Идрисов Ильдар Талгатович
Idrisov Ildar Talgatovich
кандидат юридических наук, доцент кафедры уголовного права и криминологии, Самарский университет
Candidate of Law, Associate Professor of the Department of Criminal Law and Criminology, Samara University
E-mail: ildar_idrisov1988@mail.ru

УДК: 343.241

ОБ УГОЛОВНО-ПРАВОВЫХ ПОСЛЕДСТВИЯХ НЕИСПОЛНЕНИЯ ОБЯЗАТЕЛЬСТВ, ВОЗНИКШИХ В ВИРТУАЛЬНОЙ СРЕДЕ

ON THE CRIMINAL CONSEQUENCES OF NON-PERFORMANCE OF OBLIGATIONS ARISING IN THE VIRTUAL ENVIRONMENT

Ключевые слова: научно-технический прогресс, обязательства в виртуальной среде, ответственность искусственного интеллекта, электронные платежные средства, криминализация деяний с использованием платежных систем, трендовые преступления, кибепреступность.

Keywords: scientific and technological progress, obligations in the virtual environment, responsibility of artificial intelligence, electronic payment means, criminalization of acts using payment systems, trend crimes, cybercrime.

В настоящей статье анализируются уголовно-правовые последствия неисполнения обязательств, возникших в виртуальной среде. Указывается на вынужденный характер запаздывающего развития уголовного законодательства в целях ответственности за неисполнение или ненадлежащее исполнение обязательств в виртуальной среде. В качестве современных проблемных явлений выделяются: использование беспилотных такси, распространение электронных платежных средств и систем, массовые многопользовательские онлайн-игры. В статье рассматриваются вопросы привлечения к ответственности владельцев искусственного интеллекта, указывается на необходимость не только криминализации новых деяний с использованием платежных систем, но и определения правил квалификации соответствующих преступлений с применением норм действующего Уголовного кодекса Российской Федерации. Отмечается трендовость преступлений в сфере информационных технологий, в том числе с использованием электронной

цифровой подписи. Автором формулируются некоторые предложения, направленные на предупреждение преступлений, сопряженных с неисполнением обязанностей в виртуальной среде.

This article analyzes the criminal-legal consequences of non-fulfillment of obligations that occurred in the virtual environment. Indicates the forced nature of the delayed development of criminal legislation for the purpose of liability for non-performnce or improper performance of obligations in the virtual environment. The use of driverless taxis, the spread of electronic payment means and systems, and massive multiplayer online games are highlighted as modern problematic phenomena. The article deals with the issues of bringing to justice the owners of artificial intelligence, indicates the need not only to criminalize new acts using payment systems, but also to determine the rules for qualifying relevant crimes using the norms of the current Criminal code of the Russian Federation. There is a trend in crimes in the field of information technology, including those involving the use of electronic digital signatures. The author formulates some proposals aimed at preventing crimes involving non-performance of duties in a virtual environment.

В условиях научно-технического прогресса и развития IP-технологий поэтапно вытесняется человеческий труд, автоматизируются привычные действия людей, роботизируются производственные процессы, в них внедряется искусственный интеллект. Использование электронных технологий предполагает развитие информационного потенциала страны, делает жизнь граждан более удобной и может являться, например, мощным инструментом противодействия коррупции. Вместе с тем стремительные технологические и информационные изменения влекут за собой различные варианты отклоняющегося поведения. Распространению общественно опасного поведения с использованием новых знаний и технологий способствуют условия отсутствия достаточных и своевременных государственных мер реагирования.

Между пользователями сети Интернет давно складываются онлайн-отношения, не урегулированные, но требующие правового регулирования. Следует отметить, что развитие общественных отношений обычно опережает их правовое регулирование, как это уже неоднократно подтверждалось в отношении оборота криптовалют (денежных суррогатов) [1, с. 121–126].

В настоящее время стал масштабным объем рынка электронных платежей, что связано с внедрением вычислительной техники и информационных технологий практически во все сферы

деятельности. Почти каждый гражданин Российской Федерации ежедневно использует функции платежных систем. По данным статистики, только за 2018 год было проведено 4305,1 млн платежей через кредитные организации с использованием платежных инструментов общим объемом 614 060,4 млрд рублей [2]. Развитию платежных систем сопутствует отклоняющееся поведение их участников. О степени общественной опасности преступлений, совершенных с использованием электронных платежных средств и систем как в России, так и за ее пределами, свидетельствует то, что в настоящее время продолжает расти ущерб, причиненный такими преступлениями.

Колоссальные суммы переводов денежных средств, осуществляемых через платежные системы, по мнению Е.А. Соловьевой, побуждают преступников совершать преступления не в традиционном виде, похищая наличные деньги, вещи, ценные бумаги, изобретать новые способы, посягая на безналичные, электронные денежные средства и криптовалюту [3, с. 4].

Для выявления проблематики неисполнения обязательств, возникших в виртуальной платежной среде, необходимо охарактеризовать электронные платежные средства и электронные платежные системы.

В целях оборота и осуществления расчетов такими средствами пользователь устанавливает на свой компьютер специально предназначенную для этого программу, которая поддерживает ведение локально или удаленно так называемого виртуального кошелька, который можно пополнить реальными деньгами через банковский, почтовый переводы, а также за счет перечисления из других виртуальных кошельков, однако данные средства будут выступать именно средствами «учета» существующей на реальном банковском счете наличности. Виртуальный кошелек – это специальная программа (кипер), которая необходима для учета и управления электронной наличностью, как правило, представляет собой сложный код, отражающий состояние денег в системах [4, с. 132].

Функционирование платежных систем в сети Интернет осуществляется таким образом, что правила операций устанавливают владельцы платежных систем, пользователь при регистрации должен всего лишь автоматизированно заполнить позиции элек-

тронной формы, что трактуется владельцем системы как факт согласия с предложенными условиями. При этом спустя даже небольшое количество времени как сама электронная форма целиком, так и ее отдельные поля могут произвольно быть изменены владельцем системы, что повлечет за собой наступление юридических последствий для всех пользователей, присоединившихся ранее совсем к другой оферте в электронном виде. Порядок привлечения к ответственности в данном случае за нарушение обязательств действующим законодательством не предусмотрен. Очевидной является необходимость разработки соответствующих мер реагирования, включая уголовно-правовые, в отношении неисполнения обязательств, возникших в виртуальной среде.

Сами владельцы платежных систем заинтересованы в том, чтобы не подпадать под действие законодательных предписаний, в то время как пользователь, наоборот, – в максимальном регулировании. Пробелы законодательства привлекают преступников, и активно ими используются.

Электронная коммерция стала неотъемлемой частью современной экономики. Все больше потребителей приобретают товары посредством сети Интернет, а коммерческие организации так или иначе используют возможности данной сети при осуществлении предпринимательской деятельности.

Право электронной коммерции, так же как и интернет-право, кибер-право и иные популярные ныне обозначения, не является самостоятельной отраслью права с единой концепцией, представляет собой комплекс разнородных по своей отраслевой природе правил, объединенных общностью предмета, к которому они относятся [5, с. 20]. Представляется необходимым установление порядка и условий привлечения к ответственности за неисполнение обязательств в новых сферах жизни в рамках действующих охранительных отраслей права.

С использованием электронных платежных систем могут быть совершены следующие виды преступлений: легализация (отмывание) денежных средств, полученных преступным путем; кража; мошенничество; получение или дача взятки; незаконное получение кредита и др. Количество таких преступлений растет, изменяются обстоятельства их совершения.

Проблемой является квалификация соответствующих преступлений с применением уже известных норм Уголовного кодекса РФ, прежде всего в связи с правовой неопределенностью электронных денежных средств, сложностью определения предмета, средств, способа, виновного в совершении таких преступлений. Этим объясняется высокая латентность совершаемых в платежных системах преступлений. Несмотря на неуклонный рост несанкционированных операций с использованием электронных платежных инструментов, на сегодняшний день нет официальных данных о количестве совершаемых в платежных системах преступлений. Данные обстоятельства говорят о малоизученности проблематики, запаздывающем уголовно-правовом регулировании на побочные явления эволюционного процесса.

К одной из неурегулированных областей виртуальной среды можно отнести приобретающие все большую популярность массовые многопользовательские онлайн-игры, стремительно возрастающая аудитория которых повышает активность мошенников и разработчиков вредоносного программного обеспечения.

В процессе развития и широкого распространения онлайн-игр, когда внутри виртуальных пространств появилась связь с реальными финансами, возник так называемый феномен виртуальной экономики, основная идея которого – допустимость реальных экономических отношений в процессах игровой экономической системы. Стала возможна, например, торговля виртуальными предметами за реальные денежные средства.

С точки зрения экономико-социальных отношений, к понятию «благо» относится все, что может иметь рыночную цену. Таким образом, с точки зрения реальных (не игровых) отношений в сфере онлайн-игр благом являются виртуальные (созданные игровым путем, в игре и для целей игры) предметы, наличие которых способно доставить их обладателю удовольствие и удовлетворить потребности в форме достижения определенного успеха в занятии досугом [6, с. 3]. При этом такие блага могут передаваться от игрока к игроку и иметь реальную цену. Более того, возникают определенные «виртуальные» обязанности, неисполнение которых, очевидно, может повлечь за собой негативные последствия, в том числе уголовно-правовые.

Соответственно, вполне возможно совершение преступлений в виртуальной игровой среде. К примеру, Нижегородской полицией была раскрыта кража аккаунта в игре World of Tanks стоимостью 70 000 рублей. По словам заместителя главы областного управления уголовного розыска ГУ МВД России, заявление о похищении «танка» поступило от 24-летнего мужчины. Выяснилось, что данное лицо приобрело за 70 000 рублей аккаунт в онлайн-игре World of Tanks, который был у него похищен. То есть танки, конечно, виртуальные, но деньги за них заплачены вполне реальные. Похитителя «танка» выявили при попытке перепродажи похищенного аккаунта с целью получения за него реальных денег. Злоумышленником оказался житель Лысковского района Нижегородской области. У него уже был опыт двух преступлений в среде онлайн-игр. Это не первый случай обращения в Нижегородскую полицию с аналогичными заявлениями [7].

Оборот реальных денежных средств, задействованных в отношениях между игроками различных онлайн-игр, постоянно растет, в связи с чем возникает объективная необходимость в учете движения этих средств в целях недопущения их использования в преступных целях.

В последние годы широкое распространение также получили преступления в сфере информационных технологий, такие как распространение вредоносных вирусов, взлом паролей, кража номеров банковских карт, вредоносное вмешательство через компьютерные сети в работу различных систем, которые охватываются современным термином «киберпреступность».

Одним из таких трендовых преступлений является совершение преступлений с использованием электронной цифровой подписи. Показательным является случай хищения квартиры с использованием электронной подписи у одного из жителей г. Москвы. Весной 2019 г. потерпевший узнал о том, что он якобы продал квартиру другому человеку, когда решил получить парковочное место в своем доме, но получил отказ. Все документы, переданные в Росреестр, были с подделанной электронной цифровой подписью. Самое интересное, что для подделки документов мошенники использовали старый, недействительный паспорт потерпевшего. С электронной цифровой подписью потерпевший

никогда не имел дело. В Росреестре сообщили, что формально процедура продажи была законной, так как была проверена полнота представленного пакета документов, электронная цифровая подпись являлась действующей и была принята порталом государственных услуг. Все документы, поступившие в электронном виде, соответствовали действующему законодательству и имели ЭЦП, ввиду чего основания для приостановления государственной регистрации недвижимости отсутствовали. В настоящее время по данному факту продолжается следствие [8]. В короткие сроки после данного случая в Государственную Думу был внесен законопроект о защите граждан от мошеннических действий с их недвижимостью, совершаемых при помощи электронной подписи.

Очевидно, что законодатель не может заранее предусмотреть необходимые меры предупреждения и защиты от подобных кибердействий, создать справедливый принцип ответственности или презумпцию, поскольку вначале следует разобраться с существующими разновидностями таких действий, чтобы исключить привлечение к ответственности невиновных лиц. Опережающее развитие для уголовного законодательства не характерно.

Учитывая, что разброс возрастов аудитории онлайн-игр, как и пользователей сети Интернет, велик, представляется уместным установить на законодательном уровне возможность привлечения к административной ответственности лиц, не достигших установленного минимального возраста, в целях, прежде всего, предупреждения развития подростковой преступности в сфере компьютерной информации.

Еще одним примером современного этапа развития технологий с неясными правовыми последствиями является разработка самоуправляемых автомобилей «робота-такси» или «робота в такси». Так, международная корпорация Uber в качестве приоритетных целей определила создание беспилотных такси [9]. В известной степени за управление и движение автомобиля будет отвечать искусственный интеллект, то есть фактически услугу по перевозке пассажиров оказывает робот, а не человек. Невозможно представить, что робот будет нести ответственность за

неисполнение возложенных на него обязательств. С одной стороны, ответственность за действия робота, выполняющего перевозку пассажиров от имени предпринимателя, должен нести сам предприниматель. Вместе с тем стоит задуматься о возможности рассмотрения непрогнозируемых действий и решений искусственного интеллекта как обстоятельств непреодолимой силы, то есть вовсе исключающих ответственность [10, с. 32–35]. В таком случае бремя доказывания в суде данных обстоятельств возлагается на владельцев искусственного интеллекта.

Эффективными в борьбе с неисполнением или ненадлежащим исполнением обязательств в виртуальной среде являются способы, адекватные особенностям совершенных незаконных действий. Например, информирование о реальных возможностях правоохранительных органов в расследовании преступлений, имеющих отношение к виртуальным мирам, позволит уменьшить количество соответствующих латентных случаев и создать алгоритм привлечения к ответственности виновных лиц.

Также видится необходимым определить правовую природу предметов виртуального мира, которые не являются объектами гражданских прав (вещью), по крайней мере, они не поименованы в ст. 128 ГК РФ. Очевидно, что виртуальные обязательства пользователей сети Интернет требуют регулирования на законодательном уровне. Необходимо определить ответственных за искусственный интеллект, поскольку в настоящее время квалификация по статьям УК РФ деяний, сопряженных с прогнозируемыми решениями искусственного интеллекта, исключается.

Установление уголовно-правовых запретов на совершение деяний, посягающих на отношения в виртуальной среде, должно базироваться на общей теории криминализации и специальных научных исследованиях, посвященных вопросам квалификации отдельных таких преступлений.

Внимательное отношение государственной власти к новым реалиям позволит избежать негативных последствий создания искусственного интеллекта и виртуальной деятельности для гражданского общества и человечества в целом.

* * *

1. Идрисов И.Т. Виртуализация валюты как проблема криминализации и квалификации // Актуальные вопросы права в банковской сфере: материалы Международного правового банковского форума, 10-11 октября 2019. Самара: Изд-во СГЭУ, 2019. С. 121-126.

2. Структура платежей, проведенных через кредитные организации (по платежным инструментам) [Электронный ресурс] // Официальный сайт Банка России. URL: https: //www.cbr.ru/statistics/p_sys/ print.aspx?file =sheet007.htm&pid=psrf&sid=ITM_12859 (дата обращения: 29.08.2020).

3. Соловьева Е.А. Преступления, совершаемые в платежных системах. Автореф. дисс. канд наук. Саратов, 2019. С. 4.

4. Олиндер Н.В. Криминалистическая характеристика электронных платежных средств и систем // Lex Russica. М., 2015. №10. С. 132.

5. Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. Монография. 2-е изд., перераб. и доп. М.: Статут, 2016. С. 20.

6. Атаманов Р.С. Криминалистическая характеристика мошенничества в онлайн-играх // Российский следователь. М., 2011. №21. С. 3.

7.https://www.rbc.ru/technology_and_media/02/03/2016/56d7293d9a79473f782ed597 (дата обращения: 2.09.2020).

8. http://новости-россии.ru-an.info/новости/кража-квартиры-с-использованием-цифровой-подписи-как-можно-предотвратить-мошеннические-сделки/ (дата обращения: 2.09.2020).

9. РБК: http://style.rbc.ru/objects/auto/571638db9a79472acdb34e2e.

10. Лаптев В.А. Ответственность «будущего»: правовое существо и вопрос оценки доказательств // Гражданское право. 2017. №3. С. 32-35.