

своих прав в сфере получения информации, трудовой деятельности, общения и поддержания социальных связей. Вместе с тем полагаем, что при наличии альтернативных традиционных способов реализации указанных прав (бумажные почтовые отправления, проводная телефонная связь, оплата услуг наличными деньгами и т.п.) ограничение доступа к сети Интернет не повлечет умаления иных фундаментальных прав, а лишь исключит одну из форм их реализации.

Кроме того, рассматриваемое ограничение в качестве санкции должно быть обусловлено совершением лицом соответствующих общественно-опасных действий, при которых доступ в Интернет выступает средством и способом достижения противоправных целей (хищения с использованием компьютерной техники, мошенничество, сексуальные преступления, распространение экстремистской информации, призывов к насильственным действиям и т.п.).

Таким образом, данная мера будет выступать как адекватный способ защиты интересов общества и государства и недопущения совершения указанных действий лицом в будущем. Можно провести аналогию с уже существующим уголовным наказанием, связанным с лишением права заниматься определенной деятельностью, которое направлено на достижение похожих целей.

Список использованных источников

1. Ахмет Йилдырым (Ahmet Yildirim) против Турции» (жалоба N 3111/10) [Электронный ресурс]: Постановление Европейского Суда по правам человека от 18.12.2012 // КонсультантПлюс. Россия / ЗАО "Консультант Плюс". - М., 2022.
2. Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франка Ла Рю, 16.11.2011 [Электронный ресурс] : Управление Верховного комиссара ООН по делам беженцев. – Режим доступа: <https://www.refworld.org/cgi-bin/tehis/vtx/rwmain/opensslpdf.pdf?reldoc=y&docid=50f3db872>. – Дата доступа: 01.11.2022.
3. Руководство по правам человека для Интернет-пользователей: юридические инструменты [Электронный ресурс]: рекомендация CM/Rec (2014)6 принята Комитетом министров 16.04.2014. – Режим доступа: <https://rm.coe.int/guide-to-human-rights-for-internet-users-russian-/1680768065>. – Дата доступа: 01.11.2022.
4. Smith & Ors, R. v (Rev 1) [2011] EWCA Crim 1772 (19 July 2011) [Electronic resource]: British and Irish Legal Information Institute. – Mode of access: <https://www.bailii.org/ew/cases/EWCA/Crim/2011/1772.html>. – Date of access: 01.11.2022.

Скляр Владимир Константинович

ИСПОЛЬЗОВАНИЕ ОПЕРАТИВНО-РОЗЫСКОГО НАБЛЮДЕНИЯ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ ПО НАПРАВЛЕНИЮ ВЫЯВЛЕНИЯ И ПРЕСЕЧЕНИЯ КАНАЛОВ ФИНАНСИРОВАНИЯ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ

адъюнкт ГУО «Институт национальной безопасности Республики Беларусь»

Аннотация: Наблюдение издавна используется как один из эмпирических методов познания окружающего мира. В качестве оперативно-розыскного мероприятия государство рассматривает его как один из источников информации, необходимой для обеспечения национальной безопасности. В условиях развития современных информационных технологий изучение результатов оперативно-розыскного наблюдения при пресечении каналов финансирования экстремистской деятельности представляется актуальным.

Ключевые слова: оперативно-розыскная деятельность; оперативно-розыскное мероприятие; оперативно-розыскное наблюдение

Внедрение цифровых технологий происходит быстрее, чем внедрение любых других инновационных разработок в истории человечества: всего за два десятилетия цифровыми технологиями удалось охватить около 50 процентов населения развивающихся стран и преобразовать с их помощью общества. Использование технологий, способствующих расширению коммуникационных возможностей и доступа к финансовым, коммерческим и государственным услугам, может привести к значительному снижению уровня неравенства населения.

Социальные сети связывают почти половину населения планеты. Они позволяют людям высказывать свое мнение и общаться друг с другом из любой географической точки в режиме реального времени. Вместе с тем они могут также укоренять предрассудки и сеять рознь, становясь платформой для проявления ненависти и распространения дезинформации или рупором для пропаганды [1].

Происходящие изменения геополитической обстановки вокруг Республики Беларусь за последнее десятилетие особенно ярко показывают роль социальных сетей в предпринимаемых попытках по дестабилизации обстановки в обществе, а также совершения отдельных действий, направленных на свержение действующего конституционного строя.

Так, в 2011 году распространение получила серия гражданских акций протеста «Революция через социальную сеть», вызванных якобы недовольством части населения действиями руководства страны, приведшими к финансовому кризису, девальвации белорусского рубля и резкому скачку цен. Формальными организаторами акций протеста выступали инициативные группы молодых людей через социальные сети ВКонтакте и Facebook. С целью принятия мер реагирования на проходившие массовые «молчаливые акции» Парламентом Республики Беларусь были приняты соответствующие изменения в Закон «О массовых мероприятиях в Республике Беларусь».

Основная ставка политтехнологов, которые работали на формирование протестной активности в Беларуси в 2020 году, была сделана на Telegram-каналы и чаты. Фактически были использованы современные средства

массовой коммуникации, а именно — социальные сети, при этом организована попытка повторной реализации сценария 2011 года.

В результате проводимых органами правопорядка мероприятий, установлено, что представители различных зарубежных фондов активно используют социальные сети для сбора пожертвований на оплату штрафов лицам, задержанным за участие в несанкционированных массовых мероприятиях, оплату медицинской и психологической помощи, поддержку в переобучении.

Анализ имеющихся данных свидетельствует, что описанные выше механизмы финансирования целенаправленно использовались «донорами» в связи с трудностями их оперативного мониторинга их эффективного оперативного мониторинга и пресечения фискальными, правоохранными и иными контролирующими органами.

Дополнительным негативным аспектом являлось публичное освещение фактов оказания такой помощи и безнаказанности как плательщиков, так и получателей денег. В таких условиях применение административных мер (штрафов) к участникам деструктивных действий не имело должного профилактического эффекта, поскольку нивелировалось ожидаемой финансовой поддержкой и компенсацией понесенных расходов.

С целью оперативного реагирования на изменяющиеся условия осуществления финансирования деструктивной деятельности в 2021 году по инициативе правоохранных органов были внесены изменения в содержание ст. 361² «Финансирование экстремистской деятельности» Уголовного кодекса Республики Беларусь (далее – УК Республики Беларусь), которая в новой редакции стала предусматривать ответственность за финансирование экстремистской деятельности. В то время как ранее была предусмотрена ответственность только лишь за финансирование деятельности экстремистского формирования [2].

Таким образом, правоприменительная практика, а также легализованные материалы оперативно-розыскной деятельности (далее – ОРД) послужили основанием для установления ответственности финансирования деятельности экстремистской направленности.

Фактически в основную фазу противостояния протестной активности наиболее массовых Telegram-каналов и Internet-сообществ правоохранные органы столкнулись с отсутствием правовых оснований привлечения к ответственности лиц, осуществляющих финансирование подобной деятельности, поскольку соответствующие формирования официально на тот момент не были признаны экстремистскими, хотя по сути являлись таковыми.

Одновременно с этим, результаты ОРД позволили получить информацию об особенностях финансирования деятельности экстремистской направленности с использованием социальных сетей.

В частности, материалы процессингов совершаемых платежей, направляемых на финансирование конкретных получателей в лице экстремистских фондов и формирований, содержали в себе определенный

идентификатор, который позволил определить потенциальный круг лиц, действия которых содержали отдельные признаки состава преступления, предусмотренного ст. 361² УК Республики Беларусь.

Последующее документирование противоправной деятельности указанных лиц может осуществляться как самостоятельно уполномоченными лицами правоохранительных органов, так и с привлечением иных источников.

Складывающаяся практика деятельности органов правопорядка свидетельствует, что осуществляемая ОРД в выявлении финансирования экстремистской деятельности с использованием социальных сетей позволяет получить сведения:

- о реквизитах банковской платежной карты, привязанной к персональному аккаунту;
- об используемом способе совершения платежа;
- о целях и деталях проводимого сбора, что фактически позволяет сделать вывод о полной осведомленности «донора» в совершении им финансирования противоправной деятельности, а также указывает на умышленный характер совершаемых действий;
- о состоянии совершенной платежной операций в рамках сбора пожертвований.

Одновременно с этим, получены сведения, которые являются подтверждением использования указанного механизма финансирования не только для осуществления экстремистской деятельности внутри страны, но также для финансирования участия лиц на территории иностранного государства в вооруженном формировании или вооруженном конфликте, военных действиях.

В настоящее время правоохранительными органами осуществляется формирование правоприменительной практики привлечения к ответственности лиц, осуществляющих финансирование экстремистской деятельности.

Следует отметить, что своевременное совершенствование уголовно-процессуального законодательства формирует условия для эффективного решения задач по снижению протестной активности, имеет профилактический эффект, а также несет в себе функции правового просвещения граждан в условиях широкого распространения информационных технологий.

Список использованных источников

1. Выступление Генерального секретаря ООН на 74-й Генеральной Ассамблеи Организации Объединенных Наций - <https://www.un.org/ru/un75/impact-digital-technologies>
2. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Режим доступа: <http://www.pravo.by>. – Дата доступа: 12.10.2022.