УГОЛОВНОЕ ПРАВО

УДК 343

Р. Ф. Азизов

РАЗВИТИЕ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ БОРЬБЫ С КИБЕРПРЕСТУПЛЕНИЯМИ В АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКЕ

Статья посвящена вопросам развития уголовного законодательства в сфере борьбы с киберпреступлениями в Азербайджанской Республике. В статье рассматриваются основные правовые акты, принятые за последние годы, в том числе изменения в Уголовный кодекс Азербайджанской Республики. Автор указывает на несовершенство соответствующего законодательства, на основные проблемы, связанные с ним, предлагает унифицировать терминологическую базу, используемую в уголовных нормах. Автор приходит к выводу о том, что решение проблем целесообразно искать в рамках сотрудничества в региональных организациях.

Ключевые слова: Азербайджанская Республика, информационные технологии, уголовное законодательство, Интернет, электронное право, электронная торговля, информационная безопасность, киберпреступность, спам.

R. F. Azizov

DEVELOPMENT OF CRIMINAL LEGISLATION AGAINST CYBERCRIMES IN THE REPUBLIC OF AZERBAIJAN

The article is devoted to the development of criminal legislation against cybercrimes in the Republic of Azerbaijan. The article deals with main, recently adopted legal acts, including amendments to the Criminal Code of the Republic of Azerbaijan. The author points out the imperfection of the relevant legislation, defines the main problems of the process and proposes unification of the terminology used in criminal legal norms. The author concludes that cooperation within the frameworks of regional organizations is the best solution to speed up the process.

Keywords: the Republic of Azerbaijan, informational technologies, criminal legislation, Internet, e-law, e-trade, information security, cybercrime, spam.

Бурное развитие информационных технологий на современном этапе эволюции цивилизации привело к возникновению новых форм существования человеческого общества.[1] В основе этой трансформации лежит новый — информационный — этап научно-технической революции, который внес кардинальные перемены в современный миропорядок. Необходимым условием состоятельности государства сегодня

Азизов Рашад Фикрат — докторант, Санкт-Петербургский государственный университет, Российская Федерация, 199034, Санкт-Петербург, Университетская наб., 7–9; azizoff1980@gmail.com

Azizov Rashad Fikrat — doctoral candidate, St. Petersburg State University, 7–9, Universitetskaya nab., St. Petersburg, 199034, Russian Federation; azizoff1980@gmail.com

[1] См. об этом: *Азизов Р. Ф.* К вопросу актуальности сравнительно-правового исследования правового регулирования в сети Интернет // Мировой судья. 2013. № 4. С. 8–10.

выступает наличие соотносимого с потребностями граждан информационного общества.[2] По этой причине большинство государств старается усилить свое влияние в информационных сетях, увеличить степень своего присутствия в них. Эти процессы присущи практически всем странам СНГ, в том числе и Азербайджанской Республике.

Вместе с тем как в мировых масштабах, так и в национальных границах технический и технологический прогресс не выполняет однозначной социальной функции. Формирование единого киберпространства порождает не только новые коммуникативные созидательные возможности, но и ряд девиантных, в том числе криминальных явлений.[3] Как и процесс глобализации в целом, глобальная преступность в ее современных формах, в международной среде и в параметрах национальных преступных формирований канализируется по уже глобальным коммуникациям: в сфере материального взаимодействия — через транспортные средства, энергоносители и средства связи, в сфере обмена информации — с использованием экспоненциально расширяющихся возможностей компьютерного киберпространства.

За последние несколько лет Азербайджанская Республика сделала ряд серьезных шагов в сфере борьбы с киберпреступностью. Долгое время в Республике действовали уголовные нормы, которые предусматривали ответственность за так называемые «компьютерные преступления». Эти нормы были приняты в конце 1990-х гг. и по своему составу полностью дублировали нормы российского уголовного законодательства того периода. Производство по данным статьям велось службами национальной безопасности, количество дел и решений было минимальным.

Ситуация должна была кардинально измениться после того, как информационно-коммуникационные технологии были определены основным ненефтяным приоритетом экономики.[4] Последовавшие за этим национальные проекты ознаменовались принятием целого ряда нормативных актов, включая Законы Азербайджанской Республики «Об электронной торговле»,[5] «Об электронной подписи и электронном документообороте»,[6] «О доступе к информации»[7] и др. Однако процесс обладал признаками формализма, так как большинство этих своевременных нормативных актов, вступив в законную силу, не приобрело реальной значимости. Процесс законсервировался еще на 5–6 лет, поскольку информационная инфраструктура страны явно не соответствовала необходимому уровню для полноценной интеграции

---

[2] *Джансараева Р. Е., Аратулы К.* Борьба с киберпреступлениями: Сравнительный анализ законодательства стран СНГ // Криминологический журнал Байкальского государственного университета экономики и права. 2012. № 3. С. 95.

[3] *Пономарев Д. А.* Информационные технологии как криминогенный фактор организованной преступности в условиях глобализации. Доклад на VI Международной конференции «Право и Интернет», Москва, 2004 г. // www.ifap.ru/pi/06/r16.htm (дата обращения: 30.01.2015).

[4] *Постановление* Президента Азербайджанской Республики от 17 февраля 2003 г. № 1146 «Об утверждении "Национальной стратегии развития ИКТ во благо Азербайджанской Республики на 2003–2012 гг."» // http://mincom.gov.az/qanunvericilik/serencamlar/# (дата обращения: 29.01.2015).

[5] *Закон* Азербайджанской Республики от 10 мая 2005 г. № 908 IIQ «Об электронной торговле» // http://e-qanun.az/framework/10406 (дата обращения: 29.01.2015).

[6] *Закон* Азербайджанской Республики от 9 марта 2004 г. № 602-IIQ «Об электронной подписи и электронном документообороте» // http://mincom.gov.az/qanunvericilik/qanunlar/# (дата обращения: 29.01.2015).

[7] *Закон* Азербайджанской Республики от 30 сентября 2005 г. № 1024-IIQ «О доступе к информации» // http://e-qanun.az/framework/11142 (дата обращения: 29.01.2015).

в общественные отношения таких институтов, как электронная торговля, электронное правительство и т. д. Таким образом, основной причиной неэффективности электронного законодательства стало несоответствие принимаемых актов реальному уровню развития информационного общества.

Тем не менее резкий скачок информационных технологий за последние пять лет сдвинул процесс с мертвой точки. Сегодня мы наблюдаем в Азербайджане настоящий электронный бум: повышаются статистические показатели по электронной торговле, внедряются различные проекты в рамках строительства электронного правительства, на порядок улучшена информационная инфраструктура по всей стране. С нормативной точки зрения эффективность осуществляемых проектов подтверждается тем, что в большинстве случаев своевременно принимаются подзаконные акты, регламенты, положения соответствующих исполнительных органов, т. е. процесс идет не только на бумаге. На следующем этапе нормотворческая эстафета должна быть передана законодателю для соответствующей нормативно-правовой регламентации этих общественных отношений, что обусловливает целый ряд необходимых критериев, которым должна соответствовать должная правовая база: принятию законов должны предшествовать тщательные научно-правовые исследования; нужно унифицировать терминологическую базу во избежание противоречий и пробелов в законодательстве; принимаемые акты не должны быть политически ангажированы. Особое внимание в этом процессе следует уделить уголовно-правовой составляющей.

В 2010 г. Азербайджанская Республика ратифицировала с некоторыми оговорками Конвенцию о киберпреступлениях, а летом прошлого года в Уголовный кодекс страны были внесены соответствующие изменения. В частности, понятие «компьютерные преступления» было заменено понятием «киберпреступления» — именно так называется глава УК, посвященная преступлениям в сфере информационных технологий. Кроме того, законодатель предусмотрел ответственность за создание, распространение и использование детской порнографии, в том числе и в информационных сетях. Таким образом, появился целый ряд новых составов преступлений, за которые предусматривается уголовное наказание. Однако в то же время законодатель не объяснил само значение понятия «киберпреступление», которое стало неологизмом не только для юридического, но и для обыденного азербайджанского языка.

В целом проблема отсутствия должного разъяснения терминов, используемых в новых информационно- и электронно-правовых актах, является серьезным упущением в законодательной технике. С учетом того, что информационные технологии — одна из наиболее динамично развивающихся сфер общественной жизни, эволюция информационно-коммуникационных институтов происходит перманентно, а в масштабах истории — мгновенно. Это требует от нормотворца мобильности и гибкости, потому как вчерашнее ноу-хау завтра может выйти из моды и устареть. В большинстве стран постсоветского пространства законотворческий процесс несколько консервативен; это приводит к тому, что на данном этапе технологии опережают регламентирующую их использование правовую базу. И хотя на данном этапе причины кардинально противоположны, мы вновь становимся свидетелями неэффективности нормативной базы.

Одной из важнейших задач на данном этапе является нормативное закрепление используемой в информационно-коммуникационном пространстве терминологии

(например, «Интернет», «социальная сеть», «лайк» и т. д.). В обратном случае принятие некоторых правовых норм может оказать медвежью услугу для развития инфраструктуры либо создать условия для злоупотреблений. В частности, в мае 2014 г. в УК Азербайджанской Республики внесены изменения, которые устанавливают ответственность за распространение в Интернете заведомо ложных сведений, порочащих или унижающих честь и достоинство другого лица или подрывающих его репутацию.[8]

Принятие данной нормы нацелено прежде всего на обеспечение защиты прав граждан, однако в то же время в азербайджанском законодательстве нет нормативного определения понятия «Интернет». При широком толковании понятия «Интернет» это создаст ситуацию, когда под уголовную ответственность попадают действия, осуществленные как в электронных СМИ, публичных блогах, официальных сайтах, так и на частных страницах в социальных сетях, электронной почте, комментариях. Законодатель не разграничивает сегменты интернет-пространства на сферу личного и общественного пользования. Особенно много вопросов возникает в социальных сетях, где настройки конфиденциальности дифференцируют такие функции, как личная переписка, хроника, комментарии, кнопки «Нравится», «Рекомендую», — в каждом отдельном случае мотивы и степень публичности действий социальных пользователей разнятся.

Кроме того, в такой редакции под действие закона не попадает деятельность, осуществленная в корпоративных сетях, хотя и не подключенных к глобальной Сети, но тоже имеющих десятки, а порой сотни пользователей. Некоторые информационно-коммуникационные ресурсы носят закрытый характер. Например, согласно российскому законодательству среди принципов эксплуатации и развития государственной автоматизированной системы (ГАС) Российской Федерации «Выборы» предусмотрена недопустимость ее подключения при проведении выборов и референдума к иным информационным системам и сетям связи, не применяемым в ГАС «Выборы», в частности к информационно-телекоммуникационной сети «Интернет».[9] По этой причине целесообразно использовать понятие «информационно-коммуникационные сети» или же пойти еще дальше и использовать термин «киберпространство», дав ему четкое правовое определение. При этом не обязательно придумывать колесо заново, достаточно обратиться к опыту американского законодательства.

Так, развивая определение Верховного Суда США, киберпространство можно определить как особую публичную среду общественных отношений,[10] не находящуюся на определенной территории, но доступную каждому в любой точке мира через использование информационно-коммуникационных технических средств.[11]

Такое определение подчеркивает и уникальный правовой статус, и международно-правовой характер, и информационно-коммуникационную технологическую составляющую. Из истории развития информационно-коммуникационных

---

[8] *В Азербайджане* будут наказывать за оскорбления в Интернете // www.1news.az/society/20130514041549688.html (дата обращения: 09.12.2014).

[9] *Федеральный* закон от 10 января 2003 г. № 20-ФЗ «О государственной автоматизированной системе Российской Федерации "Выборы"» // СЗ РФ. 2003. № 2. Ст. 172.

[10] *Азизов Р. Ф.* Elaw.az / Введение в электронное право. Баку, 2008. С. 42.

[11] *Рассолов И. М.* Право и Интернет. 2-е изд., доп. М., 2009. С. 6.

технологий мы знаем, что Интернет — не первая и не единственная сеть, хотя и абсолютно доминирующая. Однако в случае существенных изменений в этом сегменте мировой экономики могут получить развитие иные сети, что приведет к несостоятельности нормативных актов, ориентированных исключительно на интернет-коммуникации.

Главное же, что следует учитывать при этом, — развитие законодательства должно быть комплексным, так как очевидно, что без соответствующих изменений в гражданском, административном законодательстве введение уголовно-правовых норм как средство защиты от киберпреступлений окажется неэффективным.[12] Так, если законодатель определяет уголовно-правовую ответственность за оскорбление либо клевету в Интернете, логичным будет предположить и необходимость такой ответственности за распространение экстремистских, террористических и любых других материалов, направленных против общества, человека и гражданина. Однако в действующей редакции азербайджанского УК такие составы не предусмотрены, и это является пробелом, поскольку количество такого рода материалов увеличивается с каждым днем.

Целый ряд иных видов киберпреступлений, таких как спаминг, кибersквотинг и др., до сих пор не являются ни уголовно, ни административно наказуемыми в Азербайджанской Республике. Спам, как известно, приносит многомиллиардные убытки, дискредитирует институт электронной почты, так как чрезмерно нагружает ее, усложняет работу.[13] Тем не менее действующая редакция ст. 6 Закона Азербайджанской Республики «Об электронной торговле» разрешает рассылку такого рода рекламных сообщений, разве что ограничивая ее коммерческими целями.[14] Но ведь спам в большинстве случаев и преследует коммерческие цели, правда, при этом в абсолютном большинстве стран не признается законным средством рекламы. Что касается кибersквотинга, т. е. незаконной регистрации доменных имен лицами, не обладающими исключительными правами на товарный знак, то здесь ситуация предельно проста. Понятие «домен» в азербайджанском законодательстве использовано лишь в одном техническом подзаконном акте, при этом не раскрывающем полностью его правовое содержание,[15] что не позволяет выявить правовой статус «доменов», регламентировать права и обязанности регистрантов и тем более обеспечить в административном или уголовном порядке защиту прав добросовестных правообладателей.

Таким образом, несмотря на серьезный прорыв Азербайджанской Республики в направлении совершенствования уголовного законодательства в сфере борьбы с киберпреступлениями, целый ряд вопросов остался вне поля правовой регламентации. Поэтому на данном этапе следует предпринять активные шаги в следующих направлениях:

---

[12] *Мамонов К. Л.* Компьютерные преступления. Некоторые проблемы криминализации // Вестник Санкт-Петербургского университета. Сер. 6. Философия. Политология. Социология. Психология. Право. Вып. 1. 1994. С. 102.

[13] *Азизов Р. Ф.* Elaw.az / Введение в электронное право. С. 82.

[14] *Закон* Азербайджанской Республики от 10 мая 2005 г. № 908-IIQ «Об электронной торговле».

[15] *Постановление* Кабинета Министров Азербайджанской Республики от 31 марта 2006 г. № 91 «О правилах администрирования доменов GOV.AZ» // http://e-qanun.az/framework/12015 (дата обращения: 29.01.2015).

1) организовать на национальном уровне постоянный контроль за ситуацией в тех сферах, где могут возникнуть угрозы роста киберпреступности, объединить усилия широкой общественности, профессионалов, ученых и представителей органов власти, делового мира для надежной защиты информационных ресурсов;

2) проводить активные проекты по укреплению международного сотрудничества, усовершенствованию модельного законодательства в этой сфере, формированию и развитию связей между органами, которые занимаются обеспечением информационной безопасности и устранением последствий таких угроз.

Бесспорно, эффективное международное сотрудничество в борьбе с киберпреступностью невозможно, если в законодательстве одной страны деяние считается преступлением, а в другой уголовной ответственности не предусмотрено. Отсутствие единообразия в национальном уголовном законодательстве стран может негативно отразиться на развитии методов эффективной борьбы с киберпреступностью — явлением, для которого не существует государственных границ.[16] Одна из ключевых проблем — проблема определения юрисдикции, которая предопределяется транснациональностью рассматриваемого явления. Очень сложно определить место совершения преступления, так как при кибератаках преступники могут находиться на удаленных расстояниях, при этом физическое нахождение преступника может не совпадать с его нахождением в сети, т. е. атака может совершаться с компьютеров и серверов в третьих странах. В этом случае важно быстродействие правоохранительных органов всех стран, так как даже одна страна может стать убежищем для кибертеррористов.

Высокой оценки заслуживают инициативы отдельных стран по налаживанию конкретных соглашений с другими странами. Например, по предложению Испании пять европейских государств решили объединиться в сообщество, в рамках которого они изучают, как террористы и преступники используют ресурсы Интернета: закрываются сайты, которые уличаются в нарушении действующего закона о терроризме, осуществляется обмен данными о подозреваемых, вовлеченных в террористическую деятельность, и террористических актах и взрывах.[17] Предполагается, что именно такие формы сотрудничества особенно перспективны в рамках деятельности региональных организаций (СНГ, ГУАМ, ЕврАзЭС).

Важно осознавать, что в информационной среде большая нагрузка падает на представителей частного сектора, зачастую под угрозой остаются именно частные компьютерные системы, базы данных. В то же время развитие систем информационной безопасности идет в большей степени именно за счет частного сектора. Поэтому продуктивно привлечение представителей негосударственного сектора к процессу разработки механизмов предотвращения и устранения киберпреступлений — и при разработке программных продуктов, и при обсуждении механизмов, и при создании норм права, регулирующих эти процессы. Информационное пространство будет эффективным только тогда, когда станет открытым для общества, дающим возможность согласованно реализовывать частные и публичные интересы граждан, общества и государства на комплексной и системной основе.[18]

---

[16] *Джансараева Р. Е., Аратулы К.* Борьба с киберпреступлениями. С. 98.

[17] *С миру* по байту // Вестник онлайн. 2005. 11 марта (доступно по: http://vestnik_old.ulsu.ru/issues/738/16/ (дата обращения: 09.12.2014)).

[18] *Пономарев Д. А.* Информационные технологии как криминогенный фактор...

Соответствующее нормотворчество в сфере борьбы с киберпреступностью в Азербайджанской Республике, равно как и в других странах постсоветского пространства, должно пойти по пути внедрения концепции правового сорегулирования, предполагающей сочетание механизмов публичного (государственного и международного) управления и социального самоуправления.[19]

Статья поступила в редакцию 17 сентября 2014 г.

[19] *Азизов Р. Ф.* Правовое регулирование: информационный аспект. Дис. ... к. ю. н. СПб., 2007. С. 159.