Юрислингвистика

Legal Linguistics, 2026, 39, 96-100, doi: https://doi.org/10.14258/leglin(2026)3916

ЗАРУБЕЖНАЯ ЮРИСЛИНГВИСТИКА *УДК 811.11-112, ББК 81.1, ГРНТИ 81.1, Код ВАК 5.9.8*

Правовой портрет новых киберделиктов: анализ терминов, юрисдикций и правоприменения

Н. А. Криволап

Армавирский государственный педагогический университет

ул. Розы Люксембург 159, 352901, Армавир, Россия. E-Mail: krivolap.nicita@yandex.ru

Цель статьи – анализ перехода неологизмов цифровой среды (*doxxing, deepfake, cyberflashing*) из публичного дискурса в юридические нормы и правоприменительную практику. Опираясь на социолингвистику права и концепт перформативности правового языка, автор показывает, что термин в киберсфере выполняет не только описательную, но и конституирующую функцию: через именование вреда право задает границы согласия, приватности, допустимого распространения данных и критерии ответственности. Исследование построено как сравнительный кейс-анализ Великобритании и США с сопоставлением лингвистического профиля терминов, траекторий их нормативной кодификации, судебно-прокурорских рамок и платформенных процедур (уведомление, удаление, сохранение данных). Особое внимание уделено проблемам трансграничной юрисдикции, атрибуции субъекта, стандартам цифровой доказуемости, а также балансу свободы выражения и защиты личности. Делается акцент на технологической нейтральности и проверяемости дефиниций как условиях устойчивого регулирования быстро меняющихся цифровых практик.

Ключевые слова: киберделикты, киберпреступность, социолингвистика права, дискурс и кодификация, юрисдикция в сети.

Legal Portrait of Emerging Cyber Delicts: An Analysis of Terms, Jurisdictions, and Enforcement

N. A. Krivolap

Armavir State Pedagogical University

159 Rosa Luxemburg St., 352901, Armavir, Russia. E-mail: krivolap.nicita@yandex.ru

The article examines the shift of neologisms from the digital environment (doxxing, deepfake, cyberflashing) from public discourse into legal norms and law-enforcement practice. Drawing on the sociolinguistics of law and the concept of the performativity of legal language, the author shows that in cyberspace a term performs not only a descriptive but also a constitutive function: by naming harm, the law delineates the boundaries of consent and privacy, defines what forms of data dissemination are permissible, and sets criteria of liability. The study is designed as a comparative case analysis of the United Kingdom and the United States, juxtaposing the linguistic profiles of the terms, the trajectories of their normative codification, prosecutorial and judicial frameworks, and platform procedures (notice, takedown, data retention/preservation). Particular attention is paid to problems of cross-border jurisdiction, attribution of the perpetrator, standards of digital evidentiary reliability, and the balance between freedom of expression and personal protection. The author emphasizes technological neutrality and the verifiability of definitions as prerequisites for sustainable regulation of rapidly changing digital practices.

Key words: cyber delicts, cybercrime, sociolinguistics of law, discourse and codification, online jurisdiction.

Цифровизация общества принесла беспрецедентную связанность и эффективность, но одновременно открыла новый фронтир преступной активности – киберпреступность [Munoriyarwa and Mare 2023]. В ответ на это язык права переживает ускоренную неологизацию: в обращение входят термины, рожденные на стыке онлайн–коммуникаций, данных и автоматизированных систем [см. Витвицкий, Витвицкая, Исакова 2023; Катермина 2025; Батюшкина 2023; Казанина, Кузнецова 2025; Старкова 2021; Карабеков 2022 и т. д.]. Неологизмы *cyberflashing, deepfake, doxxing, zoom–bombing*, а также лексемы, фиксирующие вмешательство в цифровую инфраструктуру, становятся не просто метками явлений, но и рабочими инструментами нормотворчества и правоприменения. Через них право очерчивает границы

согласия и приватности, злоупотребления данными и несанкционированного доступа, формируя элементы составов и процессуальные механизмы защиты [Amoo 2024].

В этой динамике термин «киберделикты» выступает интеграционной рамкой: он собирает разнородные цифровые посягательства под единым наименованием и соотносит их с механизмами ответственности.

С лингвистической точки зрения киберделикты являются терминологической единицей, объединяющей семантику неправомерного деяния и указание на цифровую среду его совершения. Компонент «деликт» (происходит от латинского delictum) в русском юридическом языке обозначает вредоносное действие, влекущее ответственность, причем чаще именно цивилистическую. Префикс «кибер» маркирует сферу информационно–коммуникационных технологий и киберпространства [Словарь терминов по ИБ 2019]. В результате этот термин функционирует как родовое наименование с довольно вариативными границами. В научных и правовых текстах он охватывает строго определяемые виды посягательств, тогда как в медийном дискурсе может расширяться практически до любого социально вредного поведения в сети: от несанкционированного доступа и кражи данных до онлайн–травли и вмешательства в работу сервисов [Витвицкая 2023]. Синонимичные понятия «киберпреступления» и «киберправонарушения» пересекаются по содержанию, однако выбор конкретного наименования сигнализирует о желаемой рамке ответственности и квалификации деяния.

Глобальный охват интернета существенно размывает классические представления о юрисдикции и позволяет правонарушителям действовать через национальные границы. Это объективно требует согласованности правовых режимов и выстраивания механизмов международного сотрудничества, где профильные организации играют связующую роль между различными правовыми системами.

Киберпреступность – понятие зонтичное, и это сразу создает терминологическую проблему. Под одной «крышей» оказываются и банальное мошенничество, и кража идентичности, и кибершпионаж, и технически изощренные сетевые операции [Li Y 2021; Старкова 2021 и др.]. Анонимизация, цепочки прокси–серверов, размытые юрисдикционные границы – все эти факторы превращают установление субъекта в задачу со множеством неизвестных. Отсюда – растущие требования к цифровой криминалистике и, что особенно болезненно, к трансграничному сбору доказательств.

Сбор цифровых следов – процедура инвазивная по определению, и найти баланс между «нужно расследовать» и «нельзя вторгаться» удается далеко не всегда [Amoo 2024]. Дискуссия вокруг шифрования и так называемого «законного доступа» – из той же серии: правоохранители требуют ключей, а защитники приватности указывают на риски злоупотреблений. Пока эта дискуссия далека от разрешения.

Правовая система сейчас находится в точке, где реактивная логика («случилось – отреагировали») уже не работает. Нужны проактивные решения, причем согласованные – на уровне государств, международных институтов, технологического сообщества.

Важно подчеркнуть: неологизация в правовом дискурсе – процесс двунаправленный. Термины приходят и «снизу» – из пользовательского обихода, жаргона специалистов по безопасности, журналистских текстов, – и «сверху» – через академическую систематизацию, ведомственные глоссарии, судебные дефиниции. Эта гибридность, на наш взгляд, принципиальна для понимания того, как формируется (и деформируется) понятийный аппарат киберправа. Теоретическая рамка исследования опирается на социолингвистику права и объясняет, каким образом новые языковые формы переходят из публичного дискурса в нормативную ткань [Карабеков 2022; Батюшкина 2023]. В центре – идея перформативности правового языка: термины не просто описывают явления, но конструируют объекты регулирования, устанавливая границы дозволенного и определяя составы правонарушений. В этой логике неологизмы выступают «якорями смысла» для быстро меняющихся цифровых практик, позволяя связать социально распознаваемый вред с юридически операционализируемыми категориями [Катермина 2025; Amoo 2024].

Трансграничность киберугроз ставит под сомнение классические рамки юрисдикции и требует согласованных подходов к терминам, чтобы международное сотрудничество было не только политически возможным, но и лингвистически совместимым. Гармонизация дефиниций, процедур и стандартов доказуемости повышает эффективность совместных расследований, при этом поддерживая баланс между правоохранительными целями и защитой прав личности. В этом смысле неологизмы – не побочный продукт цифровизации, а важнейшие элементы инфраструктуры смысла, без которых невозможно ни точное правовое реагирование, ни устойчивое взаимодействие между государствами, платформами и обществом [Старкова 2021; Карабеков 2022].

Чтобы показать, как описанный цикл «дискурс → норма → практика → дискурс» работает не в абстракции, а в конкретных правовых режимах, далее перейдем к разбору отдельных киберделиктов как «узловых» терминов цифровой неологизации. Мы выбрали случаи, где вред социально распознаваем и регулярно артикулируется в публичном дискурсе, дефиниции конкурируют между собой или распадаются на смежные составы, и правоприменение неизбежно опирается на платформенные процедуры (уведомление, удаление, сохранение данных) и цифровые доказательства. Для каждого термина – *doxxing, deepfake, cyberflashing, zoom-bombing, unauthorized access* – сопоставим лингвистический профиль (варианты именования, семантические границы, фрейм «согласие/приватность/безопасность»), траектории кодификации и судебной интерпретации, а также правила платформ и стандарты доказуемости в Великобритании и США. Такая «поштучная» оптика позволит увидеть, где именно возникают регуляторные разрывы: в определениях, в юрисдикционной привязке, в критериях идентификации субъекта, либо в балансировке свободы выражения и права на приватность – и, следовательно, какие элементы дефиниций и процедур поддаются гармонизации без потери технологической нейтральности.

В США термин *doxxing* чаще всего «применяется» не как название отдельного состава в законе, а как публично

понятная маркировка практики, которую затем квалифицируют через уже существующие нормы (угрозы, преследование, кибersталкинг). Его нормативное «вхождение» видно по федеральным законодательным инициативам: на Congress.gov термин прямо встречается в названиях/текстах законопроектов, пытающихся описать doxxing как самостоятельный вред и формализовать признаки (перечень идентифицирующих данных, требуемый умысел, причинная связь с преследованием, исключения для общественного интереса. В правоприменительной коммуникации (пресс-релизы, описания дел) термин doxxing регулярно используется как «ярлык фабулы», но юридическое основание часто опирается, например, на федеральный запрет кибersталкинга 18 U.S.C. § 2261A; это хорошо видно по поиску по сайту DOJ, где *doxxing* фигурирует в описании поведения, а обвинение строится на иных статьях.

В результате ключевыми становятся доказуемость умысла (запугать/спровоцировать травлю) и конституционные рамки свободы выражения: публикация информации как таковая часто «нейтральна», но в связке с преследованием/угрозами становится юридически значимой. В Великобритании картина сходная: *doxxing* широко употребляется в парламентском и регуляторном дискурсе как тип онлайн-вреда, но в судебной и прокурорской практике поведение обычно раскладывается на действующие режимы – прежде всего *Protection from Harassment Act 1997* и *Malicious Communications Act 1988*, а также, по обстоятельствам, на инструменты защиты данных и частноправовые запреты/иски о нарушении приватности. Употребление термина в ориентирующих материалах также встречается в поисковой выдаче CPS.

В обоих правопорядках *doxxing* работает как «термин интерфейса» между социально узнаваемым вредом и юридической техникой, направляя внимание на стандарт доказательств (идентификация лица, контекст, повторяемость, последствия) и баланс приватности с свободой выражения, но без единообразной кодификации самого слова.

Термин *deepfake* в США и Великобритании закрепился как «имя» нового типа вреда (синтетические/сильно модифицированные аудио- и видеоматериалы), но в праве он чаще работает как интерфейсное обозначение, которое затем «переводится» на язык уже существующих составов (диффамация, мошенничество, преследование, нарушения приватности), либо становится частью точечных норм под конкретные риски – выборы и интимные изображения. В США это хорошо видно по федеральному нормотворческому дискурсу: термин *deepfake* стабильно присутствует в названиях и текстах законопроектов, однако единой федеральной статьи про *deepfake* по-прежнему нет, а ключевой юридический конфликт сводится к балансу свободы выражения и предотвращения вреда (особенно там, где контент носит политический или сатирический характер). Маркером институционализации термина выступает сама плотность его употребления в законопроектах на Congress.gov (поиск *deepfake* по массиву legislation): это фиксирует попытки формализовать признаки синтетического контента, требования к намерению (*deceive/harm*), к раскрытию факта манипуляции и к исключениям для журналистики/общественного интереса. Параллельно США демонстрируют «штатную» модель регулирования: отдельные штаты прямо используют термин *deepfake* в узких по предмету нормах – например, в Техасе введен запрет на *deep fake video* в контексте выборов (Texas Election Code § 255.004), а в Калифорнии создан гражданско-правовой механизм защиты от сексуально эксплицитных дипфейков [California Civil Code § 1708.86 URL]. Это показательно с точки зрения правоприменения: термин становится юридически значимым там, где легче описать проверяемые критерии (период до выборов; «sexually explicit»; идентифицируемость лица; отсутствие согласия; причиняемый вред), тогда как в «широких» ситуациях дипфейки чаще попадают в орбиту общих норм (*fraud/impersonation/harassment*), и термин *deepfake* остается прежде всего объяснением фабулы для суда, присяжных и платформ. На уровне правоохранительной практики термин активно используется в публичных сообщениях и пресс-релизах как социально узнаваемая этикетка угрозы; это видно хотя бы по поисковой выдаче по сайту DOJ, где *deepfake* фигурирует как описание способа совершения деяния, а юридическая квалификация опирается на другие составы. В Великобритании *deepfake* столь же устойчив в политико-правовом дискурсе, но юридическая техника чаще избегает «технологического бренда» и стремится к технологически нейтральным формулировкам вроде *altered image* / синтетически созданный материал. В этом смысле показателен *Online Safety Act 2023*: он строит регулирование вокруг категорий вреда и обязанностей (в том числе применительно к интимным изображениям и их распространению без согласия), не привязываясь к конкретному способу генерации контента, что облегчает адаптацию к новым моделям синтеза. Практически это означает, что при рассмотрении кейсов дипфейки будут «раскладываться» на уже знакомые режимы (harassment/сталкинг, вредные коммуникации, защита данных, частноправовые средства защиты приватности), а сам термин *deepfake* выступит скорее доказательственным и контекстуальным фактором: он влияет на оценку умысла, на риск офлайн-вреда и на стандарты аутентичности цифровых доказательств. В итоге и США, и UK используют *deepfake* как «узел» для связывания новой медиатехнологии с привычными охраняемыми благами (репутация, приватность, безопасность, добросовестность выборов), но расходятся в технике: США чаще допускают точечные *deepfake*-нормы на уровне штатов, а UK – нейтрализует технологию через более абстрактные категории вреда и обязанности платформ, снижая риск устаревания дефиниций.

Термин *cyberflashing* (аналог офлайн – *flashing*) описывает отправку или демонстрацию человеку непрошеного сексуально эксплицитного изображения в цифровых каналах (чаще всего – «дикпик» через мессенджеры или бесконтактные протоколы вроде AirDrop/Bluetooth). В Великобритании это один из редких примеров, где неологизм сравнительно быстро получил прямую институциональную «привязку» к уголовно-правовой норме: *Online Safety Act 2023* ввел специальное преступление, добавив в *Sexual Offences Act 2003* новый раздел 66A [Online Safety Act URL]. Тем самым *cyberflashing* перестает быть только медийной меткой и превращается в юридически операционализируемое поведение: фокус смещается на проверяемые элементы (факт отправки/передачи фото или видео гениталий,

намерение заставить адресата это увидеть, цель сексуального удовлетворения и/или причинения тревоги/унижения, отсутствие согласия/разумного основания считать, что согласие есть). Параллельно термин продолжает работать как «переводчик» для публичного дискурса и правоприменителя: его видно в парламентских дебатах [UK Parliament. Hansard URL], а также в поисковой выдаче CPS, где он выступает как понятное название вреда, который дальше квалифицируется по конкретным статутным признакам и доказывается через цифровые следы (лог отправки, метаданные, свидетельские показания, данные платформ). В США картина более «лексически рыхлая»: на федеральном уровне устойчивой кодификации именно слова *cyberflashing* нет, и термин чаще живет в описании явления и в законодательных инициативах/обсуждениях, чем в единой норме. Однако на уровне штатов появляются близкие по смыслу составы, которые фактически закрывают поведение *cyberflashing*, но формулируются технологически нейтрально – как незаконная электронная передача сексуально эксплицитного визуального материала без согласия. Показательный пример – Техас, где установлен состав *Unlawful Electronic Transmission of Sexually Explicit Visual Material* (Penal Code § 21.19): в публичном дискурсе это и есть *cyberflashing*, но юридическая техника предпочитает описывать действие и объект (электронная передача + сексуально явное изображение + отсутствие согласия/запроса), чтобы меньше зависеть от моды на термин и от конкретной технологии доставки. В результате различие UK/US проходит по линии «кодификация названия вреда» (UK) против «регулирование вреда без фиксации бренда-термина» (US); это влияет и на правоприменение: в UK проще строить единый стандарт квалификации, а в США чаще возникает мозаика составов и доказательственных порогов по штатам, при том что социальное термин *cyberflashing* продолжает выполнять роль маркера типа вреда.

Проведенный анализ показывает, что «киберделикты» формируются как зона ускоренной правовой неологизации, где слова становятся инструментами регулирования: они связывают социально узнаваемый вред с юридически доказуемыми элементами состава и тем самым направляют нормотворчество и практику. Во всех рассмотренных случаях (*doxxing, deepfake, cyberflashing*) термин чаще выступает «интерфейсом» между общественным дискурсом, платформенным управлением и правом: он помогает описать фабулу и тип вреда, но далеко не всегда фиксируется как самостоятельная правовая категория. Наиболее показательно различие правовых техник: Великобритания чаще институционализирует новые цифровые вреды через более централизованные режимы и обязанности платформ (а в случае *cyberflashing* – и через прямую уголовно-правовую норму), тогда как США в большей степени опираются на переквалификацию поведения через уже существующие составы и на фрагментарные «точечные» решения на уровне штатов (особенно по *deepfake* и электронным сексуально-эксплицитным материалам). Одновременно ключевыми ограничителями эффективности регулирования остаются трансграничность интернет-коммуникаций, сложности атрибуции, инвазивность сбора цифровых доказательств и конкуренция правовых ценностей (свобода выражения vs приватность и безопасность). В этих условиях устойчивое правовое реагирование требует не просто реактивного добавления новых «модных» терминов, а согласуемых, технологически нейтральных и проверяемых дефиниций, совместимых стандартов доказуемости и процедур взаимодействия государства и платформ. Неологизмы в итоге выступают элементами «инфраструктуры смысла», от качества которой зависит возможность гармонизации правоприменения и международного сотрудничества без эрозии прав и свобод личности.

Литература

Батюшкина М. В. Термины информационного (цифрового) права: семантика, структура, законодательные дефиниции / Юрислингвистика. – 2023. – № 28. – С. 6-12.

Витвицкая С. С., Витвицкий А. А., Исакова Ю. И. Киберпреступления: понятие, классификация, международное противодействие / Правовой порядок и правовые ценности. – 2023. – Т. 1, № 1. – С. 126–136.

Казанина Т. В., Кузнецова Е. А. Термины-неологизмы в сфере договорного права: лингвоюридические аспекты / Юрислингвистика. – 2025. – №35. – С. 12-19.

Карабеков К. О. Понятие киберпреступности в Российской Федерации и Республике Казахстан / Известия Юго-Западного государственного университета. Серия: История и право. – 2022. – Т. 12, № 5. – С. 94–102.

Катермина В. В., Плаксин В. А. «Цифровая преступность» в финансово-экономическом дискурсе (на материале английских неологизмов) / Филологические науки. Вопросы теории и практики. – 2025. – № 6. – С. 2337-2342.

Старкова Л. М. Подходы к пониманию и нормативному определению категории «киберпреступность» и смежных понятий в практике региональных международных организаций / Московский журнал международного права. – 2021. – №4. – С. 123–135.

Пройдаков Э. М., Теплицкий Л. А. Словарь терминов по информационной безопасности. 2019. URL: https://www.infosystems.ru/library/glossary/slovar-terminov-po-informatsionnoy-bezopasnosti/.

Amoo O. O., Atadoga A., Abrahams T. O., Farayola O. The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system / World Journal of Advanced Research and Reviews. – 2024. – Vol. 21, No. 2. – Pp. 205–217.

California Legislative Information. California Civil Code, Section 1708.86. URL: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1708.86

Congress.gov. URL: https://www.congress.gov/search?q=%7B%22source%22%3A%22legislation%22%2C%22search%22%3A%22deepfake%22%7D

Li Y., Cheng J., Huang C., Chen Z., Niu W. NEDetector: Automatically extracting cybersecurity neologisms from hacker forums / Journal of Information Security and Applications – 2021 – Vol. 58. Article 102784. URL: https://www.sciencedirect.com/science/article/abs/pii/S221421262100302
Munoriyarwa A., Mare A. Digital Surveillance in Southern Africa: Policies, Politics and Practices. Cham, 2023.
Online Safety Act 2023. URL: https://www.legislation.gov.uk/ukpga/2023/50/contents
UK Parliament. Hansard. Search results: “doxxing”. URL: https://hansard.parliament.uk/search?searchTerm=doxxing

References

Batyushkina, M. V. (2023). Terms of information (digital) law: semantics, structure, legislative definitions. Jurislinguistics, 28, 6–12 (in Russian).
Vitvitskaya, S. S., Vitvitskiy, A. A., Isakova, Yu. I. (2023). Cybercrimes: concept, classification, international counteraction. Legal Order and Legal Values, 1(1), 126–136 (in Russian).
Kazanina, T. V., Kuznetsova, E. A. (2025). Neologism terms in the field of contract law: linguo-legal aspects. Jurislinguistics, 35, 12–19 (in Russian).
Karabekov, K. O. (2022). The concept of cybercrime in the Russian Federation and the Republic of Kazakhstan. Proceedings of the Southwest State University. Series: History and Law, 12(5), 94–102 (in Russian).
Katermina, V. V., Plaksin, V. A. (2025). “Digital crime” in financial and economic discourse (based on English neologisms). Philological Sciences. Issues of Theory and Practice, 6, 2337–2342 (in Russian).
Starkova, L. M. (2021). Approaches to understanding and normative definition of the category “cybercrime” and related concepts in the practice of regional international organizations. Moscow Journal of International Law, 4, 123–135 (in Russian).
Proydakov, E. M., Teplitskiy, L. A. (2019). Dictionary of terms on information security. Available from: https://www.infosystems.ru/library/glossary/slovar-terminov-po-informatsionnoy-bezopasnosti/ (in Russian).
Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. World Journal of Advanced Research and Reviews, 21(2), 205–217. California Legislative Information. (n.d.). California Civil Code, Section 1708.86. Available from: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1708.86
Congress.gov. (n.d.). Search results for “deepfake”. Available from: https://www.congress.gov/search?q=%7B%22source%22%3A%22legislation%22%2C%22search%22%3A%22deepfake%22%7D
Li, Y., Cheng, J., Huang, C., Chen, Z., Niu, W. (2021). NEDetector: Automatically extracting cybersecurity neologisms from hacker forums. Journal of Information Security and Applications, 58, 102784. Available from: https://www.sciencedirect.com/science/article/abs/pii/S221421262100302
Munoriyarwa, A., Mare, A. (2023). Digital Surveillance in Southern Africa: Policies, Politics and Practices. Cham.
Online Safety Act 2023. (2023). Available from: https://www.legislation.gov.uk/ukpga/2023/50/contents
UK Parliament. Hansard. (n.d.). Search results: “doxxing”. Available from: https://hansard.parliament.uk/search?searchTerm=doxxing

Citation:
Криволап Н. А. Правовой портрет новых киберделиктов: анализ терминов, юрисдикций и правоприменения // Юрислингвистика. – 2026 – 39. – С. 96-100.
Krivolap N. A. (2026) Legal Portrait of Emerging Cyber Delicts: An Analysis of Terms, Jurisdictions, and Enforcement. Legal Linguistics, 39, 96-100.
This work is licensed under a Creative Commons Attribution 4.0. License