В европейских странах при рассмотрении конкретного дела в судах преюдициальный вопрос о конституционности применяемого акта может быть поставлен: 1) только стороной по делу (Франция); 2) любой стороной по делу или судом, рассматривающим данное дело (Италия, Испания, Бельгия, Германия, Румыния, Турция); 3) только судом (Албания). При этом стороной по делу может быть физическое лицо (граждане, иностранные граждане, лица без гражданства), юридическое лицо (государственное или частное). В большинстве европейских стран (в частности, в Германии, Италии, Испании) такой вопрос может быть поставлен перед любой судебной инстанцией.

В Республике Беларусь на сегодняшний день существует возможность опосредованного обращения граждан в Конституционный суд несколькими способами: через субъектов, имеющих право обращаться в Конституционный суд в соответствии со ст. 116 Конституции Республики Беларусь и посредством реализации ч. 2 ст. 112 Конституции Республики Беларусь. Вместе с тем механизм реализации опосредованного доступа граждан в Конституционный суд еще недостаточно разработан. Представляется важной детальная разработка механизма реализации ч. 2 ст. 112 Конституции Республики Беларусь, согласно которой, если при рассмотрении конкретного дела суд придет к выводу о несоответствии нормативного акта Конституции, он принимает решение в соответствии с Конституцией и ставит в установленном порядке вопрос о признании данного нормативного акта неконституционным. После вступления в законную силу судебного постановления суд ставит перед Верховным судом вопрос о внесении им предложения в Конституционный суд о признании данного нормативного акта неконституционным. Верховный суд обязан в месячный срок внести в Конституционный суд предложение о признании такого нормативного акта неконституционным. На практике подобных запросов было очень мало по причине недостаточной разработаннности механизма реализации такого права, хотя общие суды и адвокаты в процессе ставили вопросы о конституционности применяемых при рассмотрении дела актов. Таким образом, общие и экономические суды сами не могут напрямую обратиться в Конституционный суд с преюдициальным запросом о конституционности нормативного акта.

Данный механизм, в целом подобный классической европейской модели преюдициального запроса о конституционности, имеет ряд существенных отличий. Наиболее важное из них – принятие судом решения и только затем обращение в Конституционный суд. В данном случае имеет место сочетание признаков европейской модели возражения о неконституционности и классического варианта возражения о неконституционности (американской модели), поскольку суд, принимая решение в соответствии с Конституцией, по сути, осуществляет конституционный контроль. Таким образом, на основе анализа ч. 2 ст. 112 и ст. 116 Конституции можно сделать вывод о том, что конституционный контроль в Республике Беларусь осуществляет не только Конституционный суд, но и иные суды, что не в полной мере отвечает концепции европейской модели конституционного контроля и свидетельствует о наличии элементов смешанной модели конституционного контроля.

В связи с объединением высших судебных инстанций возникает ряд вопросов, связанных с реализацией гражданами права косвенного доступа к конституционному правосудию в Республике Беларусь. В частности, следует внести определенные коррективы в Кодекс о судоустройстве и статусе судей, касающиеся механизма реализации ч. 2 ст. 112 Конституции Республики Беларусь. В целях расширения доступа граждан к конституционному правосудию и последовательного развития белорусской модели конституционного правосудия в рамках европейской модели представляется перспективным скорректировать ч. 2 ст. 112 Конституции с целью уточнения механизма реализации преюдициального запроса о конституционности, предоставив такую возможность судам.

УДК 341.4

В.В. Меркушин

О НЕКОТОРЫХ АСПЕКТАХ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНЫМ ПРЕСТУПЛЕНИЯМ И ИНЫМ ОБЩЕСТВЕННО ОПАСНЫМ ДЕЯНИЯМ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Компьютерные преступления как разновидность преступлений в сфере высоких технологий – относительно новое в общественной жизни и юридической науке явление, представляющее достаточно существенный научный и практический интерес. Оной из основных причин этого, на наш взгляд, является значительное количество отраслей сферы высоких технологий: электроника, программное обеспечение, беспроводные технологии, робототехника, нанотехнологии, экологически чистые технологии, энергосбережение и альтернативная энергетика, системы безопасности, навигационные технологии, оборонные технологии и технологии двойного назначения, а также биотехнологии. Каждая из указанных отраслей может стать объектом, а в отдельных случаях средством преступных посягательств.

В современных условиях активно развивающегося научно-технического прогресса совершенствуются и развиваются общественно опасные деяния в сфере высоких технологий. Нередко они носят организованный транснациональный характер. Преступления в сфере высоких технологий – очень прибыльный и быстро развивающийся вид преступного бизнеса. Большинству людей он знаком по компьютерным вирусам, спаму в электронной почте, пиратским компьютерным программам, кино и музыке. По разным оценкам еще в 2008 г. компьютерные и иные преступления в сфере высоких технологий впервые в истории превысили по оборотам наркобизнес, став самым крупным видом нелегальной деятельности с ежегодным доходом от 150 млрд до 1 трлн долларов США. Кроме того, указанный вид преступности носит высоколатентный характер. Так, по данным российских ученых, в поле зрения правоохранительных органов попадает не более 10–15 % всех совершаемых компьютерных и иных преступлений в сфере высоких технологий. Достаточно много разновидностей компьютерных преступлений. Так, согласно кодификатору рабочей группы Интерпола, который был положен в основу автоматизированной информационно-поисковой системы, созданной в начале 90-х гг. XX в., их насчитывается порядка 33 наименований, среди которых, например, несанкционированный доступ и перехват, изменение компьютерных данных, компьютерное мошенничество, манипуляции с программами ввода-вывода, незаконное копирование, компьютерный саботаж, хищение информации, составляющей коммерческую тайну, и т. д.

Необходимо также констатировать отсутствие единый позиций ученых и практиков в установлении терминологически единого понятия данному виду преступности. Об этом свидетельствует использование в трудах ученых , национальных законодательствах и международных документах таких понятий, как «компьютерная преступность», «информационная преступность», High tech crime или Cyber crime, которые переводятся как «преступления в сфере высоких технологий» и «киберпреступления», и т. д.

На сегодняшний день проблема противодействия рассматриваемому виду преступности является объектом пристального внимания международных органов и учреждений в системе Организации Объединенных Наций, Интерпола, Европейского союза, Организации по безопасности и сотрудничеству в Европе, Содружества Независимых Государств, а также прочих универсальных и региональных международных организаций. Так, например, еще на 55-й сессии Генеральной Ассамблеи ООН в 2001 г. была принята резолюция «Борьба с преступным использованием информационных технологий», которая подчеркнула необходимость принятия таких мер по борьбе с преступным использованием информационных технологий, как противодействие «правовой гавани» для укрытия киберпреступников от наказания, обмен информацией, оснащение и обучение сотрудников правоохранительных органов, защита правовыми системами данных и компьютерных систем от несанкционированного вмешательства, своевременное обеспечение режимами взаимной помощи; расследование случаев преступного использования информационных технологий; предупреждение общественности о необходимости предупреждения преступного использования информационных технологий и борьбы с ним; техническая защита информации производителями программного обеспечения. Кроме того, немаловажное значение в сфере борьбы с компьютерными преступлениями отводится Конвенции ООН против транснациональной организованной преступности, принятой резолюцией Генеральной Ассамблеи № 55/25 от 15 ноября 2000 г. Необходимость применения положений данной конвенции, особенно в части криминализации определенных преступных деяний и решения практических вопросов сотрудничества правоохранительных органов в данной сфере, объясняется тем, что около 62 % компьютерных преступлений совершается в составе организованных групп, в том числе на территории нескольких стран.

Особый интерес вызывает Конвенция Совета Европы о киберпреступности, принятая в 2001 г. Она устанавливает стратегические направления противодействия киберпреступности: согласование национальных норм, определяющих составы преступлений; определение порядка расследования преступлений в мировых компьютерных сетях; создание оперативной и действенной системы международного сотрудничества в борьбе с киберпреступностью. Важность этого документа обусловливается возможностью практического сотрудничества правоохранительных органов заинтересованных государств в целях профилактики и противодействия киберпреступлениям. В настоящее время конвенция в силу не вступила, хотя и была ратифицирована такими государствами, как США, ЮАР, Канада, Мексика, Коста-Рика, Япония. География указанных государств свидетельствует больше об универсальном, чем региональном характере данной конвенции. Представляется, что увеличение числа ее участников могло бы заложить основу универсального организационно-правового механизма международного сотрудничества в борьбе с киберпреступностью и связанными с ней преступлениями.

В Европейском союзе с 2013 г. начал работу Центр по борьбе с киберпреступностью (European CyberCrime Centre (ECC)). Он стал координационным центром ЕС в борьбе с киберпреступностью. Страны – члены ЕС и европейские институты намерены поддерживать ECC для создания оперативных и аналитических возможностей расследования киберпреступлений и для сотрудничества с международными партнерами. Мандат деятельности Центра включает борьбу со следующими видами киберпреступности: преступления, совершенные организованными группами для получения преступных доходов, в частности онлайн-мошенничество; преступления, нанесшие серьезный вред жертве, в частности сексуальная эксплуатация детей; преступления, нанесшие вред критически важным инфраструктурным и информационным системам в ЕС.

В рамках СНГ наиболее важным является Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации 2001г., которое, в частности, устанавливает такие формы сотрудничества, как обмен информацией, исполнение запросов, управление в области противодействия компьютерной преступности, сотрудничество в области осуществления кадровой политики, создание информационных систем, взаимная научно-исследовательская кооперация и т. д

Республика Беларусь является участницей большинства международных соглашений (универсального и регионального характера), направленных на борьбу с преступностью, в том числе по общим вопросам и с компьютерной (Конвенция Совета Европы о киберпреступности Республикой Беларусь подписана не была). Отсутствие двусторонних соглашений в этой области можно объяснить их малой эффективностью, учитывая ярко выраженную транснациональность проблемы компьютерных преступлений и иных общественно опасных деяний в сфере высоких технологий.

УДК 343.97

С.И. Мукашев

ПРАВОВЫЕ ИНСТРУМЕНТЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В РАМКАХ СНГ

Широкое внедрение информационно-коммуникационных технологий (ИКТ) во всех областях жизнедеятельности человека оказывает положительное влияние на развитие экономики, политики, социальной сферы на национальном, региональном и универсальном уровнях.

Вся совокупность информационных отношений, связанных с функционированием ИКТ, определяется как кибернетическое пространство, где объектом права является информация, обрабатываемая с помощью ЭВМ и направляемая электронными средствами связи. За последние 10 лет количество пользователей интернета резко возросло. Международным союзом электросвязи был опубликован список государств мира (20 государств) с наибольшим количеством интернет-пользователей, куда вошла одна из стран – участниц СНГ – Российская Федерация, где этот показатель начиная с 2003 г. увеличился почти в 5,6 раза (68 млн человек, или 48 % всего населения этой страны).

Наличие огромного технического потенциала и неограниченные возможности для доступа к любой информации обусловливают возникновение киберпреступности, относящейся к разряду новых нестрановых угроз и вызовов. Так, на протяжении 1997–2005 гг. в Российской Федерации количество зарегистрированных преступлений в сфере телекоммуникации и компьютерной информации возросло более чем в 300 раз. В 2012 г. их рост составил 28,3 % по сравнению с 2011 г. Отчетливо прослеживается эта динамика на мировом уровне с учетом высокой латентности данного вида преступлений, носящих транснациональный характер.

В рамках ООН разработан ряд международных правовых инструментов в борьбе с киберпреступностью. Так, в 2002 г. Генеральной Ассамблеей ООН была принята резолюция 56/261, где содержатся План действий по осуществлению Венской декла-