

ление отстоять свой социальный статус, субъективно воспринимаемая угроза которому столь велика, что для его защиты хороши любые средства.

Субъективную предрасположенность женщин к занятию проституцией формирует десоматизация (от греч. soma – тело), суть которой состоит в отделении, отчуждении от личности женщины ее тела. Женщина не ощущает свое тело в качестве личностной ценности, бессознательно воспринимая его как нечто изолированное от нее, как предмет, которым можно распоряжаться по личному усмотрению для решения различных жизненных задач.

Алкоголизация и наркотизация активно способствуют занятию проституцией, с помощью которой можно получить необходимые средства для приобретения алкоголя и наркотиков.

По мнению современных исследователей, проституция, являясь самостоятельным негативным социальным явлением, становится причиной многих общественно опасных последствий, к которым относятся:

деградация личности, одним из проявлений которой нередко бывает преступное поведение (расширение масштабов проституции повышает преступность в целом, особенно женскую);

рост уровня смертности от алкоголизма, наркомании и суицидов, увеличение числа криминальных аборт, повышение риска заражения венерическими болезнями и ВИЧ-инфекцией;

нарушение моральных и этических норм, отрицание целомудрия;

угроза разрушения института семьи, отрицательное влияние на формирование нравственного здоровья подрастающего поколения;

падение престижа образования, труда и легальных заработков;

повышение уровня теневой занятости, сокрытие доходов, не облагаемых налогами;

незаконная миграция и нарушение правил пребывания иностранных граждан на территории различных государств.

Связь проституции с преступностью состоит в криминальном характере действий, сопутствующих проституции (сводничество и содержание притонов), в противоправном характере самой проституции, являющейся одной из детерминант преступности, а также в том, что образ жизни лиц, занимающихся проституцией, тесно связан с совершением преступлений (заражение ВИЧ, вовлечение несовершеннолетних в антиобщественную деятельность и т. д.). Кроме того, среда и образ жизни лиц, задействованных в индустрии сексуальных услуг, продуцируют преступность, связанную со сбытом наркотиков, укрывательством социально опасной деятельности, соучастием в кражах, грабежах и мошеннических действиях. Незаконный бизнес в сфере проституции сопряжен с криминальным рабством и торговлей людьми – похищением девушек и детей, пригодных для занятия проституцией, их дальнейшим содержанием в притонах.

Некоторые проститутки специализируются на хищении денег и других материальных ценностей у своих клиентов, часто используя снотворные препараты. В практике деятельности органов внутренних дел встречаются случаи применения физического или психического насилия, лишения документов, принуждения к оказанию интимных услуг жертв, оказавшихся в ловушке вследствие заманчивых предложений сняться в кино, получить высокооплачиваемую работу, выгодно выйти замуж. С развитием информационных технологий и расширением использования сети Интернет проституция прочно заняла виртуальный рынок сексуальных услуг.

Таким образом, специфика детерминации, причинности проституции обусловлена наличием целого ряда факторов социально-экономического, психологического и морально-этического характера. Рассмотренные факторы необходимо учитывать при решении задач повышения эффективности предупреждения проституции. Их устранение либо нейтрализация позволит в целом улучшить криминогенную обстановку.

УДК 343.53

*Ю.В. Харчейкина*

#### **НАРУШЕНИЕ ЦЕЛОСТНОСТИ И ДОСТУПНОСТИ КОМПЬЮТЕРНЫХ ДАННЫХ И СИСТЕМ: ФРАНЦУЗСКИЙ ОПЫТ УГОЛОВНО-ПРАВОВОЙ ОЦЕНКИ**

Информационное развитие общества, отдельных сфер деятельности, возникновение цифровой экономики и промышленного интернета стали причиной необходимости совершенствовать уголовно-правовую охрану общественных отношений в сфере обеспечения информационной безопасности. Для решения этой задачи, несомненно, оправданным является анализ законодательства и практики иностранных государств.

С точки зрения опыта построения составов преступлений против целостности и доступности компьютерных данных и систем внимание привлекает УК Франции, при разработке которого законодателем предпринята попытка максимально учесть нормы и принципы международного уголовного права, достижения юридической науки ведущих европейских государств. Из УК Франции можно взять конструктивные идеи и аргументы для национального законодательства по ряду проблемных вопросов.

Законодательное противодействие компьютерной преступности во Франции началось в конце 1980-х гг. Первым французским нормативным актом в этой сфере стал Закон от 5 января 1988 г. № 88-19 «Об информационном обмане». В целях защиты компьютерных систем от возможных злоупотреблений им были установлены санкции в отношении четырех отдельных категорий нарушений: вмешательство в работу системы автоматизированной обработки данных; мошенническое или неправомерное сохранение доступа; препятствование функционированию системы; мошенническое введение данных.

Положения Закона «Об информационном обмане» впоследствии были включены в действующий УК Франции, принятый в 1992 г. и вступивший в силу 1 марта 1994 г.

Нормы УК Франции защищают системы автоматизированной обработки данных и информационные данные как объекты собственности. Посягательства на системы автоматизированной обработки данных ввиду специфики предмета и способов противоправного воздействия отдельно выделены в гл. III разд. II «О прочих имущественных посягательствах» кн. III «Об имущественных преступлениях и проступках» УК Франции. К таким посягательствам отнесены: обманное получение или обманное сохранение доступа ко всей или части системы автоматизированной обработки данных (ст. 323-1); воспрепятствование работе или нарушение функционирования системы автоматизированной обработки данных (ст. 323-2); обманное введение информационных данных в систему автоматизированной обработки данных, а также обманное хранение, копирование, передача, изменение или уничтожение содержащихся в ней данных (ст. 323-3).

Кроме того, Законом от 21 июня 2004 г. № 2004-575 «О принципе доверия в цифровой экономике» названная глава УК Франции была дополнена ст. 323-3-1, предусматривающей ответственность за импорт, хранение, предложение, передачу или предоставление оборудования, инструмента, компьютерных программ или данных, разработанных или специально приспособленных для совершения деяний, предусмотренных ст. 323-1–323-3.

Анализ практического применения положений ст. 323-1 УК Франции в судебных решениях свидетельствует о том, что незаконное получение доступа предполагает наличие защищенной системы, а незаконное пребывание в системе не обязательно должно быть сопряжено с незаконным доступом к ней.

В решении от 30 октября 2002 г. по делу компании Tati Апелляционный суд Парижа указал, что пользователь не может быть обвинен в получении или сохранении доступа к данным веб-сайтов, который можно получить посредством простого использования общедоступного навигационного программного обеспечения (браузера). Информация, не являющаяся объектом какой-либо защиты со стороны оператора сайта или поставщика услуг, должна считаться неконфиденциальной, если не указано иное. Даже обращаясь к именованным данным, пользователь при описанных условиях не может сделать вывод, что они не публикуются с согласия заинтересованного лица, и поэтому не может рассматриваться как получающий или сохраняющий доступ незаконным путем.

Данные выводы были подтверждены в решении Палаты по уголовным делам Кассационного суда Франции от 20 мая 2015 г. № 14-81.336, в котором высшая французская судебная инстанция отметила, что сохранение доступа к системе автоматизированной обработки данных, полученного в результате технического сбоя, является преступлением в случаях, если лицо продолжает пребывать в ней после того, как обнаружило, что система защищена (имеет контроль доступа).

В ходе работы над УК Сенат Французской Республики предлагал определить систему автоматизированной обработки данных как любую систему, защищенную устройствами безопасности и состоящую из одного или нескольких блоков обработки данных, памяти, программного обеспечения, данных, органов ввода-вывода и каналов связи, которые способствуют выполнению определенной задачи. Однако в конечном итоге законодатель отказался от нормативного толкования данного термина. В результате, как отмечают французские исследователи, правоприменители широко трактуют это понятие, относя к системе автоматизированной обработки данных, в частности, жесткий диск, не подключенный к сети персональный компьютер, мобильный телефон, банковские платежные системы, веб-сайты.

Часть 2 ст. 323-1 УК Франции предусматривает более строгое наказание в случаях, когда незаконный доступ ко всей или части системы автоматизированной обработки данных либо незаконное пребывание в ней имеет определенные последствия – уничтожение или изменение данных, содержащихся в системе, ухудшение ее функционирования. Однако это касается только непреднамеренных последствий. Умышленное нарушение работы системы, уничтожение или изменение данных, содержащихся в системе, регулируются ст. 323-2 и 323-3 УК Франции. Такой подход в целом нашел отражение и в белорусском уголовном законе.

Под нарушением работы системы автоматизированной обработки данных во французской судебной практике понимается как необратимое блокирование системы автоматизированной обработки данных, так и временное нарушение работы системы или одной из ее составляющих подсистем.

Характерной тенденцией является постепенное повышение французским законодателем санкций за данные деяния. Первоначально с учетом постановления от 19 сентября 2000 г. № 2000-916 «Об изменении стоимости некоторых сумм, выраженных в законодательстве во франках, в евро» УК Франции предусматривал основные наказания в виде одного года тюремного заключения и штрафа в размере 15 тыс. евро по ст. 323-1, три года тюремного заключения и штраф в размере 45 тыс. евро – по ст. 323-2 и 323-3. В 2004 г. наказание по ч. 1 ст. 323-1 было увеличено до двух лет тюремного заключения и штрафа в размере 30 тыс. евро, а по ст. 323-2 и 323-3 – до пяти лет тюремного заключения и штрафа в размере 75 тыс. евро. Законом от 24 июля 2015 г. № 2015-912 за данные деяния, совершенные без отягчающих обстоятельств, установлена ответственность в виде тюремного заключения на срок два года и штрафа в размере 60 тыс. евро (ч. 1 ст. 323-1) и тюремного заключения на срок пять лет и штрафа в размере 150 тыс. евро (ч. 1 ст. 323-2, ч. 1 ст. 323-3).

В качестве квалифицирующего признака рассматриваемых преступлений, влекущих более строгое наказание, предусмотрено их совершение против государственной системы автоматизированной обработки персональных данных.

Таким образом, обращение к законодательному опыту Французской Республики показывает, что имеется определенное сходство его с отечественным уголовно-правовым регулированием информационной безопасности. В то же время изучение специфичности и своеобразия нормативных предписаний уголовного закона Франции, выявление их позитивных и негативных сторон предоставляют возможность предложить совершенствование уголовной ответственности за посягательства на целостность и доступность компьютерных данных и систем, внедряя в национальное законодательство с учетом его особенностей зарекомендовавшие себя положения зарубежного права.