

Секция «Уголовное право и криминология, уголовно-исполнительное право»

Перспективы нового обязательства о сообщении поставщиками цифровых услуг ЕС уголовных преступлений

Научный руководитель – Волеводз Александр Григорьевич

Ализаде Джамиль Эльдар оглы

Аспирант

Московский государственный институт международных отношений,
Международно-правовой факультет, Москва, Россия

E-mail: jamil.alizada@yandex.ru

На глобальном уровне наблюдается возрастающее стремление правительств к установлению «партнерства» с частным сектором с целью обеспечения общественной безопасности. Государственно-частное партнерство становится важной стратегией правоохранительных органов, особенно в борьбе с такими преступлениями, как отмывание денег, коррупция, терроризм и киберпреступность [3]. Частные лица призываются к партнерству из-за их владения информацией, необходимой для раскрытия преступных действий, которая зачастую недоступна государству.

Закон Европейского Союза о цифровых услугах (далее «DSA»), вступивший в силу 17 февраля 2024 года, пересматривает систему ответственности посреднических услуг в ЕС и вводит обязательство для поставщиков цифровых услуг сообщать о преступлениях. В частности, согласно статье 18 DSA, поставщики услуг хостинга, онлайн-платформы и поисковые сервисы обязаны информировать правоохранительные органы о преступлениях, представляющих угрозу жизни и безопасности.

Исторически, в правовых системах общего права, неинформирование правоохранительных органов об уголовных преступлениях не рассматривалось как нарушение закона [1]. Этот подход имел целью избежать общества, где граждане вынуждены шпионить друг за другом. Предполагалось, что обязательство о сообщении преступления должно быть сбалансированным с общественными интересами в преследовании конкретных преступлений. Подобные принципы также действовали и в континентальных правовых системах, которые не предусматривали санкций, за исключением определенных серьезных преступлений [2].

С распространением сети Интернет количество преступлений, совершаемых с использованием информационно-коммуникационных средств, значительно возросло. В ответ на это ныне принимаются законы, обязывающие поставщиков цифровых услуг сообщать о преступлениях правоохранительным органам.

Законы, требующие от частных лиц сообщать о преступлениях, должны соответствовать строгим принципам, включая ясность, пропорциональность и предсказуемость, чтобы граждане понимали, какие действия от них требуются, особенно если их невыполнение влечет наказание. При этом эти законы зачастую являются предметом споров. Во-первых, критикуется их широкий характер из-за нечетких определений преступлений и низких порогов для возникновения обязательства. Во-вторых, некоторые положения могут нарушать фундаментальные права, такие как свобода выражения мнения и неприкосновенность частной жизни. В-третьих, возникают вопросы об эффективности таких законов.

DSA пересматривает европейскую систему ответственности за «посреднические услуги». Согласно статье 18 DSA, поставщики услуг хостинга, онлайн-платформы и поисковые сервисы должны «незамедлительно информировать» правоохранительные органы, если

им «становится известна любая информация, дающая основание подозревать, что уголовное преступление, сопряженное с угрозой жизни или безопасности человека, имело место, имеет место или может произойти», и «предоставить всю имеющуюся соответствующую информацию».

Применение статьи 18 DSA на практике остается неопределенным. Во-первых, неясно, о каких преступлениях должны сообщать поставщики цифровых услуг. Очевидно, что традиционные преступления, такие как убийство или похищение, подпадают под это определение. Однако неясно, какие случаи онлайн-угроз или разжигания ненависти также подпадают под рассматриваемое требование. Представляется, что необходимо рассмотреть обязательство о сообщении преступлений в контексте права на свободу выражения мнения.

Поставщики цифровых услуг также должны предоставлять информацию, вызывающую «подозрения» в преступной деятельности. При этом закон не уточняет, какой уровень «подозрения» необходим. Низкий порог «подозрения» может привести к тому, что поставщики будут сообщать о потенциально невиновном контенте (журналистские или академические исследования).

Также возникает вопрос о моменте «осведомленности» поставщика цифровых услуг. Здесь можно провести аналогию с гражданской ответственностью за размещение незаконного контента по статье 6 DSA. Согласно этому правилу, поставщик может быть привлечен к ответственности только в том случае, если он действительно «знает» или «осведомлен» о конкретном незаконном контенте, потому что он не может владеть информацией обо всем контенте, размещаемом на его ресурсе. Поставщик может получить эту информацию в ходе собственного расследования, при этом его нельзя обязать проводить расследование. Аналогичным образом, то обстоятельство, что поставщик проводит добровольное расследование по собственной инициативе, не влечет за собой ответственность за незаконный контент, который он мог пропустить (так называемое правило «доброе самаритянина»). Таким образом, фактическая «осведомленность» возможна только посредством достаточно точных и обоснованных уведомлений, которые могут позволить добросовестному поставщику выявить незаконность контента без детальной юридической экспертизы. Нам представляется разумным применить этот подход и к «осведомленности» в контексте статьи 18 DSA. Наконец, DSA также охватывает правонарушения, которые «могут произойти», то есть планируемые или готовящиеся правонарушения. Однако неясно, на каких основаниях и по каким критериям поставщики цифровых услуг должны определить, что «правонарушение может произойти», что может привести к излишней осторожности с их стороны.

Нам представляется, что основным фактором, препятствующим эффективности нового обязательства, является его неясность. Учитывая, что различные элементы статьи 18 DSA открыты для толкования, существует риск неприменения этого положения на практике. К примеру, неясно, будет ли предоставленная поставщиками услуг информация достаточно полезной для обеспечения эффективного расследования и судебного преследования.

Таким образом, хотя статья 18 DSA базируется на ясных обоснованиях, таких как необходимость предотвращения угроз жизни и безопасности людей, перспективы ее применения остаются неоднозначными и требуют дополнительного разъяснения.

Источники и литература

- 1) Hall M., An emerging duty to report criminal conduct: banks, money laundering, and the Suspicious Activity Report. *Kentucky Law Journal* 1995/6, P. 743.
- 2) Kool R., Kool S., Kersters S., and van der Rijst T., Mind the (Knowledge) Gap: Towards a criminal duty to report child sexual abuse? *Utrecht Law Review* 2021/17, P. 33-45.

- 3) Tosza S., Internet service providers as law enforcers and adjudicators. A public role of private actors. *Computer Law & Security Review* 2021/43, P. 2.