КОМПАРАТИВИСТСКИЕ ИССЛЕДОВАНИЯ УГОЛОВНОГО ПРАВА, КРИМИНОЛОГИИ И УГОЛОВНО-ИСПОЛНИТЕЛЬНОГО ПРАВА

DOI: 10.12737/jflcl.2019.3.4

НОВЫЕ ФОРМЫ ОНЛАЙН-ПРЕСТУПНОСТИ ЗА РУБЕЖОМ

ГОЛОВАНОВА Наталья Александровна, ведущий научный сотрудник отдела зарубежного конституционного, административного, уголовного законодательства и международного права Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, кандидат юридических наук

Россия, 117218, г. Москва, ул. Большая Черемушkinsкая, 34

E-mail: foreign1@izak.ru

Статья посвящена вопросам законодательного регулирования, а также введению уголовной ответственности за новые виды преступлений, совершаемых онлайн в сети Интернет. Стремительный рост преступлений, совершаемых практически безнаказанно с использованием новых цифровых технологий, ставит перед государством задачу обеспечения безопасности в киберпространстве, особенно, когда речь идет о защите детей и молодежи.

Используя сравнительно-правовой метод, автор исследует новейшее уголовное законодательство, тенденции его развития, а также правоприменительную практику в таких странах общего права с развитой цифровой инфраструктурой, как Австралия, Великобритания, Ирландия, Канада, Новая Зеландия и США.

Особое внимание уделено криминализации ряда преступлений против личности, таких как кибербуллинг, порноместь, сексуальный груминг детей и др. Вседозволенность в Интернете, порождаемая анонимностью правонарушителя, подвергает риску сексуального насилия и различным формам эксплуатации большое количество детей в связи с созданием материалов о насилии над ними или прямой трансляцией совершаемых преступлений.

Оценивая направления развития уголовного права, автор отмечает усиление криминализации новых форм онлайн-преступлений в зарубежных странах, ужесточение уголовной ответственности не только физических, но и юридических лиц, в частности провайдеров веб-услуг, не удаляющих со своих платформ контент о насилии над детьми.

Ключевые слова: безопасный Интернет, онлайн-дезинформация, онлайн-вред, онлайн-преступления, реальные преступления, кибербуллинг, справочник педофила, порноместь, сексуальный груминг детей, вредные цифровые сообщения, сексуальное принуждение и вымогательство у детей, совершаемые онлайн.

Для цитирования: Голованова Н.А. Новые формы онлайн-преступности за рубежом // Журнал зарубежного законодательства и сравнительного правоведения. 2019. № 3. С. 42—57. DOI: 10.12737/jflcl.2019.3.4

NEW TYPES OF ONLINE CRIMES ABROAD

N.A. GOLOVANOVA, Institute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow 117218, Russian Federation

E-mail: foreign1@izak.ru

The presented article is devoted to issues of legislative regulation and the introduction of criminal liability for new types of crime committed online on the Internet. The rapid growth of crimes committed with impunity with the use of new digital technologies (such as malicious and offensive messages, including those on the basis of hatred, extortion, misinformation and manipulation of online and other crimes causing a strong emotional and psychological stress for a victim) poses to the state the task of maintaining as much security in cyberspace as in real life, especially when it comes to protecting vulnerable categories – children and young people.

The author, by means of comparative legal method, examines the latest criminal legislation, its development trends, as well as law enforcement practice in common law countries with developed digital infrastructure (Australia, United Kingdom, Ireland, Canada, New Zealand and the USA).

In the article particular attention is paid to the criminalization of such crimes against the person as cyberbullying, porn revenge, sexual grooming of children, possession of a paedophile manual etc. Permissiveness on the Internet, assured by the anonymity of the offender, exposes countless children to the risk of sexual violence and various forms of exploitation, in connection with the creation of materials about child abuse or live broadcast of the crimes committed.

Assessing the direction of criminal law development, the author notes the increasing criminalization of online forms of crime in foreign countries, toughening criminal responsibility not only of individuals, but also of legal entities, in particular, web service providers which do not remove child abuse content from their platforms.

Keywords: Safer Internet, online disinformation, online harms, online crimes, offline crimes, cyberbullying, sexual grooming of children, paedophile manual, revenge porn, harmful digital communications, online sexual coercion and extortion of children.

For citation: Golovanova N.A. New Types of Online Crimes Abroad. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = *Journal of Foreign Legislation and Comparative Law*, 2019, no. 3, pp. 42—57. (In Russ.). DOI: 10.12737/jflcl.2019.3.4

Одной из важнейших проблем современного уголовного законодательства за рубежом стало обеспечение безопасности в Интернете, который, несмотря на все свои положительные характеристики, часто используется в незаконных целях. Киберпространство, по мнению канадского профессора Уэйна Маккея, можно сравнить с большой неконтролируемой общественной игровой площадкой, где недобросовестные участники могут преследовать, запугивать и порочить других, вызывая эмоциональный и психологический стресс с относительной безнаказанностью¹.

Размещение вредной онлайн-информации, нарушающей права отдельных лиц на неприкосновенность частной жизни, использование информационных технологий для оказания влияния и вмешательства в политические процессы (например, влияние на выбор избирателей) ставит перед государствами задачу создания безопасного Интернета, которая, учитывая постоянное совершенствование информационных технологий и повсеместное распространение социальных сетей, является чрезвычайно сложной.

Размещение мгновенно разлетающихся «фейковых» новостей и другой фальшивой информации, касающейся различных аспектов жизни людей — будь то реклама продуктов или лекарств, способов лечения болезней либо трактовки политических событий (независимо от того, искажены они или неточно освещены) — вызывает беспокойство в обществе и соответствующую государственную реакцию не только посредством ужесточения уголовно-правовых норм, но путем издания законов о контроле над социальными сетями и обязательствах интернет-гигантов блокировать и удалять дезинформацию, оскорбительные и человеконенавистнические высказывания и иной вредоносный контент.

В то время когда на европейском уровне разрабатывается общая стратегия борьбы с фальшивыми новостями², в законодательстве некоторых европейских государств (Италии, Германии и Франции) уже произошли определенные сдвиги в сторону введения такого контроля или ужесточения уже действующего режима³.

Так, правительство Италии в 2018 г. создало онлайн-портал⁴, пользуясь которым граждане могут сообщать о фальшивых новостях или мошеннической рекламе. Проект, названный «Красная кнопка»⁵, предлагает пользователям указать адрес своей электронной почты, ссылку на дезинформацию и любые социальные сети, в которых она была обнаружена. Такие запросы направляются в Polizia Postale (специальное подразделение полиции, которое расследует киберпреступления) для проверки и затем — если законодательство было нарушено — дело передается в суд.

В Федеративной Республике Германия 1 сентября 2017 г. Бундестаг одобрил Закон об улучшении правоприменения в социальных сетях⁶, известный также под названием Закон о Facebook. После Второй мировой войны Германия приняла одни из самых жестких в мире законов о разжигании ненависти, в том числе ввела наказание в виде лишения свободы за отрицание Холокоста и разжигание ненависти в отношении меньшинств. В последние годы германские политики все чаще стали высказывать опасения по поводу практического отсутствия ответственности за такие деяния в Интернете⁷. Согласно новому Закону, который был принят несмотря на большое сопротивление, особенно со стороны крайне правой «Альтернативы для Германии» (AfD), назвавшей NetzDG «законом о цензуре», онлайн-платформам теперь грозит штраф в размере до 50 млн евро, если они в течение 24 часов после получения официального уведомления не удалят «заведомо незаконные» сообщения, направленные на разжигание ненависти, и другие сообщения. Для удаления «нелегального» контента компаниям предоставляется семидневный период. Таким образом, пользователи Facebook, Twitter, Youtube, Instagram и Snapchat получили еще одну возможность потребовать удаления сообщения оскорбительного характера.

Во Франции 22 декабря 2018 г. также был принят Закон № 2018-1202 о борьбе с манипулированием информацией⁸, позволяющий судье вынести рас-

⁴ URL: www.commissariatodips.it.

⁵ См.: Fake news: da oggi puoi segnalarle alla Polizia. URL: <https://www.poliziadistato.it/articolo/155a6077fdb05e3865595940>.

⁶ Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG).

⁷ См.: Oltermann P. Tough new German law puts tech firms and free speech in spotlight. URL: <https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight>.

⁸ LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information.

¹ См.: MacKay W. Respectful and Responsible Relationships: There's No App for That. The Report of the Nova Scotia Task Force on Bullying and Cyberbullying. February 2012. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2123494&download=yes.

² URL: https://eeas.europa.eu/ru/eu-information-russian/38505/spotlight/38505_bs.

³ См., например: Renda A. The Legal Framework to Address “Fake News”: Possible Policy Actions at the EU Level. URL: [http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA\(2018\)619013_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA(2018)619013_EN.pdf).

поряжение о немедленном удалении онлайн-статей, являющихся, по его мнению, дезинформацией во время избирательных кампаний. Закон гласит, что пользователям должна быть предоставлена «информация, которая является честной, ясной и прозрачной», о том, как используются их персональные данные, что сайты должны раскрывать источник финансирования, предоставленного для продвижения информации. Французское агентство по национальному вещанию вправе приостанавливать телевизионное вещание каналов, контролируемых или находящихся под влиянием иностранного государства, если они «намеренно распространяют ложную информацию, которая может повлиять на искренность голосования». Этим Законом также была восстановлена ст. 112 законодательной части Избирательного кодекса, согласно которой любое нарушение оператором обязанностей по предоставлению соответствующей информации наказывается лишением свободы на срок до одного года и штрафом в 75 тыс. евро.

В Великобритании разработка мер по усилению мер безопасности в Интернете в настоящее время выдвинута на первый план. Безопасность персональных данных в СМИ обеспечивается жестким административным регулированием, введенным Законом о персональных данных 2018 г.⁹, а также уголовно-правовыми нормами. В целом современный этап можно охарактеризовать в первую очередь как движение в сторону обеспечения большей прозрачности крупных технологических компаний, действующих в цифровой сфере, выяснения источников и целей распространения ложной или вредной информации, источников финансирования такой информации, а также разработки быстрых способов ее блокирования и удаления.

В этих целях на правительственном уровне был разработан стратегический документ — Белая книга «Онлайн-вред»¹⁰. Опубликованию данного документа предшествовали теоретические разработки и изучение проблемы онлайн-вреда в комитетах парламента и в Комиссии по реформе права.

Так, в специальном отчете «Дезинформация и “фейковые” новости», рассмотренном в Палате общин в октябре 2018 г., были сформулированы 56 рекомендаций правительству для включения в Белую книгу, предполагающих, в частности, запрет для крупных технологических компаний расширяться в геометрической прогрессии без ограничений или надлежащего регуляторного надзора¹¹.

С учетом того что законодательные инструменты для контроля в Великобритании уже существуют (например, связанные с конфиденциальностью и защитой персональных данных, нормы антимонопольного и конкурентного права), было предложено перенести их на деятельность цифровых компаний. Сфера обработки персональных данных и их использования в политических кампаниях является важной и подлежащей контролю со стороны регуляторов. Таким образом, на технологические компании должна быть возложена полная ответственность за содержание информации, которую они предоставляют на своих платформах пользователям.

В отчете также была подчеркнута необходимость установления четких юридических обязательств технологических компаний по борьбе с вредным или незаконным контентом на их сайтах и введения независимого регулирования. Так, было предложено назначить независимого регулятора, ответственного за определение, что же представляет собой вредоносный контент, и обладающего полномочиями по контролю за соблюдением технологическими компаниями Кодекса этики. Такой Кодекс должен быть разработан техническими экспертами и содержать точные указания на то, что является или не является приемлемым в социальных сетях. Эти указания должны включать описание вредного и незаконного контента, о наличии которого пользователи будут сообщать компаниям, и который можно будет легко идентифицировать самим технологическим компаниям.

Одновременно предлагалось установить четкую юридическую ответственность для технологических компаний за несвоевременное удаление вредного и незаконного контента с их платформ. В связи с этим компаниям надлежит иметь соответствующие системы для выявления и устранения различных «видов вреда» и обеспечения структур по кибербезопасности. В случае несоблюдения компаниями (включая инженеров, занимающихся созданием программного обеспечения для компаний) своих обязательств или бездействия независимый регулятор должен иметь право возбуждения против них судебного разбирательства для наложения крупных штрафов. По мнению составителей отчета, выполняющий в настоящее время эти функции Уполномоченный по вопросам информации (The Information Commissioner's Office — ICO) также нуждается в расширении полномочий, чтобы он стал кем-то вроде эффективного «шерифа на Диком Западе Интернета».

Хотя Интернет дал широкие возможности для получения информации и общения с людьми во всем мире, он также способен искажать, вводить в заблуждение и вызывать ненависть и нестабильность, поскольку функционирует в масштабе и со скоростью, беспрецедентными в истории человечества. Кроме того, платформы социальных сетей используют алгоритмы с «эхо-камерами» (echo chambers) или

⁹ Data Protection Act 2018.

¹⁰ Online Harms White Paper. April 2019. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf.

¹¹ См.: House of Commons Digital, Culture, Media and Sport Committee Disinformation and “Fake News”: Final Report Eighth Report of Session 2017-19. 14 February 2019.

«фильтрационными пузырьками» (filter bubbles), когда пользователю предоставляется только один тип контента вместо всего диапазона голосов и мнений. Все это способствует распространению дезинформации, с гарантией, что пользователи не увидят опровержений или другой информации.

На момент подготовки правительственной стратегии Великобритании характерным является отсутствие согласованности в действующем уголовном законодательстве — в части преступлений, совершаемых онлайн и офлайн, а также наличие проблем, связанных с защитой жертв таких преступлений.

Данная несогласованность была выявлена и стала предметом глубокой озабоченности Комиссии по реформе права Англии и Уэльса (Law Commission for England and Wales), которая одновременно с британским парламентом по поручению Министерства по цифровым технологиям, культуре, средствам массовой информации и спорту и Министерства внутренних дел в преддверии издания Белой книги исследовала тему онлайн-вреда. В частности, специалист в области уголовного права профессор Дэвид Ормерод указал, что действующее уголовное законодательство не способно защитить людей, пострадавших в Интернете от оскорбительных сообщений, организованной и координированной массовой травли (“Pile on” harassment) в социальных сетях или злоупотреблений, связанных с нарушением конфиденциальности.

В опубликованном 1 ноября 2018 г. аналитическом отчете, посвященном оценке состояния уголовного права, Комиссия призвала к незамедлительной реформе и консолидации существующих уголовных законов¹². Впрочем, данный отчет был ограничен лишь тематикой запугивания и преследования в Интернете и не затрагивал других проблемных тем, связанных с использованием интернет-технологий (например, вопросов сексуальной эксплуатации детей, террористических преступлений или ответственности социальных сетей); этим вопросам будет посвящен следующий документ, над которым в настоящее время работает Комиссия.

Итак, в апреле 2019 г. официальная версия Белой книги была опубликована для последующих обсуждений и консультаций. Главная идея документа, как и ожидалось, касается возложения на интернет-компании обязанности удаления незаконного и причиняющего вред контента из социальных сетей и осуществления контроля за выполнением установленных требований специальным регулятором, который будет наделен широкими полномочиями по наложению санкций.

¹² См.: Reform of the Criminal Law Needed to Protect Victims from Online Abuse says Law Commission. 1 November 2018. URL: <https://www.lawcom.gov.uk/reform-of-the-criminal-law-needed-to-protect-victims-from-online-abuse-says-law-commission/>.

В этом стратегическом документе декларируются амбициозные планы относительно новой системы подотчетности и контроля над технологическими компаниями, выходящей далеко за рамки саморегулирования. Учитывая распространенность незаконного и вредного контента в Интернете, а также уровень обеспокоенности общественности по поводу онлайн-вреда не только в Великобритании, но и во всем мире, цифровая экономика срочно нуждается в новой нормативно-правовой базе для повышения безопасности граждан в Интернете¹³, которая должна восстановить доверие общества и четко определить обязанности компаний, предоставляющих онлайн-услуги.

Новая нормативно-правовая база прояснит обязанности компаний по обеспечению безопасности пользователей Интернета в Великобритании, особенно детей, с помощью наиболее эффективных мер по борьбе с вредным контентом и иной незаконной деятельностью. Как и предлагалось, за этим будет следить независимый регулятор, который установит четкие стандарты безопасности, подкрепленные требованиями к отчетности и эффективными полномочиями по обеспечению их соблюдения. В Белой книге отмечается также, что данный проект является первой попыткой в глобальном масштабе выработать единый и последовательный подход к всеобъемлющему спектру онлайн-вреда, в то время как другие страны вводили на законодательном уровне предписания, направленные на устранение конкретных видов вреда.

В современной Великобритании Интернет является неотъемлемой частью повседневной жизни многих людей, поскольку из десяти взрослых девять пользуются Интернетом¹⁴, это же относится к детям и молодежи: 99% детей в возрасте от 12 до 15 лет посещают Интернет, тратя в среднем 20,5 часов в неделю¹⁵.

Сегодня на передний план выдвигаются два направления — особое внимание предлагается уделить недопустимой и наиболее вредной информации, которая угрожает национальной безопасности или физической безопасности детей. Злоупотребления и издевательства, размещенные на онлайн-платформах, могут быть особенно вредны для детей из-за их по-

¹³ См.: Online Harms White Paper — Executive summary. 8 April 2019. URL: <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper-executive-summary--2>.

¹⁴ См.: Ofcom (2018). Adults’ Media Use and Attitudes Report. URL: https://www.ofcom.org.uk/__data/assets/pdf_file/0011/113222/Adults-Media-Use-and-Attitudes-Report-2018.pdf.

¹⁵ См.: Ofcom (2018). Children and Parents: Media Use and Attitudes Report. URL: <https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2018>.

тенциального воздействия на психическое здоровье и благополучие.

Вместе с тем разработчики Белой книги не предлагают какого-либо общего определения онлайн-вреда, подразделяя его на три категории в зависимости от наличия четкого законодательного запрета.

К первой категории вреда, который уже имеет законодательный запрет, относятся: сексуальная эксплуатация и надругательство над детьми; террористическая деятельность; организованная иммиграционная преступность; современное рабство; экстремальная порнография; порноместь; харасмент и киберсталкинг; разжигание ненависти; поощрение самоубийства или содействие ему; подстрекательство к насилию; продажа нелегальных товаров/услуг, таких как наркотики и оружие (в открытом Интернете); незаконно загруженная информация из тюрем; секстинг, т. е. создание, хранение, копирование или распространение непристойных или сексуальных изображений детей и молодежи в возрасте до 18 лет.

Ко второй категории онлайн-вреда, который не имеет четкого законодательного определения, относятся: кибербуллинг и троллинг; информация экстремистского содержания; принудительный контроль; запугивание; дезинформация; пропаганда насилия; призыв к самоповреждению; поощрение калечащих операций на женских половых органах.

К третьей категории онлайн-вреда предлагается относить информацию, доступ которой разрешен только взрослым пользователям: легальную порнографию; использование социальных сетей в возрасте до 13 лет и до 18 лет; использование приложений для онлайн-знакомств, а также чрезмерное время нахождения в Интернете.

При этом из содержания Белой книги следует, что в сферу ее действия не попадает онлайн-вред, который охватывается иными стратегическими документами. Например, вред, причиняемый организациям в связи с нарушением законодательства о конкуренции, большинством случаев нарушения прав интеллектуальной собственности и мошенничеством, поскольку данная незаконная деятельность является предметом рассмотрения иных инициативных правительственных проектов. Например, Объединенная рабочая группа по борьбе с мошенничеством (Joint Fraud Taskforce) возглавляет программу работы по борьбе с мошенничеством, в том числе онлайн-мошенничеством, на основе партнерства между банками, правоохранительными органами и правительством.

Все убытки, понесенные физическими лицами в результате непосредственного нарушения законодательства о защите персональных данных, являющиеся прямым результатом нарушения кибербезопасности или взлома, устраняются в рамках госу-

дарственной Стратегии национальной кибербезопасности (National Cyber Security Strategy 2016 to 2021)¹⁶.

Весь вред, причиняемый в темной паутине (dark web), а не в открытом Интернете, охватывается правительственной Стратегией борьбы с серьезной и организованной преступностью (Serious and Organised Crime Strategy)¹⁷.

Таким образом, можно констатировать, что новая стратегическая политика по безопасности в Интернете охватывает лишь ограниченный круг вопросов, предполагая усиление ответственности юридических лиц, и каких-либо рычагов для согласованности и реформы уголовного законодательства по защите от онлайн-вреда не содержит.

Вместе с тем, как и другие отрасли права, уголовное право с появлением Интернета получило новый импульс для своего развития, поскольку наряду с «традиционными» преступлениями появилась киберпреступность, которая быстро меняется и приобретает новые формы. Ее стремительному распространению, помимо прочего, способствуют три основных фактора — глобальные технологии, включая социальные сети и развитие новых форм коммуникации; появление у преступников возможности шифроваться и действовать анонимно, что затрудняет задачу по их выявлению; а также изменения в поведении людей, которые, не ощущая опасности и раскрывая свои персональные данные в силу незнания или легкомысленности, становятся жертвами таких преступлений.

Безусловно, государства, столкнувшиеся с онлайн-преступлениями, способными повлечь разрушительные последствия для жертв, в том числе для их психического здоровья и благополучия, вынуждены не только создавать новые правоохранительные структуры с дополнительными полномочиями, но и менять свою карательную политику, вводя составы онлайн-преступлений и ужесточая уголовно-правовые меры¹⁸. Как представляется, особый интерес законодательного регулирования уголовной ответственности за киберпреступления представляет опыт государств, имеющих высокую степень цифровизации, в частности, принадлежащих к семье общего права (Австралия, Великобритания, Канада, Новая Зеландия, США).

Следует отметить, что законодательство, направленное на противодействие использованию цифровых технологий в преступных целях, в Великобритании

¹⁶ URL: <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>.

¹⁷ URL: <https://www.gov.uk/government/publications/serious-and-organised-crime-strategy-2018>.

¹⁸ О современных направлениях криминализации в зарубежных странах см.: Криминализация и декриминализация как формы преобразования уголовного законодательства: монография / отв. ред. В.П. Кашенов. М., 2018. С. 208—273.

действует с момента издания Закона о злоупотреблении компьютером 1990 г.¹⁹ С этого времени в него неоднократно вносились изменения, направленные на ужесточение санкций за определенные преступные деяния, связанные с использованием современных технологий. Изменения касались как собственно киберпреступлений (Cyber-dependent crimes), так и традиционных деяний, совершенных с использованием компьютеров, компьютерных сетей или других форм коммуникационных технологий, используемых в качестве инструмента для достижения преступных намерений; дополнения часто содержат указания на способ совершения преступления или предполагают возможность использования современных технологий.

Однако большинство актов, устанавливающих уголовную ответственность за конкретные преступления, не содержат специальных указаний на цифровой способ их совершения. Поэтому в качестве ориентира британские правоохранительные органы используют опубликованное на сайте Королевской прокурорской службы (Crown Prosecution Service) Руководство по уголовному преследованию киберпреступности²⁰. Оно содержит пространные разъяснения относительно каждого из существующих в английском уголовном праве киберпреступлений, объединенных в особые группы: экономическая киберпреступность; вредоносные и оскорбительные сообщения; деяния, направленные против конкретных лиц (включая насилие против женщин и девочек); половые преступления против детей и неприличные изображения детей; экстремальная порнография, непристойные публикации и запрещенные изображения.

Безусловно, это вызвано некодифицированностью британского законодательства и разбросанностью уголовно-правовых норм по различным законодательным и подзаконным актам²¹. А поскольку в ближайшее время кодификация уголовного права не планируется, на первый план в Великобритании, правительство которой поставило задачу подготовки нового законодательства, обеспечивающего безопасность в Интернете²², выдвинута задача создания

одного или нескольких консолидирующих статутах, в которых были бы сосредоточены предписания, связанные с онлайн-преступностью.

Одним из таких проектов стал «Билль об уголовных преступлениях (Злоупотребление цифровыми технологиями и услугами) (консолидация)», находившийся в 2016 г. на рассмотрении в Палате общин²³. Хотя дальнейшего движения этот законопроект не получил, он представляет определенный интерес, поскольку в нем сделана первая попытка дать дефиницию цифрового преступления (digital crime), согласно которой таким деянием «является любое преступление, совершенное с использованием цифровых устройств, технологий, систем и услуг, в том числе в целях совершения или подготовки к совершению преступления, пособничества, подстрекательства, содействия или сокрытия преступления, или распоряжение доходами от преступления».

В законопроекте также предлагалось относить к цифровым преступлениям любое преступление против личности, когда цифровые устройства, технологии, системы и услуги используются, помимо прочего, в целях запугивания, преследования, совершения преступления на почве ненависти, злоупотреблений со стороны бывшего супруга или партнера (в том числе порноместь), совершения кражи личных данных, троллинга и груминга детей при подготовке к использованию их для сексуальной или другой формы эксплуатации.

Как видно из предложенного определения, дополнительный акцент сделан на преступлениях против личности, хотя в современной Великобритании в 2018 г. одним из наиболее часто совершаемых преступлений стало кибермошенничество. По мнению полиции Лондона, истинный масштаб этой проблемы может быть гораздо более значительным, поскольку отдельной статистики по преступлениям против бизнеса не ведется²⁴.

Одним из новых видов онлайн-преступлений стало романтическое мошенничество (online romance), связанное с использованием сайтов знакомств в целях получения персональной информации или денег. Обращает на себя внимание тот факт, что этот вид мошенничества стремительно нарастает не только в Великобритании, но и во всем мире, о чем свидетельствуют данные из разных стран. Например, в Гонконге, по данным полиции, за первые девять месяцев 2018 г. мошенники, специализирующиеся на онлайн-знакомствах, похитили у потерпевших 398 млн гонконгских долларов (примерно 51 млн долл. США), что в три раза превысило показатели 2017 г. Мошенники очень искусны как в психологических манипу-

¹⁹ Computer Misuse Act 1990; подробнее см.: Голованова Н.А. Уголовное право Англии: учеб. пособие для бакалавриата и магистратуры. М., 2017. С. 144—148; Семькина О.С. Противодействие киберпреступности за рубежом // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6. С. 104—113.

²⁰ Cybercrime — prosecution guidance. Legal Guidance, Cyber / online crime. URL: <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>.

²¹ См. подробнее: Голованова Н.А. К вопросу о классификации источников современного английского уголовного права // Журнал российского права. 2014. № 11. С. 96—106.

²² New Laws to make Social Media Safer. 20 May 2018. URL: <https://www.gov.uk/government/news/new-laws-to-make-social-media-safer>.

²³ Criminal Offences (Misuse of Digital Technologies and Services) (Consolidation) Bill (HC Bill 151).

²⁴ См.: ONS crime stats: fraud & cyber crime still dominate. URL: <https://www.techuk.org/insights/news/item/13518-ons-crime-stats-fraud-cyber-crime-still-dominate>.

ляциях, так и в использовании онлайн-технологий, эксплуатируя естественные человеческие потребности в общении с любимым человеком²⁵.

Как отмечает полиция Финляндии, 90% жертв романтического мошенничества составляют женщины в возрасте 45—74 лет; с половиной всех жертв первоначально связь устанавливалась через Facebook; с остальными потерпевшими преступники связывались через сайты знакомств и чаты; почти все жертвы не имеют семей²⁶. В Австралии романтическое мошенничество в 2016 г. стало вторым по величине причиненного ущерба видом мошенничества (42 млн австралийских долларов)²⁷.

Но если романтическое мошенничество обычно преследуется в уголовном порядке в соответствии с уже имеющимся законодательством, то противодействие преступлениям, связанным с кибербуллингом, порнографией и сексуальной эксплуатацией и насилием над детьми в Интернете, потребовало дальнейшего законодательного регулирования.

С распространением Интернета преступление, связанное с травлей в социальных сетях, называемое кибербуллингом, оказалось еще более жесткой формой запугивания или издевательств, чем уже известный буллинг²⁸, вызывая у жертвы сильный стресс и отчаяние, доводя жертву до мыслей о самоубийстве, особенно когда речь идет о детях и подростках. Ведь аудитория онлайн-издевательств может возрасти до неопределенного числа получателей такой информации, а исполнитель при этом может остаться анонимным. Еще один очевидный урок погружения в проблемы кибербуллинга — это осознание того разрыва, который существует между молодым и старшим поколениями в отношении технологий и способов общения людей. Появление социальных сетей глубоко изменило взаимодействие и связь людей с внешним миром. Взрослые часто не справляются как с новыми технологиями, так и с языком социальных сетей, и разрыв между молодыми и старыми, а также между родителями и детьми становится очень велик. Для многих молодых людей «виртуальная реальность» является их реальностью, а жизнь проходит онлайн в таких местах, как Facebook, Twitter, чатах и в бесконечном потоке текстовых сообщений и электронных писем.

²⁵ См.: Police warned people to be alert when making friends online and to take any request to send money as sign of a scam. URL: <https://www.scmp.com/news/hong-kong/law-and-crime/article/2177139/huge-explosion-online-romance-scams-hong-kong-2018>.

²⁶ См.: Online Romance Scams. URL: <https://www.riku.fi/en/various+crimes/property+crime/fraud/online+romance+scams>.

²⁷ URL: https://www.police.nsw.gov.au/crime/frauds_and_scams/fraud_categories/dating_and_romance_scams.

²⁸ Подробнее об ответственности за буллинг см.: Голованова Н.А. Проблемы борьбы с буллингом // Журнал российского права. 2018. № 8. С. 113—123.

Для борьбы с опасностями кибербуллинга взрослые должны лучше понимать ту жизненно важную роль социальных сетей, «виртуальной реальности», которые могут быть для молодежи важнее, чем природа и даже настоящие окружающие их люди. Трансформирующий, даже революционный характер социальных сетей и их влияние, особенно на молодых людей, заслуживает глубокого изучения.

Возможности, предоставляемые сегодняшними и будущими технологиями, впечатляют, однако новая технология также может стать мощным оружием, используемым в целях причинения вреда. Буллинг в школах и других учебных заведениях существует очень давно, но совсем недавно стал признаваться проблемой, требующей законодательных мер.

Буллинг и кибербуллинг поднимают некоторые из самых больших и самых сложных проблем в обществе. В основе проблемы издевательств лежит необходимость поддержания уважительных и ответственных отношений между молодежью и обществом в целом. Речь идет о ценностях общества (или их потере), о нарушении уважения к другим людям и необходимости того, чтобы граждане, молодые и старые, брали на себя ответственность за свои действия и бездействие. Во многих случаях мишенями являются молодые люди, которые уже изолированы, потому что они отличаются от большинства учащихся.

Это различие может основываться на поле, расе, сексуальной ориентации, происхождении аборигенов, инвалидности или любых других характеристиках, которые выделяют их. Не «вписаться» в школу и не стать частью «в толпе» — тяжелое бремя, которое нужно нести, и издеательства усиливают это чувство отчужденности. Это весьма сложное явление, поскольку хулиганы, жертвы и свидетели часто взаимозаменяемы, а сегодняшние жертвы могут стать хулиганами завтрашнего дня. Исследования показывают, что жертвы кибербуллинга испытывают серьезные медицинские и другие последствия. Это связано с рядом негативных результатов, таких как высокий уровень тревоги, суицидальные мысли, депрессия и психосоматические проблемы, а также поведенческие проблемы, такие как агрессивное поведение и чрезмерное употребление алкоголя. Кроме того, исследования показали, что жертвы кибербуллинга испытывают более серьезные последствия для психического здоровья, чем жертвы традиционных издевательств. Например, исследование, проведенное в Австралии и Швейцарии в 2010 г., в котором участвовали 374 швейцарских подростка и 1320 австралийских подростков, показало, что у подростков, ставших жертвами кибербуллинга, отмечались значительно более высокие уровни депрессивных симптомов, чем у жертв традиционного издеательства²⁹.

²⁹ См.: Perren S. et al. Bullying in School and Cyberspace: Associations with Depressive Symptoms in Swiss and Australian

К аналогичному выводу пришли авторы еще одного австралийского исследования, проведенного в 2012 г., согласно которому жертвы кибербуллинга испытывали большие социальные трудности и более высокий уровень тревоги и депрессии, чем жертвы традиционного буллинга³⁰.

Анонимность, доступная преследователю, еще больше усложняет картину, поскольку устраняет традиционное требование дисбаланса власти между хулиганом и жертвой и затрудняет проверку личности преступника. Поскольку отправители электронных издевательств или почты, содержащей человеконенавистнические высказывания, не видят реакцию получателя, они могут не замечать причиненного ими вреда. Другим результатом анонимности в Интернете является то, что учителя все чаще становятся мишенями: каждый пятый учитель³¹.

Проблема кибербуллинга в наши дни стала бедствием во многих развитых государствах. Об этом говорят исследователи из разных стран, например австралийские ученые Коллет Лангос и Рик Сарре³² считают, что кибербуллинг значительно отличается от традиционной травли, поскольку этому способствуют информационно-коммуникационные технологии. Использование таких технологий развивает у хулигана ощущения защиты от последствий запугивающих действий. Наличие «экрана» может действовать в качестве «разъединения» (разделителя) между онлайн-действиями и «реальными» последствиями этих действий, которые также могут способствовать «отторжению» преступника. Для описания такого состояния авторы употребляют термин «дезингибирование» (т. е. эйфоризирующий эффект, снижение самоконтроля), под которым понимается отсутствие торможения. Дезингибирование в данном случае означает неспособность контролировать импульсивное поведение, мысли или чувства. При использовании Интернета оно проявляется в том, что при общении онлайн люди делают то, что не делают в реальной жизни.

Режим онлайн позволяет преступнику чувствовать себя приободренным в результате использова-

ния дезинформации, потому что «требуется меньше энергии и силы, чтобы выразить вредные комментарии с помощью клавиатуры, чем голосом». Преступник, который защищен от визуальной или слуховой реакции своей жертвы наличием экрана, менее подвержен влиянию эмпатии, сопереживанию. Поэтому ему относительно легко причинить боль другому человеку, страдания которого не видны, и действия, причиняющие вред, физически и временно отдалены от их последствий.

Возникает вопрос: какими правовыми средствами в этом случае должен воспользоваться потерпевший? Трагическая серия молодежных самоубийств в Новой Шотландии (Канада) сначала послужила толчком к созданию в 2011 г. Целевой группы для изучения проблем кибербуллинга³³, а затем и к принятию первого в Канаде Закона о кибербезопасности 2013 г.³⁴, который предусмотрел возможность обращения жертвы кибербуллинга в суд в гражданском порядке с иском о возмещении ущерба. В Новой Шотландии также было создано первое канадское подразделение CyberSCAN по расследованию таких случаев, которое работает с жертвами, семьями, школами и др., расследуя жалобы, собирая доказательства, и оказывает помощь в прекращении запугивания в Интернете.

Однако некоторые специалисты из США считают, что ситуация с кибербуллингом в школах требует признания его отдельным преступлением, которое должно преследоваться в системе уголовного правосудия³⁵. Законодательная практика отдельных юрисдикций США уже следует в этом направлении, например, в штате Невада рассылка электронных сообщений с целью запугивания, причинения тревоги, паники, вмешательства в работу государственной школы с целью вызвать панику или гражданские беспорядки с 2010 г. преследуется в уголовном порядке³⁶.

В Австралии кибербуллинг как таковой не нашел определения в законодательстве и не преследуется в качестве отдельного преступления. Действительно, нет конкретного закона, криминализирующего это явление.

Тем не менее австралийские исследователи выделяют несколько его форм³⁷:

Adolescents // Child and Adolescent Psychiatry and Mental Health, 2010, vol. 4, no. 1, p. 28.

³⁰ См.: Campbell M. Victims' Perceptions of Traditional and Cyberbullying, and the Psychological Correlates of their Victimization // Emotional and Behavioural Difficulties, 2012, vol. 17, iss. 3, no. 1, pp. 389, 398.

³¹ См.: Mishna F. et al. The Ongoing Problem of Bullying in Canada: A Ten-Year Perspective // Canadian Social Work, 2010, vol. 12, no. 2, p. 43; Shariff S. Confronting Cyberbullying: What Schools Need to Know to Control Misconduct and Avoid Legal Consequences. New York, 2009.

³² См.: Langos C., Sarre R. Responding to Cyberbullying: the Case for Family Conferencing // Deakin Law Review, 2015, vol. 20, no. 2.

³³ См.: MacKay A.W. Op. cit.

³⁴ Cyber-safety Act SNS 2013, с 2.

³⁵ См.: Barge J.D. Policy for Prohibiting Bullying, Harassment and Intimidation. URL: https://www.gadoe.org/Curriculum-Instruction-and-Assessment/Curriculum-and-Instruction/Documents/GaDOE%20Bullying%20Policy_August%202011.pdf.

³⁶ Nevada Code 2010 Title 34 Education. Ch. 392 Pupils. NRS 392.915. URL: <https://law.justia.com/codes/nevada/2010/title34/chapter392/nrs392-915.html>.

³⁷ URL: <https://doi.org/10.21153/dlr2015vol20no2art525>.

запугивание (harassment) — неоднократная отправка оскорбительных сообщений;

киберсталкинг (cyberstalking) — интенсивные преследования и клевета, которые включают угрозы или создают значительный страх у жертвы. Запугивание становится киберсталкингом, когда жертва опасается за свою личную безопасность;

клевета (denigration) может включать в себя оскорбительный комментарий, она может происходить вербально или включать распространение оскорбительного, сексуального или несексуального изображения;

остракизм (exclusion, cyberostracism) — жертва преднамеренно исключается из доступа в онлайн-зоны, такие как определенный чат или дискуссионная группа, участниками этих онлайн-доменов;

обман (outing and trickery) — с помощью манипулирования жертвой преступник получает информацию, которую затем публикует, чтобы унижить жертву;

использование чужого имени или маскировка (impersonation or masquerading) — преступник притворяется жертвой и посылает оскорбительное сообщение, которое, похоже, исходит от жертвы;

«счастливая пощечина» (happy slapping), или «избиение ради развлечения» — съемка физического нападения на жертву и последующее распространение фильма, чтобы публично унижить жертву. Этот вид «развлечений» городских банд, появившийся в Англии накануне 2005 г., обычно направлен против случайных прохожих, которых вначале бьют по лицу, сбивают с ног, а затем избивают, записывая избиение на телефон или камеру. Первоначально, как и следовало ожидать от названия, нападения были довольно незначительными розыгрышами. Но по мере того, как повальное увлечение распространялось, нападения становились все более жестокими с причинением тяжких телесных повреждений. Атаки, которые были спонтанными на школьных площадках или в общественном транспорте, стали более организованными, часто проводились в районах, где камеры видеонаблюдения или свидетели не могли их зафиксировать³⁸. Этот вид кибербуллинга нашел своих последователей и в России. Как указывают Ж.Б. Киреева, Н.В. Петрашева, в Новосибирске в 2016 г. трое подростков ногами в область головы избили бездомного и выложили видео в Интернет под язвительным названием «урок вежливости»³⁹.

И хотя, как отмечалось выше, специальной нормы о кибербуллинге в австралийском законодательстве нет, такие правонарушения в большинстве слу-

чаев могут преследоваться в уголовном порядке на основании существующих преступлений по законам штатов и федеральным законам. Примечательно, что в Южной Австралии в 2013 г. был принят Закон о кино съемках, который дополнил законодательство 1953 г. о преступлениях, рассматриваемых в суммарном порядке⁴⁰. В частности, новый Закон установил запрет на съемку лица без его согласия, с последующим распространением фильма с использованием информационных технологий. В настоящее время этот Закон охватывает съемку и распространение любого поведения, которое считается «унизительным или унижающим достоинство», и таким образом всесторонне регулирует одну из наиболее серьезных форм кибербуллинга — Happy slapping. Южная Австралия стала первой юрисдикцией в Австралии, принявшей такое законодательство. Виновный подлежит наказанию в виде штрафа в сумме 10 тыс. австралийских долларов или тюремного заключения на срок до двух лет.

Что касается несовершеннолетних правонарушителей, виновных в кибербуллинге, то, как и во всех других юрисдикциях Австралии, система ювенальной юстиции обеспечивает особую защиту молодежи в возрасте до 18 лет с учетом их потребностей. Так, Закон Южной Австралии о несовершеннолетних правонарушителях 1993 г. распространяется на молодых людей в возрасте старше 10, но моложе 18 лет; лицо, не достигшее 10-летнего возраста, не может быть привлечено к уголовной ответственности. Доктрина общего права *doli incapax* применяется к молодежи в возрасте от 10 до 14 лет во всех юрисдикциях Австралии. Однако считается, что молодой человек от 15 до 17 лет достиг зрелости и несет полную ответственность за свои действия в соответствии с уголовным законодательством.

Особое внимание уделяется реституции жертвам, укреплению отношений (особенно семейных отношений) и предотвращению нарушения работы несовершеннолетнего правонарушителя или ухудшения чувства расовой, этнической или культурной самобытности несовершеннолетнего. В соответствии с Законом многоуровневая система досудебных процедур применяется для рассмотрения всех преступлений несовершеннолетних; эти правонарушения хотя и могут включать в себя основные преступления, предъявляемые по обвинению, но на практике по большей части являются «незначительными» преступлениями.

В зависимости от тяжести «незначительного» преступления молодому человеку может быть вынесено «неформальное» или «формальное» предупреждение. «Неформальное» предупреждение не влечет су-

³⁸ URL: <https://www.phrases.org.uk/meanings/170890.html>.

³⁹ См.: Киреева Ж.Б., Петрашева Н.В. Социальная обусловленность криминализации отдельных видов общественно опасных посягательств // Журнал правовых и экономических исследований. 2017. № 1. С. 58—62.

⁴⁰ Summary Offences (Filming Offences) Amendment Act 2013 (SA). The Act amends Part 5A of the Summary Offences Act 1953 (SA).

димости и может быть использовано только с согласия молодого человека. Оно может быть применено за «тривиальные» преступления, когда сотрудник полиции считает, что данный вопрос не требует каких-либо формальных действий. Поэтому неофициальное предупреждение включает элемент усмотрения со стороны присутствующего сотрудника полиции.

«Формальное» предупреждение обычно подразумевает какое-либо обязательство: принесение извинения жертве и (или) выполнение общественных работ. Оно должно быть оформлено в письменном виде и признано правонарушителем (также в письменной форме) и, если это практически возможно, должно осуществляться в присутствии родителя или опекуна несовершеннолетнего. Отказ несовершеннолетнего правонарушителя от «формального» предупреждения (например, от обязательства принести извинения жертве) может привести к передаче дела на рассмотрение так называемой семейной конференции, системы, принятой в 1994 г. в Южной Австралии и в других районах Австралии вслед за Новой Зеландией.

Семейная конференция — это механизм восстановительного правосудия, направленный на то, чтобы, не вовлекая несовершеннолетнего в систему уголовного правосудия, обсудить действия правонарушителя, его влияние на жертву, а также достичь определенного результата, например выплаты компенсации, принесение извинений или привлечение правонарушителя к участию в общественных работах (не более 300 часов) и т. п.

Еще одной из форм кибербуллинга, которая стала подлежать преследованию и наказанию в уголовном порядке за рубежом, является *порноместь* — обнаружение в Интернете интимных фотографий или видео без согласия изображенного лица с целью причинения ему тревоги или страданий. Такого рода оскорбительные деяния чаще всего совершаются бывшими супругами или партнерами; нередко угрозы публикации таких изображений сопровождаются шантажом и вымогательством.

В США первоначально было принято считать, что *порноместь* является той областью, где уголовное законодательство не в состоянии идти в ногу с техническим и социальным прогрессом и адекватно противостоять подобным злоупотреблениям, предлагалось использовать другие средства правовой защиты, в частности гражданско-правовые. Однако со временем ситуация в США изменилась, а первыми штатами, которые ввели уголовную ответственность за *порноместь*, стали Нью-Джерси и Калифорния⁴¹.

В наши дни криминализация *порноместь* стала обычным явлением. Так, в Канаде в 2014 г. несанкционированное распространение интимных изображений было криминализировано после принятия Закона о защите канадцев от онлайн-преступности⁴². В соответствии с ним уголовной ответственности подлежит каждый, кто сознательно публикует, распространяет, передает, продает, делает доступным или рекламирует интимный образ человека, зная, что последний не дает своего согласия на такие действия либо согласился на них необдуманно (ст. 162.1 УК Канады). Лицу, виновному в совершении данного преступления, грозит наказание в виде лишения свободы на срок до пяти лет.

Кроме того, Закон предусматривает удаление таких изображений из Интернета и возмещение расходов, связанных с их удалением, за счет нарушителя, конфискацию имущества, использованного для совершения преступления, издание судом постановления, запрещающего правонарушителю выезжать за границу в целях предотвращения распространения таких изображений, а также ограничение использования осужденным компьютера или Интернета.

В Новой Зеландии Закон о вредных цифровых сообщениях 2015 г.⁴³ был издан как конкретный политический ответ на кибербуллинг, онлайн запугивание и преследование (*harassment*) и *порноместь*, он установил специальный режим, применяемый только к онлайн-публикациям, причиняющим серьезный эмоциональный вред.

По мнению новозеландского профессора Урсулы Чир, в основу Закона положены 10 принципов, согласно которым цифровое сообщение не должно: нарушать конфиденциальность других людей; носить угрожающий или оскорбительный характер, содержать непристойности, лживые утверждения, раскрывать сведения, полученные в качестве доверительных; подстрекать других к отправке подобных сообщений; подстрекать или поощрять человека к самоубийству; порочить человека в связи с его (ее) цветом кожи, расой, этническим или национальным происхождением, религией, полом, сексуальной ориентацией или инвалидностью⁴⁴.

Нарушение данного Закона наказывается лишением свободы на срок до двух лет или штрафом. Предусмотрено также, что при рассмотрении дела суд может принять во внимание любые факторы, которые он сочтет важными, включая: анализ использованных выражений; возраст и характеристики жертвы; анонимность; повторность; степень распространения

⁴² Protecting Canadians from Online Crime Act 2014.

⁴³ Harmful Digital Communications Act 2015.

⁴⁴ См.: *Cheer U.* Abusive and Offensive Communications: the Criminal Law of New Zealand. URL: <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/11/New-Zealand-U-Cheer.pdf>.

⁴¹ *Salter M., Crofts T.* Responding to Revenge Porn: Challenges to online Legal Impunity. URL: https://www.academia.edu/7833345/Responding_to_revenge_porn_Challenges_to_online_legal_impunity.

цифрового сообщения; ложность; контекст, в котором оно появилось.

В Великобритании, где существуют различные юрисдикции, согласно разъяснениям Королевской прокурорской службы Великобритании вредоносные и оскорбительные сообщения (в том числе сообщения, отправленные через социальные сети; кибербуллинг/троллинг; виртуальный моббинг) относятся к киберпреступлениям. В Англии и Уэльсе отдельного закона нет, поэтому подобные деяния могут преследоваться в уголовном порядке на основании Закона о злонамеренных коммуникациях 1988 г.⁴⁵ и ст. 127 Закона о связи 2003 г.⁴⁶ В Шотландии уголовная ответственность за публикацию фотографии или фильма, в том числе в цифровой форме, с изображением человека в интимной ситуации либо угрозу опубликования была введена Законом об оскорбительном поведении и причинении сексуального вреда 2016 г.⁴⁷

Сходный закон был принят в 2018 г. в Австралии. Федеральный закон об усилении онлайн-безопасности (распространение интимных изображений без согласия)⁴⁸ внес ряд изменений в действующее законодательство — в Закон об усилении онлайн-безопасности 2015 г.⁴⁹ и в федеральный УК 1995 г.

Еще одна проблема, которая заслуживает особого внимания, связана с обеспечением онлайн-безопасности детей. Сегодня, когда дети и подростки проводят много времени в Интернете, часто раскрывая личную информацию, касающуюся их места жительства, школы, фамилий, она может быть использована преступниками-педофилами для манипулирования жертвами и установления с ними отношений. Поскольку киберпространство имеет потенциал, позволяющий правонарушителям одновременно посягать на сотни детей, дети в результате такого контакта могут подвергаться угрозам и запугиванию. Компрометирующая информация может быть опубликована на различных онлайн-платформах, доступных другим лицам, на сайтах социальных сетей, на многопользовательских игровых порталах и других веб-форумах⁵⁰.

В целях защиты несовершеннолетних от сексуальных посягательств в Интернете в зарубежных

странах можно выявить тенденцию к дальнейшему ужесточению мер уголовной ответственности. Например, канадский законодатель счел необходимым обеспечить дополнительную защиту детей от сексуальной эксплуатации путем криминализации таких деяний, как детский секс-туризм, передача, обеспечение доступа либо распространение детской порнографии посредством Интернета, умышленное нахождение на сайтах, являющихся источником распространения детской порнографии, заманивание ребенка (*luring a child*) для последующих встреч с помощью компьютерных технологий, а также упростил процедуру привлечения этих лиц к уголовной ответственности (ст. 172.1 УК Канады)⁵¹.

Предметом большой общественной озабоченности в Великобритании также стал вопрос о сексуальной эксплуатации детей с использованием онлайн-технологий. В документе, посвященном вопросам борьбы с сексуальной эксплуатацией детей, опубликованном британским правительством в 2017 г., отмечается особая обеспокоенность общества сложившейся ситуацией⁵². В последние годы, учитывая особый рост числа подобных преступлений, британский законодатель уже резко ужесточил санкции за ряд половых преступлений и ввел новые составы, связанные с владением и размещением в Интернете экстремальных порнографических изображений жестоких половых актов, угрожающих жизни человека или способных привести к серьезным травмам, изображений зоофилии или некрофилии, с незаконным использованием интимных фотографий и фильмов сексуального характера, владением порнографическими изображениями изнасилований и т. д.

В целях защиты детей в 2015 г. была введена уголовная ответственность за такое новое для Великобритании преступление, как сексуальный груминг детей (*grooming*) в Интернете с целью дальнейших контактов с ними⁵³. Термин «груминг» (производное от *groom* — жених) в контексте сексуальной эксплуатации детей впервые был использован в 1985 г. в статье “Chicago Tribune”, посвященной методам, используемым педофилами⁵⁴. С распространением Интернета в 1990-х гг. этот термин получил негативный и бранный оттенок и стал повсеместно применяться (войдя в многочислен-

⁴⁵ Malicious Communications Act 1988.

⁴⁶ Communications Act 2003; подробнее см.: *Gillespie A. Obscene Conversation, the Internet and the Criminal Law // The Criminal Law Review*, 2014, iss. 5, pp. 350—368.

⁴⁷ Abusive Behaviour and Sexual Harm (Scotland) Act 2016.

⁴⁸ Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018.

⁴⁹ Enhancing Online Safety Act 2015.

⁵⁰ Child Sexual Abuse: Guidelines on Prosecuting Cases of Child Sexual Abuse. URL: <https://www.cps.gov.uk/legal-guidance/child-sexual-abuse-guidelines-prosecuting-cases-child-sexual-abuse>.

⁵¹ См.: *Чернухина Л.С.* Соотношение федерального и провинциального законодательства Канады в области защиты детей от домашнего насилия // Журнал зарубежного законодательства и сравнительного правоведения. 2016. № 6.

⁵² См.: Tackling Child Sexual Exploitation: Progress Report. 16 February 2017. URL: <https://www.gov.uk/government/publications/tackling-child-sexual-exploitation-progress-report>.

⁵³ Serious Crime Act 2015.

⁵⁴ См.: Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review. 2017. URL: https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf.

ные словари, включая Кембриджский словарь для продвинутых учащихся и Оксфордский словарь английского языка) для определения незаконной «дружбы», общения с ребенком особенно через интернет-чат с целью убедить его вступить в сексуальные отношения.

В отчете Международного центра пропавших и эксплуатируемых детей 2017 г. отмечено, что сексуальный груминг в отношении детей с помощью Интернета и связанных с ним технологий является растущей мировой проблемой. Бесчисленное количество детей подвергается риску сексуального насилия и различным формам эксплуатации, например, в связи с созданием материалов о сексуальном насилии над детьми или прямой трансляцией изнасилования.

Современное уголовное законодательство многих зарубежных государств предусматривает ответственность за такие действия, хотя термин «груминг» используется не всегда. Чаще всего уголовные законы идут по пути перечисления запрещенных действий, например «онлайн-общение с ребенком с последующей встречей», «онлайн-общение с ребенком без последующей встречи», «онлайн-разговоры на сексуальные темы», «онлайн-демонстрация детям взрослой порнографии», «давление на ребенка или принуждение его к созданию сексуального образа». Вместе с тем, как отмечается в упомянутом отчете, крайне важно, чтобы законодательство об онлайн-груминге криминализировало все его виды, независимо от того, намерен преступник перевести отношения в автономный режим или нет, поскольку все большее число случаев груминга происходит полностью онлайн⁵⁵. Такое предложение содержалось, например, в пояснительной записке к ирландскому законопроекту о введении уголовной ответственности за груминг детей 2014 г. (Criminal Law (Child Grooming) Bill)⁵⁶. Однако позднее ирландский законодатель отказался от использования нормы о груминге и сформулировал норму более широко — использование информационных и коммуникационных технологий для облегчения сексуальной эксплуатации ребенка (ст. 8 Закона Ирландской Республики об уголовном праве (половые преступления) 2017 г.⁵⁷), сохранив, однако, предлагавшуюся ранее максимальную санкцию в виде лишения свободы на срок до 14 лет.

Еще одним новым преступлением, ответственность за которое также была установлена в 2015 г. в Великобритании, стало владение «справочником педофила» (possession of paedophile manual), т. е. руководством по совращению ребенка или любым материалом, содержащим советы или рекомендации по сексуальному насилию над детьми. Под «справочни-

ком педофила» закон понимает как материальные, так и электронные документы (например, письма или информацию, загруженную в компьютер). Бремя доказывания в таких случаях возлагается на обвиняемого. Виновный может быть наказан тюремным заключением на срок до трех лет.

Выступая в 2018 г. на слушаниях в парламенте Великобритании, Уилл Керр, бывший в то время главой команды по борьбе с преступлениями против уязвимых жертв Национального агентства по борьбе с преступностью (National Crime Agency — NCA), указал, что одновременно онлайн могут совершаться несколько преступлений, и не только связанных с созданием и распространением непристойных изображений детей, но и изнасилование ребенка в другой стране (например, на Филиппинах, в Таиланде или Камбодже), заказанное преступником по Интернету. По мнению Керра, все труднее четко разграничивать онлайн- и офлайн-преступления, поскольку границы этих преступных деяний стали размываться, хотя при совершении подобных преступлений Интернет продолжает играть доминирующую роль⁵⁸. С этим выводом трудно не согласиться.

Отвратительным примером подобного преступления стало дело Ричарда Хакла, которого средства массовой информации назвали «худшим из когда-либо существовавших британских педофилов». В 2016 г. этот 30-летний мужчина признал себя виновным в 71 изнасиловании, сексуальном нападении и других формах жестокого обращения с 23 детьми младшего возраста в период с 2006 по 2014 г. в бедной общине Куала-Лумпура в Малайзии, куда он внедрился под видом благотворительности.

Во время слушания дела суд отметил, что в размещенной в сети книге Хакла даны подробные описания 200 детей, подвергшихся насилию. Хакл публиковал онлайн свои взгляды на легитимность педофилии, описывая педофилов как несправедливо подавляемое меньшинство, и хвастался своими подвигами в течение 18-месячного периода. Он подготовил руководство для педофилов с советами, как найти жертву и избежать разоблачения. Стремясь извлечь выгоду из своих преступлений, он размещал фотографии детей на веб-сайте под названием “PedoFunding”⁵⁹.

Считается, что Великобритания после США и Канады является третьим по величине потребителем в мире изображений сексуального насилия над детьми, и полиция ежемесячно «арестовывает примерно 450 мужчин, защищая 700 детей»⁶⁰. В целях выяв-

⁵⁸ См.: Oral evidence: Policing for the Future, HC 515. Tuesday, 13 March 2018. URL: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/policing-for-the-future/oral/80543.html>.

⁵⁹ URL: <https://www.2harecourt.com/2016/06/03/brian-oneill-qc-prosecutes-britains-worst-ever-paedophile/>.

⁶⁰ Oral evidence: Policing for the Future, HC 515. Tuesday, 13 March 2018.

⁵⁵ Online Grooming of Children for Sexual Purposes.

⁵⁶ An Bille um an Dlí Coiríúil (Grúmaeireacht Leanaí), 2014 Criminal Law (Child Grooming) Bill 2014. URL: <https://data.oireachtas.ie/ie/oireachtas/bill/2014/89/eng/initiated/b8914d.pdf>.

⁵⁷ Criminal Law (sexual offences) Act 2017.

ления и уголовного преследования этих преступлений в Национальном агентстве по борьбе с преступностью Великобритании в 2006 г. была создана специальная команда специалистов по онлайн-защите детей от эксплуатации (Child Exploitation and Online Protection — CEOP)⁶¹, в функции которой входит выявление основных угроз и координация противодействия на национальном и международном уровнях.

Одним из новых преступных проявлений стал такой феномен, упоминаемый в Докладе Европола 2017 г.⁶², как сексуальное принуждение и вымогательство у детей в Интернете (online sexual coercion and extortion of children). Частично это преступление совпадает с онлайн-грумингом, однако в отличие от него преступления по финансовым мотивам совершаются не одиночками, а в основном организованными группами, находящимися за пределами ЕС. Этот вид преступлений как одно из новых явлений цифровой эпохи изучен недостаточно и нуждается в разработке законодательных и превентивных стратегий. Дети не являются основной целью шантажа и вымогательства в Интернете, однако они страдают более других, поскольку становятся наиболее уязвимой группой.

Несмотря на все предпринимаемые усилия, в Стратегии Соединенного Королевства по борьбе с серьезной и организованной преступностью 2018 г. было признано, что значительная часть сексуальной эксплуатации и надругательств над детьми, особенно в Интернете, продолжает оставаться латентной⁶³. Хотя значительная доля жестокого обращения с детьми, по утверждению министра внутренних дел Великобритании Саджида Джавида, происходит в семьях, за последние пять лет количество онлайн-изображений насилия над детьми увеличилось на 700%, и 80 тыс. человек в Великобритании представляют определенную сексуальную угрозу для детей в Интернете, при-

чем публикуемые материалы все чаще касаются детей младшего возраста⁶⁴.

Как уже было упомянуто в начале статьи, это вынудило правительство Великобритании подготовить стратегический документ — Белую книгу «Онлайн-вред» с целью дальнейшей разработки нового законодательства, предусматривающего усиление уголовной ответственности «веб-гигантов», не удаляющих со своих платформ контент о насилии над детьми. И это несмотря на принятие Закона о персональных данных, который уже предусматривает гигантские штрафы для компаний за нарушение установленных правил — максимальный штраф может составить 17 млн фунтов стерлингов или 4% от общего годового оборотного капитала предприятия, в зависимости от того, что больше. Предполагается также создание фонда в размере 250 тыс. фунтов стерлингов для поддержки новых идей по выявлению и пресечению сексуального насилия над детьми онлайн⁶⁵.

Оценивая законодательное регулирование последних лет в странах, принадлежащих к семье общего права, отметим, во-первых, нарастающую криминализацию новых форм онлайн-преступлений, связанных с травлей, издевательствами и запугиванием, посягающих на права личности в цифровом мире и особо направленных на сексуальную эксплуатацию детей, а, во-вторых, ужесточение уже имеющегося уголовного законодательства, устанавливающего ответственность не только физических, но и юридических лиц, в частности провайдеров веб-услуг.

Выявленная тенденция развития законодательства в зарубежных странах, и в частности в Великобритании, обусловлена не только данью международным обязательствам этих государств, присоединившихся, например, к Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуального насилия (CETS N 201), но и реально существующей угрозой причинения вреда миллионам пользователей в связи с бесконтрольным развитием Интернета.

⁶¹ URL: <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/child-exploitation-online-protection-ceop>.

⁶² См.: Online Sexual Coercion and Extortion as a Form of Crime Affecting Children / Law Enforcement Perspective. 2017. URL: <https://www.europol.europa.eu/publications-documents/online-sexual-coercion-and-extortion-form-of-crime-affecting-children-law-enforcement-perspective>.

⁶³ См.: Serious and Organised Crime Strategy. November 2018. URL: <https://www.gov.uk/government/publications/serious-and-organised-crime-strategy-2018>.

⁶⁴ См.: Home Office, Speech by the Home Secretary: Keeping our children safe, 3 September 2018. URL: <https://www.gov.uk/government/speeches/keeping-our-children-safe>.

⁶⁵ См.: Government response to the Internet Safety Strategy Green Paper. May 2018. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Barge J.D. Policy for Prohibiting Bullying, Harassment and Intimidation. URL: https://www.gadoe.org/Curriculum-Instruction-and-Assessment/Curriculum-and-Instruction/Documents/GaDOE%20Bullying%20Policy_August%202011.pdf.

Campbell M. Victims' Perceptions of Traditional and Cyberbullying, and the Psychological Correlates of their Victimisation // Emotional and Behavioural Difficulties, 2012, vol. 17, iss. 3, no. 1.

Cheer U. Abusive and Offensive Communications: the Criminal Law of New Zealand. URL: <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/11/New-Zealand-U-Cheer.pdf>.

Fake news: da oggi puoi segnalarle alla Polizia. URL: <https://www.poliziadistato.it/articolo/155a6077fdb05e3865595940>.

- Gillespie A. Obscene Conversation, the Internet and the Criminal Law // *The Criminal Law Review*, 2014. iss. 5.
- Government response to the Internet Safety Strategy Green Paper. May 2018. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf.
- Home Office, Speech by the Home Secretary: Keeping our children safe, 3 September 2018. URL: <https://www.gov.uk/government/speeches/keeping-our-children-safe>.
- House of Commons Digital, Culture, Media and Sport Committee Disinformation and "Fake News": Final Report Eighth Report of Session 2017-19. 14 February 2019.
- Langos C., Sarre R. Responding to Cyberbullying: the Case for Family Conferencing // *Deakin Law Review*, 2015, vol. 20, no. 2.
- MacKay W. Respectful and Responsible Relationships: There's No App for That. The Report of the Nova Scotia Task Force on Bullying and Cyberbullying. February 2012. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2123494&download=yes.
- Mishna F. et al. The Ongoing Problem of Bullying in Canada: A Ten-Year Perspective // *Canadian Social Work*, 2010, vol. 12, no. 2.
- Ofcom (2018). Adults' Media Use and Attitudes Report. URL: https://www.ofcom.org.uk/__data/assets/pdf_file/0011/113222/Adults-Media-Use-and-Attitudes-Report-2018.pdf.
- Ofcom (2018). Children and Parents: Media Use and Attitudes Report. URL: <https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2018>.
- Oltermann P. Tough new German law puts tech firms and free speech in spotlight/ URL: <https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight>.
- Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review. 2017. URL: https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf.
- Online Harms White Paper — Executive summary. 8 April 2019. URL: <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper-executive-summary--2>.
- Online Romance Scams. URL: <https://www.riku.fi/en/various+crimes/property+crime/fraud/online+romance+scams>.
- Online Sexual Coercion and Extortion as a Form of Crime Affecting Children / Law Enforcement Perspective. 2017. URL: <https://www.europol.europa.eu/publications-documents/online-sexual-coercion-and-extortion-form-of-crime-affecting-children-law-enforcement-perspective>.
- ONS crime stats: fraud & cyber crime still dominate. URL: <https://www.techuk.org/insights/news/item/13518-ons-crime-stats-fraud-cyber-crime-still-dominate>.
- Oral evidence: Policing for the Future, HC 515. Tuesday, 13 March 2018. URL: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/policing-for-the-future/oral/80543.html>.
- Perren S. et al. Bullying in School and Cyberspace: Associations with Depressive Symptoms in Swiss and Australian Adolescents // *Child and Adolescent Psychiatry and Mental Health*, 2010, vol. 4, no. 1.
- Police warned people to be alert when making friends online and to take any request to send money as sign of a scam. URL: <https://www.scmp.com/news/hong-kong/law-and-crime/article/2177139/huge-explosion-online-romance-scams-hong-kong-2018>.
- Reform of the Criminal Law Needed to Protect Victims from Online Abuse says Law Commission. 1 November 2018. URL: <https://www.lawcom.gov.uk/reform-of-the-criminal-law-needed-to-protect-victims-from-online-abuse-says-law-commission/>.
- Renda A. The Legal Framework to Address "Fake News": Possible Policy Actions at the EU Level. URL: [http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA\(2018\)619013_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA(2018)619013_EN.pdf).
- Salter M., Crofts T. Responding to Revenge Porn: Challenges to online Legal Impunity. URL: https://www.academia.edu/7833345/Responding_to_revenge_porn_Challenges_to_online_legal_impunity.
- Shariff S. Confronting Cyberbullying: What Schools Need to Know to Control Misconduct and Avoid Legal Consequences/ New York, 2009.
- Tackling Child Sexual Exploitation: Progress Report. 16 February 2017. URL: <https://www.gov.uk/government/publications/tackling-child-sexual-exploitation-progress-report>.
- Голованова Н.А. К вопросу о классификации источников современного английского уголовного права // *Журнал российского права*. 2014. № 11.
- Голованова Н.А. Проблемы борьбы с буллингом // *Журнал российского права*. 2018. № 8.
- Голованова Н.А. Уголовное право Англии: учеб. пособие для бакалавриата и магистратуры. М., 2017.
- Киреева Ж.Б., Петрашева Н.В. Социальная обусловленность криминализации отдельных видов общественно опасных посягательств // *Журнал правовых и экономических исследований*. 2017. № 1.
- Криминализация и декриминализация как формы преобразования уголовного законодательства: монография / отв. ред. В.П. Кашепов. М., 2018.
- Семыкина О.С. Противодействие киберпреступности за рубежом // *Журнал зарубежного законодательства и сравнительного правоведения*. 2016. № 6.
- Чернухина Л.С. Соотношение федерального и провинциального законодательства Канады в области защиты детей от домашнего насилия // *Журнал зарубежного законодательства и сравнительного правоведения*. 2016. № 6.

REFERENCES

- Barge J.D. Policy for Prohibiting Bullying, Harassment and Intimidation. Available at: https://www.gadoe.org/Curriculum-Instruction-and-Assessment/Curriculum-andInstruction/Documents/GaDOE%20Bullying%20Policy_August%202011.pdf.
- Campbell M. Victims' Perceptions of Traditional and Cyberbullying, and the Psychological Correlates of their Victimisation. *Emotional and Behavioural Difficulties*, 2012, vol. 17, iss. 3, no. 1.
- Cheer U. Abusive and Offensive Communications: the Criminal Law of New Zealand. Available at: <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2018/11/New-Zealand-U-Cheer.pdf>.
- Chernukhina L.S. Co-Relation of Federal and Provincial Legislation of Canada in the Field of Protection of Children from Domestic Violence. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = *Journal of Foreign Legislation and Comparative Law*, 2016, no. 6, pp. 120–126. (In Russ.)
- Criminalization and Decriminalization as a Form of Transformation of Criminal Legislation. Ed. by V.P. Kashepov. Moscow, 2018. 280 p. (In Russ.)
- Fake news: da oggi puoi segnalarle alla Polizia. Available at: <https://www.poliziadistato.it/articolo/155a6077fdb05e3865595940>.
- Gillespie A. Obscene Conversation, the Internet and the Criminal Law. *The Criminal Law Review*, 2014, iss. 5.
- Golovanova N.A. Challenges to Combat Bullying: a Legislative Response. *Zhurnal rossijskogo prava* = *Journal of Russian Law*, 2018, no. 8, pp. 113–124. (In Russ.)
- Golovanova N.A. Criminal Law of England. Moscow, 2017. 188 p. (In Russ.)
- Golovanova N.A. To the Question of Classification of Sources of Contemporary English Criminal Law. *Zhurnal rossijskogo prava* = *Journal of Russian Law*, 2014, no. 11, pp. 96–107. (In Russ.)
- Government response to the Internet Safety Strategy Green Paper. May 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf.
- Home Office, Speech by the Home Secretary: Keeping our children safe, 3 September 2018. Available at: <https://www.gov.uk/government/speeches/keeping-our-children-safe>.
- House of Commons Digital, Culture, Media and Sport Committee Disinformation and "Fake News": Final Report Eighth Report of Session 2017-19. 14 February 2019.
- Kireeva Zh.B., Petrasheva N.V. Social Conditioning of Criminalization of Different Types of Socially Dangerous Offences. *Zhurnal pravovyykh i ekonomicheskikh issledovaniy*. 2017, no. 1, pp. 58–62. (In Russ.)
- Langos C., Sarre R. Responding to Cyberbullying: the Case for Family Conferencing. *Deakin Law Review*, 2015, vol. 20, no. 2.
- MacKay W. Respectful and Responsible Relationships: There's No App for That. The Report of the Nova Scotia Task Force on Bullying and Cyberbullying. February 2012. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2123494&download=yes.
- Mishna F. et al. The Ongoing Problem of Bullying in Canada: A Ten-Year Perspective. *Canadian Social Work*, 2010, vol. 12, no. 2.
- Ofcom (2018). Adults' Media Use and Attitudes Report. URL: https://www.ofcom.org.uk/__data/assets/pdf_file/0011/113222/Adults-Media-Use-and-Attitudes-Report-2018.pdf.
- Ofcom (2018). Children and Parents: Media Use and Attitudes Report. Available at: <https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2018>.
- Oltermann P. Tough new German law puts tech firms and free speech in spotlight/ Available at: <https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight>.
- ONS crime stats: fraud & cyber crime still dominate. Available at: <https://www.techuk.org/insights/news/item/13518-ons-crime-stats-fraud-cyber-crime-still-dominate>.
- Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review. 2017. Available at: https://www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-of-Children_FINAL_9-18-17.pdf.
- Online Harms White Paper — Executive summary. 8 April 2019. Available at: <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper-executive-summary--2>.
- Online Romance Scams. Available at: <https://www.riku.fi/en/various+crimes/property+crime/fraud/online+romance+scams>.
- Online Sexual Coercion and Extortion as a Form of Crime Affecting Children / Law Enforcement Perspective. 2017. Available at: <https://www.europol.europa.eu/publications-documents/online-sexual-coercion-and-extortion-form-of-crime-affecting-children-law-enforcement-perspective>.
- Oral evidence: Policing for the Future, HC 515. Tuesday, 13 March 2018. Available at: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/home-affairs-committee/policing-for-the-future/oral/80543.html>.
- Perren S. et al. Bullying in School and Cyberspace: Associations with Depressive Symptoms in Swiss and Australian Adolescents. *Child and Adolescent Psychiatry and Mental Health*, 2010, vol. 4, no. 1.
- Police warned people to be alert when making friends online and to take any request to send money as sign of a scam. Available at: <https://www.scmp.com/news/hong-kong/law-and-crime/article/2177139/huge-explosion-online-romance-scams-hong-kong-2018>.

Reform of the Criminal Law Needed to Protect Victims from Online Abuse says Law Commission. 1 November 2018. Available at: <https://www.lawcom.gov.uk/reform-of-the-criminal-law-needed-to-protect-victims-from-online-abuse-says-law-commission/>.

Renda A. The Legal Framework to Address “Fake News”: Possible Policy ACtions at the EU Level. Available at: [http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA\(2018\)619013_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA(2018)619013_EN.pdf).

Salter M., Crofts T. Responding to Revenge Porn: Challenges to online Legal Impunity. Available at: https://www.academia.edu/7833345/Responding_to_revenge_porn_Challenges_to_online_legal_impunity.

Semykina O.S. Combating Cybercrime in Foreign Countries. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya* = *Journal of Foreign Legislation and Comparative Law*, 2016, no. 6, pp. 104–114. (In Russ.)

Shariff S. Confronting Cyberbullying: What Schools Need to Know to Control Misconduct and Avoid Legal Consequences. New York, 2009.

Tackling Child Sexual Exploitation: Progress Report. 16 February 2017. Available at: <https://www.gov.uk/government/publications/tackling-child-sexual-exploitation-progress-report>.