Цифровизация уголовного законодательства: непростые последствия простых решений

Евгений Александрович РУССКЕВИЧ,
профессор кафедры уголовного права Университета имени О.Е. Кутафина (МГЮА), доктор юридических наук, доцент
russkevich@mail.ru
125993, Россия, г. Москва, ул. Садовая-Кудринская, д. 9

Аннотация. *В статье анализируются отдельные изменения Уголовного кодекса РФ, направленные на повышение эффективности противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет.*
Автор отмечает, что цифровой способ совершения преступления далеко не всегда свидетельствует об увеличении общественной опасности деяния. Дополнение уголовного закона указанием на совершение преступления с использованием сети Интернет должно компенсировать реально сложившийся разрыв в степени общественной опасности между традиционной формой осуществления преступного посягательства и его цифровым аналогом. Неоправданная цифровая казуализация уголовного закона приводит к нарушению сложившихся моделей законодательного определения отдельных преступлений, а равно вступает в противоречие с доктринальными положениями, характеризующими содержание и пределы объективной стороны конкретных составов преступлений. Автор также отмечает отсутствие единого подхода к учету цифрового способа совершения преступления в рамках Особенной части УК РФ.
Ключевые слова: *цифровая преступность, компьютерные преступления, преступления в сфере компьютерной информации, цифровизация уголовного закона*

DOI: 10.17803/2311-5998.2025.129.5.026-033

Eugene A. RUSSKEVICH,
Professor of the Department of Criminal Law of the Kutafin Moscow State Law University (MSAL), Dr. Sci. (Law), Associate Professor
russkevich@mail.ru
9, ul. Sadovaya-Kudrinskaya, Moscow, Russia, 125993

Digitalization of Criminal Legislation: Complex Consequences of Simple Solutions

Abstract. *The article analyzes certain amendments to the Criminal Code of the Russian Federation aimed at increasing the effectiveness of counteracting crimes committed using information and telecommunications networks, including the Internet.*

The author notes that the virtual network method of committing a crime does not always indicate an increase in the social danger of the act. Supplementing the criminal law with an indication of the commission of a crime using the Internet should compensate for the real gap in the degree of social danger between the traditional form of committing a criminal offense and its digital analogue.

Unjustified digital casualization of the criminal law leads to a violation of the established models of legislative definition of individual crimes, and also contradicts the doctrinal provisions characterizing the content and limits of the objective side of specific crimes. The author also notes the lack of a unified approach to taking into account the digital method of committing a crime within the framework of the Special Part of the Criminal Code of the Russian Federation.

Keywords: *digital crime, computer crimes, crimes in the field of computer information, digitalization of criminal law*

В осмыслении проблемы противодействия цифровой преступности нельзя не учитывать то вполне очевидное обстоятельство, что сетевое пространство стало местом ежедневной социальной активности подавляющего большинства населения страны. Для современного человека взаимодействовать с другими в сети Интернет так же естественно, как и вступать в социальные интеракции в физическом пространстве. В этом смысле онлайн-коммуникация уже вряд ли требует какого-то особого отношения со стороны законодателя.

Это не означает, что право не должно меняться с учетом процессов цифровизации. Появление новых цифровых благ и отношений, построение цифровой экономики и т.п., конечно же, требуют необходимого правового регулирования и охраны. При этом в таких условиях само по себе запаздывание права является вполне ожидаемым. Отставание социального контроля от технологии и тех качественных изменений, которые она привносит как в общественно полезные, так и во вредоносные формы поведения человека, имеет естественные причины и в истории наблюдалось не единожды.

Вместе с тем, как можно легко убедиться, этого всегда достаточно для тревожных настроений в обществе. В последние годы почти на каждом научно-представительском мероприятии, посвященном проблемам борьбы с преступностью, докладчики знакомят слушателей с новыми угрозами и вызовами цифровизации, щедро употребляя при этом труднопроизносимые англицизмы. За иноплеменными словами, надо признать, зачастую скрываются традиционные и уже хорошо разработанные в науке уголовно-правовые конструкции, но производимый эффект от этого страдает мало — слушатели довольно часто проникаются убеждением о глубоком кризисе уголовного права и необходимости системных изменений в свете процессов цифровизации. Диссонансом этому попурри из предложений криминализовать или как-то иначе отразить в тексте уголовного закона майнинг, треш-стриминг, буллинг, сталкинг, доксинг, хейтинг, флейминг, фишинг, кардинг, зумбомбинг и т.п. является справедливое утверждение о том, что «уголовное право не может идти впереди “телеги”, потому

что если новые отношения еще не сложились и не понятно о чем вообще идет речь, то и формулировать запрет в этой области весьма чревато»[1].

Думается, что, когда речь идет о правовом регулировании и совершенствовании механизма уголовно-правовой охраны, эмоциональные нарративы должны быть проигнорированы. Фиксируемое отставание права в условиях цифровизации само по себе не может выступать поводом для утверждения о глубоком кризисе и необходимости новых, соответствующих Индустрии 4.0 социальных регуляторов.

Нельзя упускать из виду, что довольно часто употребляемый тезис об экспоненциальном росте цифровых преступлений не свидетельствует об общем увеличении преступности. Речь идет о качественном изменении ее структуры, когда физический способ заменяется и вытесняется своим цифровым alter ego. Иными словами, самой преступности больше не становится, она просто меняется, оцифровывается.

На поверку также оказывается, что цифровизация мало что добавляет и без труда «укладывается» в содержание законодательных моделей подавляющего большинства составов преступлений. Кража не перестает быть тайным хищением чужого имущества, будучи совершенной посредством неправомерного доступа к банковскому мобильному приложению потерпевшего. Равно как и клевета, мошенничество, распространение порнографии и многие иные посягательства в своих цифровых проявлениях полностью вписываются в уже имеющиеся законодательные конструкции. Даже предполагаемая модель «убийства будущего», когда умышленное причинение смерти другому человеку будет осуществлено хакером дистанционно путем неправомерного воздействия на имплантированное устройство, полностью охватывается действующей редакцией ст. 105 УК РФ.

Дополнение уголовного закона указанием на совершение того или иного преступления цифровым способом должно либо восполнять имеющийся пробел в уголовно-правовой охране, либо компенсировать реально сложившийся разрыв в степени общественной опасности между традиционной формой осуществления преступного посягательства и его цифровым аналогом, как то, думается, справедливо реализовано в нормах об ответственности за отдельные преступления, связанные с оборотом запрещенных предметов и криминогенной пропагандой.

К сожалению, довольно часто информационный шум вокруг проблемы противодействия цифровым преступлениям, без оглядки на действительные потребности правоприменения с одновременным созданием либо укреплением в сознании населения в некотором роде мифических угроз, заглушает попытки удержать законодателя от очередного принятия решения по дополнению УК РФ очередным «цифровым аватаром» традиционного состава преступления в отсутствие четкого понимания, чем конкретно обусловлена оценка того или иного посягательства как обладающего более высокой степенью общественной опасности.

За прошедшие годы стал понятен общий подход законодателя к проблеме. Ответом на цифровое проявление преступного посягательства является корректировка соответствующей нормы уголовного закона указанием на совершение

[1] *Хилюта В. В.* Уголовное право в социальном измерении (контуры перемен и новой стратегии развития) : монография. М., 2023. С. 125.

деяния «с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет». Таким образом, онлайн-коммуникация прочно вошла в систему средств дифференциации уголовной ответственности. Насколько обоснован этот подход, покажет, конечно же, время. Сейчас не может не настораживать то, что в условиях все ускоряющейся конвергенции физического и виртуального в жизни современного человека законодатель идет по пути принципиального разделения и последовательного ужесточения ответственности за цифровой способ совершения преступного посягательства. И уже можно обозначить и осмыслить непростые последствия таких решений в сфере цифровой модернизации уголовного закона.

Прежде всего надо сказать о том, что курс на адаптирование положений уголовного закона к процессам цифровизации сопряжен с нарушением сложившихся моделей законодательного описания отдельных преступлений. Ярким тому примером выступает действующая редакция нормы об ответственности за мошенничество в сфере компьютерной информации (ст. 159[6] УК РФ). Компьютерное мошенничество, совершаемое путем неправомерного вмешательства в функционирование средств обработки, хранения и (или) передачи данных, при отсутствии признаков обмана или злоупотребления доверием, представляет собой юридический оксюморон, законотворческое недоразумение. Как известно, мошенничество немыслимо без обманного поведения либо злоупотребления доверительными отношениями. Если законодатель и желал выделить отдельную форму хищения, совершаемого исключительно путем модификации компьютерных данных, следует констатировать, что попытка эта до настоящего времени терпит неудачу и требует вполне конкретных решений. Здесь можно обратиться к опыту Республики Беларусь, где ответственность установлена именно за хищение путем модификации компьютерной информации (ст. 212 УК РБ)[2].

Помимо этого, учет цифрового способа вступает в противоречие с положениями (обоснованными в науке и поддержанными на уровне судебного толкования), раскрывающими содержание объективной стороны конкретных составов преступлений. Так, одним из последних решений законодателя по оцифровке Особенной части УК РФ явилось дополнение сразу многих ее норм указанием на квалифицирующий признак в виде совершения общественно опасного посягательства «с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет)»[3].

Начнем с того, что здесь, конечно же, представляет интерес не только цифровой аспект. Законодатель признал квалифицированным убийством или причинением вреда здоровью всякое умышленное применение насилия в отношении другого человека, совершенное публично, т.е., например, в общественном месте и в присутствии других лиц. Социально-правовые предпосылки ужесточения ответственности в таком случае, пожалуй, мало проявлены.

[2] URL: https://pravo.by/document/?guid=3871&p0=hk9900275 (дата обращения: 17.03.2025).

[3] Федеральный закон от 08.08.2024 № 218-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // СПС «КонсультантПлюс».

Указание на демонстрацию в сети Интернет сразу ставит вопрос о толковании пределов объективной стороны соответствующих преступлений. Если согласиться с подходом, согласно которому такое преступление надлежит считать юридически оконченным не с наступления конкретных общественно опасных последствий, а с момента публичного показа или размещения для публичного обозрения соответствующих видео- или фотоматериалов (размещение информации в общем доступе в сети Интернет, массовая рассылка по электронной почте и т.п.)[4], то следует сделать вывод, что новые квалифицированные виды насильственных преступлений уже преодолели свою физическую природу и приобрели в некотором смысле виртуальное содержание.

Это, в свою очередь, приводит к постановке множества вопросов: образует ли признаки оконченного преступления, например, лишение жизни потерпевшего при несостоявшейся попытке размещения соответствующих материалов в сети Интернет? Что следует признавать местом и временем совершения такого преступления? Можно ли такое насильственное преступление считать длящимся? Можно ли признавать соисполнителем лицо, которое, хотя и не применяло насилие к потерпевшему, но осуществляло съемку совершения преступления или трансляцию в сети Интернет? И эти вопросы (подумать только — о «длящемся убийстве» (!)) нельзя не ставить. Но вот отвечать на них предстоит следователям и судьям, которые уже сейчас должны как-то применять закон в состоянии очередной правовой неопределенности.

Другим непростым последствием является то, что цифровая казуализация (создание «цифровых двойников» традиционных уголовно-правовых запретов) нарушает внутренние системные связи уголовного закона. Так, Федеральным законом от 30.11.2024 № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации»[5] глава 28 УК РФ была дополнена специальной нормой об ответственности за неправомерные действия в отношении персональных данных (ст. 272^1 УК РФ). Из ее содержания следует, что предметом преступления являются сведения, составляющие персональные данные гражданина, однако лишь в форме компьютерной информации. При этом диспозиция ст. 137 УК РФ приобрела ссылочный характер, поскольку была дополнена оговоркой о том, что она не распространяется на случаи, предусмотренные ст. 272^1 УК РФ.

В результате указанных изменений сложилась ситуация, при которой уголовно-правовое противодействие незаконным действиям в отношении персональных данных гражданина принципиально разделено по одному критерию — хранятся ли соответствующие сведения в цифровом или ином виде (например, на бумажном носителе). При этом разглашение персональных данных в телефонном разговоре образует преступление, предусмотренное ст. 137 УК РФ, а направление сообщения или фотографии с той же информацией в мессенджере уже подпадает под действие ст. 272^1 УК РФ.

Более того, поскольку в ст. 272^1 УК РФ установлена ответственность и за незаконное использование персональных данных в цифровой форме,

---

[4] См.: *Шарапов Р. Д.* Квалификация преступлений, совершенных с использованием информационно-телекоммуникационных сетей // Законность. 2024. № 3. С. 33—38.

[5] Российская газета. 06.12.2024. № 278.

то осуществление нежелательного телефонного звонка гражданину путем считывания с экрана компьютера номера телефона и сведений о фамилии, имени и отчестве абонента образует признаки преступления. Означает ли это, что теперь каждый нежелательный телефонный вызов от так называемых звонарей представляет собой факт совершения преступления, предусмотренного ст. 272[1] УК РФ? Если так, тогда мы на пороге «регистрационного апокалипсиса» по ст. 272[1] УК РФ, поскольку ежедневно миллионы граждан России получают такие звонки, причем многократно.

Важно отметить и то, что незаконное использование, равно как и хранение персональных данных не в компьютерной форме, уже преступлением не является. Искать научное или хотя бы логическое объяснение тому, почему сама цифровая форма персональных данных обусловливает наличие основания для реализации уголовной репрессии, пожалуй, не сто́ит.

И наконец, еще одним непростым последствием явилось отсутствие единого подхода к учету цифрового способа совершения преступления в Особенной части УК РФ. В стремлении адаптировать уголовный закон к условиям цифровой трансформации общественных отношений законодатель зачастую проявляет неоправданное усердие. Примером тому является норма об ответственности за незаконные действия в отношении особо охраняемых диких животных и водных биологических ресурсов (ст. 258[1] УК РФ). Статья привлекает внимание дублирующим содержанием квалифицирующих признаков совершения преступления «с использованием сети Интернет» и «с публичной демонстрацией в сети Интернет». Обращение к самой хронологии внесения изменений и изучение пояснительных записок к законопроектам[6] позволяет сделать вывод, что появление двух самостоятельных цифровых способов совершения преступления не планировалось и явилось следствием реализации двух самостоятельных законотворческих инициатив.

Если подводить некий итог, можно заключить, что простые законодательные решения в области «оцифровки» УК РФ влекут далеко не простые последствия

[6] См.: паспорт проекта федерального закона № 308781-7 «О внесении изменений в статьи 245 и 258[1] Уголовного кодекса Российской Федерации и статьи 150 и 151 Уголовно-процессуального кодекса Российской Федерации» (в целях усиления уголовной ответственности за жестокое обращение с животными) (внесен депутатами Государственной Думы ФС РФ О. В. Шеиным, В. В. Бурматовым, Е. Г. Драпеко, С. А. Вострецовым, К. Г. Слыщенко, И. В. Осиповым, Н. В. Маловым, А. Б. Выборным, О. Н. Смолиным, В. В. Белоусовым, О. А. Николаевым, О. А. Ниловым, С. М. Мироновым, А. Г. Аксаковым, А. В. Канаевым, А. Н. Грешневико) // СПС «КонсультантПлюс» ; паспорт проекта федерального закона № 356397-7 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации» (по вопросу совершенствования уголовного законодательства Российской Федерации в сфере противодействия преступлениям, связанным с незаконной добычей и оборотом водных биологических ресурсов, диких животных, в том числе занесенных в Красную книгу Российской Федерации) // СПС «КонсультантПлюс».

как для общего состояния уголовного закона, так и для правоприменения (оказывают дизруптивное воздействие на механизм уголовно-правовой охраны[7]).

Сто́ит, пожалуй, сказать и о том, что в этом можно усмотреть и очередную попытку неоправданно возложить на уголовный закон решение проблемы, которая требует системного и комплексного подхода. Противодействие цифровой преступности обладает той несомненной особенностью, что в его структуре в значительной степени преобладают организационно-технические либо сугубо технические составляющие. Предупреждение посягательств, совершаемых с компьютерной информацией и компонентами информационно-коммуникационной инфраструктуры, прежде всего реализуется за счет разработки и внедрения механизмов программно-технической защиты, в том числе от неосторожного поведения субъектов, допущенных к эксплуатации компьютерного оборудования, в том числе самих пользователей. В данном отношении крайне важным представляется обеспечение неукоснительного соблюдения установленных стандартов информационной безопасности в деятельности хозяйствующих субъектов. То, что далеко не все организации в силу объективных и (или) субъективных причин стремятся осуществлять свою деятельность на уровне последних стандартов киберзащищенности, — известный факт.

Надо обратить пристальное внимание на то, что изначально и по настоящее время коммерческий эффект (прибыль) от внедрения конкретного цифрового решения полностью превалирует над соображениями обеспечения информационной безопасности. Никто из хозяйствующих субъектов не желает отказываться от конкурентных преимуществ, которые дают технологии. Никто и не будет от них отказываться инициативно из соображений социальной ответственности. Винить в этом бизнес, пожалуй, не сто́ит. Бизнес должен заниматься своим делом и крепить тем самым отечественную экономику. Здесь разумное (минимально необходимое) участие в этом процессе должно проявить государство путем выработки общих правил и стандартов кибербезопасности для всех участников.

Немаловажно также государству озаботиться, наконец, тем, кто и с какими ресурсами будет бороться с современной цифровой преступностью, принимая во внимание уже давно возникший и усугубляющийся с каждым годом кадровый кризис в системе правоохранительных органов[8].

Иными словами, простые решения по «цифровому декорированию» отечественного уголовного закона необходимо сменить на реальные меры по противодействию преступлениям, совершаемым с использованием информационно-коммуникационных технологий. Думается, что такой подход несколько поправит в целом тупиковый путь подгонки уголовно-правовых конструкций под те или иные проявления цифровизации, лишенный необходимых социальных, юридических и научных оснований.

---

[7] См.: *Русскевич Е. А.* Уголовное право и «цифровая преступность»: проблемы и решения : монография. М., 2019. С. 20.

[8] Глава МВД заявил о критической нехватке полицейских и следователей // РБК. 10.08.2023. URL: https://www.rbc.ru/politics/10/08/2023/64d4d2629a7947695baea197?ysclid=m8dhdvh2q5607811322 (дата обращения: 10.03.2025).

Все вышеизложенное не следует расценивать как попытку обосновать ненужность любых изменений уголовного закона в условиях цифровизации. Речь идет лишь о том, что такие изменения должны иметь прочные и научно верифицированные предпосылки, носить не спонтанный, а тщательно выверенный характер. Так, например, давно уже назрела проблема надлежащего уголовно-правового ответа случаям так называемого криптовирусного вымогательства, когда злоумышленник, осуществив шифрование компьютерных данных пользователя, требует передать ему денежные средства как условие снятия блокировки доступа к компьютерной информации. Действующая редакция ст. 163 УК РФ не вполне пригодна для применения в таких случаях. Чтобы быть точным — неприменима в тех из них, где нет никаких признаков угрозы уничтожения или повреждения имущества, а равно шантажа.

И казалось бы, проблемных примеров — множество на практике, и обстоятельное обсуждение в научной литературе имеется, а воз и ныне там. Пожалуй, не хватает «хайпа» обозначенной проблеме, слишком она прагматична и даже приземленна. Куда уж ей до флейминга или зумбомбинга.

БИБЛИОГРАФИЯ

1. *Русскевич Е. А.* Уголовное право и «цифровая преступность»: проблемы и решения : монография. — М. : Инфра-М, 2019. — 227 с.
2. *Хилюта В. В.* Уголовное право в социальном измерении (контуры перемен и новой стратегии развития) : монография. — М. : Юрлитинформ, 2023. — 440 с.
3. *Шарапов Р. Д.* Квалификация преступлений, совершенных с использованием информационно-телекоммуникационных сетей // Законность. — 2024. — № 3. — С. 33—38.