Квалификация преступлений, связанных с использованием современных электронных сущностей: опыт Германии[1]

Печегин Д. А.,
кандидат юридических наук, старший научный сотрудник
Института законодательства и сравнительного правоведения при Правительстве РФ
E-mail: crim5@izak.ru

Аннотация. *Комплексное правовое регулирование отношений, возникающих в связи с развитием цифровой экономики, в настоящее время предполагает установление оснований и условий привлечения лиц к ответственности за неправомерные действия в новой криптосфере правоотношений, в том числе уголовной. При этом наиболее остро данный вопрос встает в связи с появлением и эволюцией криптовалют — цифровых сущностей, которые стирают любые границы, позволяя «уходить» от учета доходов, уплаты налогов, контроля финансовых потоков и пр. Последнее связано с теми рисками и угрозами, которые несут в себе эти «новые деньги». Ведь в отличие от использования цифровых технологий (т.е. соответствующего программного обеспечения) в преступных целях, где требуется определенная квалификация злоумышленника, воспользоваться криптовалютой для совершения неправомерных действий могут практически все.*

Еще с 2013 г. правительство ФРГ стало признавать Bitcoin цифровой валютой с указанием, что такая валюта не относится ни к электронным деньгам, ни к так называемой «функциональной» валюте (в том числе, и иностранной). В дальнейшем виртуальные валюты на территории ФРГ были признаны финансовым инструментом (2017 г.), а в банковском законодательстве ФРГ они были признаны частными денежными средствами и специфическими единицами финансового учета.

В статье анализируются отдельные аспекты квалификации преступлений в Германии, связанных с использованием современных электронных сущностей.

Ключевые слова: *уголовная ответственность, денежные суррогаты, предпринимательская деятельность, криптовалюта, блокчейн, современные электронные сущности.*

В ФРГ возобладал подход (циркуляр Министерства финансов ФРГ от 27.02.2018), соответствующий позиции Европейского Суда от 22.10.2015, согласно которой для целей налогообложения транзакции с использованием криптовалют определены как платежные услуги, и, соответственно, не должны облагаться налогом на добавленную стоимость, но подлежат учету при расчете налога на доходы. С учетом этого криптовалюта определяется в ФРГ как эквивалент законных средств платежа, а криптовалютные транзакции позиционируются в ФРГ как основанный на договоре альтернативный способ оплаты.

Компании, связанные с криптовалютными операциями, в ФРГ приравнены к финансовым компаниям и должны соответствовать четким лицензионным требованиям. В частности, уставной капитал подобных компаний должен составлять 730 000 евро и более, а менеджмент фирмы должен обладать соответствующей профессиональной квалификацией и отчитываться перед Федеральным управлением финансового надзора ФРГ[2]. Сам же биткоин (Bitcoin) в ФРГ законно стал приниматься к оплате не только в рознично-торговой сети, но и в банковском, и в корпоративном секторе.

Однако новые «деньги» несут в себе чрезмерное количество рисков[3], которые могут оказать негативное влияние не только на благосостояние конкретных граждан, но и национальную экономику, о чем свидетельствуют многочисленные факты. «Анонимность»[4]

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16062 «Концепция правового обеспечения цифровизации сферы публичных финансов».

[2] http: // www.bgbl.de / xaver / bgbl / start.xav?startbk = Bundesanzeiger _ BGBl&jumpTo = bgbl102s2010.pdf (дата обращения: 18.12.2018).

[3] Печегин Д. А. Крипториски // РЖПИ. № 3. 2017. С. 153.

[4] В своей основе криптовалюты анонимны, хотя уже существуют программы, позволяющие деанонимизировать конечного владельца той или иной криптовалюты либо криптокошелька.

и неподконтрольность национальным органам власти привлекает к современным денежным суррогатам теневой экономический оборот, на что неоднократно обращалось внимание в зарубежной литературе[5]. Благодаря анонимности владельцев «криптокошельков», так называемые денежные суррогаты получили популярность при покупке нелегальных товаров, легализации (отмывании) доходов, добытых преступным путем.

Полиция ФРГ все чаще сталкивается с преступниками и целыми группировками, которые совершают преступления в сети Интернет с использованием высокотехнологичного оборудования. Центральной задачей правоохранительных органов ФРГ в данной сфере является превенция совершения противоправных действий. Реакция на развитие преступности так называемой экономики 2.0, 3.0 и т.д. должна быть адекватной. Криминалистические техника и методики также должны соответствовать уровням 2.0, 3.0 и пр. Этим занимаются отделы по противодействию киберпреступности и цифровым расследованиям уголовного розыска той или иной земли ФРГ.

Тем не менее, расследование против киберпреступников дополнительно осложняется некоторыми факторами. Например, киберпреступники все чаще действуют из Darknet — так называемого «темного» Интернета. В этой области сети Интернет преступники могут использовать специальные инструменты и технологии шифрования для обеспечения максимальной анонимности своего трафика.

Другим фактором, осложняющим возможность борьбы с киберпреступностью, является то, что большинство преступлений в данной сфере не являются локальными, в связи с чем необходимо, чтобы государственные органы на федеральном и национальном уровне более тесно сотрудничали в международном контексте. Однако на международном уровне до сих пор не разработаны даже единые принципы или основания взаимодействия стран в рамках понимания природы и использования современных цифровых сущностей, что во многом обусловлено национальными различиями в сфере законодательного регулирования тех или иных вопросов, возникающих в сфере инноваций и валютно-денежных отношений.

Между тем все преступные действия в виртуальном мире так или иначе связаны, как полагают представители немецкой юридической доктрины[6], с интерфейсом выхода в реальный мир. Это ключ к успеху расследования со стороны соответствующих отделов уголовного розыска конкретной земли ФРГ[7].

Киберпреступность в ФРГ включает в себя все преступления, направленные против сети Интернет, дополнительных сетей данных информационных систем или их данных в соответствии с общенациональным определением. Киберпреступность включает в себя и такие преступления, которые совершаются с помощью информационной технологии.[8]

Немецкий правоприменитель, таким образом, исходит из широкого понимания киберпреступлений и включает в их перечень, помимо прочего, деяния, совершенные посредством высказывания (включая распространение порнографии и экстремистскую пропаганду), а равно вторжение в личную сферу жизни человека, мошенничество и компьютерное мошенничество, атаки программного и аппаратного обеспечения (включая подготовку к хищению информации), подделку документов при помощи компьютера, фальсификацию данных, существенных для доказывания, прочие компьютерные преступления[9]. Другими словами данная категория преступлений в немецком уголовном законодательстве в своей основе относится к имущественным деяниям. Однако реалии киберпреступности и масштабы роста количества уголовно-наказуемых деяний в этой сфере сильно опережают законодателя.

---

[5] Polasik M., Piotrowska A.,Wisniewski T., Kotkowski R., Lightfoot G. Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry. P. 20-21; https://ssrn.com/abstract=2516754 (дата обращения: 22.11.2018); Luther W. J. Bitcoin and the Future of Digital Payments. 14 p.; https://ssrn.com/abstract=2631314 (дата обращения: 22.11.2018); Bryans D. Bitcoin and Money Laundering: Mining for an Effective Solution // 89 Ind. L.J. 2014. P. 441-472; https://ssrn.com/abstract=2317990 (дата обращения: 22.11.2018).

[6] Например: https://www.bitcrime.de/presse-publikationen/pdf/BITCRIME-RegulRep.pdf (дата обращения: 18.12.2018); Brenig C., Accorsi R., Müller G. Economic Analysis of Cryptocurrency Backed Money Laundering // ECIS Completed Research Papers. 2015. Paper 20 // https://aisel.aisnet.org/ecis2015_cr/20/ (дата обращения: 18.12.2018); Grzywotz J., Köhler O., Rückert C. Cybercrime mit Bitcoins — Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention // StV. 2016. № 11. P. 753-759, https://www.bitcrime.de/presse-publikationen/ (дата обращения: 18.12.2018).

[7] Так, полиция Баден-Вюртемберга уже несколько лет назад ввела специальную должность киберкриминалиста. Особенно квалифицированные ИТ-специалисты осуществляют свою службу в отделе противодействия киберпреступности и цифровых расследований уголовного розыска, а также в соответствующих уголовных инспекциях 12 региональных полицейских штабов.

[8] https://lka.polizei-bw.de/wp-content/uploads/sites/14/2017/06/Cybercrime_Digitale_Spuren.pdf (дата обращения: 22.11.2018); https://cyberleninka.ru/article/v/kiber-i-internet-prestupnost-v-germanii-i-rossii-vozmozhnosti-sravnitelnogo-issledovaniya (дата обращения: 22.11.2018).

[9] Зигмунт О. А. Кибер- и интернет-преступность в Германии и России: возможности сравнительного исследования // Юридическая наука и правоохранительная практика. 2015. № 4(34). С. 182.

Анализируя зарубежное законодательство в связи с насущностью определения порядка и оснований наступления ответственности в условиях новой криптосферы правоотношений можно, в целом, выделить четыре подхода к изменению уголовного законодательства: 1) введение в конкретные составы, перечисленные в Особенной части, дополнительных положений, связанных с криптосферой; 2) установление и определение новых составов преступлений; 3) использование уже имеющихся составов преступлений для регламентации ответственности в условиях новой криптосферы правоотношений; 4) частичное или полное использование всех перечисленных вариантов одновременно.

Федеральная служба уголовной полиции ФРГ (Bundeskriminalamt) представила ежегодный отчет о состоянии киберпреступности в стране за 2017 г.[10] В данном отчете были отражены сведения и о преступлениях, связанных с криптовалютой. Причем многие вредоносные программы сегодня акцентируются на том, чтобы нелегально и незаметно использовать ИТ-ресурсы той или иной компании либо отдельного пользователя для того, чтобы осуществлять скрытый криптомайнинг, в том числе известной цифровой валюты биткоин. Причем для этого сегодня не обязательно заражать компьютер конкретного пользователя, соответствующие скрипты, которые будут «высасывать» энергоресурс вашего компьютера теперь можно встраивать в сайты и видео (музыку). Зайдя на тот или иной ресурс и нажав кнопку «Play» пользователь автоматически разрешает такому ресурсу использовать вычислительную мощность его компьютера до тех пор, пока он данным ресурсом пользуется. Сложность квалификации такого деяния заключается в том, что такие программы зачастую не нарушают целостность самой системы, а просто нагружают ее гораздо сильнее, пока пользователь обращается к интернет-ресурсу. Иными словами, как только пользователь закроет сайт или браузер, то соответствующий скрипт прекратит свое выполнение и не будет наносить вреда системе пользователя. УК ФРГ содержит самостоятельный состав преступления, предусмотренный § 303a, который устанавливает ответственность за неправомерное удаление, преобразование, приведение в непригодное состояние и изменение данных пользователя.

Однако для того, чтобы квалифицировать описанный выше случай по § 303a УК ФРГ, соответствующий скрипт должен проникнуть в уязвленную систему и образовать в этой системе условия для постоянной связи с соответствующим сервером. В последнем случае такое деяние подпадает под признаки преступления, предусмотренного § 303a УК ФРГ, поскольку тут, скорее всего, произойдет тайное и несанкционированное изменение данных пользователя. Вместе с тем для такого вывода программное обеспечение соответствующего компьютера, по идее, должно стать единым, по подобию блокчейн-технологии, когда любое изменение требует создания нового блока, что позволит легко выявить несанкционированные изменения системы. Но даже и без такой структуры программного обеспечения конкретного пользователя данный случай, в целом, подпадает под § 303a УК ФРГ.

Земельный суд г. Кемптена (Бавария) в своем решении[11] от 27.07.2017 указал, что изменение данных по смыслу абз. 1 § 303a УК ФРГ имеет место в результате нарушения функций данных, которые приводят к изменению их информационного содержания или показателя. Под это подпадает любая форма преобразования содержимого сохраненных данных, причем не имеет значения, является ли это объективным улучшением. Решающее значение имеет, скорее, то, что состояние системы отличается от предыдущего. При этом сам пользователь обязан предпринять меры по защите своей информации, например, воспользоваться брандмауэром, который не позволит обычном пользователю без специальной подготовки получить доступ к информационной системе.

Однако это не означает, что преступник в последнем случае избежит ответственности. В рассмотренном деле только на 75% зараженных компьютеров брандмауэр был включен автоматически, тогда как в 25% случаев такая программа была деактивирована. Вместе с тем, вредоносное программное обеспечение скрытно устанавливалось на компьютеры пользователей и обладало возможностью обходить защиту брандмауэра. Поэтому все установленные судом случаи были верно квалифицированы по § 303a УК ФРГ.

С другой стороны, современные технологии позволяют, как мы выяснили выше, обходиться и без изменения соответствующих данных либо заражения компьютера, что требует самостоятельного осмысления с точки зрения описания преступного деяния в доктрине уголовного права и далее, соответственно, в уголовном законодательстве. В частности, отдельного осмысления требует та граница, за пределами которой будет установлена уголовная ответственность при несанкционированном использовании ресурсов компьютера пользователя, посетившего тот или иной интернет-ресурс. Ведь данные скрипты весьма успешно могут использоваться

[10] https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017 (дата обращения: 12.12.2018).

[11] BGH 1 StR 412/16 — Beschluss vom 27. Juli 2017 (LG Kempten) // https://www.hrr-strafrecht.de/hrr/1/16/1-412-16.php (дата обращения: 12.12.2018).

рекламодателями взамен обращения к баннерам, которые иногда слишком навязчиво предлагают какой-либо товар пользователю и в большей степени нагружают операционную систему компьютера пользователя. Однако данная проблема в науке уголовного права ФРГ не решена.

Сегодня нередки и такие случаи, когда компьютеры, особенно ИТ-системы компаний и их серверы, намеренно заражаются вирусной программой в целях скрытого криптомайнинга. Так, в июне 2017 г. во всем мире произошло массовое разрушительное воздействие вредоносного программного обеспечения на ИТ-системы предприятий. Эти события коснулись и ФРГ. Вредоносная программа «NotPetya»[12] изначально заразила несколько компаний, преимущественно в Украине, для выявления уязвимости в бухгалтерском программном обеспечении. Вредоносные программы затем распространялись самостоятельно и на многие другие компании, которые также использовали упомянутое программное обеспечение. Наряду с предприятиями в Украине предприятия во многих других государствах были заражены этим вирусом. В результате заражения указанные системы перестали функционировать и в целом вышли из строя. После первоначального акта заражения вредоносная программа распространилась самостоятельно на другие уязвимые системы, даже за пределами уже зараженных компаний. Это свидетельствует о растущем техническом развитии вредоносных программ.

В итоге отдельные компании не смогли полностью восстановить свои ИТ-инфраструктуры в течение нескольких недель после атаки. Датская судоходная компания MAERSK и компания фрахтовых услуг TNT Express полагают, что понесенные ими убытки составили более 300 млн долл. США. В целом ущерб, нанесенный вредоносным вирусом, только в Европе оценивается более чем в 1 млрд евро.

Распространение описанного вредоносного программного обеспечения было направлено на уничтожение данных и блокирование (саботирование) бизнес-процессов. Данный случай, таким образом, является актом кибер-саботажа, что подпадает под действие § 303b УК ФРГ. Однако на практике такие случаи фиксируются очень редко. Связано это с тем, что злоумышленники стараются разработать такую программу, которая длительное время не позволяла бы себя обнаружить. Кроме того, сами компании могут обращаться с тем или иным заявлением в правоохранительные органы спустя большое количество времени, а в расследовании цифровых преступлений именно время становится ключевым фактором. Все это осложняет деятельность органов полиции ФРГ по противодействию преступлениям в сфере цифровых инноваций.

Предложенный краткий анализ проблемы и ее решения в ФРГ показал, что в немецкой доктрине констатируются случаи совершения преступлений с использованием цифровых технологий. Зачастую эти деяния носят трансграничный характер, что существенно осложняет возможность правоохранительных органов ФРГ своевременно и в полном объеме получать доказательства при производстве уголовных дел. Помимо этого наблюдаются определенные сложности в квалификации преступлений, совершенных с использованием цифровых технологий, так как большинство из них немецкий правоприменитель пытается подвести под уже существующие составы. Вместе с тем данный подход не позволяет однозначно прийти к выводу о том, что наказание, определенное действующими нормами УК ФРГ, действительно соответствует той общественной опасности, которую заключают в себе совершенные с использованием цифровых технологий преступления. Кроме того, представленный выше анализ требует регламентации в немецком уголовном законодательстве новых составов. Представляется, что выявленные проблемы можно решить на качественном уровне только при наличии международного стандарта противодействия преступлениям, совершаемым с использованием современных цифровых технологий.

Список литературы

1. Зигмунт О. А. Кибер- и интернет-преступность в Германии и России: возможности сравнительного исследования // Юридическая наука и правоохранительная практика. 2015. № 4(34). С. 180-188.
2. Кучеров И. И. Криптовалюта (идеи правовой идентификации и легитимации альтернативных платежных средств). М., 2018. 204 с.
3. Мансуров Г. З. К проблеме пределов применения денежных суррогатов // Банковское право. 2004. № 4. С. 19-22.
4. Печегин Д. А. Крипториски // РЖПИ. 2017. № 3. С. 151-157.
5. Талапина Э. В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. 2018. № 2. С. 5-17.
6. Хабриева Т. Я. Право перед вызовами цифровой реальности // Журнал российского права. 2018. № 9. С. 5-16.
7. Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 85-102.
8. Brenig C., Accorsi R., Müller G. Economic Analysis of Cryptocurrency Backed Money Laundering // ECIS

[12] https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf (дата обращения: 12.12.2018).

Completed Research Papers. 2015. Paper 20; https://aisel.aisnet.org/ecis2015_cr/20/.
9. Bryans D. Bitcoin and Money Laundering: Mining for an Effective Solution // 89 Ind. L.J. 441. 2014; https://ssrn.com/abstract=2317990.
10. Grzywotz J., Köhler O., Rückert C. Cybercrime mit Bitcoins — Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention // StV. 2016. № 11. P. 753-759.
11. Luther W. J. Bitcoin and the Future of Digital Payments. 14 p.; https://ssrn.com/abstract=2631314.
12. Pechegin D. A. Criminal Responsibility in the Cryptosphere // European Researcher. Series A. 2018. № 9(1). P. 50-57; http://www.erjournal.ru/journals_n/1521800996.pdf.
13. Polasik M., Piotrowska A., Wisniewski T., Kotkowski R., Lightfoot G. Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry // 20(1) International Journal of Electronic Commerce. 2015; https://ssrn.com/abstract=2516754.

Qualification of Crimes Related to the Use of Modern Electronic Entities: the Experience of Germany

Pechegin D.A.,
PhD in Law, Senior Researcher,
the Institute of Legislation and Comparative Law
under the Government of the RF
E-mail: crim5@izak.ru

Abstract. *Comprehensive legal regulation of relations arising in connection with the development of the digital economy currently involves the establishment of the grounds and conditions for bringing persons to responsibility for illegal actions in the new crypto sphere of legal relations, including criminal liability. At the same time, this issue is most acute in connection with the emergence and evolution of crypto — currencies-digital entities that erase any boundaries, allowing you to «move away» from accounting for income, paying taxes, controlling financial flows, and so on. The latter is related to the risks and threats posed by this «new money». After all, unlike the use of digital technologies (i.e. the appropriate software) for criminal purposes, where a certain qualification of the attacker is required, almost everyone can use the cryptocurrency to commit illegal actions.*
Since 2013, the German Government began to recognize Bitcoin as a digital currency, indicating that such currency does not apply to electronic money or to the so-called «functional» currency (including foreign currency). In the future, virtual currencies in Germany were recognized as a financial instrument (2017), and in the banking legislation of Germany they were recognized as private funds and specific units of financial accounting.
The article analyzes some aspects of the qualification of crimes related to the use of modern electronic entities in Germany.
Keywords*: criminal liability, cash equivalents, entrepreneurship, cryptocurrency, surrogates, blockchain, modern electronic entities.*

References

1. Zigmunt O. A. Kiber- i internet-prestupnost v Germanii i Rossii: Vozmozhnosti sravnitelnogo issledovaniya // Yuridicheskaya nauka i pravookhranitelnaya praktika. 2015. № 4(34). S. 180-188.
2. Kucherov I. I. Kriptovalyuta (idei pravovoj identifikatsii i legitimatsii alternativnykh platezhnykh sredstv). M., 2018. 204 s.
3. Mansurov G. Z. K probleme predelov primeneniya denezhnykh surrogatov // Bankovskoe pravo. 2004. № 4. S. 19-22.
4. Pechegin D. A. Kriptoriski // RZHPI. 2017. № 3. S. 151-157.
5. Talapina E. V. Pravo i tsifrovizatsiya: novye vyzovy i perspektivy // Zhurnal rossijskogo prava. 2018. № 2. S. 5-17.
6. Khabrieva T.Ya. Pravo pered vyzovami tsifrovoj realnosti // Zhurnal rossijskogo prava. 2018. № 9. S. 5-16.
7. Khabrieva T.Ya., Chernogor N. N. Pravo v usloviyakh tsifrovoj realnosti // Zhurnal rossijskogo prava. 2018. № 1. S. 85-102.
8. Brenig C., Accorsi R., Müller G. Economic Analysis of Cryptocurrency Backed Money Laundering // ECIS Completed Research Papers. 2015. Paper 20; https://aisel.aisnet.org/ecis2015_cr/20/.
9. Bryans D. Bitcoin and Money Laundering: Mining for an Effective Solution // 89 Ind. L.J. 441. 2014; https://ssrn.com/abstract=2317990.
10. Grzywotz J., Köhler O., Rückert C. Cybercrime mit Bitcoins — Straftaten mit virtuellen Währungen, deren Verfolgung und Prävention // StV. 2016. № 11. P. 753-759.
11. Luther W. J. Bitcoin and the Future of Digital Payments. 14 p.; https://ssrn.com/abstract=2631314.
12. Pechegin D. A. Criminal Responsibility in the Cryptosphere // European Researcher. Series A. 2018. № 9(1). P. 50-57; http://www.erjournal.ru/journals_n/1521800996.pdf.
13. Polasik M., Piotrowska A., Wisniewski T., Kotkowski R., Lightfoot G. Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry // 20(1) International Journal of Electronic Commerce. 2015; https://ssrn.com/abstract=2516754.