Научная статья
https://doi.org/10.24412/2220-2404-2024-12-11
УДК 343.2/.7

ЦИФРОВОЕ УГОЛОВНОЕ ПРАВО: ПЕРСПЕКТИВЫ ФОРМИРОВАНИЯ И РАЗВИТИЯ (ЧАСТЬ 2)

Лебедев С.Я., Джафарли В.Ф.
Российский государственный университет имени А.Н. Косыгина

Аннотация. *Цель. Статья продолжает тематику цифровизации уголовно-правового ресурса в рамках научно-исследовательского проекта «Цифровое уголовное право». По мнению авторов, главный приоритет безопасности заключается в том, что в результате предлагаемого цифрового пресечения киберпреступления его общественная опасность будет технологически нивелироваться мгновенно. В процессе изучения проблем были использованы общенаучные (анализ, синтез, индукция и дедукция) и частно-научные (уголовно-правовой и криминологический) методы познания. Выводы и заключения: материалы публикации могут быть использованы в целях цифровой модернизации уголовного законодательства и правоохранительной практики, формирования и развития системы криминологической кибербезопасности значимых объектов от всей совокупности преступных посягательств.*

Ключевые слова: *цифровое уголовное право, цифровые преступления, цифровые наказания, криминологическая кибербезопасность, цифровая модернизация законодательства и правоохранительной практики.*

DIGITAL CRIMINAL LAW: PROSPECTS OF FORMATION AND DEVELOPMENT (PART 2)

Semyon Ya. Lebedev, Vugar F. Dzhafarli
Kosygin Russian State University

Abstract. *Goal. The article continues the topic of digitalization of the criminal law resource within the framework of the research project "Digital Criminal Law". According to the authors, the main priority of security is that as a result of the proposed digital suppression of cybercrime, its public danger will be technologically leveled instantly. In the process of studying the problems, general scientific (analysis, synthesis, induction and deduction) and private scientific (criminal law and criminological) methods of cognition were used. Conclusions and conclusions: The materials of the publication can be used for the purpose of digital modernization of criminal legislation and law enforcement practice, the formation and development of a system of criminological cybersecurity of significant objects from the totality of criminal encroachments.*

Keywords: *digital criminal law, digital crimes, digital punishments, criminological cybersecurity, digital modernization of legislation and law enforcement practice.*

Введение.

Современная правоохранительная практика пытается задействовать для целей оперативной и объективной фиксации правонарушений и адекватного реагирования на них современные технические и технологические ресурсы, минимизировать в этом деле стандартный человеческий ресурс. В результате подобной модернизации обеспечивается не только адекватность и оптимальность общего правоохранительного реагирования на правонарушения, но и нивелируется известная коррупционная составляющая любого правоохранительного процесса с «человеческим» лицом. Примером такой правоохранительной инновации, отчасти, могут служить цифровые технологии, применяемые для фиксации совершаемых правонарушений в аппаратно-программном комплексе (АПК) «Безопасный город», в системе видеоконтроля над участниками дорожного движения, в программном комплексе системы «Антифрод», нацеленной на предотвращение мошеннических транзакций и др.

Обсуждение.

Отмеченный во введении к данному исследовании потенциал правового и технологического механизма наводит на вполне резонный вопрос: Разве не может существующий уголовно-правовой ресурс быть с таким же успехом реализован в информационно-телекоммуникационном

формате? Думается, что вполне. То есть, при обнаружении с помощью специально созданной цифровой уголовно-правовой программы контроля в киберпространстве над какой-либо криминальной угрозой (например, распространяемой в интернет-сети рекламной информации о продаже наркотиков, организации сексуальных услуг с предложением в качестве объекта для осуществления таковых подростков, материалов экстремистского или, ещё серьезнее, террористического характера, вовлечения несовершеннолетних в суицидальное поведение и т.д., и т.п.), такая антикриминогенная цифровая система будет моментально блокировать эту криминальную угрозу сформированным под соответствующую норму Уголовного кодекса РФ IT-программным алгоритмом.

Конечно, учитывая отмеченный ранее непреложный факт анонимности источника криминогенной угрозы, трудно будет мгновенно отправить такому субъекту вердикт о его уголовной ответственности (по аналогии с цифровым ресурсом камер видеонаблюдения за участниками дорожного движения). Однако думается, что это уже «другая история», а именно уголовно-процессуальная и, соответственно, уголовно-исполнительная, со своими цифровыми механизмами реализации. Нам представляется важным, в этом случае, главный приоритет безопасности – в результате предлагаемого цифрового пресечения киберпреступления, правовую основу которого составит цифровой уголовный закон, его общественная опасность будет технологически нивелироваться мгновенно. То есть, криминальная (точнее, уголовно наказуемая) киберугроза в этом случае, безусловно, оперативно блокируется, причём также эффективно, как технологически блокируется сегодня выявленная специалистами кибербезопасности любая иная информационная угроза в киберпространстве.

Сейчас же существует весьма противоречивая система правового обеспечения ограничения доступа к какой-либо криминогенной киберинформации, действие которой растягивается во времени на долгий срок, в течение которого угроза продолжает себя активно позиционировать и, следовательно, достигать своего общественно опасного эффекта. Так, в соответствии со ст. 15.3 «Порядок ограничения доступа к информации, распространяемой с нарушением закона» Федерального закона «Об информации, информационных технологиях и о защите информации», «…в случае обнаружения в информационно-телекоммуникационных сетях… информации…, которая создаёт угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности… Генеральный прокурор Российской Федерации или его заместители обращаются в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации… с требованием о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию…». Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации… на основании обращения… незамедлительно уведомляет редакцию сетевого издания о необходимости удаления указанной информации… Незамедлительно с момента получения от федерального органа исполнительной власти… уведомления… редакция сетевого издания обязана удалить информацию…» [1].

Сложно представить себе факт подобной правоохранительной реакции на какое-либо правонарушение в реальном пространстве. По меньшей мере, он выглядел бы весьма анекдотично, если не сказать больше - абсурдно. Представим себе полицейского, заметившего факт совершения преступления (например, разбойное нападение), не устремляющего свое профессиональное мастерство на его пресечение, а докладывающего об обнаружении такового по инстанции Генеральному прокурору. Тот же, изучив ситуацию, выносит мотивированное обращение в МВД, а уже оно, руководствуясь вышестоящим вердиктом, действует, по своим внутренним инстанциям… – и так далее, по аналогии с сегодняшним нормативно предопределенным пресечением криминогенной информации в киберпространстве.

Представляется, что в сфере цифрового обеспечения безопасности от различного рода криминальных угроз, особенно активно позиционирующих себя в киберпространстве, технологии их цифровой правоохранительной фиксации станут со временем более результативными. В данном случае, технологический контроль над нормативно обусловленным, а потому «правопослушным» поведением, способен автоматически выявлять любые несанкционированные (нештатные) внешние и внутренние угрозы безопасности. Правоохранителям останется лишь процессуально фиксировать факт правонарушения и установить его источник для определения меры юридической ответственности и организации соответ-

ствующей процедуры судопроизводства. Помимо всего прочего, в этом случае одновременно будет срабатывать превентивный эффект цифрового правоохранительного (вместе с технологическим) контроля, ибо совершение какого-либо правонарушения в киберпространстве станет рискованным для замыслившего его субъекта и потому просто невыгодным, а, по сути, бессмысленным. Разумеется, подобная технология безопасности потребует создания собственного правового (и, безусловно, цифрового) механизма ее обеспечения. Однако это всего лишь дело времени, причем, судя по интенсивности развития цифровых технологий, весьма непродолжительного.

Футурологически оценивая перспективы будущего уголовного закона и уголовно-процессуальные практики его применения в цифровых условиях, можно уверенно прогнозировать, что и те, и другие будут напрямую связаны с новыми информационными технологиями, развитие которых, в свою очередь, представляет собой единственно верную идеологическую, а вместе с ней и информационно-технологическую направленность достижения цели обеспечения безопасности личности, общества и государства уголовно-правовыми и криминологическими средствами. Подчеркнем, цифровыми их форматами.

Таким образом, решение проблемы уголовно-правовой охраны общественных отношений от цифровой преступности видится в формировании совместного с законодателями, правоохранителями, специалистами в сфере общественной, экономической, национальной и информационно-технологической безопасности полномасштабной государственной программы правового цифрового обеспечения пресечения криминогенных угроз в информационно-телекоммуникационной сфере, фактически *системы цифрового уголовного судопроизводства, основанного на цифровом уголовном праве (цифровом уголовном кодексе)*, позволяющей в ближайшей и относительно отдаленной перспективе:

- осуществлять оперативную идентификацию преступлений, совершаемых в киберпространстве и в реальном пространстве с использованием информационно-телекоммуникационных технологий, и обеспечивать в отношении таковых цифровую уголовно-правовую реакцию (пресечение) по аналогии с действующей системой традиционного уголовного судопроизводства;

- производить оперативный анализ криминогенных угроз (преступлений и стимулирующих их криминогенных факторов) в киберпространстве в российском сегменте сети и ИКТ инфраструктуре;

- обеспечивать криминологический мониторинг киберпреступлений;

- выявлять базовые и инновационные сценарии развития киберпреступности;

- обеспечивать адекватную и оптимальную цифровую правоохранительную реакцию на криминогенные угрозы в киберпространстве.

Разработанные и представленные авторами в настоящем издании теоретические основы цифрового уголовного права и базовые алгоритмы правовых норм цифрового уголовного кодекса пока объективно выступают *научно-исследовательским проектом*. Между тем они, несомненно, закладывают фундамент формирования и реализации в недалеком будущем реальных правовых основ цифровой трансформации уголовно-правовых механизмов обеспечения криминологической кибербезопасности, способных обеспечивать:

- сквозную цифровую идентификацию, анализ и оценку состояния криминогенных угроз (преступлений и их детерминантов) в киберпространстве;

- цифровое уголовно-процессуальное документирование киберпреступлений и соответствующее ему цифровое уголовно-процессуальное, а вслед за ним - цифровое уголовно-исполнительное производство;

- сквозной цифровой документооборот в рамках уголовно-процессуального и уголовно-исполнительного законодательства.

Реализация проекта позволит оснастить правоохранительную систему доступным и долговременным высокотехнологичным правовым инструментом выявления и анализа криминогенных угроз в киберпространстве и обеспечить необходимую адекватную и оптимальную по своим вновь созданным цифровым ресурсам уголовно-правовую реакцию на их распространение.

Помимо собственно цифрового правоохранительного обеспечения безопасности от преступности в киберпространстве, проект будет нацелен на инновационную профессиональную базовую подготовку (переподготовку и повышение квалификации) специалистов для формирования нового кадрового правоохранительного ресурса, прежде всего уголовно-правового и связанного с ним уголовно-процессуального обеспечения кибербезопасности от преступности в системе общественной и национальной безопасности Российской Федерации.

Конечной целью предлагаемого проекта должно стать безусловное снижение масштабов киберпреступлений, развитие эффективной государственной системы кибербезопасности, нацеленной в целом на безопасное развитие информационного общества в Российской Федерации.

Представляя настоящее исследование на суд юридической общественности, авторы сознают, что до того времени, пока «аналоговый» текст уголовного закона, включающий в себя определения цифровых преступлений и соответствующих за их совершение цифровых наказаний, не будет переложен, образно говоря, на «цифровую партитуру», говорить о сложившемся цифровом уголовном праве нельзя. Причем, даже ту часть, каковая обнаруживает в себе присутствующие в реальном уголовном праве и, соответственно, в реальном уголовном законе диспозиции с преступлениями, носящими информационно-телекоммуникационный характер, цифровым уголовным правом можно, если и называть, то весьма условно. Цифровым, по глубокому убеждению авторов, может называться только действительно ц и ф р о в о й уголовно-правовой ресурс в прямом смысле этого слова, то есть облаченный в информационно-телекоммуникационный (цифровой) формат. Здесь непременно следует рассчитывать на инновационный информационно-технологический потенциал, способный сформировать и в последующем реализовывать в правоохранительной практике основанный на предлагаемой теоретической концепции цифрового уголовного права его материализованный инновационный уголовно-правовой ресурс – цифровой уголовный кодекс. Подчеркнем, что предлагаемые к формированию в ответ на цифровую преступность цифровое уголовное право и его формализованный конструкт – цифровой уголовный закон – это не инициация каких-то инновационных подотраслей существующего уголовного права и уголовного закона, а, в прямом смысле слова, инициация цифровых воплощений уголовного права и уголовного закона, то есть создание программных цифровых алгоритмов уголовно-правового контроля над цифровой (во всех ее проявлениях) преступностью.

Авторы с нетерпением ожидают конструктивной реакции со стороны, прежде всего, представителей научного и правоохранительного сообществ, причем не только из сфер уголовного права и криминологии, но и уголовно-процессуального и уголовно-исполнительного права, криминалистики, оперативно-разыскной деятельности, а равно со стороны представителей всех иных отраслей права, столкнувшихся с проблемами цифровизации правоотношений в своих предметных сферах правового регулирования, от всех, кому небезразличны проблемы безопасности в современном гибридном мире.

Более подробно о направлениях (векторах) реализации научно-исследовательского проекта «Цифровое уголовное право» - в соответствующих монографических исследованиях [2; 3; 4].

Результаты.

Произведенный уголовно-правовой, криминологический и технологический анализ позволяет предположить, что технологический контроль над нормативно обусловленным, а поэтому «правопослушным» поведением, способен автоматически выявлять любые несанкционированные (нештатные) внешние и внутренние угрозы безопасности. Правоохранителям останется лишь процессуально фиксировать факт правонарушения и установить его источник для определения меры юридической ответственности и организации соответствующей процедуры судопроизводства.

Заключение.

Изложенное позволяет сделать вывод о наличии превентивного эффекта цифрового правоохранительного (вместе с технологическим) контроля, поскольку совершение какого-либо правонарушения в киберпространстве станет рискованным для замыслившего его субъекта и потому просто невыгодным, а, по сути, бессмысленным. Разумеется, подобная технология безопасности требует создания собственного правового (и, безусловно, цифрового) механизма ее обеспечения, один из перспективных вариантов которого и предложен авторами.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность автора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Литература:

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (посл. ред.) // СПС КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/?ysclid=lt9wjsbmlf24611532.

2. Джафарли В.Ф. Криминология кибербезопасности: в 5 т. / под ред. С.Я. Лебедева. М.: Проспект, 2022. 1392 с.

3. Джафарли В.Ф. Криминологическая кибербезопасность: теоретические, правовые и технологические основы / под ред. С.Я. Лебедева. 2-е изд., перераб. и доп. М.: Проспект, 2024. 480 с.

4. Лебедев С.Я., Джафарли В.Ф. Цифровое уголовное право. М.: Издательство Проспект, 2024. 392 с.

References:

1. Lebedev S.Y. Law and security in the digital world / Collection of articles based on the materials of the IV All-Russian scientific and practical conference "Criminal law impact and its role in crime prevention". Saratov: Saratov State Law Academy, 2019.

2. Dzhafarli V.F. Criminology of cybersecurity: in 5 volumes / edited by S.Y. Lebedev. M.: Prospekt, 2022. 1392 p.

3. Dzhafarli V.F. Criminological cybersecurity: theoretical, legal and technological foundations / ed. by S.Y. Lebedev. 2nd ed., reprint. and additional m.: Prospect, 2024. 480 p.

4. Lebedev S.Y., Jafarli V.F. Digital criminal law. Moscow: Prospekt Publishing House, 2024. 392 p.

Информация об авторах:

Лебедев Семен Яковлевич, Заслуженный юрист РФ, доктор юридических наук, профессор, заведующий кафедрой уголовного права и адвокатуры, Российский государственный университет имени А.Н. Косыгина, e-mail: lebesem@yandex.ru.

Джафарли Вугар Фуад оглы, доктор юридических наук, доцент, профессор кафедры уголовного права и адвокатуры, Российский государственный университет имени А.Н. Косыгина, e-mail: nizami.66@mail.ru.

Semyon Ya. Lebedev, Doctor of Law, Professor, Honored Lawyer of the Russian Federation, Head of the Department of Criminal Law and Advocacy, Kosygin Russian State University.

Vugar F. Dzhafarli, Doctor of Law, Associate Professor, Professor of the Department of Criminal Law and Advocacy, Kosygin Russian State University.