Научная статья
УДК 34:004:340.1.721:004.8
EDN: https://elibrary.ru/bvlgsu
DOI: https://doi.org/10.21202/jdtl.2025.19

Техноэтические и правовые аспекты киберзапугивания: структурный анализ дисбаланса сил в цифровой среде

Фотиос Спайропулос

Университет Филипс, Никосия, Кипр
Юридическая компания Spyropoulos Law Firm

Ключевые слова

алгоритмическая прозрачность,
искусственный интеллект,
киберзапугивание,
международное сотрудничество,
право,
технологическая грамотность,
цифровая безопасность,
цифровые платформы,
цифровые технологии,
этика

Аннотация

Цель: исследование направлено на концептуализацию понятия киберзапугивания с точки зрения права, техноэтики и анализ дисбаланса сил в цифровом пространстве как основополагающего фактора причинения вреда в Сети.

Методы: в работе применяется концептуально-аналитическая методология, базирующаяся на междисциплинарном анализе теоретических положений права, техноэтики, философии технологий и социальной психологии. Методологический инструментарий дополнен построением оригинальных концептуальных моделей на основе анализа структурных факторов цифрового пространства, разработкой схем причинно-следственных связей и созданием таксономии форм киберзапугивания. Особое внимание уделено компаративному анализу регулятивных подходов различных юрисдикций и выявлению пробелов в существующих правовых нормах.

Результаты: установлено, что киберзапугивание представляет собой сложный многоуровневый феномен, возникающий на пересечении архитектурных особенностей цифровых платформ, асимметрии технологических компетенций между участниками интеракций и системной фрагментированности законодательного регулирования. Выявлены критические пробелы в ключевых международных правовых инструментах, проявляющиеся в отсутствии унифицированных определений киберзапугивания, недостаточной проработке механизмов трансграничного сотрудничества и нерелевантном учете специфики цифровой среды. Проанализированы фундаментальные этические вопросы, связанные с автоматизированной модерацией контента на основе алгоритмов машинного обучения, проблематикой распределения ответственности между платформами, государственными регуляторами и индивидуальными пользователями, а также противоречиями между обеспечением безопасности и сохранением пользовательской автономии. Выделены четыре основных типа дисбаланса сил: технологический, информационный, социальный и институциональный, каждый из которых требует специфических стратегий преодоления.

Научная новизна: впервые предложен комплексный подход к анализу киберзапугивания как структурно обусловленного злоупотребления цифровой властью через призму техноэтики. Разработанные концептуальные модели представляют новые инструменты для понимания распределенной природы ответственности в цифровой экосистеме и формирования этически обоснованных стратегий профилактики. Введена концепция неправомерного использования информации как центрального механизма систематического злоупотребления властью в цифровой среде.

Практическая значимость: результаты исследования адресованы ученым-правоведам, государственным деятелям и разработчикам цифровых платформ, предлагая практические решения в области этического аудита алгоритмов, создания гибридных систем модерации с участием искусственного интеллекта и человека, формирования международных целевых групп и развития, основанных на правах человека принципов цифровой грамотности. Предложения автора направлены на создание более безопасной, подотчетной и инклюзивной цифровой среды для всех участников.

Для цитирования

Спайропулос, Ф. (2025). Техноэтические и правовые аспекты киберзапугивания: структурный анализ дисбаланса сил в цифровой среде. *Journal of Digital Technologies and Law*, *3*(3), 472–496. https://doi.org/10.21202/jdtl.2025.19

Содержание

Введение

Хотя явление киберзапугивания и становится все более распространенным, оно не имеет общепринятого определения как в Европе, так и на международном уровне (Smith et al., 2013). По данным ЮНИСЕФ, киберзапугивание определяется как «травля

с использованием цифровых технологий»[1]. Аналогичным образом, Европейская комиссия описывает это явление как «неоднократное словесное или психологическое преследование, осуществляемое отдельным лицом или группой лиц, использующих цифровые платформы для распространения вредоносного контента, такого как оскорбительные сообщения или непристойные фотографии, с целью ущемить или унизить жертву»[2].

Организация Объединенных Наций определяет киберзапугивание как форму насилия в Сети, характеризующуюся такими свойствами, как дисбаланс сил, анонимность и широкий охват. В отличие от традиционной травли даже одиночное вредоносное действие в Интернете может считаться актом киберзапугивания, поскольку цифровой контент отличается продолжительностью и широким распространением[3]. Это динамическое, еще развивающееся определение отражает уникальные риски, связанные с цифровыми платформами, включая постоянную доступность и возможность тиражирования вредоносных материалов, которые усугубляют уязвимость жертвы (Langos, 2012; Menesini et al., 2012; Slonje & Smith, 2008).

Научные определения часто опираются на традиционную концепцию травли, предложенную в работе Olweus (1993). Они подчеркивают такие свойства, как использование цифровых инструментов, намерение причинить вред и повторяющиеся действия (Englander et al., 2017; Mouzaki, 2010; Juvonen & Gross, 2008). Центральное место в киберзапугивании занимают использование агрессором технологических преимуществ, тогда как у жертвы может не быть средств для самозащиты, а также анонимность и публичность, обеспечиваемые цифровыми платформами (Kowalski, 2018; Smith et al., 2008; Nocentini et al., 2010; Hinduja & Patchin, 2006). Метафорическое определение Li (2007) – «новая бутылка, но старое вино» – говорит о том, что киберзапугивание повторяет традиционную травлю, в то же время используя отличительные черты цифровых технологий.

Искусственный интеллект (далее – ИИ) вносит дополнительные сложности в эту ситуацию, выступая как инструментом борьбы с киберзапугиванием, так и потенциальной проблемой. Системы на базе ИИ все чаще используются для обнаружения вредоносного контента, служат посредниками при взаимодействии и помогают предотвратить распространение оскорбительных материалов. Однако эти системы часто сталкиваются с ограничениями, такими как трудности в понимании контекста, культурных нюансов или в различении вредоносных намерений от сатиры или критики. Кроме того, агрессоры начали использовать инструменты искусственного интеллекта, такие как дипфейки или автоматизированные боты, для усиления вреда, манипулирования контентом или более широкомасштабных атак. Эти разработки подчеркивают необходимость создания надежных, прозрачных и этичных систем искусственного интеллекта для эффективного противодействия киберзапугиванию (Hasan et al., 2023; Raj et al., 2022).

Психологические и социальные последствия киберзапугивания, особенно среди детей и подростков, значительны – от проблем с психическим здоровьем до разрушенных

1 UNICEF, n.d. Cyberbullying: What is it and how to stop it. https://clck.ru/3NQaBe

2 European Commission. (2009). Safer Internet Programme: Protecting children online. https://clck.ru/3NQaRi

3 United Nations. (2016). Ending the Torment: Tackling Bullying from Schoolyard to Cyberspace. https://clck.ru/3NQaWz; United Nations. (2016). Convention on the Rights of the Child: General Comment No. 20 (2016) on the Implementation of the Rights of the Child during Adolescence (CRC/C/GC/20). https://clck.ru/3NQaZ3

отношений (Campbell & Bauman, 2018). Кроме того, опасность этого явления усугубляется за счет таких форм поведения, как несанкционированное распространение откровенных изображений («секстинг») и др. (Katerelos et al., 2011; Chakraborty et al., 2021).

Эффективной борьбе с киберзапугиванием в глобальном масштабе по-прежнему препятствует отсутствие общепринятого определения этого явления. Устранение этого пробела требует комплексных подходов, включающих образовательные кампании, программы повышения цифровой грамотности, ужесточение правовых норм и международное сотрудничество. При разработке мер, направленных на создание более безопасного и справедливого цифрового пространства, важно признать уникальность явления киберзапугивания, в том числе растущую роль искусственного интеллекта в его развитии.

1. Неправомерное использование информации как систематическое злоупотребление властью при киберзапугивании

Отличительной чертой киберзапугивания, представляющего собой систематическое злоупотребление властью, является неправомерное использование информации в цифровой среде. В этих условиях агрессор использует технологические инструменты для манипулирования, контроля и причинения вреда, извлекая выгоду из уникальных возможностей Интернета. В отличие от традиционных форм травли цифровая сфера позволяет преступникам преодолевать физические границы, использовать масштабируемость онлайн-платформ, анонимность и неуничтожимость цифрового контента для усиления своих действий (Courakis, 2005; Lazos, 2001; Furnell, 2006).

Центральное место в этом явлении занимает расширенная модель дисбаланса сил (рис. 1), которая позволяет понять динамику распределения сил при цифровой травле. Модель выделяет ключевые факторы, способствующие причинению вреда, включая способность агрессора манипулировать информацией, использовать анонимность и охватывать широкую аудиторию. Эти элементы не только расширяют возможности агрессора, но и усиливают уязвимость жертв, оказывая устойчивое и всеобъемлющее воздействие.

Ключевым дополнением к этой модели является концепция неправомерного использования информации, которая включает в себя такие действия, как несанкционированный доступ, манипулирование или распространение частного контента. Киберагрессоры часто используют информацию в качестве оружия, чтобы подорвать психологическое благополучие своих жертв и их социальный статус. В качестве примеров можно привести публикацию конфиденциальных фотографий, создание поддельных профилей или распространение клеветнических материалов. Эти действия иллюстрируют, как цифровая среда изменяет традиционную динамику сил, позволяя агрессорам утверждать свое превосходство и избегать ответственности (Spyropoulos, 2011; Katerelos et al., 2011).

Систематическое неправомерное использование информации еще более усугубляется различиями в технических знаниях и знакомстве с технологиями. Агрессоры часто обладают продвинутыми навыками, которые позволяют им использовать цифровые инструменты с большей точностью, в то время как жертвы, особенно если они имеют ограниченную цифровую грамотность, не в состоянии эффективно реагировать. Этот пробел в знаниях усугубляет дисбаланс сил, заставляя жертв чувствовать себя изолированной и бесправной (Vandebosch & Van Cleemput, 2008; Ybarra & Mitchell, 2004a, 2004b).

Эта динамика подтверждается теорией доступности Гибсона (Gibson, 2014), которая объясняет, как цифровые инструменты формируют поведение пользователей. При киберзапугивании такие технологические возможности, как анонимность и масштабируемость вреда, позволяют агрессорам действовать безнаказанно, усиливая психологический и социальный ущерб, наносимый жертвам (Topcu-Uzer & Tanrıkulu, 2018). Например, широкая доступность таких платформ, как социальные сети, позволяет преступникам охватывать более широкую аудиторию, одновременно защищая себя от разоблачения.

На макроуровне этот дисбаланс сил связан с более широкими структурными факторами. Так, доступ к технологическим знаниям часто зависит от социально-экономических различий, что усиливает системное неравенство. Те, кто находятся в привилегированном положении, с большей вероятностью приобретут передовые знания и ресурсы, что позволит им манипулировать информацией как инструментом контроля и доминирования. Эта динамика отражается и в более масштабных явлениях, таких как политическое киберзапугивание, кибертерроризм и информационная война, где контроль над технологиями и данными занимает центральное место в борьбе за влияние (Millard, 2009; Zannis, 2005; Bosworth et al., 1999).

Предлагаемая усовершенствованная модель дисбаланса сил при киберзапугивании подчеркивает взаимосвязь между этими индивидуальными и системными факторами. Она иллюстрирует, как агрессоры используют технологические инструменты и пробелы в знаниях для укрепления своего превосходства, что усложняет задачу противодействия. Модель предусматривает разработку целевых стратегий, направленных на устранение этих дисбалансов как на индивидуальном, так и на структурном уровне (рис. 1).

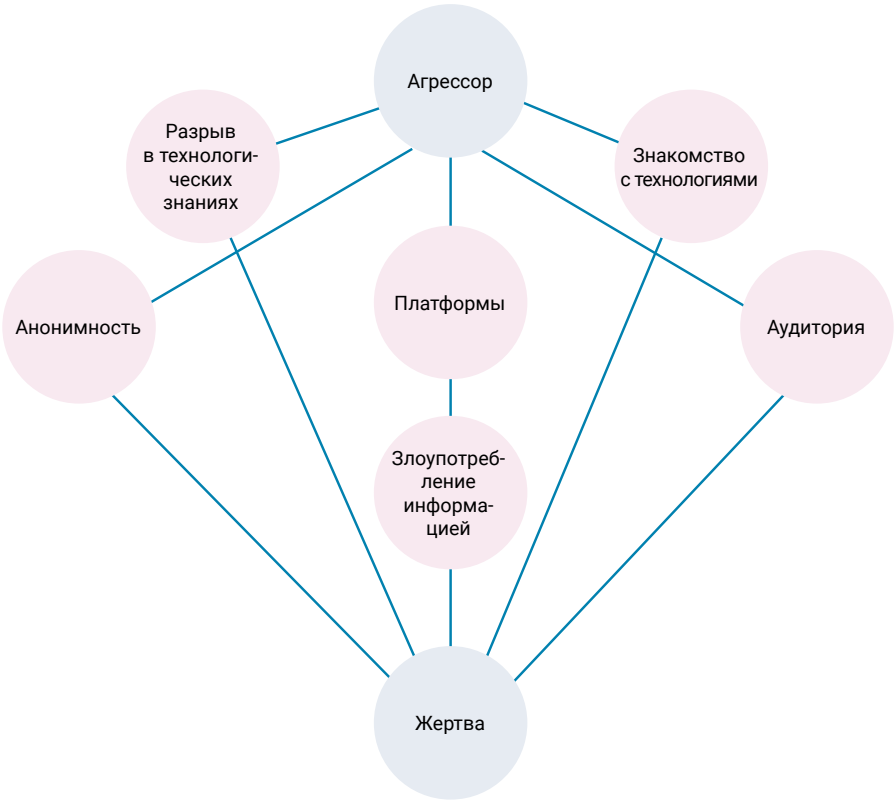

Рис. 1. Усовершенствованная модель дисбаланса сил при киберзапугивании, включающая роль злоупотребления информацией и технологической грамотности в динамике киберзапугивания

Таким образом, систематическое неправомерное использование информации лежит в основе дисбаланса сил, присущего киберзапугиванию. Это явление обусловлено не только поведением отдельных людей, но и технологическими и системными факторами, которые меняют традиционные представления об ущербе и контроле. Решение этой проблемы требует многогранного подхода. Меры противодействия должны быть направлены на устранение пробелов в цифровой грамотности, повышение возможностей граждан к противодействию и укрепление подотчетности платформ. Кроме того, для восстановления баланса сил в цифровой сфере решающее значение имеет обеспечение равного доступа к технологиям и внедрение надежных этических и правовых гарантий. Интегрируя эти стратегии, заинтересованные стороны смогут создать более безопасную, справедливую и инклюзивную цифровую среду.

2. Киберзапугивание и этика в сфере технологий: анализ потоков с точки зрения технологической этики

Киберзапугивание представляет собой не только социотехнический феномен, но и фундаментальную этическую проблему в эпоху цифровых технологий. Как отмечает Luppicini (2018), этика технологий предлагает концепцию, через призму которой можно исследовать взаимосвязь технологий и общечеловеческих ценностей, проливая свет на феномен злоупотребления цифровыми платформами в целях проявления агрессии или причинения вреда. Киберзапугивание, т. е. преднамеренное и повторяющееся вредоносное поведение, осуществляемое с помощью цифровых устройств, усугубляет эти процессы, поскольку агрессоры используют такие возможности, как анонимность, вирусность и непрерывность воздействия на жертву (Langos, 2012; Menesini et al., 2013).

Техноэтические последствия этого феномена разнообразны. Во-первых, киберзапугивание подрывает принцип цифрового достоинства, определяемый как право людей существовать в онлайн-пространстве, не подвергаясь унижению и вредоносному воздействию (Verbeek, 2011). Платформы часто не могут эффективно обеспечить соблюдение этого принципа, хотя и обладают технологическими возможностями для смягчения или выявления вредоносного контента[4]. Это свидетельствует о разрыве между технологическим потенциалом и этической практикой. Как утверждает Moor (2005), новые технологии требуют развития этических норм для предупреждения злоупотребления и развития общественного благосостояния.

Во-вторых, киберзапугивание подчеркивает дисбаланс сил, заложенный в цифровых инфраструктурах. Возможности для причинения вреда распределены неравномерно; агрессоры часто лучше владеют технологиями, в то время как жертвам может не хватать цифровой грамотности или доступа к эффективным механизмам информирования (Spyropoulos, 2011; Katerelos et al., 2011). Эта асимметрия позволяет структурированно распределить техноэтическую ответственность между несколькими участниками, как показано на рис. 2.

[4] Hinduja, S., & Patchin, J. W. (2014). Cyberbullying: Identification, Prevention and Response. Cyberbullying Research Center. https://clck.ru/3NQcNU

Рис. 2. Распределение техноэтической ответственности, показывающее солидарные роли частных лиц, платформ, государства и образовательных учреждений в борьбе с киберзапугиванием

Этот концептуальный инструмент определяет четыре основных уровня ответственности:

1. Ответственность на уровне проектирования. На этом основополагающем уровне находятся системные дизайнеры и разработчики. Они осуществляют выбор архитектуры платформы, функций модерации и доступности, что определяет взаимодействие с пользователями. Если платформа разрешает анонимность без какой-либо системы гарантий или поощряет распространение вредоносного контента без привлечения к ответственности, то вероятность появления киберзапугивания повышается (Capurro, 2009; Tavani, 2011).

2. Ответственность на уровне операторов. Операторы платформы и модераторы контента этически обязаны отслеживать, обнаруживать и удалять вредоносный контент, сохраняя при этом свободу выражения мнений. Неспособность действовать оперативно или прозрачно способствует виктимизации (Zuboff, 2019).

3. Ответственность на уровне пользователей. Этическое поведение – это не только обязанность организаций. Пользователи должны проявлять эмпатию, сдержанность и гражданственность в цифровой среде. Прививать эти техноэтические ценности призваны образовательные программы, ориентированные на молодежь (Chen, 2017; Ortega-Ruiz et al., 2012).

4. Ответственность на законодательном уровне. Такие механизмы, как Общий регламент ЕС по защите персональных данных, обеспечивают прозрачность, подотчетность и соблюдение прав пользователей, воплощая техноэтические нормы в юридических терминах[5]. Более подробно эти механизмы будут рассмотрены в последующих разделах.

[5] European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. https://eur-lex.europa.eu

Как показывает рис. 2, техноэтическая ответственность за киберзапугивание носит не линейный, а распределенный и взаимозависимый характер. Ни одна из сторон не может решить проблему изолированно. Техноэтический анализ подчеркивает эту взаимосвязь.

Кроме того, новые уровни сложности возникают за счет автоматизации и средств обнаружения на основе искусственного интеллекта. Такие системы предназначены для выявления злоупотреблений, но они также могут создавать предвзятость или упускать нюансы контекста (Ioannou et al., 2018). Поэтому неизменными остаются требования прозрачности и надзора со стороны человека (Tavani, 2011).

Итак, с точки зрения техноэтики явление киберзапугивания показывает необходимость распределения ответственности, разработки этической системы, активного вмешательства и воспитания уважения к цифровому достоинству на всех уровнях социотехнической экосистемы.

3. Взаимосвязь между этикой в сфере технологий, киберзапугиванием и его предотвращением

Техноэтика дает важнейшую основу для изучения этических аспектов киберзапугивания и разработки политики и стратегий по смягчению его последствий. Особо подчеркивая требование совместной ответственности отдельных пользователей, технологических платформ и регулирующих органов, техноэтика выступает за создание более безопасной и справедливой цифровой среды. Предотвращение киберзапугивания и борьба с ним требуют комплексного подхода, выходящего за рамки применения технологических решений или отдельных законодательных мер. Важно отметить, что большинство из этих методов профилактики давно применяются в психологии для развития эмоциональной устойчивости, эмпатии и осознанности поведения. Таким образом, эффективные меры включают в себя этические принципы, образовательные инициативы и инновационные психосоциальные стратегии, обеспечивающие баланс между техническим прогрессом, правами человека и благополучием общества (Hinduja & Patchin, 2009).

Общий регламент по защите данных (GDPR) представляет собой один из самых значимых правовых инструментов для защиты персональных данных в Европейском союзе[6], особенно в контексте причинения вреда в Сети. Документ закрепляет такие принципы, как минимизация объема данных и право на их удаление. Это дает возможность сохранять контроль над своим цифровым присутствием и добиваться возмещения ущерба в случае неправомерного использования личной информации. Общий регламент по защите данных – это не просто механизм регулирования; он воплощает в себе основные техноэтические ценности: прозрачность, подотчетность и автономию, обеспечивая действенную этическую защиту в сфере цифровых прав. Тем самым он способствует созданию более уважительной и ориентированной на человека цифровой среды[7].

---

6 Там же.

7 European Parliament and Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148. Official Journal of the European Union, L333, 80–137. https://clck.ru/3QGqvZ

Не менее важен Закон об искусственном интеллекте (AI Act), принятый Европейским союзом в качестве первой глобальной нормы регулирования технологий искусственного интеллекта (Regulation (EU) 2024/1689). Этот закон использует подход к классификации систем искусственного интеллекта с точки зрения категорий риска – от минимального до высокого. Инструменты, используемые для модерации контента и выявления вредоносного поведения в Сети, такого как киберзапугивание, обычно относятся к категории систем высокого риска, требующих строгого соблюдения требований прозрачности, справедливости и надзора. Это гарантирует, что системы искусственного интеллекта, используемые на платформах социальных сетей или в образовательных учреждениях, являются точными, беспристрастными и контролируются операторами-людьми. Кроме того, Закон об искусственном интеллекте запрещает манипулятивные технологии, которые могут пагубно влиять на поведение пользователей. Это отражает принципы приверженности защите прав пользователей и развития этических инноваций.

Конвенция Организации Объединенных Наций против киберпреступности, принятая в 2024 г., представляет собой важную глобальную веху в борьбе с преступлениями, совершаемыми с помощью ИКТ. Она обеспечивает всеобъемлющую основу для борьбы с киберпреступностью, включая незаконный доступ к системам, утечку данных и онлайн-мошенничество. При этом в ней не содержится положений непосредственно о киберзапугивании. Это подчеркивает, что сохраняются трудности в выработке единого глобального подхода к решению этой широко распространенной проблемы. Несмотря на этот пробел, несколько положений конвенции имеют косвенное отношение к киберзапугиванию. Например, ст. 14 касается сексуального насилия над детьми в Интернете, а ст. 16 направлена против несанкционированного распространения изображений интимного характера, что часто связано с киберзапугиванием. Кроме того, ст. 18 устанавливает ответственность платформ, способствующих вредоносной деятельности, а ст. 34 предусматривает меры по оказанию помощи жертвам и их защите[8].

Отсутствие прямых положений о киберзапугивании в Конвенции Организации Объединенных Наций против киберпреступности[9] подчеркивает необходимость принятия дальнейших поправок или дополнительных протоколов. Для устранения этого пробела необходима согласованная международная система борьбы с киберзапугиванием, особенно учитывая транснациональный характер многих инцидентов в этой сфере. Жертвы киберзапугивания часто сталкиваются со значительными препятствиями на пути к правосудию, если преступники действуют в разных юрисдикциях. Разработка универсального определения киберзапугивания заложила бы основу для скоординированных усилий, обеспечив более четкие пути для подачи судебных исков и оказания помощи жертвам. Кроме того, приведение Конвенции в соответствие с техноэтическими принципами повысило бы ее применимость, поскольку это гарантировало бы, что регулирующие меры отражают этические императивы справедливости, подотчетности и защиты пользователей.

---

8 United Nations General Assembly. (2024). United Nations Convention against Cybercrime: Strengthening international cooperation for combating crimes committed via ICT systems and evidence sharing. https://clck.ru/3NQc2k

9 Там же.

Несмотря на эти ограничения, Конвенция служит важным шагом на пути к глобальному сотрудничеству в борьбе с киберпреступлениями. Ее акцент на трансграничное сотрудничество и разделение ответственности государств-членов создает основу, которая может быть адаптирована для решения специфических проблем при киберзапугивании. Поскольку цифровые платформы непрерывно развиваются, в будущие редакции Конвенции необходимо включить положения, непосредственно касающиеся киберзапугивания, что повысило бы актуальность и эффективность документа.

Интегрируя техноэтические принципы в такие инновационные нормативные документы, как Общий регламент по защите данных, Закон об искусственном интеллекте и Конвенция Организации Объединенных Наций против киберпреступности (United Nations General Assembly, 2024), заинтересованные стороны могут создать цифровую экосистему, в которой приоритетными являются безопасность, подотчетность и инклюзивность. Для разработки согласованных стратегий, отвечающих этическим требованиям, важное значение имеет сотрудничество между правительствами, платформами и структурами гражданского общества. Например, партнерские отношения между исследовательскими организациями и государственными органами способствуют разработке передовых инструментов для выявления и смягчения ущерба. Кроме того, этичную и эффективную работу платформ обеспечивает продвижение передовых практик, таких как подотчетность, прозрачность и аудит алгоритмов.

4. Практические и междисциплинарные рекомендации

4.1. Технологические средства

Роль технологий в предотвращении киберзапугивания и борьбе с ним становится все более значимой, поскольку современные платформы внедряют инновационные решения для борьбы с вредоносными действиями в Интернете. Для обнаружения и удаления вредоносного контента крупные платформы используют передовые инструменты искусственного интеллекта. Согласно Meier с соавт. (2016), системы искусственного интеллекта особенно эффективны при мониторинге в режиме реального времени, выявлении подозрительного поведения и предотвращении распространения оскорбительных сообщений. Например, автоматизированные системы могут значительно снизить поток оскорбительных комментариев, своевременно удаляя вредоносный контент.

Однако, хотя ИИ предлагает мощные инструменты для сдерживания вредоносного контента, он не лишен ограничений. Как отмечал Цукерберг[10], системы ИИ с трудом понимают сложные контексты и культурные нюансы, что делает их менее эффективными в ситуациях, требующих вынесения суждений. Для обеспечения точности и беспристрастности при модерации контента необходим гибридный подход, сочетающий технологию искусственного интеллекта с контролем со стороны человека. Это согласуется с подходом Цукерберга[11] , который состоит в вовлечении пользователей с помощью таких инструментов, как Community Notes. Они позволяют

[10] Zuckerberg*, M. (2024). It's time to get back to our roots around free expression. Facebook Watch. https://clck.ru/3NQcAk (* Является соучредителем компании Meta, запрещенной на территории РФ, находящейся в списке экстремистских организаций).

[11] Является соучредителем компании Meta, запрещенной на территории РФ, находящейся в списке экстремистских организаций.

пользователям корректировать контекст и совместно устранять фейковую информацию или вредоносный контент.

С точки зрения техноэтики использование технологий наблюдения и мониторинга в борьбе с киберзапугиванием должно обеспечивать баланс между безопасностью и конфиденциальностью. Floridi (2014) утверждает, что жизненно важное значение для предотвращения практик притеснения имеют прозрачность, уважение прав личности и надежная защита данных. Этичное использование технологий требует наличия систем, которые уделяют приоритетное внимание человеческому достоинству и в то же время предоставляют эффективные решения для снижения вреда, наносимого в Сети.

Помимо совершенствования технологических инструментов, первостепенное значение имеет сотрудничество с участием множества заинтересованных сторон. Государство, гражданское общество и технологические платформы должны совместно разрабатывать протоколы модерации контента для обеспечения баланса между эффективностью и справедливостью. Такое сотрудничество должно быть направлено на создание прозрачных систем, в которых приоритетное внимание уделяется предотвращению вреда и защите прав пользователей. Объединяя опыт и ресурсы, заинтересованные стороны могут разрабатывать решения, характеризующиеся адаптивностью и учетом культурных особенностей. Это позволит преодолеть проблему киберзапугивания в различных цифровых средах.

Дальнейшее повышение эффективности стратегий профилактики возможно путем партнерских отношений с образовательными учреждениями. Школы и университеты могут обучать принципам цифровой этики и мерам противодействия, а также навыкам, необходимым для безопасного и ответственного использования цифрового пространства. Такие программы должны делать упор на критическое мышление, эмпатию и цифровую грамотность, способствуя формированию культуры уважения и подотчетности среди молодого поколения. Совместные инициативы педагогов, государственных органов и платформ должны создать всеобъемлющие образовательные подходы, которые устранят коренные причины киберзапугивания и одновременно будут способствовать этичному цифровому поведению.

Эффективно решить сложные проблемы киберзапугивания возможно, лишь сочетая технологические инновации с этическими принципами и междисциплинарным сотрудничеством. Такой подход способен не только уменьшить ущерб, но и поддержать более общие принципы справедливости, подотчетности и уважения человеческого достоинства, обеспечивая соответствие технического прогресса общественным ценностям.

4.2. Цифровое гражданство и стимулирование ответственного поведения

Техноэтика подчеркивает жизненно важное значение воспитания цифровой гражданственности, выступая за формирование ответственного и уважительного поведения при онлайн-взаимодействиях. Воспитание гражданственности в цифровом мире включает в себя такие важные принципы, как демонстрация уважения к другим, поддержание чувства ответственности в виртуальной среде и воздержание от вредоносного поведения, включая киберзапугивание. Продвижение этих ценностей является неотъемлемой частью предотвращения неправомерных действий в Интернете.

Оно укрепляет социальную ответственность и способствует формированию культуры уважения в цифровой и образовательной среде в целом[12].

4.3. Защита пострадавших

Эффективная защита жертв киберзапугивания требует создания структурированных систем отчетности, ориентированных на их интересы. Такие системы должны обеспечивать надежное и конфиденциальное информирование об инцидентах, при этом гарантируя, что жертвы будут чувствовать себя в безопасности, получать поддержку и расширять свои возможности на протяжении всего процесса. Решающее значение для эффективного рассмотрения жалоб имеют прозрачность и доверие, создавая среду, в которой люди могут с уверенностью обратиться за помощью. С точки зрения техноэтики технологические инструменты должны обеспечивать приоритетность благополучия пострадавших, интегрируя функции, повышающие безопасность и предлагающие доступные способы информирования и поддержки.

Для достижения этих целей необходимы конфиденциальные и безопасные каналы информирования. Ключевую роль в этом могут сыграть образовательные учреждения и коммуникационные платформы, внедрив системы, позволяющие учащимся и пользователям сообщать о травле или домогательствах, не опасаясь мести или нападения. Такие каналы информирования должны быть спроектированы таким образом, чтобы гарантировать анонимность и защиту пользователей, обеспечивая при этом быстрое и эффективное разрешение споров. Например, в работе Ioannou с соавторами (2018) подчеркивается важность интеграции таких инструментов в школьные социальные сети и цифровые платформы. Это укрепит этические подходы как в образовательной, так и в онлайн-среде.

В дополнение к этим механизмам правительствам следует рассмотреть возможность финансирования специальных горячих линий по борьбе с киберзапугиванием. Это может обеспечить пострадавшим немедленный доступ к психологической поддержке и консультациям со стороны подготовленных специалистов, предлагающих советы и помощь с учетом их потребностей. Такие инициативы могут устранить серьезные пробелы в деле помощи пострадавшим, особенно в тех случаях, когда они не имеют доступа к другим ресурсам. Работая с психологическими и эмоциональными аспектами киберзапугивания, такие горячие линии способствуют комплексной защите пострадавших и укреплению психического благополучия.

В дополнение к мерам реагирования можно использовать упреждающий подход к защите пострадавших путем разработки индекса цифровой устойчивости. Этот инструмент позволит оценить способность уязвимых групп, таких как дети и подростки, безопасно и эффективно справляться с киберрисками. Он может оценивать такие факторы, как цифровая грамотность, эмоциональная устойчивость и доступ к системам поддержки, позволяя получить ценную информацию о конкретных потребностях групп риска. Индекс цифровой устойчивости может помочь определить проблемные области и послужить руководством для разработки целевых мер в области образования, повышения осведомленности и при корректировании государственной политики.

---

[12] Bynum, T. W. (2008). Computer and Information Ethics. In The Stanford Encyclopedia of Philosophy. https://clck.ru/3NQcEy

Такие стратегии, ориентированные на пострадавших, не только смягчают непосредственные последствия киберзапугивания, но и способствуют формированию культуры эмпатии и поддержки в цифровом и образовательном пространстве. Tavani (2011) подчеркивает, что приоритетность благополучия жертв и воспитание чувства безопасности являются необходимым условием повышения сопротивляемости пострадавших и дают им возможность восстановить контроль в рамках цифрового взаимодействия. Совместные усилия государства, платформ и структур гражданского общества имеют решающее значение для обеспечения эффективности и широкого доступа к этим системам.

Возможная комплексная система защиты жертв включает защищенные каналы отчетности, финансируемые государством службы поддержки и такие инструменты, как индекс цифровой устойчивости. Эти меры, основанные на принципах техноэтики, направлены на решение многогранных проблем киберзапугивания и способствуют созданию более инклюзивной и благоприятной цифровой среды.

4.4. Этические дилеммы

Использование технологий для предотвращения киберзапугивания, хотя и приносит значительные выгоды, ставит сложные этические и юридические дилеммы, требующие тщательного изучения. Одним из ключевых вопросов является защита конфиденциальности, особенно в контексте методов слежения за данными, используемых платформами социальных сетей. Эти методы направлены на выявление подозрительных действий и предотвращение киберзапугивания, но сопряжены с неизбежным риском злоупотребления властью. Сбор и анализ больших массивов данных, часто проводимый без явно выраженного согласия пользователя, может привести к потенциальным нарушениям прав на неприкосновенность частной жизни и личную автономию, которые охраняются такими нормами, как Общий регламент защиты данных. Это поднимает важные вопросы о том, в какой степени конфиденциальность может быть нарушена для обеспечения безопасности в Интернете.

Другая насущная проблема связана с внедрением алгоритмов модерации контента. Хотя эти инструменты предназначены для обнаружения и удаления вредоносного контента, они часто не учитывают нюансов, позволяющих отличить ненавистнические высказывания от правомерных проявлений сарказма или критики. Это может привести к непреднамеренной цензуре, ограничению свободы выражения мнений, то есть права, закрепленного в международных соглашениях, таких как Европейская конвенция по правам человека (ст. 10 ЕКПЧ)[13]. Такой сценарий подрывает демократический обмен идеями и говорит о необходимости гарантий для предотвращения злоупотреблений.

Эти дилеммы подчеркивают важность соблюдения баланса между правами на неприкосновенность частной жизни и свободу выражения мнений и необходимостью защиты безопасности и достоинства пользователей. Техноэтика предлагает основу для решения этих проблем, выступая за повышение прозрачности методов

[13] Council of Europe. (1950). European Convention on Human Rights, Article 10: Freedom of Expression. https://clck.ru/3NQngR

наблюдения и подотчетность при разработке и внедрении алгоритмов модерации контента. Принятие этой основы поможет предотвратить злоупотребления, укрепить доверие к цифровым платформам и обеспечить соблюдение основных прав при технологическом вмешательстве, одновременно повышая безопасность в Интернете.

4.5. Усиление сотрудничества и перспективы на основе использования данных

Транснациональный характер киберзапугивания требует принятия единых и совместных глобальных ответных мер. Из-за своей способности преодолевать национальные границы киберзапугивание бросает вызов традиционным границам юрисдикций и требует гармонизации правовых рамок для обеспечения последовательной защиты жертв во всем мире. Децентрализованная структура Интернета часто позволяет преступникам использовать различия в национальных законах, что делает необходимым международное сотрудничество. Для эффективного решения этих проблем необходим глобальный подход, основанный на общих принципах справедливости, подотчетности и прав человека.

В этом контексте ключевой рекомендацией является создание Международной целевой группы по предотвращению киберзапугивания, которая способствовала бы проведению трансграничных расследований, обмену информацией и поддержке скоординированных усилий правоохранительных органов. Этот орган мог бы устранить пробелы в отношении юрисдикций путем разработки международно признанных протоколов для ведения дел о киберзапугивании и обеспечения привлечения виновных к ответственности независимо от географического местонахождения. Кроме того, это могло бы способствовать приведению национальных правовых рамок в соответствие с международными стандартами, уменьшению фрагментации политических мер и обеспечению справедливой правовой защиты пострадавших.

На уровне государственной политики многообещающие подходы к борьбе с киберзапугиванием демонстрируют несколько национальных инициатив. Государства реализуют различные стратегии, начиная от кампаний по повышению цифровой грамотности и технологических инструментов и заканчивая специализированными правовыми нормами, описывающими специфический вред от агрессии в Сети. Например, в Греции было представлено цифровое приложение «Безопасность для молодых»[14]. Это инновационный инструмент, предназначенный для оказания помощи несовершеннолетним в возрасте от 12 лет в борьбе с онлайн-угрозами. Приложение обеспечивает прямую связь со службами экстренной помощи, незаметные экстренные уведомления об угрозах в режиме реального времени и безопасную систему подачи сообщений о злоупотреблениях через Единый цифровой портал государственного управления. Придавая приоритетное значение доступности, конфиденциальности и оперативности, данная инициатива выражает технo-этический подход к цифровой безопасности, позволяющий несовершеннолетним

[14] Ministry of Citizen Protection, Hellenic Police and Vodafone Foundation. (2024). SAFE.YOUth: Digital Application for the Protection of Minors. https://clck.ru/3NQcsT

безопасно справляться с кризисными ситуациями. Однако серьезной проблемой остается обеспечение равного доступа к этому инструменту, особенно для маргинализированных групп населения или лиц с ограниченной технической грамотностью.

Несмотря на прогресс в реализации таких национальных инициатив, как «Безопасность для молодых», серьезной проблемой в существующих правовых системах является их адаптируемость к возникающим технологическим угрозам. Многие законы сосредоточиваются на традиционных механизмах онлайн-травли, но не учитывают распространение вредоносного контента под управлением алгоритмов, злоупотребление искусственным интеллектом и роль цифровой анонимности в закреплении злоупотреблений. В будущем нормативно-правовая база должна учитывать эту меняющуюся динамику, особенно в отношении алгоритмов социальных сетей, игровых платформ и контента, созданного с помощью искусственного интеллекта (например, дипфейков). Расширение правовой защиты в этих областях имеет решающее значение для целей актуальности и эффективности законодательных мер.

С точки зрения криминологии киберзапугивание отражает дисбаланс сил, т. е. преступники действуют безнаказанно, используя анонимность и широкий охват цифровых платформ. Хотя юридические механизмы привлечения к ответственности предоставляют жертвам средства правовой защиты, необходимы долгосрочные культурные и системные изменения, чтобы устранить более общие социальные механизмы, которые способствуют цифровой агрессии. Более целостный подход к профилактике и борьбе с этим явлением (Vandebosch, 2019) предполагает интеграцию принципов восстановительного правосудия (Guardabassi & Nicolini, 2024; Duncan, 2016), применение программ реабилитации правонарушителей (Othman et al., 2024) и создание надежных систем поддержки пострадавших.

Наряду с правовыми и институциональными мерами реагирования, решающее значение для понимания тенденций киберзапугивания и разработки эффективных мер вмешательства имеет интеграция информации, основанной на реальных данных. Проведение метаанализа распространенности киберзапугивания и изучение факторов риска, связанных с конкретными платформами, помогает в разработке целенаправленных стратегий профилактики (Sathya & Fernandez, 2024; Kim et al., 2021). Например, изучение того, как алгоритмы усиливают вредоносный контент или как анонимность способствует преследованию, дает ценную информацию о снижении негативного воздействия этих технологий (Johora et al., 2024; Meier et al., 2016).

Другой многообещающий способ борьбы с киберзапугиванием состоит в заключении соглашений об анонимном обмене данными между цифровыми платформами и исследовательскими институтами. Платформы социальных сетей собирают огромное количество поведенческих данных, которые, при условии ответственной анонимизации, могут быть использованы для выявления форм злоупотреблений и разработки упреждающих решений. Прозрачные соглашения, соблюдающие баланс между правом на неприкосновенность частной жизни и задачами исследований, могут обеспечить как развитие инноваций, так и защиту отдельных пользователей (Floridi, 2014).

Укрепление международного сотрудничества, совершенствование национальной правовой базы и использование аналитических данных являются условиями для разработки согласованной глобальной стратегии борьбы с киберзапугиванием. Такие инициативы, как «Безопасность для молодых» в Греции, демонстрируют потенциал

цифровых инструментов в борьбе с онлайн-угрозами, но они должны дополняться всеобъемлющими мерами на международном уровне. Интеграция принципов технэтики, которые ставят во главу угла подотчетность, цифровые права и равный доступ к механизмам защиты, имеет ключевое значение для создания более безопасной, инклюзивной и устойчивой цифровой среды для будущих поколений.

Заключение

Киберзапугивание как распространенная форма цифровой агрессии является примером неправомерного использования технологий для причинения вреда, запугивания или унижения людей. Решение этой многогранной проблемы требует целостного подхода, который объединяет меры профилактики, правовые механизмы, технологические инновации и этические соображения. Центральное место в этой работе занимает признание структурного неравенства, например, в отношении доступа к технологиям и грамотности. Эти различия усиливают уязвимость и закрепляют дисбаланс сил при цифровом взаимодействии (Lazos, 2001). Вооружение пользователей знаниями и формирование этической культуры использования информации остаются важнейшими шагами на пути к продвижению ответственного взаимодействия в цифровой среде (Tsouramanis, 2005).

В рекомендациях относительно мер государственной политики особое внимание должно уделяться адаптивным и перспективным правовым рамкам как на национальном, так и на международном уровнях. Правительствам следует налаживать сотрудничество в целях гармонизации законов, направленных на борьбу с киберзапугиванием, обеспечивая согласованность и подотчетность в различных юрисдикциях. Создание Международной целевой группы по предотвращению киберзапугивания, а также Глобального договора о предотвращении киберзапугивания может послужить базой для трансграничных расследований и обеспечить единые стандарты борьбы с этой проблемой. Эти структуры должны быть динамичными и включать такие передовые технологии, как искусственный интеллект, блокчейн и алгоритмическая прозрачность, которые дают возможность как наносить, так и предотвращать ущерб.

Принятие комплексных мер реагирования требует сотрудничества между заинтересованными сторонами. Технологические платформы несут главную ответственность за разработку и внедрение надежных систем модерации контента, механизмов прозрачности и мер защиты пользователей. Правительства должны принять адаптивные законы, обеспечивающие баланс между свободами личности и защитой от вреда в Сети. Организации гражданского общества и образовательные учреждения также играют ключевую роль в формировании этических норм, повышении осведомленности и оказании поддержки пострадавшим.

Краеугольным камнем борьбы с киберзапугиванием остается профилактика. Образовательные учреждения должны включать в учебные планы вопросы цифровой грамотности, повышения сопротивляемости и этичного использования технологий, что позволит учащимся ответственно ориентироваться в онлайн-пространстве. Эта работа должна дополняться информационно-просветительскими кампаниями и инициативами по вовлечению родителей, финансируемыми за счет бюджета. Необходимо формировать культуру эмпатии и ответственности. Кроме того, важно преодолеть цифровой разрыв и обеспечить равный доступ к технологиям. Это имеет

решающее значение для устранения системного неравенства, которое усугубляет киберзапугивание. Обеспечение всех пользователей, особенно уязвимых групп, инструментами и знаниями для безопасного взаимодействия в цифровом пространстве соответствует этическим принципам инклюзивности и социальной справедливости.

При внедрении технологических инструментов, таких как модерация контента с помощью искусственного интеллекта и технологии слежки, сохраняются этические дилеммы сочетания эффективности с уважением к частной жизни и человеческому достоинству. Принципы техноэтики – ответственность, подотчетность и инклюзивность – отвечают целям общественного благополучия и должны лежать в основе этих инноваций.

В заключение отметим, что борьба с киберзапугиванием требует междисциплинарного, основанного на сотрудничестве подхода, который подразумевает инновационные меры государственной политики, участие всех заинтересованных сторон и этическое предвидение. Устраняя первопричины киберзапугивания, содействуя равному доступу к технологиям и воспитывая культуру ответственности, общество может уменьшить вред от этого негативного явления. Тем самым мы сможем гарантировать, что технологические достижения будут способствовать созданию более безопасной и инклюзивной цифровой экосистемы, в которой приоритетными являются права, достоинство и благополучие всех пользователей.

Список литературы

Bosworth, K., Espelage, D. L., & Simon, T. R. (1999). Factors associated with bullying behavior in middle school students. *The Journal of Early Adolescence*, *19*(3), 341–362. https://doi.org/10.1177/0272431699019003003

Chakraborty, S., Bhattacherjee, A., & Onuchowska, A. (2021). Cyberbullying: A review of the literature. SSRN. http://dx.doi.org/10.2139/ssrn.3799920

Campbell, M., & Bauman, S. (2018). Cyberbullying: Definition, consequences, prevalence. In M. Campbell & S. Bauman (Eds.), *Reducing Cyberbullying in Schools* (pp. 3–16). Academic Press. https://doi.org/10.1016/B978-0-12-811423-0.00001-8

Capurro, R. (2009). Digital ethics. *The Information Society*, *25*(3), 183–186. https://doi.org/10.1080/01972240902848902

Chen, C. W. Y. (2017). "Think before you type": The effectiveness of implementing an anti-cyberbullying project in an EFL classroom. *Pedagogies*, *13*(1), 1–18. https://doi.org/10.1080/1554480X.2017.1363046

Courakis, N. (2005). *Criminological horizons. Vol. II: Pragmatic approach and individual issues*. 2nd ed. Athens – Komotini: Ant. N. Sakkoula (In Greek).

Duncan, S. H. (2016). Cyberbullying and restorative justice. In R. Navarro, S. Yubero & E. Larrañaga (Eds.). *Cyberbullying Across the Globe* (pp. 239–257). Cham: Springer International Publishing.

Englander, E., Donnerstein, E., Kowalski, R., Lin, C. A., & Parti, K. (2017). Defining cyberbullying. *Pediatrics*, *140*(Supplement_2), S148–S151. https://doi.org/10.1542/peds.2016-1758u

Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford: Oxford University Press.

Furnell, S. M. (2006). *Computer Insecurity: Risking the System*. Oxford: Chandos Publishing.

Gibson, J. J. (2014). The theory of affordances (originally published 1979). In G. Bridge & S. Watson (Eds.). *The People, Place, and Space Reader* (pp. 56–60). London: Routledge.

Guardabassi, V., & Nicolini, P. (2024). Adolescence and cyberbullying: a restorative approach. In *INTED2024 Proceedings* (pp. 4562–4570). IATED. https://doi.org/10.21125/inted.2024.1183

Hasan, M. T., Hossain, M. A. E., Mukta, M. S. H., Akter, A., Ahmed, M., & Islam, S. (2023). A review on deep-learning-based cyberbullying detection. *Future Internet*, *15*(5), 179. https://doi.org/10.3390/fi15050179

Hinduja, S., & Patchin, J. W. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, *4*(2), 148–169. https://doi.org/10.1177/1541204006286288

Hinduja, S., & Patchin, J. W. (2009). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Thousand Oaks, CA: Sage Publications.

Ioannou, A., Blackburn, J., Stringhini, G., De Cristofaro, E., Kourtellis, N., & Sirivianos, M. (2018). From risk factors to detection and intervention: a practical proposal for future work on cyberbullying. *Behaviour & Information Technology*, *37*, 258–266. https://doi.org/10.1080/0144929X.2018.1432688

Johora, F. T., Khan, M. S. I., Kanon, E., Rony, M. A. T., Zubair, M., & Sarker, I. H. (2024). A data-driven predictive analysis on cyber security threats with key risk factors. *arXiv preprint arXiv:2404.00068*.

Juvonen, J., & Gross, E. F. (2008). Extending the school grounds? Bullying experiences in cyberspace. *Journal of School Health*, *78*(9), 496–505. https://doi.org/10.1111/j.1746-1561.2008.00335.x

Katerelos, I., Tsekeris, C., Lavdas, M., & Demetriou, K. (2011). A psychosociological approach to Internet use and mass online role-playing games. In K. Siomos & G. Floros (Eds.), *Research, prevention, management of risks in Internet use*. Larissa: Hellenic Society for the Study of Internet Addiction Disorder. (In Greek).

Kim, S., Razi, A., Stringhini, G., Wisniewski, P. J. and De Choudhury, M. (2021). A human-centered systematic literature review of cyberbullying detection algorithms. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW2). https://doi.org/10.1145/3476066

Kowalski, R. (2018). Cyberbullying. In J. P. Forgas, R. F. Baumeister & T. F. Denson (Eds.), *The Routledge International Handbook of Human Aggression* (pp. 131–142). London: Routledge. https://doi.org/10.4324/9781315618777-11

Langos, C. (2012). Cyberbullying: The challenge to define. *Cyberpsychology, Behavior, and Social Networking*, *15*(6), 285–289. https://doi.org/10.1089/cyber.2011.0588

Lazos, G. (2001). *Information Technology and Crime*. Athens: Nomiki Bibliothiki. (In Greek).

Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior*, *23*(4), 1777–1791. https://doi.org/10.1016/j.chb.2005.10.005

Luppicini, R. (2018). *The Changing Scope of Technoethics in Contemporary Society*. Hershey, PA: Information Science Reference. https://doi.org/10.4018/978-1-5225-5094-5

Meier, A., Reinecke, L., & Meltzer, C. E. (2016). "Facebocrastination"? Predictors of using Facebook* for procrastination and its effects on students' well-being. *Computers in Human Behavior*, *64*, 65–76. https://doi.org/10.1016/j.chb.2016.06.011

Menesini, E., Nocentini, A., & Palladino, B. E. (2012). Empowering students against bullying and cyberbullying: Evaluation of an Italian peer-led model. *International Journal of Conflict and Violence*, *6*(2), 313–320. https://doi.org/10.4119/ijcv-2922

Menesini, E., Nocentini, A., & Camodeca, M. (2013). Morality, values, traditional bullying, and cyberbullying in adolescence. *British Journal of Developmental Psychology*, *31*(1), 1–14. https://doi.org/10.1111/j.2044-835X.2011.02066.x

Millard, G. (2009). Stephen Harper and the politics of the bully. *Dalhousie Review*, *89*(3), 329–336.

Moor, J. H. (2005). Why we need better ethics for emerging technologies. *Ethics and Information Technology*, *7*(3), 111–119. https://doi.org/10.1007/s10676-006-0008-0

Mouzaki, D. (2010). International scientific conference on: "Dealing with cyberbullying from a legal perspective". *The Art of Crime*, *15*. (In Greek).

Nocentini, A., Calmaestra, J., Schultze-Krumbholz, A., Scheithauer, H., Ortega, R., & Menesini, E. (2010). Cyberbullying: Labels, behaviours and definition in three European countries. *Australian Journal of Guidance & Counselling*, *20*(2), 129–142. https://doi.org/10.1375/ajgc.20.2.129

Olweus, D. (1993). *Bullying at School: What We Know and What We Can Do*. Oxford, UK: Blackwell.

Ortega-Ruiz, R., Del Rey, R., & Casas, J. A. (2012). Knowing, building and living together on internet and social networks: the ConRed cyberbullying prevention program. *International Journal of Conflict and Violence*, *6*(2), 303–313. https://doi.org/10.4119/ijcv-2921

Othman, S. N., Alziboon, M. F., Dawood, M., Sachet, S. J., & Moroz, I. (2024). New rehabilitation against electronic crimes by young people. *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico*, *22*, 363–385. https://doi.org/10.5281/zenodo.13732745

Raj, M., Singh, S., Solanki, K., & Selvanambi, R. (2022). An application to detect cyberbullying using machine learning and deep learning techniques. *SN Computer Science*, *3*(5), 401. https://doi.org/10.1007/s42979-022-01266-w

Sathya, J., & Fernandez, F. M. H. (2024). Predictive analysis in healthcare systems. In A. J. Anand, K. Kalaiselvi & J. M. Chatterjee (Eds.), *Artificial Intelligence – Based System Models in Healthcare* (pp. 131–152). Wiley. https://doi.org/10.1002/9781394242528.ch6

* Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology*, *49*(2), 147–154. https://doi.org/10.1111/j.1467-9450.2007.00611.x

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, *49*(4), 376–385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

Smith, P. K., del Barrio, C., & Tokunaga, R. S. (2013). Definitions of bullying and cyberbullying: How useful are the terms? In S. Bauman, D. Cross & J. Walker (Eds.), *Principles of cyberbullying research: Definitions, measures, and methodology* (pp. 26–40). New York: Routledge/Taylor & Francis Group.

Spyropoulos, F. (2011). The manifestations of deviant behavior on the Internet – Reflections on the needs of modernization of Greek criminal legislation. In K. Siomos & G. Floros (Eds.), *Research, Prevention, Management of Risks in Internet Use*. Larissa: Hellenic Society for the Study of Internet Addiction Disorder. (In Greek).

Tavani, H. T. (2011). *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing* (3rd ed). Hoboken, NJ: Wiley.

Topcu-Uzer, C., & Tanrıkulu, İ. (2018). Technological solutions for cyberbullying. In M. Campbell & S. Bauman (Eds.), *Reducing cyberbullying in schools* (pp. 33–47). Academic Press. https://doi.org/10.1016/B978-0-12-811423-0.00003-1

Tsouramanis, Ch. (2005). *Digital Crime – The (Un)Safe Side of the Internet*. Athens: V. Katsaros Publications. (In Greek).

Vandebosch, H. (2019). Cyberbullying prevention, detection and intervention. In W. Heirman, M. Walrave & H. Vandebosch (Eds.), *Narratives in Research and Interventions on Cyberbullying among Young People* (pp. 29–44). Cham: Springer. https://doi.org/10.1007/978-3-030-04960-7_3

Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. *CyberPsychology & Behavior*, *11*(4), 499–503. https://doi.org/10.1089/cpb.2007.0042

Verbeek, P.-P. (2011). *Moralizing Technology: Understanding and Designing the Morality of Things*. Chicago: University of Chicago Press. https://doi.org/10.7208/chicago/9780226852904.001.0001

Ybarra, M. L., & Mitchell, K. J. (2004a). Online aggressors/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry*, *45*, 1308–1316. https://doi.org/10.1111/j.1469-7610.2004.00328.x

Ybarra, M. L., & Mitchell, K. J. (2004b). Youth engaging in online harassment: Associations with caregiver-child relationships, Internet use, and personal characteristics. *Journal of Adolescence*, *27*, 319–336. https://doi.org/10.1016/j.adolescence.2004.03.007

Zannis, A. (2005). *Cybercrime*. Athens-Komotini: Sakkoulas Publications. (In Greek).

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

Сведения об авторе

Спайропулос Фотиос – научный сотрудник, PhD, доцент в области уголовного права и криминалистики, факультет права, Университет Филипс; старший партнер юридической компании Spyropoulos Law Firm
Адрес: Кипр, 28008, г. Никосия, ул. Ламиас, д. 4-6; Греция, 11474, г. Афины, Александрас авеню, д. 81
E-mail: fspyropoulos@gmail.com
ORCID ID: https://orcid.org/0000-0001-5950-3583
Google Scholar ID: https://scholar.google.com/citations?user=iKQYLWoAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 29 мая 2025 г.
Дата одобрения после рецензирования – 12 июня 2025 г.
Дата принятия к опубликованию – 25 сентября 2025 г.
Дата онлайн-размещения – 30 сентября 2025 г.