УДК 343 **DOI: 10.34670/AR.2022.61.60.058**

Совершенствование законодательства и механизмы для эффективного противодействия киберпреступлениям

Гантамирова Залина Эмидиевна

Кандидат педагогических наук,
доцент кафедры отечественной истории,
Чеченский государственный университет им. А.А. Кадырова,
364093, Российская Федерация, Грозный, ул. Асланбека Шерипова, 32;
e-mail: Zalina.1712@mail.ru

Туркаева Лаура Вахитовна

Кандидат педагогических наук,
старший преподаватель,
Грозненский государственный нефтяной технический университет,
364024, Российская Федерация, Грозный, пр. Исаева, 100;
e-mail: turkaevalaura@mail.ru

Дакаев Абдал-Самад Адалхалимович

Студент,
Чеченский государственный педагогический университет,
364051, Российская Федерация, Грозный, пр. Исаева, 62;
e-mail: turkaevalaura@mail.ru

Аннотация

С быстрым развитием интернет-технологий растет число случаев кибермошенничества и других незаконных и преступных явлений. В статье рассматриваются такие вопросы как правовые пробелы в управлении кибертравли, трудности с юрисдикцией и предотвращение преступлений, связанных с кибермошенничеством и т.д. В связи с постоянно меняющейся тенденцией мира встает вопрос, что такое кибернасилие? В настоящее время нет четкого определения, и оно является более обобщенным с местной точки зрения. Например, разжигание ненависти, ложные новости, насильственные террористические высказывания и т.д. Считается, что в эпоху Интернета необходимо иметь четкое определение кибернасилия, но это определение должно быть динамичной, постоянно меняющейся и расширяющейся концепцией. Молодежь следует поощрять к свободному выражению своих взглядов и осуществлению своих прав в любых условиях, как онлайн, так и офлайн. Они должны иметь возможность выражать свои идеи и мнения, не нападая на тех, кто с ними не согласен, тем самым способствуя построению демократического международного общества. Построение действительно справедливого и равноправного мира требует культуры взаимного уважения и понимания. Связанный мир может быть достигнут только в том случае, если все люди будут придерживаться принципов общения. Для достижения этой цели нам еще предстоит пройти долгий путь.

Для цитирования в научных исследованиях

Гантамирова З.Э., Туркаева Л.В., Дакаев А.А. Совершенствование законодательства и механизмы для эффективного противодействия киберпреступлениям // Вопросы российского и международного права. 2022. Том 12. № 8А. С. 400-407. DOI: 10.34670/AR.2022.61.60.058

Ключевые слова

Кибернасилие, интернет, киберпреступность, юриспруденция, уголовная ответственность, судебный процесс, цифровая экономика.

Введение

«Кибернасилие» – это термин, используемый в Интернете, который обычно относится к незаконным и преступным действиям, таким как запугивание, клевета, преследование и домогательства, осуществляемые в Интернете. Кибернасилие – это новый тип незаконного и преступного явления, возникающий с развитием интернет-технологий. С появлением новых социальных инструментов, таких как Instagram (принадлежит корпорации Meta, признанной в РФ экстремистской), Twitter и коротких видеороликов, Интернет все чаще становится питательной средой для клеветы, запугивания и других видов насилия. Воздействие насилия на жертв развилось от модели сообщества до модели киберпространства, что также означает, что побочные эффекты насилия для жертв являются более обширными и продолжительными. С первых дней поиска человеческой плоти до недавней диффамации в Интернете, методы и виды кибернасилия постоянно меняются, что создает множество новых проблем для закона.

Интернет-идентичность – это относительно новая концепция, и поэтому не существует прецедента, на который можно было бы ссылаться в отношении того, как интегрировать технологии в нашу повседневную жизнь и как различать наши онлайн и офлайн-роли. Хотя Интернет является мощным инструментом, с помощью которого многие единомышленники или сообщества могут общаться друг с другом, он также часто служил платформой для очернения, преследования и оскорблений тех, кто выходит в Интернет, даже у себя дома.

Методика

Результаты показывают, что 7 из 10 молодых людей подвергались киберзапугиванию. Понятие «киберзапугивание» часто рассматривается как идиосинкразическое явление, но на самом деле оно является продолжением вековой проблемы буллинга.

Многочисленные опросы неизменно показывают, что примерно каждый второй молодой человек, который подвергается издевательствам, никогда не рассказывает другим об издевательствах из-за страха, смущения или неверия. Запугивание, как онлайн, так и офлайн, может серьезно повредить физическому и психическому здоровью молодых людей и привести к резкому увеличению дополнительного стресса.

Многие молодые люди ищут признания сверстников через социальные сети. Это нехорошая тенденция, так как самооценка и уверенность в себе человека становятся условными чертами, на которые большое влияние оказывают внешние взгляды. Это также делает молодежь уязвимой для риторики кибератак, основанной на внешнем виде, наводняя общество поверхностными культурными ценностями, которые ставят внешний вид на первое место.

Субкультура становится все более распространенной в Интернете: фотографии распространяются через онлайн-сообщества, и члены сообщества оценивают индекс привлекательности фотографий. Многие молодые люди готовы присоединиться к этим сообществам в надежде, что их харизма будет признана, что повысит их самооценку. К сожалению, эти сообщества часто наводнены сообщениями об издевательствах, знают они об этом или нет, и их внешний вид уязвим.

Интернет является уникальным источником издевательств. Например, пользователи сети съезжаются со всего мира, и географических ограничений в общении нет. Другими словами, люди могут подвергаться издевательствам за пределами их соответствующих офлайн-сообществ. Киберзапугивание часто наносит удар по достоинству человека, над которым издеваются публично, и подпитывается поведением участников онлайн-общения, которые любят, комментируют и делятся запугивающим контентом.

Основная часть

Иногда злоумышленники вообще не знают человека, над которым издеваются; во многих случаях сообщения о травле отправляются анонимно, что затрудняет выявление киберзапугивания. Без вмешательства руководящего органа очень сложно найти виновных в буллинге. Таким образом, анонимное издевательство может значительно подорвать доверие жертвы травли, уменьшить их чувство безопасности и сделать жертву паранойей и подозрительностью. Часто анонимная травля оказывает гораздо большее негативное влияние, чем травля со стороны знакомых.

Традиционное насилие — это уличное насилие, а кибернасилие означает, что насильственное поведение переносится из физического пространства в киберпространство, демонстрируя тем самым характеристики, отличные от уличного насилия. Во-первых, виновные в кибернасилии могут не иметь слишком большой субъективной вины, но вытекающее из этого ущемление законных интересов очень серьезно. Например, онлайн-распространители слухов действуют только из-за недовольства человеком, о котором ходят слухи, но из-за быстрого распространения сетевой информации широкий круг пользователей сети может знать клеветническую информацию или распространять слухи только для того, чтобы привлечь внимание пользователей сети.

Распространять слухи, приводило к серьезным последствиям, таким как самоубийство человека, о котором ходили слухи. Во-вторых, виновные в кибернасилии могут иметь многоуровневые отношения, такие как сложные отношения между производителями информации, распространителями, экспедиторами, вторичными экспедиторами, несколькими форвардерами и т.д. [Аносов, 2018].

Производители информации могут не распространять информацию. Коммуникатором из-за утечки информации, коммуникатор может вообще не знать человека, о котором ходят слухи, а экспедитор, второй экспедитор, множественный экспедитор и т.д. также могут быть вовлечены в процесс ретрансляции, что приводит к ответственности. В-третьих, это включает в себя обязательство пруденциальной проверки онлайн-платформ. Перед лицом очевидной клеветы, издевательств и другой информации о насилии в Интернете онлайн-платформы обязаны проводить проверку на «законность и соответствие» и своевременно удалять «незаконную и криминальную информацию».

Существуют различные виды кибернасилия, в том числе киберзапугивание, кибердиффамация, и киберпреследование. Если закон вмешается вовремя, он также может

сыграть хорошую направляющую роль. Кибернасилие как новый вид противоправного и преступного явления сопряжено с риском ущемления законных интересов и, естественно, имеет основание для наказания.

Закон также регулирует, что, например, диффамация в Интернете может быть причастна к преступлению диффамации в уголовном праве. Судебное толкование «двух верхов» при рассмотрении уголовных дел, таких как диффамация в информационных сетях, предусматривает, что если одна и та же клеветническая информация фактически нажимается, просматривается более 5000 раз или повторно публикуется более 500 раз с использованием информационной сети для клеветы. Во-вторых, признание клеветы преступлением частного обвинения и анонимность киберпространства заставят потерпевших столкнуться с трудностями в получении доказательств. Наконец, юридическая ответственность онлайн-платформ недостаточно ясна, что приводит к спорам и трудностям в применении закона [Степанова, Явчуновская, 2011].

За неоднократным запретом кибернасилия стоит проблема аномии, вызванная развитием интернет-технологий, то есть анонимность киберпространства, широкий спектр влияния и быстрота распространения, что приводит к дисбалансу и искажению вопросов онлайн-дискурса, а также частые случаи насилия в онлайн-дискурсе и других проблем аномии. Объективно говоря, в Интернете меняются и криминологические модели, такие как ссоры и провоцирование неприятностей, терроризм и т.д., а также возрастают риски ущемления законных интересов.

Некоторые ученые отмечают: «Речевая стратосфера в алгоритмическом обществе продолжает усиливать разделение речевых сообществ, а замкнутый процесс, с усложнением алгоритмов, образовался относительно маломасштабно «речевой анклав», что привело к усилению фрагментации речевого поля и утрате информационного разнообразия, тем самым увеличивая общественные риски и затрудняя принятие публичных решений» [Эффективное предупреждение преступности…, 2000].

Децентрализованное законодательство и централизованное законодательство являются двумя законодательными режимами борьбы с кибернасилием. Первый содержит положения о предотвращении кибернасилия и наказании, разбросанные по административному праву, уголовному праву и другим законам; эффективная связь между гражданской ответственностью, административной ответственностью и уголовной ответственностью [Барышева, 2016].

Теоретической основой законодательства о борьбе с кибернасилием является юриспруденция предметной области. Построение национальной законодательной системы противодействия кибернасилию является комплексным социально-системным проектом, для которого все более характерны пересеченность, интеграция, систематизация и динамика, поэтому приверженность проблемно-ориентированному подходу преследует не только системную целостность и самоорганизованность, но и требует своевременно реагировать на требования общества, чтобы разумно реагировать на кибернасилие. В краткосрочной перспективе необходимо изучить зарубежный опыт, соединить действующее законодательство нашей страны с потребностями противодействия кибернасилию, сформулировать ряд нормативно-правовых актов, усовершенствовать правовые положения о «антикибернасилии» в уголовном праве, уголовно-процессуальном праве, административном праве, экономическом праве и т.д. Полная правовая система для предотвращения и наказания кибернасилия.

В последние годы киберпреступность превратилась в раковую опухоль, которая влияет на развитие цифровой экономики РФ. Публичные данные показывают, что в 2020 году количество подозреваемых в киберпреступлениях, возбужденных органами прокуратуры по всей стране, увеличилось почти на 50% по сравнению с прошлым годом, а количество случаев онлайн-

мошенничества, азартных игр и других дел было многочисленным, что серьезно угрожало интересам людей и повлияли на общественный порядок. Уголовное право является первой отправной точкой для сдерживания высокого уровня киберпреступности, но сфера киберпреступности отличается от традиционной сферы, и споры о юрисдикции всегда были узким местом, влияющим на управление киберпреступностью.

Органы государственной власти и местного самоуправления подчас подвергаются еще большему воздействию киберпреступников, организующих шпионаж, хищение данных из государственных или частных стратегических информационных систем и препятствующих их нормальной работе [Галушкин, 2014].

Хотя в законодательстве РФ применяется модель центра судебной юрисдикции, важность юрисдикции по расследованию также должна быть подтверждена в судебной практике. Ключом к своевременному пресечению киберпреступности является то, что органы общественной безопасности могут выявлять случаи и арестовывать преступников. Киберпреступления в основном носят технический характер. Органы общественной безопасности в регионах с развитой интернет-отраслью обладают сильными возможностями для расследования больших данных. Судебная интерпретация «признание и юрисдикция в первую очередь» побуждает «способных людей работать больше, а сильных людей больше управлять». Для расширения подведомственности киберпреступлений, прежде всего, следует закрепить самостоятельный статус следственной подведомственности и играть ее процессуальную руководящую роль. Указанная юрисдикция также должна быть подтверждена в ходе разбирательства.

Заключение

Борьба с киберпреступностью требует как материального права, так и процессуального права. Разумное расширение юрисдикции способствует повышению энтузиазма судебных органов в борьбе с киберпреступностью. Пользуясь возможностью борьбы с киберпреступностью, наша страна должна постоянно реформировать свою юрисдикцию и вносить свой вклад в кибермощь. Интернет принес новые проблемы, и только постоянно обновляя систему уголовно-процессуального права, он может предложить решение для управления глобальным киберпространством.

Интернет разрушил исторические, социальные и экономические барьеры на пути человеческого общения, позволив людям общаться с кем угодно, включая друзей, семью, знаменитостей и мировых лидеров. В целом открытые каналы связи полезны для человеческого прогресса, поскольку они способствуют сотрудничеству и совместному обучению. Однако в современном обществе любой, кто пользуется социальными сетями, уязвим для киберзапугивания. Прозрачность и заразительность Интернета могут изменить темперамент человека и даже его долгосрочную судьбу за считанные секунды, независимо от того, кто он и какой жизненный опыт у него есть.

Каждый имеет право на гражданские свободы и право жить достойно, как и другие. Для этого нужно знать, что над людьми не издеваются из-за их расы, пола, религии или инвалидности. Основной причиной издевательств над кем-то является плохое отношение или плохая ситуация агрессора. Ключевым моментом здесь является то, что отношения и ситуации могут быть изменены с помощью соответствующей помощи и обучения, но идентичность людей не меняется и не затрагивается издевательствами, и никто не должен пытаться изменить свою идентичность.

Молодежь следует поощрять к свободному выражению своих взглядов и осуществлению

своих прав в любых условиях, как онлайн, так и офлайн. Они должны иметь возможность выражать свои идеи и мнения, не нападая на тех, кто с ними не согласен, тем самым способствуя построению демократического международного общества.

Построение действительно справедливого и равноправного мира требует культуры взаимного уважения и понимания. Связанный мир может быть достигнут только в том случае, если все люди будут придерживаться принципов общения. Для достижения этой цели нам еще предстоит пройти долгий путь.

Библиография

1. Аносов А.В. Специально-криминологическое предупреждение преступлений, совершаемых с использованием высоких технологий // Труды Академии управления МВД России. 2018. № 4 (48). С. 93-97.
2. Барышева К.А. Преследование как новый вид уголовно-наказуемого деяния // Пробелы в российском законодательстве. 2016. № 8. С. 178-182.
3. Галушкин А.А. К вопросу о кибертерроризме и киберпреступности // Вестник РУДН. Серия: Юридические науки. 2014. № 2. С. 44-49.
4. Елагина А.С. Подходы к совершенствованию международного уголовного права // Вопросы российского и международного права. 2018. Том 8. № 10А. С. 96-101.
5. Елагина А.С. Интерпретация трендов уровня преступности: нормальные и шоковые изменения // Вопросы российского и международного права. 2018. Том 8. № 11А. С. 144-152.
6. Елагина А.С. Доктринальные основания прав личности в международном праве: поиск новой парадигмы // Вопросы российского и международного права. 2018. Том 8. № 9А. С. 282-287.
7. Степанова И.Б., Явчуновская Т.М. Подросток и насилие: проблемы и факты // Криминологический журнал Байкальского государственного университета экономики и права. 2011. № 4. С. 50-55.
8. Эффективное предупреждение преступности: в ногу с новейшими достижениями // Материалы Десятого Конгресса Организации Объединенных Наций по предупреждению киберпреступности и обращению с правонарушителями. 2000. URL: A_CONF.187_4_Rev.3-RU.pdf
9. Al-Khater W. A. et al. Comprehensive review of cybercrime detection techniques //IEEE Access. – 2020. – Т. 8. – С. 137293-137311.
10. Bossler A. M., Berenblum T. Introduction: new directions in cybercrime research //Journal of Crime and Justice. – 2019. – Т. 42. – №. 5. – С. 495-499.

Improvement of legislation and mechanisms for effective counteraction to cybercrime

Zalina E. Gantamirova

PhD in Pedagogy,
Associate Professor of the Department of National History,
Chechen State University,
364049, 32, Sheripova str., Grozny, Russian Federation;
e-mail: Zalina.1712@mail.ru

Laura V. Turkaeva

PhD in Pedagogy, Senior Lecturer,
Grozny State Oil Technical University,
364024, 100, Isaeva ave., Grozny, Russian Federation;
e-mail: turkaevalaura@mail.ru

Abdal-Samad A. Dakaev

Graduate Student,
Chechen State Pedagogical University,
364068, 62, Isaeva ave., Grozny, Russian Federation;
e-mail: turkaevalaura@mail.ru

Abstract

With the rapid development of Internet technology, the incidence of cyber fraud and other illegal and criminal phenomena is on the rise. The article deals with issues such as legal gaps in the management of cyberbullying, difficulties with jurisdiction and prevention of crimes related to cyberfraud, etc. With the ever-changing trend of the world, the question arises, what is cyberviolence? Currently there is no clear definition and it is more generalized from a local point of view. For example, hate speech, false news, violent terrorist speech, etc. It is believed that in the age of the Internet it is necessary to have a clear definition of cyberviolence, but this definition must be a dynamic, ever-changing and expanding concept. Young people should be encouraged to freely express their views and exercise their rights in all settings, both online and offline. They should be able to express their ideas and opinions without attacking those who disagree with them, thereby contributing to the building of a democratic international society. Building a truly just and equal world requires a culture of mutual respect and understanding. A connected world can only be achieved if all people adhere to the principles of communication. To achieve this goal, we still have a long way to go.

For citation

Gantamirova Z.E., Turkaeva L.V., Dakaev A.A. (2022) Sovershenstvovanie zakonodatel'stva i mekhanizmy dlya effektivnogo protivodeistviya kiberprestupleniyam [Improvement of legislation and mechanisms for effective counteraction to cybercrime]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 12 (8A), pp. 400-407. DOI: 10.34670/AR.2022.61.60.058

Keywords

Cybercrime, Internet, jurisprudence, criminal liability, judicial process, digital economy.

References

1. Anosov A.V. (2018) Spetsial'no-kriminologicheskoe preduprezhdenie prestuplenii, sovershaemykh s ispol'zovaniem vysokikh tekhnologii [Special-criminological prevention of crimes committed with the use of high technologies]. *Trudy Akademii upravleniya MVD Rossii* [Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia], 4 (48), pp. 93-97.
2. Barysheva K.A. (2016) Presledovanie kak novyi vid ugolovno-nakazuemogo deyaniya [Stalkering as a new type of criminal offense]. *Probely v rossiiskom zakonodatel'stve* [Gaps in Russian legislation], 8, pp. 178-182.
3. Elagina A.S. (2018) Podkhody k sovershenstvovaniyu mezhdunarodnogo ugolovnogo prava [Approaches to the improvement of international criminal law]. Voprosy rossiiskogo i mezhdunarodnogo prava [Matters of Russian and International Law], 8 (10A), pp. 96-101.
4. Elagina A.S. (2018) Interpretatsiya trendov urovnya prestupnosti: normal'nye i shokovye izmeneniya [Interpretation of crime trends: normal and shock changes]. Voprosy rossiiskogo i mezhdunarodnogo prava [Matters of Russian and International Law], 8 (11A), pp. 144-152.
5. Elagina A.S. (2018) Doktrinal'nyye osnovaniya prav lichnosti v mezhdunarodnom prave: poisk novoy paradigmy [Doctrinal foundations of individual rights in international law: the search for a new paradigm].Voprosy rossiiskogo i

mezhdunarodnogo prava [Matters of Russian and International Law], 8 (9A), pp. 282-287.
6. (2000) Effektivnoe preduprezhdenie prestupnosti: v nogu s noveishimi dostizheniyami [Effective crime prevention: keeping up with the latest developments]. In: *Materialy Desyatogo Kongressa Organizatsii Ob"edinennykh Natsii po preduprezhdeniyu kiberprestupnosti i obrashcheniyu s pravonarushitelyami* [Proceedings of the Tenth United Nations Congress on the Prevention of Cybercrime and the Treatment of Offenders]. Available at: A_CONF.187_4_Rev.3-RU.pdf [Accessed 08/08/2022]
7. Galushkin A.A. (2014) K voprosu o kiberterrorizme i kiberprestupnosti [On the issue of cyberterrorism and cybercrime]. *Vestnik RUDN. Seriya: Yuridicheskie nauki* [PFUR Herald. Series: Legal Science], 2, pp. 44-49.
8. Stepanova I.B., Yavchunovskaya T.M. (2011) Podrostok i nasilie: problemy i fakty [A teenager and violence: problems and facts]. *Kriminologicheskii zhurnal Baikal'skogo gosudarstvennogo universiteta ekonomiki i prava* [Criminological journal of the Baikal State University of Economics and Law], 4, pp. 50-55.
9. Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. IEEE Access, 8, 137293-137311.
10. Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. Journal of Crime and Justice, 42(5), 495-499.