Д. В. Лобач
канд. юрид. наук, доц.
Владивостокский государственный университет экономики и сервиса

УГОЛОВНОЕ ПРАВО РОССИИ В ЦИФРОВУЮ ЭПОХУ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

В современных условиях трансформации общества, обусловленной интенсивным развитием цифровой сферы социальной коммуникации, наблюдается динамика и тенденция к качественным изменениям действующего законодательства, что продиктовано возникновением новых и нарождающихся явлений и процессов информационно-коммуникационной среды. Эти процессы и явления проецируют новые социальные отношения, которые объективно становятся целями нормативно-правового регулирования, а как следствие – возникает правовая институционализация новых сфер или сегментов социального взаимодействия, выражаемая в регулятивном или охранительном правовом

обеспечении новых отношений. Действительно, сегодня мы можем видеть, что вопросы о цифровизации затрагивают разные отрасли российского права.

Вместе с тем, несмотря на интенсивную законодательную практику в области регламентации отношений, связанных с развитием цифровой экономики в таких сферах, как гражданский оборот, финансовые технологии, интеллектуальная собственность, телекоммуникации, коммерция, судопроизводство, нотариат, администрирование, стандартизация, в отрасли уголовного права (и уголовной политике в целом) наблюдается определенный недостаток нормативно-правового регулирования охранительных отношений, возникающих в результате совершения общественно опасных деяний. Дело в том, что потенциал уголовного законодательства в области обеспечения информационной безопасности и других объектов уголовно-правовой охраны ограничен главным образом криминализацией деяний в сфере компьютерной информации (глава 28 УК РФ) и установлением такого квалифицирующего обстоятельства, как совершение соответствующего криминального деяния посредством использования средств массовой информации или информационно-телекоммуникационных сетей (включая сеть "Интернет").

Криминализация общественно опасных деяний в сфере компьютерной информации охватывает неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ, нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, а также неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Вместе с тем обращает на себя внимание некая неопределенность отдельных составов преступлений, обусловленная веяниями научно-технического прогресса. Признавая необходимость и объективную потребность обеспечения информационной безопасности, следует отметить, что конститутивные признаки объективной стороны отдельных преступлений требуют своего юридического уточнения в целях правильного правоприменения в обозримом будущем. Так, например, норма, устанавливающая ответственность за агрессивную войну (ст. 353 УК РФ), по своей юридической природе является бланкетной и отсылает к резолюции Генеральной Ассамблеи ООН от 14 декабря 1974г. «Определение агрессии», где раскрываются акты, составляющие применение вооруженной силы одним государством против суверенитета, территориальной целостности и политической независимости другого государства. В то же время дефиниция, агрессии как она предложена в упомянутой резолюции, была сформулирована с учетом развития обычных вооружений без учета возможности применения кибернетического (информационного) оружия.

Схожая ситуация возникает и с уголовно-правовой нормой, предусматривающей ответственность за применение запрещенных средств и методов ведения войны (ст. 356 УК РФ). Так же как и норма об агрессии, данное законоположение отсылает к ряду конвенций международного гуманитарного права, которые ориентированы на запрещение недопустимых с позиции идеи гуманизма методов и средств ведения войны. Однако надо понимать, что информационное оружие (кибероружие) на сегодняшний день не имеет международно-правового режима, а как следствие – является юридически неопределенным. Учитывая общую тенденцию ведения боевых действий с использованием комбинированных стратегий, сочетающих применение обычного вооружения вместе с использованием информационно-коммуникационных средств подавления систем обороны противника, следует признать, что данные уголовно-правовые нормы должны интерпретироваться в расширенном контексте с учетом современных реалий развития вооружений.

Что касается усиления уголовной ответственности за совершение преступлений посредством использования средств массовой информации или информационно-телекоммуникационных сетей (включая сеть "Интернет"), то российский законодатель

закрепляет данный квалифицирующий признак в отношении таких преступлений, как доведение до самоубийства (п. «д» ч. 2 ст. 110 УК РФ), склонение к совершению самоубийства или содействие совершению самоубийства (п. «д» ч. 3 ст. 110.1 УК РФ), организация деятельности, направленной на побуждение к совершению самоубийства (ч. 2 ст. 110.2 УК РФ), клевета (ч. 2 ст. 128.1 УК РФ), вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (п. «в» ч. 2 ст. 151.2 УК РФ), публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ч. 2 ст. 205.2 УК РФ), незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества (п. «б» ч. 2 ст. 228.1 УК РФ), обращение фальсифицированных, недоброкачественных и незарегистрированных лекарственных средств, медицинских изделий и оборот фальсифицированных биологически активных добавок (ч. 1.1 ст. 238.1 УК РФ), незаконные изготовление и оборот порнографических материалов или предметов (п. «б» ч. 3 ст. 242 УК РФ), изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (п. «г», ч. 3 ст. 242.1 УК РФ), использование несовершеннолетнего в целях изготовления порнографических материалов или предметов (п. «г» ч. 2 ст. 242.2 УК РФ), жестокое обращение с животными (п. «г» ч. 2 ст. 245 УК РФ), незаконные добыча и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации (ч. 1.1 ст. 258.1 УК РФ, п. «б» ч. 2 ст. 258.1 УК РФ), публичные призывы к осуществлению экстремистской деятельности (ч. 2 ст. 280 УК РФ), публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ч. 2 ст. 280.1 УК РФ).

С позиции теории криминализации нельзя не отметить тот факт, что российский законодатель проявляет непоследовательность в ужесточении ответственности за деяния, которые также могут совершаться посредством использования средств массовой информации или информационно-телекоммуникационных сетей (включая сеть "Интернет"). В этом аспекте не понятно, почему российский законодатель не устанавливает данный квалифицирующий признак в отношении преступлений, предусмотренных ст. ст. 127.1, 133, 135, 154, 240, 240.1 и 241 УК РФ [1]. С позиции юридической техники небезупречными представляются нормы, предусматривающие ответственность за публичные призывы к агрессивной войне (ст. 354 УК РФ) и реабилитацию нацизма (ст. 354.1 УК РФ), так как среди квалифицирующих признаков указывается на использование средств массовой информации безотносительно к возможному использованию сети "Интернет".

Наблюдается законодательная непоследовательность и неопределённость в вопросе установления уголовной ответственности за преступления против собственности в сфере компьютерной информации. Дело в том, что еще в 2012 г. федеральным законом N 207-ФЗ [2] в Уголовный кодекс РФ была внесена норма (ст. 159.6 УК РФ), устанавливающая уголовную ответственность за хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Криминализация этого деяния обусловлена объективными условиями, характеризуемыми широким распространением по всему миру хакерской деятельности, направленной на обогащение через хищение чужого имущества. При этом правоприменительная практика в подобных случаях ориентирована на признание идеальной совокупности преступлений,

предусмотренных ст. 159.6 и ст. 272 УК РФ. Однако почему-то законодатель проявляет непоследовательность в том плане, что по закономерной логике следовало бы также закрепить аналогичную норму применительно к причинению имущественного ущерба путем обмана или злоупотребления доверием, ответственность за которое предусмотрена ст. 165 УК РФ [4, с. 148].

Интегративное использование современных технологических новаций в эпоху становления информационного общества также предопределяет вопрос о перспективных направлениях правовой регламентации использования электронной подписи в условиях современной российской действительности, когда все чаще актуализируются криминальные риски и угрозы в отношении владельцев (пользователей) электронной подписью. Можно отметить возможную криминализацию общественно опасных деяний, посягающих на отношения, возникающие в сфере экономической деятельности. Так, ещё в 2018 г. по инициативе Минкомсвязи России был подготовлен проект Федерального закона «О внесении изменений в некоторые законодательные акты Российской Федерации в связи с совершенствованием регулирования в сфере электронной подписи» [5], в котором предлагалось дополнить главу 22 Уголовного кодекса РФ статьей 200.6, устанавливающей уголовную ответственность в отношении специального субъекта за умышленное нарушение порядка выдачи (вручения) квалифицированного сертификата ключа проверки электронной подписи. Несмотря на то что представленный законопроект не был поддержан в условиях развития электронного документооборота, данная инициатива сохраняет свою актуальность.

В заключение следует отметить, что цифровая трансформация социальных отношений и развитие цифровой экономики объективно предопределяет потребность в адаптационной оптимизации национального законодательства в целях повышения эффективности правового регулирования новых отношений. Не является в этом плане исключением и уголовное право, которое, как и другие отрасли российской системы права, должно адекватно реагировать на новые и нарождающиеся вызовы и угрозы в информационной среде.

Список использованных источников

1. Уголовно-правовые риски в сфере цифровых технологий: проблемы и предложения [Электронный ресурс]. – Режим доступа: https://urfac.ru/?p=2909#_ftnref11 – Дата доступа: 27.01.2021.

2. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации [Электронный ресурс] : Федеральный закон от 29.11.2012 № 207-ФЗ (ред. от 03.07.2016) // КонсультантПлюс. Россия / ЗАО «Консультант Плюс».

3. О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс] : постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 // КонсультантПлюс. Россия / ЗАО «Консультант Плюс».

4. Чучаев, А.И., Грачев, Ю.В., Маликов, С.В. Цифровизация и ее уголовно-правовые риски / А.И. Чучаев, Ю.В. Грачев, С.В. Маликов // Правосудие. - 2019. - Т. 1, № 2. - С. 133–155.

5. О внесении изменений в некоторые законодательные акты Российской Федерации в связи с совершенствованием регулирования в сфере электронной подписи [Электронный ресурс]: проект Федерального закона (подготовлен Минкомсвязью России) (не внесен в ГД ФС РФ, текст по состоянию на 04.09.2018) // КонсультантПлюс. Россия