УДК 34

ОСОБЕННОСТИ КВАЛИФИКАЦИИ ЦИФРОВЫХ ПРЕСТУПЛЕНИЙ ПРОТИВ ЛИЧНОСТИ

Сергиенко И.И.
Юридический институт
НИУ «БелГУ»,
Студент четвертого курса
Белгород, Россия

Трегубчак Е.Р.
Юридический институт
НИУ «БелГУ»,
Студентка четвертого курса
Белгород, Россия

Шумилина О.С.
Юридический институт
НИУ «БелГУ»,
доцент кафедры уголовного права и процесса,
к.ю.н., доцент

Белгород, Россия

Аннотация: В статье рассматриваются проблемы уголовно-правовой квалификации преступлений против личности, совершаемых с использованием цифровых и информационно-телекоммуникационных технологий. Анализируется соотношение понятий «цифровое преступление» и «преступление в сфере компьютерной информации», исследуются нормы Уголовного кодекса Российской Федерации. Отдельное внимание уделено законодательной технике закрепления использования информационно-телекоммуникационных сетей в качестве квалифицирующего признака и отягчающего обстоятельства, а также проблеме конкуренции этих норм. Сформулированы предложения по совершенствованию уголовного законодательства в исследуемой сфере.

Ключевые слова: цифровые преступления, преступления против личности, информационно-телекоммуникационные сети, квалификация преступлений, кибербуллинг, неприкосновенность частной жизни.

FEATURES OF CLASSIFYING DIGITAL CRIMES AGAINST *PERSONALITY*

Sergienko I.I.
Law Institute
National Research University "BelSU",
Fourth -year student
Belgorod, Russia

Tregubchak E.R.
Law Institute
National Research University "BelSU",
Fourth -year student
Belgorod, Russia

Shumilina O.S.
Law Institute
National Research University "BelSU",
Associate Professor at the Department of Criminal Law and Procedure,
Candidate of Legal Sciences, Associate Professor
Belgorod, Russia

Abstract: The article examines the problems of criminal -legal crimes against the person committed using digital and information and telecommunications technologies. The relationship between the concepts of "digital crime" and "crime in the field of computer information" is analysed, and the provisions of the Criminal Code of the Russian Federation are examined. Special attention is paid to the legislative technique of enshrining the use of information and telecommunications networks as a qualifying feature and an aggravating circumstance, as well as to the problem of competition between these provisions. Proposals for improving criminal legislation in the area under study are formulated.

Keywords: digital crimes, crimes against the person, information and telecommunications networks, classification of crimes, cyberbullying, privacy.

Цифровизация общественных отношений затронула и ту область уголовного права, которая традиционно считалась наиболее консервативной, а именно охрану личности, её жизни, здоровья, чести и достоинства. Если преступления в сфере компьютерной информации выделены законодателем в самостоятельную главу 28 Уголовного кодекса Российской Федерации [1] и имеют собственный объект посягательства, связанный с безопасностью компьютерной информации как таковой, то посягательства на личность, совершаемые с использованием цифровых технологий, такой обособленности лишены. Их специфика заключается не в изменении объекта охраны, жизни, здоровья, чести, достоинства или частной жизни человека, а в изменении способа и средства совершения деяния, что порождает самостоятельный круг проблем квалификации, требующий отдельного научного осмысления.

Актуальность темы обусловлена несколькими обстоятельствами. Во-первых, распространение сети «Интернет» и мобильных коммуникаций существенно расширило круг общественно опасных деяний, посягающих на личность: наряду с традиционными угрозами, клеветой и оскорблением появились такие формы, как «кибербуллинг», «доксинг», склонение к самоубийству через закрытые интернет-сообщества, распространение изображений без согласия потерпевшего. Во-вторых, законодатель реагирует на эти явления не системно, а точечно, дополняя отдельные статьи Особенной части Уголовного кодекса Российской Федерации указанием на информационно-телекоммуникационные сети как на способ совершения преступления, что порождает неравномерность правового регулирования. В-третьих, в науке уголовного права до сих пор отсутствует единое понимание самого термина «цифровое преступление», что затрудняет выработку общих подходов к квалификации соответствующих деяний.

Понятие «цифровое преступление» не имеет легального определения. И.А. Ефремова, анализируя особенности квалификации преступлений в сфере компьютерной информации, обращает внимание на то, что правоприменитель нередко объединяет компьютерные преступления, посягающие на безопасность информации, с деяниями, для которых цифровая среда выступает лишь инструментом совершения посягательств на иные охраняемые уголовным законом отношения [2]. Представляется, что именно это разграничение является ключевым для темы настоящей статьи: преступления против личности, совершаемые в цифровой среде, не образуют самостоятельной группы составов с единым объектом, а представляют собой определенный, межотраслевой в рамках Особенной части феномен, объединённый общим признаком способа совершения деяния.

Доктринальные попытки выработать обобщающее понятие цифрового посягательства многообразны. Другие авторы, например Д.В. Жмуров считают, что под цифровой кражей необходимо понимать отчуждение цифровых прав или технологических ресурсов путем определенных манипуляций с компьютерной информацией [3]. Данный тезис разработан в основном для имущественных посягательств, однако показывает общий методологический прием, а именно специфику предмета преступления.

Учёта способа совершения преступления против личности с помощью цифровых технологий ведется в уголовном праве РФ несколькими способами В качестве первого можно выделить включение данного признака преступления в диспозицию состава конкретной статьи УК РФ. Так, часть вторая статьи 128.1 Уголовного кодекса Российской Федерации устанавливает повышенную ответственность за клевету, совершённую публично с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет». Аналогичным образом сформулирована часть вторая статьи 110.2 Уголовного кодекса Российской Федерации, предусматривающая

ответственность за организацию деятельности, направленной на побуждение к совершению самоубийства, сопряжённую с использованием публично демонстрирующего произведения, средств массовой информации или информационно-телекоммуникационных сетей. Второй путь – закрепление использования информационно-телекоммуникационных сетей в качестве общего отягчающего обстоятельства, применимого при назначении наказания за любое преступление, если соответствующий признак не учтён законодателем в конкретном составе. Пункт «т» части первой статьи 63 Уголовного кодекса Российской Федерации относит к таким обстоятельствам совершение умышленного преступления с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях, включая сеть «Интернет».

Отдельного анализа заслуживает статья 137 Уголовного кодекса Российской Федерации, устанавливающая ответственность за нарушение неприкосновенности частной жизни. Основной состав охватывает незаконное собирание или распространение сведений, составляющих личную или семейную тайну лица, без его согласия, в том числе распространение этих сведений в публичном выступлении, публично демонстрирующем произведении или средствах массовой информации. Обращает на себя внимание, что, в отличие от статьи 128.1, законодатель не включил в основной состав статьи 137 прямого указания на информационно-телекоммуникационные сети как самостоятельный способ распространения сведений. Формально распространение сведений о частной жизни через социальную сеть или мессенджер, не относящиеся к средствам массовой информации, оказывается за пределами буквального перечня способов, названных в части первой, что вынуждает правоприменителя либо прибегать к расширительному толкованию понятия «распространение», либо

квалифицировать содеянное по общей норме без учёта специфики цифровой среды.

Отдельного внимания заслуживает вопрос о квалификации незаконного собирания и распространения персональных данных как формы посягательства на частную жизнь личности. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» устанавливает общие требования к обработке персональных данных и закрепляет принцип получения согласия субъекта персональных данных на их обработку [4]. Нарушение указанных требований само по себе влечёт административную ответственность, однако при наличии признаков незаконного собирания сведений, составляющих личную или семейную тайну, деяние подлежит квалификации по статье 137 Уголовного кодекса Российской Федерации. Разграничение административно-правовой и уголовно-правовой ответственности в этой сфере проводится по объёму и характеру нарушения: собирание общедоступных персональных данных, обрабатываемых с нарушением процедурных требований, как правило, не образует состава преступления, тогда как целенаправленное собирание сведений, составляющих охраняемую законом тайну, без согласия лица, таковой образует. Практика показывает, что размытость данной границы приводит к неединообразному применению закона, особенно в делах, связанных с так называемым «доксингом» – публикацией персональных данных лица с целью его преследования или запугивания.

Немаловажную роль в определении пределов уголовно-правовой охраны личности в цифровой среде играет Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [5]. Данный Федеральный Закон устанавливает и регламентирует основные понятия и принципы, а также регулирует правоотношения, возникающие в связи с поиском, получением, передачей и

распространением информации. Также он определяет круг субъектов, которые могут быть привлечены к ответственности.

Необходимо выделить ряд направлений для совершенствования действующего законодательства и практики правоприменения.

В Особенной части УК РФ необходима унификация законодательной техники для закрепления цифрового способа совершения преступления. Помимо этого, важно методическое обеспечение квалификации различных форм вовлечения несовершеннолетних в преступную деятельность. Также одно из направлений связано с улучшением криминалистического обеспечения расследования цифровых преступлений против личности.

Последовательное совершенствование законодательной техники и методического обеспечения правоприменительной деятельности в данной сфере представляется необходимым условием эффективной уголовно-правовой охраны личности в условиях цифровой трансформации общества.

Библиографический список

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.12.2025) // Собрание законодательства Российской Федерации. 1996.
2. Ефремова И.А. ОСОБЕННОСТИ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ПРОТИВОДЕЙСТВИЯ ИМ // Правоприменение. 2025. №1.
3. Жмуров Д.В. ЦИФРОВАЯ КРАЖА: ПОНЯТИЕ, СОДЕРЖАНИЕ, ЖЕРТВЫ И ИХ КЛАССИФИКАЦИЯ // Всероссийский криминологический журнал. 2023. №1.
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 08.08.2024) // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3451. – Доступ из справ.-правовой системы «КонсультантПлюс».

5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 28.04.2025) // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3448. – Доступ из справ.-правовой системы «КонсультантПлюс».