DOI: 10.18372/2307-9061.58.15320
УДК 343.436(045)

В. В. Филинович,
кандидат юридических наук
ORCID ID: https://orcid.org/0000-0001-8824-615X

КИБЕРСТАЛКИНГ: ПРОБЛЕМЫ ПРАВОВОЙ ЗАЩИТЫ

Национальный авиационный университет
проспект Любомира Гузара, 1, 03680, Киев, Украина
E-mail: vvfilinovich@gmail.com

Цель: *исследовать особенности и сущность кибersталкинга как преступления в киберсреде, указать на правовые возможности защиты жертв такого преступления.* ***Методы исследования:*** *исследование было проведено с применением общепризнанных методов научного познания, таких как: аналитический, сравнительно-правовой, системно-структурный и другие.* ***Результаты:*** *исследовано понятие, сущность, характеристики кибersталкинга и связанных с ним категорий, указано на проблемы защиты пользователей Сети в связи с указанным преступлением, даны рекомендации по преодолению рассматриваемой проблемы.* ***Обсуждение:*** *дискуссия в статье затрагивает аспекты поиска путей решения проблемы кибersталкинга, необходимости улучшения и дополнения действующего отечественного законодательства, его гармонизации с международными стандартами.*

Ключевые слова: *кибersталкинг; киберпреследование; киберпреступление; кибербезопасность, права человека в Интернете*.

Постановка проблемы и ее актуальность. Сегодня мы уже не представляем нашей жизни без интернета. Мы общаемся в мессенджерах, делаем покупки в онлайн-шопах, заказываем еду, даже управляем своей домашней бытовой техникой при помощи мобильного телефона, будучи вне дома. Организации же ведут бизнес, проводят аккаунтинг и подобные процедуры также при помощи Всемирной Сети. Даже наши власти используют так называемый e-government. Таким образом, интернет – он повсюду, во всех сферах нашего существования.

Именно это и привело к тому, что множество преступлений, как против государства в целом, так и против отдельных групп и даже конкретных личностей, совершаются онлайн с использованием компьютеров и прочих устройств («гаджетов»). Мошенничество и подлог, подмена личности, утечка персональных данных, хакинг, спамминг, харрасмент – это лишь малая толика тех киберпроблем, с которыми многие из нас сталкиваются ежедневно. Особенно активизировались в последнее время так называемые кибersталкеры, чья деятельность нередко приводит к ужасным последствиям.

Цель данной статьи – исследовать особенности и сущность кибersталкинга как преступления в киберсреде, указать на правовые возможности защиты жертв такого преступления.

Изложение основного материала. Киберпреследование (кибersталкинг) – это относительно новое явление, именно поэтому до сих пор нет единого определения данного понятия, которое было приятным и для правоохранительных органов, и для средств массовой информации. Поэтому прежде стоит ознакомиться с наиболее частоупоребимыми терминами.

Так, кибersталкинг, согласно Оксфордскому словарю, – это повторяющееся использование электронных устройств связи для преследования или запугивания кого-либо, например, путем отправки писем с угрозами по электронной почте.

Схожее понимание кибersталкинга и в среде ИТ-технологий, так Д. Балабан под киберпреследованием понимает преследование, которое осуществляется через онлайн-каналы (например, социальные сети, форумы или электронную почту) и может приобретать множество различных форм, а также поддерживается в течение определенного временного отрезка [1].

Согласно мнению С. Сымановича, киберпреследование или онлайн-преследование – это неоднократное использование Интернета или других электронных средств с целью преследования или запугивания человека или группы. Общие характеристики данного понятия включают в себя ложные обвинения или публикацию оскорбительных заявлений, мониторинг чьей-либо онлайн-активности или физического местоположения, угрозы, кражу личных данных, уничтожение данных или манипуляции с ними путем отправки вируса на устройства жертвы [7].

Если откинуть частицу «кибер», то можно отметить, что сталкинг, то есть преследование – это повторяющийся нежелательный контакт, который приносит беспокойство человеку, угрожает ему, вызывая у него страх. При этом речь не идет о конкретном физическом контакте, но нередко сталкинг приводит к физическому насилию, так как сталкер стремится сохранить чувство власти и контроля, в т.ч. посредством домашнего насилия [9].

Таким образом, можно говорить о том, что действия, именуемые кибersталкингом, включают в себя запугивание, домогательства, ложные обвинения, клевету, отслеживание жертвы и подобные акты, совершаемые при помощи гаджетов, подключенных ко Всемирной Сети.

Как сталкерами (преследователями), так и непосредственными жертвами такого правонарушения могут быть субъекты любого возраста, пола, цвета кожи, с любым уровнем образования, профессиональной и социально-экономической принадлежностью, вероисповеданием [4]. Сталкер может быть абсолютно незнаком жертве, либо наоборот, нередко такие правонарушители действуют онлайн на условиях анонимности и привлекают к участию в преследовании других субъектов, неизвестных жертве.

Статистика в отношении кибersталкинга довольно пугающая. Так, например, в США ежегодно около 1 миллиона женщин и 370 тысяч мужчин становятся его жертвами. При этом, по мнению А.А. Мур, каждая 12-я женщина и каждый 45-й мужчина будут подвергаться сталкингу на протяжении всей своей жизни. В среднем же продолжительность преследования составляет около 2-х лет, либо больше, когда сталкером выступает интимный партнер [3].

Согласно данным из отчета за 2020 Ditch the Label, всемирно известной благотворительной организации по вопросам противодействия кибербуллингу, онлайн-издевательства («кибербуллинг») проявляются на 25% чаще по сравнению с предыдущим годом. Указанный документ зиждется на опросе, проведенном среди 13387 британских подростков в возрасте 12-18 лет. Согласно ему, за 2020 год 26% респондентов стали свидетелями буллинга и кибербуллинга, 25% – стали жертвами, еще 3% – сами совершали подобные издевательства над другими людьми [8, с. 6].

А.А. Мур указывает на то, что жертвами киберпреследований, в основном, становятся девушки в возрасте 18-29 лет. При этом исследовательница ссылается и на данные Университета Рутгерса и Университета Пенсильвании, согласно которым 45% сталкеров – это женщины, а 56% – мужчины. Хотя общенациональная статистика по Соединенным штатам говорит о том, что сталкеров-мужчин куда больше, а именно около 87% [3].

И если со всемирно признанными сверхгосударствами вроде США дела в этом направлении обстоят относительно хорошо (так, например, большинство штатов имеют локальные законы в отношении противодействия кибербуллингу и кибersталкингу), то что же с остальной частью мира? К сожалению, многие жители постсоветских просторов уверены, что киберпреследования не так уж и опасны, ведь чаще всего касаются обидных высказываний и подобных «разговорных» действий, а не действий реальных, «физических».

Но это огромное заблуждение! Ведь онлайн-домогательства довольно часто перерастают в преследование в реальной «оффлайн» жизни. И жертвами такого сталкинга, уже без приставки «кибер» в большинстве случаев становятся женщины. И если «обзывания» в Сети кому-то кажутся проблемой, высосанной из пальца, то как тогда быть с жертвами откровенной травли, изнасилований и даже убийств, которые также начинались как онлайн-сталкинг и буллинг?! Именно поэтому вопрос кибersталкинга и борьбы с ним действительно серьезный.

Отметим, что наиболее распространенной формой киберпреследования считается рассылка так называемых «писем ненависти» или непристойных и-мейлов с угрозами. Помимо этого кибersталкеры нередко вторгаются в различные онлайн-обсуждения, чаты, группы, где и распространяют злонамеренную информацию. Рассылка компьютерных вирусов – особо сложная форма кибersталкинга и далеко не единственная. Все они опасны тем, что в любой момент могут перерасти в преследование в реальной жизни (например, в форме звонков с угрозами, актов вандализма против собственности жертвы и даже физических нападений [4].

Кибersталкинг, он же «межличностный терроризм», по определению Б.Х. Шпитцберга и Г. Хублера, нередко сопровождается преследованием в реальном времени или офлайн, т.е. в реальной жизни [6, с. 68].

Как же понять, что имеет место киберпреследование, и пора обращаться в соответствующие органы? Как указывает П. Босидж, указанному правонарушению сопутствуют (вместе или по-отдельности): злой умысел, повторяющиеся злонамеренные действия, реакция жертвы в виде страдания, персональная направленность, преследование цели отомстить без реальных на то причин, игнорирование предупреждений о необходимости прекратить злонамеренные действия [2, с. 9-10].

К сожалению, в большинстве случаев жертвы кибersталкинга не сообщают об инцидентах в правоохранительные органы. Этому есть две основные причины: пострадавший не уверен, что имеет дело с реальным преступлением, а также опасается несерьезного отношения к своей проблеме со стороны соответствующих органов [4]. Указанное в равной мере применимо и к Украине, где отсутствует действующий механизм и коррелирующие ему нормы в отношении реакции на рассматриваемое правонарушение. Также наши правоохранительные органы недостаточно квалифицированы, не могут вовремя распознавать серьезность киберпреследования или провести адекватное расследование инцидента.

В некоторых странах такое деяние считается уголовно наказуемым. Так, например, в штате Калифорния, США, интернет-преследование карается в соответствии с нормативно-правовым регулированием о преследовании, клевете и подобном. Сталкер, уличенный в содеянном, получит судебный запрет либо будет наказан иным способом вплоть до тюремного заключения [5]. Вообще в Соединенных Штатах практически каждый штат имеет свой закон, регулирующий вопросы киберпреследования и киберзапугивания.

Что касается законодательства других стран, то, например, в Австралии с 1999 года действует Закон о преследовании, в т.ч. предусматривающий сталкинг с использованием любых технологий. На Филиппинах М. Вильяр, в поддержку законодательства, внес на рассмотрение сената проект резолюции № 164 о росте числа случаев киберпреследований, вследствие чего сенатские комитеты обязали провести расследование в целях принятия серии НПА, направленных на пресечение киберпреследования и других киберпреступлений, а также защиту онлайн-пользователей в стране.

Уголовный кодекс Польши еще в 2011 году признал преследование, равно как и киберпреследование, уголовным преступлением. В Великобритании действует Закон 1997 года о защите от преследований, а Закон о защите свобод 2012 года гарантирует гражданам защиту от киберпреследований. В Испании жертва абсолютно легально, и при этом анонимно, может обратиться с информацией о киберпреступлении в четыре службы безопасности: Grupo de Delitos Telemáticos, Brigada de Investigación Tecnológica, Mossos d'Esquadra и Ertzaintza.

В Законе о наказаниях Эстонии предусмотрена уголовная ответственность за назойливое преследование в виде повторных (последовательных) попыток коммуникации с другим лицом, слежки за ним, либо вмешательства в его личную жизнь против воли жертвы и подобные действия с целью запугивания, унижения, незаконного сбора информации. Таким образом, благодаря столь широкому формулированию понятия преследования можно говорить и о наказуемости кибersталкинга [10].

Также уголовную ответственность за кибersталкинг предусмотрели пакистанский Закон 2007 года о предотвращении электронных преступлений и нигерийский Закон 2015 года о киберпреступности, а сингапурский НПА 2014 года в отношении защиты от домогательств запрещает кибер-харрасмент (т.е. домогательство).

А как дела обстоят дела с противодействием проблеме кибersталкинга в Украине? Главным Законом государства является Конституция, с нее и начнем. Так, ее статья 32 прямо указывает на то, что вмешательство в личную и семейную жизнь человека запрещено. Исключение составляют законодательно предусмотренные случаи и только с учетом интересов национальной безопасности, прав человека и экономического благосостояния [13].

Статья 182 Уголовного кодекса нашей страны посвящена нарушениям неприкосновенности частной жизни человека. Так, согласно ее пункту 1, для того, кто нелегально собирает, сберегает, использует, удаляет, распространяет конфиденциальную информацию о других лицах, предусмотрены такие виды наказания как штраф (500-1000 необлагаемых минимумов доходов граждан), исправительные работы (от 2-х лет), арест (до полугода) либо ограничение свободы (до 3-х лет). При повторном правонарушении того же толка штраф не предусмотрен, но возможны арест, ограничение либо лишение свободы [14].

Предмет преступления в данном случае – конфиденциальная информация о субъекте, то есть данные о частной жизни человека, а именно о его семейном положении, религиозной принадлежности, имущественном положении и образовании, его состоянии здоровья, а также дате и месте появления на свет, прочие сведения. Согласно комментарию к УК, частную жизнь составляет сфера жизнедеятельности отдельно взятого лица, в т.ч. его с другими людьми, приватные активности, отношения в семье – все, что касается его образа жизни. При этом информация, которую ранее опубликовали в средствах массовой информации или иным способом, не считается, согласно нашему законодательству, конфиденциальной [11].

Нарушающих ваши права кибersталкеров можно было бы попытаться также привлечь к ответу за клевету, если бы не проблема ее декриминализации. Так, до 2001 года, пока действовал УК 1960 года, за распространение неправдивых домыслов, порочащих честь другого человека, была предусмотрена уголовная ответственность. Но УК 2001 года исключил из своего содержания данный вопрос на основании признания клеветы личным неимущественным правовым нарушением, относящимся к ведению гражданско-правовой сферы.

Также стоит отметить, что Конституция Украины в статье 3 провозгласила честь и достоинства каждого из нас высшей социальной ценностью, а в статье 28 указала на право каждого человека на уважение его достоинства. Таким образом, если своими сталкерскими действиями виновник нарушает указанное право, мы должны обращаться в суд с иском о защите чести и достоинства. Такое нам гарантирует статья 23 Гражданского кодекса Украины [15]. Но стоит учесть, что нужна хорошая доказательная база наличия соответствующих действий, ведь нарушитель не признает своей вины. Что в данном случае можно использовать в качестве доказательств: показания свидетелей; аудио- и видеозаписи, порочащие честь и достоинство личности; фотокопии веб-страниц («скриншоты»), где обидчик оскорблял жертву, угрожал ей и т.п.

Обратите внимание еще и на то, что сталкерские действия, даже без физического контакта, могут нанести вред здоровью жертвы. И та, вследствие стресса, сильных переживаний теряет способность, желание нормально жить и трудиться. В таком случае пострадавший должен

немедленно обратиться в медицинское учреждение, чтобы получить справку, которая и подтвердит указанное состояние. Позже на основании такого документа жертва сможет в суде потребовать от обидчика возмещения материального и морального ущерба, в т.ч. траты на лечение, медикаменты и прочее.

Европейская конвенция по правам человека вступила в силу для Украины 11 сентября 1997 года, и согласно ее ст. 8 у каждого из нас есть право на уважение нашей личной, семейной жизни, жилища и корреспонденции, вмешательство извне запрещено, иначе как в интересах нацбезопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других лиц [12]. Таким образом, личная информация не должна разглашаться без согласия на то человека, в соответствии с его справедливыми ожиданиями, что подтверждено решением по делу Flinkkilä and Others v. Finland; Saaristo and Others v. Finland – оба 2010 года). К указанному типу данных относятся, в т.ч., полное имя человека (подтверждено решением по делу Kurier Zeitungsverlag und Druckerei GmbH v. Austria, 2012), адрес его проживания (подтверждено решением по делу Alkaya v. Turkey, 2012). Таким образом, публикация личных и идентифицирующих данных интернет-пользователя является прямым нарушением вышеупомянутой статьи 8 ЕКПЧ.

Выводы. К сожалению, в Украине вопрос правовой защиты жертв сталкинга, а тем более кибersталкинга, не урегулирован абсолютно. Можно говорить о том, что сегодня пользователи Сети в основном становятся жертвами онлайн-унижений (как одной из составляющих кибербуллинга, куда входит и кибersталкинг). Но, как сами жертвы, так и невольные свидетели подобного обычно игнорируют подобное, считая феномен слишком распространенным и, что главное, практически не наказуемым. Также нередки случаи кибersталкинга в чистом виде, с физическими угрозами и сексуальными домогательствами (как в цифровой, так и в оффлайн-среде).

По данным статистики, именно женщины, в особенности молодые девушки, чаще всего подвергаются кибersталкингу. И отсутствие достаточного нормативного регулирования проблемы, а также средств защиты – все это помогает сталкерам, т.е. реальным преступникам, оставаться безнаказанными.

Идеальным решением, по нашему мнению, стало бы инкорпорирование некоторых норм законодательства США, в частности, штата Калифорнии, которые уже показали свою действенность в отношении субъектов, склонных к цифровому преследованию. Так, если сталкеров (кибersталкеров) начнут штрафовать и отправлять в тюрьму, это точно приведет к повышению их уровня осведомленности, а, значит, к понижению уровня случаев кибersталкинга. Только конкретные виды наказания, и только «ежовые рукавицы» – иначе никак.

Литература

1. Balaban D. What Cyberstalking Is and How to Prevent It. *The State of Security*. 2018. URL: https://www.tripwire.com/state-of-security/ security-awareness/what-cyberstalking-prevent/.

2. Bocij P. Cyberstalking: Harassment in the Internet Age and How to Protect Your. New York: Praeger, 2004. 288 p. Pp. 9-10.

3. Moore A.A. Cyberstalking and Women. *ThoughtCo*. 2019. URL: https://www.thoughtco. com/cyberstalking-and-women-facts-3534322.

4. Pettinari D. Cyberstalking investigation and prevention. *Computer Crime Research Center*. 2002. URL: https://www.crime-research.org/ library/ Cyberstalking.htm.

5. Smith K. Tougher California laws protect victims of digital harassment. *San Gabriel Valley Tribune*. 2016. URL: https://www.sgvtribune.com/ 2016/02/09/ tougher-california-laws-protect-victims-of-digital-harassment/.

6. Spitzberg B.H., Hoobler G. Cyberstalking and the technologies of interpersonal terrorism. *New media & society*. 2002. P. 67-88. https://doi.org/ 10.1177/ 14614440222226271

7. Symanovich S. Cyberstalking: Help protect yourself against cyberstalking. *NortonLifeLock*. 2019. URL: https://us.norton.com/internetsecurity-

how-to-how-to-protect-yourself-from-cyberstal kers.html.

8. The Annual Bullying Survey 2020 / S. Bauman, L. Hacket, H. Everet, G. Bailey. UK: DitchtheLabel, 2020. 38 p.

9. Violence & domestic abuse – Stalking. *The Women's Center*. 2010. URL: https://web.archive.org/web/20131213210301/http://www.thewomenscenter.org/content.asp?contentid=555.

10. Андерсоне Д.А. Киберпреследование – разновидность преступных деяний в сфере защиты персональных данных: II-га Міжнар. наук.-практ. конф. ІТ-право: проблеми і перспективи розвитку в Україні. 2017. URL: http://aphd.ua/publication-348/.

11. Коментар до статті 182. Порушення недоторканності приватного життя / Коментар до Кримінального кодексу – Юридичні послуги Online. 2020. URL: http://yurist-online.com/ukr/uslugi/yuristam/kodeks/024/179.php.

12. Конвенція про захист прав людини і основоположних свобод: Рада Європи; Конвенція, Міжнародний документ від 04 лист. 1950 р.

13. Конституція України від 28 чер. 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

14. Кримінальний кодекс України від 05 квіт. 2001 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25-26. Ст. 131.

15. Цивільний кодекс України від 16 січ. 2003 р. № 435-IV. *Відомості Верховної Ради України*. 2003. №№ 40-44. Ст. 356.

References

1. Balaban D. What Cyberstalking Is and How to Prevent It. *The State of Security*. 2018. URL: https://www.tripwire.com/state-of-security/ security-awareness/what-cyberstalking-prevent/.

2. Bocij P. Cyberstalking: Harassment in the Internet Age and How to Protect Your. New York: Praeger, 2004. 288 p. Pp. 9-10.

3. Moore A.A. Cyberstalking and Women. *ThoughtCo*. 2019. URL: https://www.thoughtco.com/cyberstalking-and-women-facts-3534322.

4. Pettinari D. Cyberstalking investigation and prevention. *Computer Crime Research Center*. 2002. URL: https://www.crime-research.org/ library/ Cyberstalking.htm.

5. Smith K. Tougher California laws protect victims of digital harassment. *San Gabriel Valley Tribune*. 2016. URL: https://www.sgvtribune.com/2016/02/09/tougher-california-laws-protect-victims-of-digital-harassment/.

6. Spitzberg B.H., Hoobler G. Cyberstalking and the technologies of interpersonal terrorism. *New media & society*. 2002. P. 67-88.

7. Symanovich S. Cyberstalking: Help protect yourself against cyberstalking. *NortonLifeLock*. 2019. URL: https://us.norton.com/internetsecurity-how-to-how-to-protect-yourself-from-cyberstalkers.html.

8. The Annual Bullying Survey 2020 / S. Bauman, L. Hacket, H. Everet, G. Bailey. UK: DitchtheLabel, 2020. 38 p.

9. Violence & domestic abuse – Stalking. *The Women's Center*. 2010. URL: https://web.archive.org/web/20131213210301/http://www.thewomenscenter.org/content.asp?contentid=555.

10. Andersone D.A. Kiberpresledovanie – raznovidnost' prestupnyh dejanij v sfere zashhity personal'nyh dannyh: II-ga Mizhnar. nauk.-prakt. konf. IT-pravo: problemy i perspektyvy rozvytku v Ukraini. 2017. URL: http://aphd.ua/publication-348/.

11. Komentar do statti 182. Porushennja nedotorkannosti pryvatnogo zhyttja / Komentar do Kryminal'nogo kodeksu – Jurydychni poslugy Online. 2020. URL: http://yurist-online. com/ukr/uslugi/yuristam/kodeks/024/179.php.

12. Konvencija pro zahyst prav ljudyny i osnovopolozhnyh svobod: Rada Jevropy; Konvencija, Mizhnarodnyj dokument vid 04 lyst. 1950 r.

13. Konstytucija Ukrai'ny vid 28 cher. 1996 r. № 254k/96-VR. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 1996. № 30. St. 141.

14. Kryminal'nyj kodeks Ukrai'ny vid 05 kvit. 2001 r. № 2341-III. *Vidomosti Verhovnoi' Rady* Ukrai'ny. 2001. № 25-26. St. 131.

15. Cyvil'nyj kodeks Ukrai'ny vid 16 sich. 2003 r. № 435-IV. *Vidomosti Verhovnoi' Rady Ukrai'ny*. 2003. №№ 40-44. St. 356.

V. Filinovych

CYBERSTALKING: PROBLEMS OF LEGAL PROTECTION

National Aviation University
Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine
E-mail: vvfilinovich@gmail.com

Purpose: *to investigate the features and essence of cyberstalking as a crime in the cyber environment, to point out the legal possibilities of protecting victims of such a crime.* ***Research methods:*** *the research was carried out using generally recognized methods of scientific knowledge, such as: analytical, comparative legal, systemic and structural and others.* ***Results:*** *the concept, essence, characteristics of cyberstalking and related categories were investigated, the problems of protecting Internet users in connection with this crime were indicated, recommendations were given to overcome the problem under consideration.* ***Discussion:*** *the discussion in the article touches upon the aspects of finding ways to solve the problem of cyberstalking, the need to improve and supplement the current domestic legislation, its harmonization with international standards.*

Today, many crimes, both against the state as a whole, and against individual groups and even specific individuals, are committed online using computers and other devices (also known as «gadgets»). Fraud and forgery, identity substitution, personal data leakage, hacking, spamming, harassment - these are just a few of the cyber problems that many of us face on a daily basis. The so-called cyberstalkers, whose activities often lead to dire consequences, have become especially active in recent years. We can say that the actions called cyberstalking include intimidation, harassment, false accusations, defamation, victim tracking and similar acts committed using gadgets connected to the World Wide Web.

Many residents of the post-Soviet expanses are sure that cyber-harassment is not so dangerous, because most often it concerns offensive statements and similar «conversational» actions, rather than real, «physical» actions. But this is a huge misconception, because online harassment quite often turns into harassment in real «offline» life. And in most cases women become victims of such stalking. It is very important to know how this issue is settled in Ukraine, what legal norms can help each of us protect ourselves if cyberstalking affects us or our loved ones.

Keywords: *cyberstalking; cyberbullying; cybercrime; cybersecurity, human rights on the Internet.*