приготовления к совершению последнего.

Это разъяснение особенно актуально для преступлений, связанных с незаконным оборотом наркотических средств, психотропных веществ или их аналогов, в связи с чем Пленум Верховного Суда РФ в качестве примера дополнительно указывает, что сбыт наркотического средства квалифицируется по признаку, предусмотренному п. «б» ч. 2 статьи 228.1 УК РФ, если соответствующее лицо с использованием сети «Интернет» подыскивает источник незаконного приобретения наркотических средств с целью последующего сбыта или соучастников незаконной деятельности по сбыту наркотических средств, либо размещает информацию для их приобретателей. Аналогичная квалификация содеянного производится и в случаях, когда при совершении преступления в соучастии связь между соучастниками в ходе приготовления и совершения преступления обеспечивалась с использованием указанных сетей «Интернет», например, при совместном осуществлении незаконного сбыта наркотических средств с использованием так называемых закладок.

Так, кассационным определением оставлены без изменения приговор и апелляционное определение, которыми П. признан виновным в совершении преступлений, предусмотренных ч. 3 ст. 30, п. «г» ч. 4 ст. 228.1 УК РФ (2 преступления) и ч. 3 ст. 30, п. «б» ч. 2 ст. 228.1 УК РФ. При этом указано, что из исследованных судом и приведенных в приговоре доказательств следует, что два покушения на незаконный сбыт психотропных веществ, группой лиц по предварительному сговору, в крупном размере,

а также покушение на незаконный сбыт наркотических средств, группой лиц по предварительному сговору, в значительном размере П. совершены с использованием информационно-телекоммуникационной сети «Интернет», посредством которой он вступил в предварительный преступный сговор, направленный на незаконный сбыт наркотических средств и психотропных веществ, с соучастником преступления, от которого впоследствии также через сеть «Интернет» получал сведения о местонахождении отдельных партий психотропных веществ и наркотических средств, предназначенных для незаконного сбыта, которые П. должен был забирать и раскладывать по одиночным тайникам-закладкам, фотографировать местонахождения этих закладок, и, с добавлением географических координат и текстовых пояснений, самостоятельно прикреплять эти фотографии и сведения к витрине «Интернет-магазина», используемого для незаконного сбыта наркотических средств и психотропных веществ. С учетом данных обстоятельств суд правильно усмотрел наличие в преступных действиях П. по всем инкриминируемым ему деяниям квалифицирующего признака, предусмотренного п. «б» ч. 2 ст. 228 УК РФ[1].

В п. 22 постановления Пленума даны важные разъяснения, касающиеся особенностей юридической оценки отдельных действий, предусмотрен-

[1] См.: Кассационное определение Третьего кассационного суда общей юрисдикции от 1 марта 2022 г. № 77-633/2022 // СПС «КонсультантПлюс».

ных статьями 242 и 242.1 УК РФ, связанных с незаконным оборотом порнографических материалов с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет».

Распространение порнографических материалов определяется как незаконное предоставление конкретным лицам либо неопределенному кругу лиц возможности их использования. Способами распространения таких материалов могут являться, в частности, их направление в личном сообщении конкретному лицу, рассылка определенному или неопределенному кругу лиц (например, в чатах или в мессенджерах), размещение на личных страницах и на страницах групп пользователей ссылки для загрузки (скачивания) файлов порнографического содержания.

Публичная демонстрация с использованием электронных или информационно-телекоммуникационных сетей отличается от распространения тем, что она состоит в открытом показе порнографических материалов либо в создании условий для просмотра таких материалов неограниченным кругом лиц, но не связана с предоставлением возможности самостоятельного их использования, например, сохранять на своем компьютерном устройстве либо размещать на интернет-страницах от своего имени. Публичная демонстрация может осуществляться в прямом эфире, включая использование сайтов для потокового вещания — стриминговых сервисов), а равно посредством размещения соответствующей информации (материалов, сведений) на личных страницах

и на страницах групп пользователей (в социальных сетях или на интернет-страницах).

Особенностью рекламирования порнографических материалов или предметов является направленность распространяемой любыми способами информации, адресованной неопределенному кругу лиц, на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке. При этом нахождение порнографических материалов в свободном доступе, в том числе на момент совершения указанных действий, на квалификацию последних не влияет.

Отметим, что данные разъяснения ориентируют суды на разграничение указанных действий, связанных с незаконным оборотом порнографических материалов и предметов, а также на выяснение обстоятельств, подтверждающих или опровергающих наличие таких действий по конкретному делу.

Так, Судебная коллегия по уголовным делам Верховного Суда РФ отменила кассационное определение, которым П. был оправдан в совершении преступления, предусмотренного п. «б» ч. 3 ст. 242 УК РФ, состоявшем в незаконном распространении и публичной демонстрации порнографических материалов с использованием сети «Интернет», и направила дело на новое кассационное рассмотрение.

Судебная коллегия по уголовным делам Верховного Суда РФ пришла к выводу о том, что судом кассационной инстанции оставлено без внимания, что П., будучи осведомленным об ответственном размещении любой информации (в том числе ссылок —

репостов) на персональной странице и возможности наступления правовых последствий, проигнорировал правила пользования сайтом, разместил и длительное время хранил на ней в открытом доступе ссылку на видеофайл порнографического характера, оставив возможность доступа к своей странице любого пользователя сети «Интернет», при этом ограничения на доступ к своей странице им не устанавливались.

Данное обстоятельство подтвердилось в ходе оперативно-розыскного мероприятия, в рамках которого оперуполномоченным осуществлен свободный доступ на страницу с последующим просмотром и копированием видеофайла с порнографическим содержанием. Сведения о свободном доступе к данной информации содержатся и в показаниях свидетеля.

Сам по себе факт, что П. видеофайл порнографического характера никому не предлагал и не передавал, о чем указано в кассационном определении, а лишь разместил на него ссылку в открытом доступе на своей странице, не свидетельствует об отсутствии у него умысла на незаконный оборот порнографических материалов, поскольку он позволял другим пользователям сети «Интернет» просматривать содержание указанного видеофайла, что, как установлено судом, и имело место.

Суд кассационной инстанции, отменяя состоявшиеся судебные решения, не дал оценку действиям П., исходя из того, что, по смыслу закона, публичная демонстрация с использованием электронных или

информационно-телекоммуникационных сетей, включая сеть «Интернет», заключается в открытом показе порнографических материалов, либо предоставлении неограниченному числу лиц возможности просмотра таких материалов, и следовательно, как демонстрация могут расцениваться действия и совершенные в прямом эфире, и состоящие в размещении (материалов, сведений) на личных страницах и в группах (в социальных сетях или на интернет-страницах), в том числе репост – размещение ссылки непосредственно на информацию в источнике первичного размещения. Также оставлено без внимания то обстоятельство, что П. был признан виновным и осужден не только за распространение порнографических материалов, но и за их публичную демонстрацию, однако каких-либо суждений по данной части обвинения приведено не было[1].

Пленум Верховного Суда РФ в п. 23 постановления подчеркнул необходимость выяснения умышленной формы вины, присущей преступлениям, совершаемым с использованием электронных или информационно-телекоммуникационных сетей. По делам о таких преступлениях подлежит установлению, в частности, что лицо осознавало содержание и общественную опасность соответствующих действий,

[1] См.: Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 8 декабря 2022 г. № 1-УДП22–10-К3 // Официальный сайт Верховного Суда РФ: URL: http://www.vsrf.ru/ (дата обращения: 28.12.2022).

включая характер распространяемой, рекламируемой или демонстрируемой информации, предоставление доступа к ней широкому кругу лиц.

Например, Судебная коллегия по уголовным делам Верховного Суда РФ оставила без изменений кассационное определение, которым за отсутствием состава преступления было прекращено уголовное дело в отношении М., обвинявшегося в приобретении, хранении в целях распространения, а также распространении материалов с порнографическими изображениями несовершеннолетних, в отношении лица, не достигшего четырнадцатилетнего возраста с использованием информационно-телекоммуникационной сети «Интернет» (п. «а» и п. «г» ч. 2 ст. 242.1 УК РФ). При этом Судебная коллегия, в частности, указала, что приведенные в кассационном представлении прокурора доказательства подтверждают сам факт скачивания М. видеоролика порнографического содержания на свой компьютер и размещение его в открытой папке, доступной для просмотра иными лицами. Также указана ссылка на показания М., полученные в ходе предварительного следствия, как на доказательство его виновности, однако по поводу его утверждений об удалении видеоролика, имеющих существенное значение для правильного разрешения дела, какие-либо суждения не приводятся.

Принимая во внимание то обстоятельство, что удаление видеоролика исключало доступ к нему как самого М., так и иных лиц, показания в судебном заседании М., который отрицал наличие у него умысла

на распространение порнографических материалов, Судебная коллегия нашла обоснованным вывод суда кассационной инстанции об отсутствии доказательств, свидетельствующих о том, что М. совершил действия, направленные на распространение видеоролика порнографического содержания, что стороной обвинения не было представлено каких-либо доказательств того, что М. предлагал или передавал иным лицам скачанный им видеофайл. Как правильно указано в кассационном определении, совершенные М. действия по скачиванию и хранению видеоролика порнографического содержания на своем персональном компьютере, сами по себе не позволяют сделать бесспорный вывод о наличии у него умысла на их распространение[1].

Поскольку производство по уголовным делам о преступлениях в сфере компьютерной информации, предусмотренных статьями 272, 273, 274 и 274.1 УК РФ, и иных преступлениях, совершаемых с использованием электронных и информационно-телекоммуникационных сетей, связано с разрешением ряда сложных технических вопросов, в том числе с устранением сомнений относительно признания той или иной информации компьютерной, в п. 24 постановления Пленума судам рекомендовано привлекать к участию в судебном разбирательстве специалистов в соответствующей области.

---

[1] См.: Определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 4 августа 2022 г. № 127-УД22–12-К4 // СПС «КонсультантПлюс».

ПОСТАНОВЛЕНИЕ
ПЛЕНУМА ВЕРХОВНОГО СУДА РФ
от 28 июня 2022 г. № 20

«О НЕКОТОРЫХ ВОПРОСАХ СУДЕБНОЙ ПРАКТИКИ ПО УГОЛОВНЫМ ДЕЛАМ О ПРЕСТУПЛЕНИЯХ ПРОТИВ ПРАВОСУДИЯ»

В связи с вопросами, возникающими у судов, и в целях обеспечения единообразного применения ими законодательства об уголовной ответственности за преступления против правосудия, предусмотренные статьями 301–303, 306, 307 Уголовного кодекса Российской Федерации, Пленум Верховного Суда Российской Федерации, руководствуясь статьей 126 Конституции Российской Федерации, статьями 2 и 5 Федерального конституционного закона от 5 февраля 2014 года № 3-ФКЗ «О Верховном Суде Российской Федерации», постановляет дать судам следующие разъяснения:

1. Обратить внимание судов на необходимость при рассмотрении уголовных дел о преступлениях, предусмотренных статьями 301–303, 306, 307 Уголовного кодекса Российской Федерации (далее также — УК РФ), руководствоваться положениями федеральных законов, которые наряду с Уголовно-процессуальным кодексом Российской Федерации (далее также — УПК РФ) регламентируют основания и порядок содержания лиц, задержанных по подозрению в совершении преступления, проведения оперативно-розыскных мероприятий и использования результатов оперативно-розыскной деятельности, порядок осуществления судебно-экспертной

деятельности, а также учитывать нормы, содержащиеся, в частности, в Арбитражном процессуальном кодексе Российской Федерации, Гражданском процессуальном кодексе Российской Федерации, Кодексе административного судопроизводства Российской Федерации, Кодексе Российской Федерации об административных правонарушениях, устанавливающие порядок собирания, проверки, оценки доказательств и определяющие состав, полномочия, права, обязанности участников соответствующего вида судопроизводства.

2. Под ***заведомо незаконным задержанием****, ответственность за которое предусмотрена частью 1 статьи 301 УК РФ, следует понимать совершение дознавателем, начальником подразделения дознания, начальником органа дознания, следователем, руководителем следственного органа или по их поручению иным должностным лицом умышленных действий, направленных на незаконное применение меры процессуального принуждения в виде задержания подозреваемого при отсутствии предусмотренных статьей 91 УПК РФ оснований и обязательных условий, либо бездействие, выражающееся в умышленном непринятии уполномоченным должностным лицом установленных законом мер к освобождению лица, задержанного по подозрению в совершении преступления.*

3. Как заведомо незаконное задержание должны квалифицироваться, в частности, умышленные действия, совершаемые с целью незаконного применения к лицу данной меры процессуального принуждения, в результате которых лицо задерживается по подозрению в совершении преступления в порядке, предусмо-