УДК 349

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОСРЕДСТВОМ ОХРАНИТЕЛЬНЫХ НОРМ

Д. Г. Полещук

Белорусский государственный университет,
ул. Ленинградская 8, Минск, 220030, Беларусь

Становление информационного общества неразрывно связано с рисками совершения противоправной деятельности в цифровой среде, для предупреждения которой задействованы нормы административно-деликтного и уголовного права. В публикации раскрывается содержание актуальных направлений правового обеспечения информационной безопасности с использованием охранительных норм, рассматриваются текущее состояние, проблемы и перспективы совершенствования законодательства с учетом последних его изменений.

Ключевые слова: информационная безопасность; кибербезопасность; охранительные нормы; искусственный интеллект, персональные данные, фейки.

TOPICAL DIRECTIONS OF LEGAL SUPPORT OF INFORMATION SECURITY THROUGH PROTECTIVE NORMS

D.G. Poleshchuk

Belarusian State University,
8 Leningradskaya street, Minsk, 220030, Belarus

The formation of the information society is inextricably linked with the risks of illegal activities in the digital environment, for the prevention of which the norms of administrative-tort and criminal law are involved. The publication reveals the content of current trends in the legal support of information security through protective norms, discusses the current state, problems, and prospects for improving legislation, taking into account its latest developments.

Keywords: information security; cybersecurity; protective norms; artificial intelligence, personal data, fakes.

В современном обществе, характеризующемся масштабным процессом цифровизации, об информационной безопасности говорится немало. Новые цифровые технологии наряду с формированием условий для экономического роста и упрощением коммуникации создают значительные риски совершения противоправных действий в отношении личности, организаций и даже целых государств. Это отражается и в национальной Концепции

информационной безопасности Республики Беларусь, определяющей *информационную безопасность* как состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере [1].

В то же время информационная сфера достаточно широка, что позволяет говорить о различных общественных отношениях, подлежащих охране нормами Кодекса Республики Беларусь об административных правонарушениях (далее – КоАП) и Уголовного кодекса Республики Беларусь (далее – УК), не ограничиваясь лишь защитой цифровой информации и поддерживающей ее инфраструктуры. Как отмечает О.С. Макаров, проблема нормативного обеспечения информационной безопасности во многих государствах – участниках СНГ, включая и Беларусь, заключается в том, что в этой сфере не проводилась систематизация законодательства и нормы хаотично «размазаны» по разным сферам и отдельным нормативным правовым актам [2, с. 124].

В этой связи полагаем возможным выделить следующие аспекты правового обеспечения информационной безопасности с использованием охранительных норм:

кибербезопасность или компьютерная безопасность (ст. 23.4 КоАП, гл. 31 УК) и противодействие связанным с ними административным правонарушениям и преступлениям (ст. 11.1-11.2 КоАП, ст. 208, 209, 212, 216 УК);

защита информации, распространение и (или) предоставление которой ограничено законодательными актами (ст. 23.5-23.8 КоАП, ст. 177, 178, 203, 203^1, 203^2, 226^1, 254-255, 373-375, 375^1, 407-408 УК);

защита от информации негативного характера, в том числе от «фейков», деструктивного информационного воздействия (ст. 19.6-19.8, 19.10-19.12, ч. 4 и 5 ст. 23.5, ч. 1 ст. 24.26, КоАП, ст. 130, 130^1, 130^2, 198^1, 340, 341^1, 342^1, 343, 343^1, 361, 369^1 УК).

Как видим, «локомотивом» в формировании публичной ответственности за посягательства против информационной безопасности выступают уголовно-правовые нормы. До принятия в 2021 г. соответствующих изменений в раздел XII и гл. 31 УК [3], которые действовали еще с момента его принятия и ранее именовались «Преступления против информационной безопасности», для целей уголовного закона информационная безопасность фактически сужалась исключительно до компьютерной безопасности. Это стало предпосылкой изменения наименований данных структурных элементов УК («Преступления против компьютерной безопасности»).

Наряду с уточнением объекта данной группы преступлений под влиянием требований времени и на основе наработанной правоприменительной практики впервые произошел комплексный их пересмотр, включающий изменение порядка уголовного преследования (введено частное обвинение в

отношении близких лица), используемой терминологии, конструкций и признаков составов преступлений, а также их санкций. Так, введены специальные положения об уголовной ответственности за распространение вредоносных компьютерных программ (а не только носителей с ними) и их сбыт, имеющие место в сети Интернет.

Следует отметить, что компьютерная преступность в настоящее время все больше носит ярко выраженный транснациональный и сетевой характер, по сути вызывая объективную необходимость построения эффективной системы обеспечения международной кибербезопасности. Как минимум, на уровне охранительных норм для этого требуется взаимное согласование и совершенствование положений материального права государств, устанавливающего преступность и наказуемость деяний, посягающих на цифровую информацию, информационные (компьютерные) системы, сети и машинные носители.

Тем не менее, по результатам проведенных за последнее время корректировок отечественного охранительного законодательства, направленного в том числе на усиление кибербезопасности (компьютерной безопасности), в масштабах белорусской юрисдикции в определенной степени сохраняется и даже возник ряд проблемных вопросов, требующих своего осмысления на перспективу.

В частности, в числе таковых можно назвать:

гармонизацию норм охранительного законодательства Республики Беларусь и других государств в сфере кибербезопасности, особенно в рамках Евразийского экономического союза, СНГ и с учетом прошедших апробацию подходов Европейской конвенции о киберпреступности [4], соответствующих национальным интересам в информационной сфере (например, в Беларуси однозначно не решен вопрос об ответственности за незаконный оборот паролей, кодов доступа и иных аналогичных данных, существуют различия в признаках несанкционированного доступа к компьютерной информации);

определение оптимальной конструкции уголовного наказуемого *несанкционированного доступа к компьютерной информации* (принимая во внимание признаки иных составов преступлений гл. 31 УК и правонарушения в ст. 23.4 КоАП, на практике могут быть затруднения в оценке того, как последствия в виде существенного вреда могут находиться в причинно-следственной связи с фактом несанкционированного доступа к компьютерной информации (деяние фактически окончено при ознакомлении с информацией);

оценку необходимости применения мер ответственности за уничтожение, блокирование или модификацию компьютерной информации при отсутствии существенного вреда или наличии реальной угрозы его

наступления (это связано с трансформацией ранее действующей ст. 351 УК в материальный состав преступления (теперь ст. 350 УК), а также установлением в КоАП административной ответственности только за несанкционированный доступ к компьютерной информации);

единообразное использование квалифицирующих признаков в конструкциях всех составов преступлений против компьютерной безопасности (например, признак повторности не включен в ст. 354 УК);

определение эффективной санкции за совершение компьютерных правонарушений и преступлений (используемая санкция должна иметь реальный предупредительный эффект, поскольку во многих случаях виновные лица сознательно готовы претерпеть наказание в обмен на достижение цели противоправной деятельности);

предупреждение и профилактику мошенничества, совершаемого с использованием мобильных телефонов и мессенджеров («вишинга»), формирование цифровой грамотности всех слоев населения (учитывая совершение многих преступлений с использованием информационных технологий на территории различных государств, значительно проще и экономически выгоднее выработать комплекс мер по их профилактике (возможно и на межгосударственном уровне), чем затем их расследовать).

Обособленное место в контексте обеспечения кибербезопасности и информационной безопасности в целом занимает *проблема появления искусственного интеллекта и роботов в охранительных правоотношениях*.

Вероятно, иные аспекты информационной безопасности уже находятся под их воздействием (например, распространение фейковых новостей, анализ поведения человека посредством его личной информации, «больших данных» и др.). Значительное число правонарушений и преступлений фактически может быть совершено с использованием новых технологий, однако возникает вопрос о субъекте ответственности в таких случаях. В данном аспекте позволим себе согласиться с А.Л. Савенком, что пока не будут разработаны соответствующие правовые нормы, человек не может возлагать на технику (робота) ответственность за вред, причиненный в процессе ее функционирования, при этом вряд ли допустимо передавать искусственному интеллекту право на создание другого искусственного интеллекта [5 с. 9–10]. В силу непредсказуемости последствий, в том числе связанных с совершением незаконных действий с вредоносными компьютерными программами, персональными данными, различных компьютерных атак на критически важные объекты информатизации, автономия искусственного интеллекта может быть чрезвычайна опасна. Это обусловливает характер и степень публичной ответственности человека (пользователя, разработчика) за противоправную деятельность, вызванную использованием искусственного интеллекта или робота.

Информация подлежит защите не только в зависимости от ее формы, но и от содержания, в связи с чем КоАП и УК обеспечивают соблюдение правового режима информации, распространение и (или) предоставление которой ограничено законодательными актами (информация о частной жизни и персональные данные, охраняемые законом тайны, государственные секреты и др.). Актуальным направлением правового обеспечения информационной безопасности личности является формирование охранительных норм о защите персональных данных, без оборота которых уже невозможно представить отношения в цифровой среде. Данное направление получило широкую огласку в 2021 г. в результате принятия первого в республике Закона от 7 мая 2021 г. № 99-З «О защите персональных данных» (вступил в силу с 15 ноября 2021 г.), введения специальных статей об ответственности за незаконные действия с персональными данными – ст. 23.7 КоАП (с 1 марта 2021 г.), а при наличии существенного вреда правам, свободам и законным интересам гражданина или тяжких последствий – ст. 203^1 и 203^2 УК (с 19 июня 2021 г.). Правильное применение указанных охранительных норм требует знания особенностей нового законодательства (например, оно распространяет свое действие в основном на автоматизированную обработку персональных данных), а также разграничения с другими категориями информации ограниченного распространения, которые могут включать в себя персональные данные. Кроме того, по мере становления правоприменительной практики в рамках указанного аспекта обеспечения информационной безопасности усматриваются предпосылки для разрешения следующих вопросов:

разграничение ответственности за посягательства в отношении специальных персональных данных и персональных данных, которые к ним не относятся, что косвенно находит отражение в Классификации информационных ресурсов (систем), содержащих персональные данные, в целях определения предъявляемых к ним требований технической и криптографической защиты персональных данных, утвержденной приказом Национального центра защиты персональных данных от 15 ноября 2021 № 12 [6] (видится, что посягательства в отношении персональных данных, касающихся религиозных убеждений, здоровья или половой жизни, привлечения к административной или уголовной ответственности являются более общественно опасными, чем деяния в отношении фамилии, имени, отчества и даты рождения гражданина);

установление справедливой сопоставимой санкции за посягательства в отношении персональных данных и иных категорий информации ограниченного распространения (например, разглашение врачебной тайны, повлекшее тяжкие последствия, по своему характеру, видимо, должно

наказываться строже, чем распространение персональных данных любым лицом, повлекшее существенный вред).

Защита информационного пространства от информации негативного характера также является одним из стратегических направлений обеспечения информационной безопасности и сохранения информационного суверенитета. В условиях глобального использования сети Интернет особую актуальность на государственном уровне приобретает противодействие различного рода заведомо ложной информации или «фейкам» (от англ. fake – подделка, фальшивка) – не соответствующей действительности, вводящей в заблуждение информации, которая может причинить вред государственным или общественным интересам. Фактически, с учетом положений ст. 38 Закона от 17 июля 2008 г. № 427-З «О средствах массовой информации» такая информация, равно как и гиперссылки на нее, относятся к категории запрещенной.

В силу меняющейся геополитической обстановки защита от фейков как элемент информационной безопасности, в отличие от противодействия преступлениям против кибербезопасности, слабо поддается регулированию на межгосударственном уровне и даже наоборот становится ключевым средством ведения информационной войны.

Зачастую в обществе можно услышать тезис о том, что распространение фейков оправдывается конституционным правом на свободу выражения мнения (слова). Однако это не абсолютное право, поскольку законом допускается его ограничение в целях защиты государственных и общественных интересов, прав и свобод других лиц, что влечет уголовно-правовые и иные санкции и основано как на международных стандартах (п. 3 ст. 19 Международного пакта о гражданских и политических правах), так и на положениях Конституции Республики Беларусь (ст. 23).

Помимо возможности применения мер административного воздействия, предусмотренных законодательством о средствах массовой информации (например, ограничение доступа к интернет-ресурсам), национальное административно-деликтное и уголовное законодательство устанавливает определенный пласт норм, направленных на защиту от наиболее общественно опасных (вредных) фейков (ст. 19.6, ч. 4 и 5 ст. 23.5 КоАП, ст. 130^1, 130^2, 340, 369^1 УК и др.). Тем не менее, учитывая скорость распространения информации в цифровой среде, уже сейчас существуют предпосылки для оценки достаточности имеющихся на национальном уровне мер уголовной ответственности за распространение фейков, влекущих общественно опасные последствия, или создающих реальную угрозу их наступления (например, за доведение до неопределенного круга лица заведомо ложной информации, способствующей установлению социальной напряженности, информации, влекущей причинение вреда здоровью, крупного ущерба гражданам

и организациям, а также иной фейковой информации, фактически побуждающей к причинению лицом самому себе телесных повреждений).

На основании изложенного следует резюмировать, что правовое обеспечение информационной безопасности посредством охранительных норм за последнее время претерпело значительные изменения, отражает процессы всеобщей цифровизации, имеет предпосылки для совершенствования по направлениям усиления кибербезопасности и безопасности использования искусственного интеллекта, защиты информации ограниченного распространения, защиты от «фейков» и в перспективе призвано учитывать актуальные угрозы причинения вреда интересам личности, общества и государства в информационной сфере на национальном и международном уровнях.

Библиографический список

1. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Макаров, О. С. Системный взгляд на нормативное обеспечение информационной безопасности в Республике Беларусь / О. С. Макаров // Право и государство. – 2020. – № 8. – С. 124–129.

3. Об изменении кодексов по вопросам уголовной ответственности [Электронный ресурс] : Закон Респ. Беларусь, 26 мая 2021 г., № 112-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

4. Конвенция о преступности в сфере компьютерной информации [Электронный ресурс] : [заключена в г. Будапеште 23.11.2001 г.] // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2022.

5. Савенок, А. Л. Правовое регулирование применения технологий искусственного интеллекта / А. Л. Савенок // Право в современном белорусском обществе : сб. науч. тр. / Нац. центр законодательства и правовых исслед. Респ. Беларусь, редкол.: Н. А. Карпович (гл. ред.) [и др.]. – Минск : Колорград, 2021. – Вып. 16. – С. 4–10.

6. О классификации информационных ресурсов (систем) [Электронный ресурс] : приказ Нац. центра защиты перс. данных Респ. Беларусь, 15 нояб. 2021 г., № 12 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.