Научная статья
УДК 34:004:349.2:004.8
EDN: https://elibrary.ru/mqtnqg
DOI: https://doi.org/10.21202/jdtl.2024.32

Новые подходы к исследованию ИИ-преступности: конституирование цифровой криминологии

Фотиос Спайропулос

Университет Филипс, Никосия, Кипр
Spyropoulos Law Firm, Афины, Греция

Ключевые слова

искусственный интеллект,
киберпреступность,
право,
преступление,
преступность,
техноэтика,
цифровая криминология,
цифровое общество,
цифровые технологии,
этика

Аннотация

Цель: опираясь на современные научные подходы к «цифровому обществу» и новые подходы в криминологии, выявить и определить цифровую криминологию, направленную на изучение возможных способов использования искусственного интеллекта преступниками, в том числе в рамках так называемой ИИ-преступности.

Методы: проблемы связи искусственного интеллекта с преступностью в «гибридном мире» переосмысливаются в статье преимущественно с учетом междисциплинарности, на уровне которой аргументы подкрепляются соответствующими отсылками к «цифровой криминологии» и ее небинарному образу мышления в рамках техносоциального подхода, несистематического обзора литературы.

Результаты: в исследовании отмечается, что в цифровом обществе технологии интегрируются в жизнь людей, включая сферы преступности, виктимизации и правосудия, стирая границы между онлайн- и офлайн-реальностью, создавая гибридный мир человека и технологий, где преступления происходят в виртуальных сетях. Показано, что искусственный интеллект обладает потенциалом для достижения целей социального благополучия и устойчивого развития, однако необходимо учитывать риски, связанные с нарушением прав человека. Обосновывается необходимость междисциплинарного подхода для обеспечения безопасного использования технологий, борьбы с неравенством в сфере образования, помощи в осуществлении правосудия и распознавании девиантного или преступного поведения в сети. Подчеркивается, что в контексте зарождающейся техноэтики пока отсутствует или, скорее, находится в процессе формирования идея о том, что эта неофициальная норма, основанная на обыденных представлениях, станет «опорным камнем» для характеристики опосредованного онлайн-поведения как девиантного или преступного.

Научная новизна: в статье с точки зрения техноэтики выдвигается ряд подходов к феномену использования информационно-коммуникационных технологий в преступных целях под влиянием искусственного интеллекта. При этом отмечены социальные вызовы, возникающие в результате технологических сбоев (например, прогнозирование и предотвращение преступлений путем трансформации деятельности органов охраны правопорядка, усиления наблюдения и практики уголовного правосудия) в «цифровом обществе».

Практическая значимость: идеи, лежащие в основе данного исследования, могут быть использованы при разработке предложений по внесению изменений и дополнений в действующее уголовное законодательство, а также в педагогической деятельности, особенно при реализации образовательных курсов или модулей по проблемам преступности в контексте цифровой трансформации общества.

Для цитирования

Спайропулос, Ф. (2024). Новые подходы к исследованию ИИ-преступности: конституирование цифровой криминологии. *Journal of Digital Technologies and Law*, *2*(3), 636–656. https://doi.org/10.21202/jdtl.2024.32

Содержание

Введение

Многочисленные и разнообразные пути проникновения цифровых технологий в повседневную жизнь в последние годы позволяют сделать вывод о том, что теперь «жизнь стала цифровой». «Мы все больше становимся субъектами цифровых данных, нравится нам это или нет, согласны мы на это или нет» (Lupton, 2015b).

Более того, в цифровую эпоху мы наблюдаем все более широкое использование технологий и искусственного интеллекта (далее – ИИ) для решения различных задач, а также повышения производительности и эффективности. На протяжении десятилетий ученые в области компьютерных наук были настолько очарованы неограниченным потенциалом новых технологий, что негативные последствия этих систем, по всей видимости, преуменьшались, а зачастую и вовсе игнорировались (Hayward & Maas, 2020)[1]. Этот подход, известный под названием «технооптимизм»

[1] Schneier, B. (2008, March 20). Inside the twisted mind of the security professional. Wired. https://clck.ru/3CzSKg

(Danaher, 2022), отличается неспособностью эффективно сбалансировать выгоды и риск, что отражалось в Кодексе Google с его прежним лозунгом «Не причини зла»[2].

Однако в последнее время ученые используют ряд новых исследовательских подходов, рассматривая возможные изменения преступности под воздействием того, что Greenfield (2017) выразительно назвал «радикально новыми технологиями и ИИ сетевой эры».

Специалисты в области технологий и криминалистики сегодня осознают, что системы искусственного интеллекта открывают множество новых возможностей для серьезной преступности, а также позволяют применять сомнительные методы работы полиции (Hayward & Maas 2020; Ionescu et al., 2020; Broadhurst et al., 2019). В частности, увеличение числа преступлений, совершаемых в цифровом мире, доказывает, что быстро развивающиеся технологии создают новые возможности для преступников и в то же время способствуют повышению уровня и сложности преступлений[3] (Lee & Chua, 2023; Di Nicola, 2022). При этом еще не изучены многие социальные проблемы, возникающие в связи с технологическими изменениями (например, прогнозирование и предупреждение преступлений путем трансформации деятельности полиции, усиления наблюдения и практики уголовного правосудия) (Brown, 2006a; Hayward, 2012; Holt & Bossler, 2014).

1. Искусственный интеллект: проблемы определения

Дать определение понятию «искусственный интеллект» непросто; это явление кажется уже распространенным, но в то же время оно четко не определено. В популярной культуре и новостных репортажах об ИИ часто фигурируют причудливые сюжеты с участием пресловутых «роботов-убийц» или систем наблюдения, как в антиутопиях (Hayward & Maas, 2020). Однако в повседневной жизни ИИ действует на гораздо более прозаическом уровне, управляя всем – от «умных» телевизоров до приложений – переводчиков с иностранных языков. По словам К. Пайпера, «в разговорах об ИИ много путаницы, дезинформации, непонимания – во многом потому, что мы используем термин ИИ для обозначения множества различных понятий»[4].

Граница между тем, что считается собственно ИИ, и другими технологиями размыта. Более того, термин «интеллект» в контексте парадигмы ИИ – это сложное и глубоко неоднозначное философское и научное понятие. О нем не упоминают, когда приводят философские и технические аргументы в спорах о том, удастся ли когда-нибудь разработать ИИ, обладающий сознанием и достаточно сложный, чтобы мы беспокоились о его нравственности и защищали ее (Boddington, 2017). Возможно, нас смущает именно общий и неопределенный характер этого явления; не в последнюю очередь это происходит потому, что каждый предполагаемый вариант будущего ИИ вызывает свой ряд вопросов, связанных с безопасностью, этикой, законностью и ответственностью.

---

2 Mayer, D. (2016). Why Google Was Smart To Drop Its ‘Don’t Be Evil’ Motto. Fast Company.

3 Ife, C. C., Davies, T., Murdoch, S. J., & Stringhini, G. (2019). Bridging information security and environmental criminology research to better mitigate cybercrime. arXiv preprint arXiv:1910.06380. https://clck.ru/3CzSMo

4 Piper, K. (2018). The case for taking AI seriously as a threat to humanity, Vox. https://clck.ru/3CzSPd

Так называемый аспект «двойного назначения» технологий – не новая проблема, когда речь идет о киберпреступности или (кибер-)безопасности. Хотя ИИ может использоваться для атак на государственные структуры, правительства также применяют его для расширения своих возможностей. Однако появляются новые уязвимости, так как возникают злоупотребления и злонамеренное использование технологий. Одно из законных применений ИИ – это системы для предотвращения и обнаружения преступлений (Dilek et al., 2015; Li et al., 2010; Lin et al., 2017; McClendon & Meghanathan, 2015), но существует также вероятность злоупотребления этой технологией и использования ее для незаконной деятельности (Kaloudi & Li, 2020; Sharif et al., 2016; Mielke & Chen, 2008; van der Wagen & Pieters, 2015). Важнейшей проблемой является использование злоумышленниками систем, не относящихся к искусственному сверхинтеллекту, для автоматизации, обеспечения и расширения масштабов киберпреступлений известных типов, а также появление совершенно новых возможностей для киберпреступлений.

Для того чтобы общество смогло решить эту проблему, необходимо дать четкие ответы на простые вопросы: «Что именно представляет собой ИИ?», «Каковы его возможности и пределы?» и «Каковы последствия его распространения и использования в обществе как в качестве инструмента для достижения преступных или незаконных целей, так и в качестве средства обеспечения безопасности и социального контроля?»

2. Подходы к техноэтике

Термин «техноэтика» был предложен в 1974 г. аргентино-канадским философом Mario Bunge (Bunge, 1977) для обозначения особой ответственности технологов и инженеров за развитие этики как отрасли технологии.

«Этику можно определить как кодекс или набор принципов, по которым живут люди. Этика говорит о том, что считается морально правильным и что считается неправильным. Когда люди выносят моральные суждения, они делают не описательные заявления о том, что сделано, а нормативные или предписывающие заявления о том, что должно быть сделано, о моральном долге и обязательствах. Таким образом, этическая теория или моральная философия – это учение о правилах или принципах, лежащих в основе моральных решений, обоснование моральных суждений. Применение этической теории может помочь пользователям, вплоть до определения того, как люди должны вести себя в различных областях применения технологий.

Соответственно, техноэтика – это междисциплинарная область, задача которой – определить соответствующее отношение или систему взглядов на применение технологий в реальных жизненных ситуациях. Среди ряда этических теорий, наиболее актуальных для сферы применения технологий, можно выделить последовательный, деонтологический и утилитарный подходы. Техноэтика занимается изучением влияния этики на технологии, технологические изменения, технологический прогресс и их прикладные аспекты. Это относится как к устоявшимся областям, таким как биоэтика, компьютерная этика или инженерная этика, так и к новым направлениям исследований, таким как нейроэтика (Heller, 2012).

Rocci Luppicini подчеркивает: «...техноэтика основана на предпосылке, что крайне важно развивать диалог, направленный на определение этического использования технологий, защиту от их неправильного применения и разработку продуманных принципов, которые помогут направлять новые технологические достижения на благо общества в различных социальных контекстах и этических измерениях» (Luppicini, 2008).

Следует сказать, что техноэтика – это быстро развивающаяся область этики, обусловленная стремительным развитием технологий и их интеграцией в повседневную жизнь. Она использует обширные знания из таких научных направлений, как информация и коммуникации, общественные науки, технические и естественно-научные дисциплины, прикладная этика и философия. Задача техноэтики – выявить этические преимущества технологий, защитить от их неправильного использования и наметить общие принципы, которые приведут за собой новые достижения в области развития и применения технологий на благо общества.

Отвечая на вопрос, зачем нам нужны техноэтика и технологическое сознание, можно сказать следующее. С развитием технологий искусственного интеллекта и машинного обучения мы, несомненно, столкнемся с технологиями, которые будут способны учиться и творить, иметь собственное сознание. Поэтому нам необходимо обратиться к вопросам технологического сознания и техноэтики, чтобы найти ответы на возникающие моральные дилеммы, связанные с технологиями, и направить эти развивающиеся технологии таким образом, чтобы они приносили пользу человечеству, ведь любой алгоритм можно использовать как во благо, так и во зло.

3. Достижения, пробелы и вызовы этики искусственного интеллекта

Технологический прогресс всегда находится в центре динамики экономической системы, прямо или косвенно влияя на все виды экономической и производственной деятельности. Происходящие значительные изменения вызывают соответствующие перемены в целом ряде видов производственной и экономической деятельности. В то же время они выступают мощным фактором возникновения дисбаланса, появления новых или воспроизводства существующих примеров неравенства и несправедливости как на уровне рынка труда, структуры занятости и экономики, так и на уровне социально-экономического развития экономик, секторов, регионов и стран на европейском и международном уровнях.

Вопросы, возникающие в связи с развитием технологий, и в частности, с развитием искусственного интеллекта, все больше занимают ученых, компании и государственные органы. Так, совместная работа исследовательского отдела компании Dell Technologies и Института будущего привела к выводу, что «зависимость людей от машин перерастет в отношения сотрудничества, в которые люди привнесут такие качества, как креативность, целеустремленность и предприимчивость»[5].

Когда говорят об этических проблемах и вызовах, связанных с технологиями и искусственным интеллектом, обычно подразумевается, что речь идет о чем-то плохом с моральной точки зрения. И конечно, большая часть дебатов об ИИ вращается вокруг морально проблематичных эффектов, для которых необходимо найти решение. Однако стоит подчеркнуть, что технологии и новые достижения в области ИИ сулят многочисленные выгоды (Berendt, 2019)[6]. Во многих программных доку-

[5] Barbaschow, A. (2019, October 8). Machines as consumers: The future according to Dell Technologies. ZDNET.

[6] Faggella, D. (2020). Everyday examples of artificial intelligence and machine learning. Boston, MA: Emerj. https://clck.ru/3CzSZw

ментах, посвященных ИИ, основное внимание уделяется экономическим преимуществам ИИ, которые, как ожидается, будут обусловлены достижением более высоких уровней эффективности и производительности. Это этические ценности, поскольку они обещают увеличение благосостояния, что позволит людям жить лучше и, таким образом, будут способствовать или даже станут необходимыми для процветания человека (см. подробнее: Экспертная группа высокого уровня ЕС по ИИ[7]).

Однако в последнее время обещания повысить эффективность, снизить затраты и ускорить исследования и разработки сменились опасениями, что эти сложные, непрозрачные системы могут принести человечеству больше вреда, чем пользы. Этические проблемы ИИ неоднократно описывались; в основном такие работы развивают давнюю традицию обсуждения этики и ИИ в научной литературе (Coeckelbergh, 2019; Dignum, 2019; Müller, 2020), но все чаще рассматривают эту проблему также с точки зрения политики[8]. Самыми известными вопросами в области этики являются следующие: а) нарушение конфиденциальности данных; б) раскрытие чувствительной информации; в) дезинформация и дипфейки; г) отсутствие надзора и принятия ответственности; д) использование ИИ (распознавание лиц, потеря рабочих мест, отслеживание состояния здоровья, проверка достоверности данных, усиление существующих предубеждений, отсутствие объяснимости и интерпретируемости и т. д.).

Таким образом, важно подчеркнуть, что правовые и этические проблемы, с которыми сталкивается общество в связи с появлением искусственного интеллекта, включают аспекты соблюдения приватности, надзора, предвзятости и дискриминации, а также потенциально затрагивают философский вопрос о роли человеческого суждения. В результате использования новых цифровых технологий возникают опасения по поводу того, что они могут стать источником неточностей и утечек данных. Поэтому необходимо принимать фундаментальные решения, чтобы обеспечить защиту личных свобод и надлежащее использование данных.

Опасения (оправданные или неоправданные) возникают в связи с распространением машин с искусственным «суперинтеллектом». Но реальная опасность заключается не в доминировании сверхинтеллектуальных машин, а в том, что они еще недостаточно «умны», чтобы справиться с поставленными перед ними задачами. Интеллект машин будет продолжать совершенствоваться, но, по крайней мере, в обозримом будущем уровня человеческого интеллекта они не достигнут. В результате усилится потребность в человеческих навыках и ценностях, чтобы преодолеть разрыв и смягчить риски, создаваемые мощным искусственным интеллектом в современных сложных человеческих сообществах. Ключом к устранению таких рисков является инвестирование в человеческий капитал и его развитие, а также осуществление ответственного мониторинга искусственного интеллекта. Это позволит поддерживать доверие общества к этой технологии. Среди моральных ценностей машин с искусственным интеллектом человеческие ценности часто отсутствуют. Чтобы добиться их соответствия, человек должен владеть обеими, поставив первые (ценности машин) на службу вторым (человеческим

7 EU's High-Level Expert Group on Artificial Intelligence. (2019). Ethics guidelines for trustworthy AI. Brussels: European Commission. https://clck.ru/3CzSbj

8 Ibid.

ценностям). Не нужно обвинять ИИ в моральных промахах человечества. «Зеркало искусственного интеллекта» является полезным инструментом для диагностирования общества; с его помощью люди могут многое узнать о его слабостях и ограничениях, а также о новых открытиях и решениях, которые он предлагает. Будущее искусственного интеллекта и человеческого общества будет решаться не за людей, а людьми. ИИ и роботы не должны решать за человека, но человек должен решать, что правильно, а что нет.

В последнее время в общественных науках стало популярным понятие «цифровое общество». Это общество, характеризующееся беспрецедентно быстрым прохождением потока информации через глобальные сети. Но самая важная особенность цифрового общества заключается в том, что оно рассматривает эти технологии как неотъемлемую часть более крупной социальной структуры и признает, что цифровые технологии, медиа и сети включены в нашу повседневную жизнь (Lupton, 2015a, 2015b), в том числе в части совершения преступлений, виктимизации и правосудия. В частности, Baym (2015) отмечает, что отличительной чертой цифровых технологий является то, как они изменили взаимодействие людей друг с другом. Такое переплетение цифрового и социального также называют цифровизацией общества, при которой «технология – это общество, а общество невозможно понять или представить без его технологических инструментов» (Castells, 1996).

С другой стороны, цифровая криминология относится к быстро развивающейся научной области, которая применяет криминологические, социальные, культурологические теории, теорию технических систем и соответствующие методы исследования для изучения преступности, делинквентного/девиантного поведения и правосудия в цифровом обществе (Stratton et al., 2017). Более того, она заново пересматривает криминологические теории в поисках новых научных идей, бросая вызов классическим дихотомиям: Интернет против физического мира, виртуальное против реального – как для предотвращения, так и для противодействия преступности в цифровой среде, в Интернете, а также в целом в контексте новых технологий, в контексте развития техноэтики. Таким образом, цифровая криминология расширяет границы современной криминологической теории и исследований, а более широкое и непрерывное обсуждение технологий, социальности, преступности, девиантности и правосудия способствует формированию новых концептуальных основ и эмпирических направлений в киберпространстве и в картировании цифровой преступности.

4. Задачи и перспективы криминологии в «гибридном» мире

Хотя прошло уже более пятнадцати лет с начала широкого распространения социальных сетей, появления дополненной реальности и искусственного интеллекта, большая часть криминологических исследований по-прежнему традиционно фокусируется на информационных системах и интернет-технологиях, рассматривая их либо как объекты преступлений, либо как инструменты для совершения других традиционных преступлений (Hayward & Maas, 2020; Holt & Bossler, 2014). Более того, многие подходы основываются на внутреннем дуализме, т. е. киберпреступность по-прежнему рассматривается как зеркальная или сетевая версия своих аналогов в физическом мире, отличаясь от них средствами совершения и пространственными масштабами, но не сущностью и характером (Grabosky, 2001).

4.1. Терминология и типология ИИ-преступности

В попытке определить место ИИ в криминологии, в соответствующей научной литературе можно встретить такие термины, как «киберпреступность на основе ИИ» (Wang, 2020), «ИИ-киберпреступность» (Hoanca & Mock, 2020), «ИИ-преступность» (King et al., 2020), «вредоносный ИИ» (Hibbard, 2015; Johnson & Verdicchio, 2017), «злонамеренный ИИ»[9], «злонамеренное использование и злоупотребление ИИ» (Blauth et al., 2022) и др.

По мнению большинства исследователей, использование ИИ может способствовать развитию существующих форм преступности («киберпреступность») или появлению новых форм преступности («киберзависимая преступность») (Akdemir & Lawless, 2020; Grabosky, 2001). ИИ потенциально позволяет совершать атаки, которые по своим масштабам и охвату превосходят те, которые ранее были возможны при использовании других технологий (Blauth, et al., 2022). Поэтому предпочтительнее использовать термин «преступление с использованием ИИ», поскольку такие возможности существуют как в сфере киберпреступности (пересекаясь с традиционными терминами кибербезопасности), так и в других сферах (причем некоторые из этих угроз возникают как продолжение существующей преступной деятельности, а другие являются новыми). Термин «ИИ-преступление», предложенный в работе King et al. (2020) для описания ситуации, когда ИИ-технологии используются для совершения действий, которые уже определены как преступные в соответствующем законодательстве, напротив, следует считать слишком узким для создания широкой типологии, которая не ограничивается деяниями, являющимися преступлением в любом государстве. Например, создание и распространение дезинформации или ложных сведений может расцениваться как нанесение вреда по некоторым национальным законам, но необязательно является уголовным преступлением. Поэтому понятие «злонамеренное использование и злоупотребление» ИИ (King et al., 2020)[10] служит очень интересной альтернативой.

В рамках этого широкого спектра вариантов Hoanca & Mock (2020) разделяют киберпреступность с использованием ИИ на три крупные, слабо пересекающиеся области: использование ИИ для совершения киберпреступлений в Интернете, использование ИИ через новые каналы киберпреступности с выходом в физическое пространство и использование ИИ или знаний об ИИ для атаки на другие системы искусственного интеллекта путем искажения данных или алгоритмов. Эти области во многом пересекаются, и степень их пересечения будет расти. В то же время, пытаясь расширить криминологическую парадигму за счет учета «связи между технологиями и преступностью» Hayward и Maas (2020), квалифицируют использование термина «преступное использование ИИ» и выделяют три категории: (1) преступления с использованием искусственного интеллекта, (2) преступления по отношению к ИИ и (3) преступления, совершенные искусственным интеллектом. По их мнению, ИИ относится к первой категории «ИИ-преступности», являясь мощным инструментом

[9] Yampolskiy, R. V. (2016). Taxonomy of pathways to dangerous AI. arXiv:1511.03246v2, 143–148. https://clck.ru/3CzVKL

[10] Ciancaglini, V. (2020). Malicious uses and abuses of artificial intelligence. Trend Micro Research. United Nations Interregional Crime and Justice Research Institute (UNICRI); Europol's European Cybercrime Centre (EC3). https://clck.ru/3CzSmK

для «злонамеренного» преступного использования путем внедрения новых угроз или изменения внутренних характеристик уже существующих. Современные угрозы могут распространяться в физической среде[11]. Атаки, направленные на обман или «обход» системы ИИ, использующие уязвимости системы и проводя обратный инжиниринг, относятся ко второй категории «ИИ-преступности» – преступлениям «по отношению к ИИ». Уже давно существует возможность «испортить» данные, используемые для обучения системы. Известно, что, после того как пользователи завалили чат-бот «Тэй» от Microsoft Twitter[12] массой фраз правого толка, он за один день стал расистским[13]. В третьей категории «ИИ-преступности» – «преступления, совершенные искусственным интеллектом» – важнейшим аспектом является актуальный вопрос о правовом статусе ИИ и его потенциальном использовании в качестве «криминального прикрытия/пособника». Примером такой ситуации, по мнению Hayward & Maas (2020), является дело группы художников, которые в 2015 г. опубликовали в даркнете бота для совершения различных покупок; в результат бот стал покупать наркотики и был арестован швейцарской полицией[14].

4.2. Подход техноэтики к проблеме ИИ-преступности

Понимание этических аспектов различных типов технологий затрудняется тем, что в академических кругах существует тенденция к созданию информационных групп в отдельных областях и дисциплинах. Техноэтика (далее – ТЭ) помогает объединить отдельные области знания вокруг общей темы (в нашем случае это технологии, а именно ИИ). Она является целостной по своей природе и представляет объединяющее понятие для всех областей прикладной этики, которые фокусируются на человеческой деятельности, связанной с технологиями, включая экономику, политику, глобализацию, здравоохранение и медицину, а также научные исследования и разработки. ТЭ предлагает изменить, в сущности, представление человека о себе и его взгляд на реальность. Здесь кроются самые глубокие причины провала технико-научной парадигмы, которая не учитывает ни природу человека, ни природу живых существ в целом. Мы должны отказаться от технонауки, которая подразумевает примат науки над технологией, и принять новую реляционную парадигму, основанную на постмодернизме. Техноэтика возникла из необходимости противостоять тенденции, присущей большей части технологий, а именно тенденции отделять технологии от свободы и вместо этого утвердить технологию как духовную деятельность, выдающийся продукт человеческого духа и признать ее движущей силой, а не просто реципиентом теоретических разработок в области этики. Можно сказать, что основной вклад техноэтики заключается в рассмотрении новых этических проблем.

---

11 См. также Brundage, M., Avin, S., Clark, J. et al. (2018). The malicious use of artificial intelligence. https://clck.ru/3CzSuH

12 Социальная сеть, заблокированная на территории Российской Федерации за распространение незаконной информации.

13 Gershgorn, D. (2016). Here's how we prevent the next racist chatbot. Popular Science. https://clck.ru/3CzSxm

14 См. также Kasperkevic, J. (2015). Swiss police release robot that bought ecstasy online. The Guardian. https://clck.ru/3CzSzB

Поэтому неудивительно, что многие современные дискуссии о технологическом прогрессе ведутся в рамках ТЭ. Таким образом, они неизбежно поднимают важные вопросы о соблюдении прав человека, неприкосновенности частной жизни, ответственности и рисках, и на эти вопросы необходимо дать надлежащий ответ. Более того, в отличие от традиционной прикладной этики, которая делает акцент на этическом отношении к живым существам, ТЭ является «биотехноцентричной».

В научных дискуссиях возможные преступления с использованием ИИ в основном подразделяются на три открытые категории в зависимости от связи между преступностью и ИИ:

– преступления против ИИ (например, взлом устройств, защищенных системой распознавания лиц);

– ИИ для предотвращения преступлений (например, выявление мошеннических операций на финансовых рынках);

– ИИ для совершения преступлений (например, шантаж людей с помощью дипфейков) (Caldwell et al., 2020).

Как в исследованиях в области искусственного интеллекта, так и в практике регулирования проявляется стремление достичь баланса между преимуществами инноваций и возможным нанесением вреда или нарушениями. В последнее время исследования в области ИИ переживают всплеск активности. Однако одним из непреднамеренных последствий это процесса является потенциальная переориентация технологий ИИ на содействие преступным действиям, т. е. ИИ-преступность (иными словами, теоретическая возможность создания ИИ была осуществлена благодаря опубликованным экспериментам по автоматизации мошенничества по отношению к пользователям социальных сетей, а также демонстрации манипуляций ИИ на моделях рынка)[15, 16] (Nguyen et al., 2015). Важность ИИ-преступности как отдельного явления еще не получила признания. Исследование этических и социальных последствий ИИ сосредоточивается на вопросах регулирования и контроля использования ИИ в гражданских целях, тогда как работы, касающиеся ИИ-преступности, делаются в рамках самых разных дисциплин, включая социально-правовые исследования, информатику, психологию, робототехнику и т. д. Недостаточное число работ, посвященных ИИ-преступности, подрывает возможности для формирования прогнозов и решений относительно новой области – преступной деятельности, совершаемой ИИ. Это касается возможности новых преступлений в категории «преступлений белых воротничков» (LoPucki, 2017), а также поднимает вопросы о правосубъектности ИИ и вызывает опасения по поводу использования таких машин в качестве «посредников», их уголовной ответственности. В частности, речь идет о тех случаях, когда ограничения моделей ответственности подрывают правовую определенность, т. е. когда агенты, искусственные или нет, совершают преступные действия или бездействие, но условия ответственности за конкретное преступление недостаточны для того, чтобы привести к уголовной ответственности (King at al., 2020; Bayern, 2016; Williams, 2017; McAllister, 2018).

---

15 Huang, S., Papernot, N., Goodfellow, I., Duan, Y., & Abbeel, P. (2017). Adversarial attacks on neural network policies. arXiv preprint arXiv:1702.02284. https://clck.ru/3CzT6s

16 Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572. https://clck.ru/3CzT8m

Таким образом, техноэтический подход поднимает важнейшие проблемы и вопросы, требующие рассмотрения, а также опасения по поводу дестабилизации концепций. Основополагающей концепцией уголовного права, которая подвергается дестабилизации, является идея уголовной ответственности. ИИ как «независимый» посредник в преступлении ставит серьезные вопросы о базовых правовых нормах, таких как намеренно совершенное преступление (actus reus), преступный умысел (mens rea) и различные вопросы о пороге осведомленности. Вторая концепция, которая, вероятно, подвергается пересмотру, – это важность социального контроля, идея демократических ценностей и пределы защиты государством прав человека. Речь идет о масштабируемом, всеобъемлющем, неизбежном наблюдении и потенциальном использовании ИИ и робототехники для обеспечения правопорядка[17] (Zardiashvili et al., 2019), включая критический анализ того, как в рамках демократии обеспечить подотчетность прогностической деятельности полиции, основанной на машинном обучении. Концепция скрытого государственного управления включает повсеместное, но негласное наблюдение, беспилотники с ИИ и датчики «умных городов». Новые формы «широкого наблюдения» являются вездесущими, но при этом тонкими, негласными и скрытыми (Hayward & Maas, 2020). Концепция государства-оракула состоит в следующем: от обнаружения и ликвидации нарушений закона к их прогнозированию и предотвращению с помощью систем ИИ, которые должны улавливать тонкие закономерности и делать (предположительно) точные прогнозы будущего поведения, в том числе преступного (Danaher, 2022).

Однако, когда мы обращаем основное и исключительное внимание на киберпространство, непосредственно и однозначно ссылаясь на Интернет и технологии «виртуального или искусственного интеллекта» (категории киберпреступности, которые легко однозначно отличить от соответствующих категорий в «не-киберпространстве»), мы можем упустить из виду разнообразные проявления внутренней природы цифровых данных и коммуникаций (Jaishankar, 2008). В современных условиях сдвиги в цифровой среде являются результатом динамической взаимосвязи характеристик технологии и ее использования (Goldsmith & Brewer, 2014). «Стремление к репрезентации» девиантного «виртуального я» (Yar, 2012) тесно связано с более широкими тенденциями: как самосоздания субъектности с помощью новых коммуникационных платформ, так и искусственного интеллекта – способности машин думать, общаться и принимать решения способами, которые раньше были возможны только для человека (сетевая реальность, сетевая совместимость, сетевое содержание и др.)[18].

В свете этих проблем S. Brown (2006a) предлагает создать цифровую криминологию, которая выходит за рамки традиционной и обращается к «техно-социальным теориям» (Latour, 1993; Lash, 2002; Haraway, 1987, 1991; Castells, 2001), поскольку одной из особенностей цифровых технологий является то, как они изменили способы взаимодействия между людьми (Baym, 2015). По ее мнению, важно отметить, что анализ киберпреступности, вероятно, чересчур нацелен на абсолютные различия между «виртуальной» и «воплощенной, реальной» преступностью, а понимание «новой»

[17] Interpol and UNICRI. (2019). Artificial Intelligence and Robotics for Law Enforcement. https://clck.ru/3CzTGP

[18] Institute for the Future (IFTF). (2019). Future of connected living – augmented humans in a networked world: Research Report. https://clck.ru/3CzTPY

киберпреступности опирается почти исключительно на метафоры и «перенос» «старых» правовых и теоретических подходов (Aas, 2007; Hayward, 2012; Wood, 2016). В криминологии «нет видения критичности природы мира как гибрида человека и техники...» (Brown, 2006b), в котором все преступления происходят в сетях, отличающихся только степенью виртуальности/реальности (воплощения). Поэтому криминологи сегодня должны рассматривать преступление и преступность на стыке биологии и технологии, природы и общества, объекта и действующего субъекта, искусственного разума и человека. Не следует сводить изучение киберпреступности к технологиям и сетям как средствам распространения информации, расширяющим преступные возможности. Сегодня ученые предлагают «понимать цифровую/сетевую (преступную) деятельность как процессы, т. е. явления, находящиеся в постоянном диалоге и изменении с другими явлениями/технологиями в гибридном мире человека и технологий» (Brown, 2006a).

Заключение

Эпоха разрозненных подходов и дихотомий, вероятно, подходит к концу. Возможно, настало время для синергии, особенно на междисциплинарном уровне. Зачем цепляться за дихотомии, если мы можем гармонизировать подходы и перспективы? И все это в контексте «цифрового общества», которое признает технологии частью более широкой социальной структуры и допускает интеграцию цифровых технологий, медиа и сетей в жизнь человека, включая преступность, виктимизацию и правосудие.

В исследовании Baym (2015) подробно показано размывание границ между онлайн- и офлайн-реальностью; отмечается, что главной особенностью цифровых технологий является то, что они изменили способ взаимодействия людей друг с другом в сетевой реальности, в мире, который теперь воспринимается как гибрид человека и технологии (Brown, 2006a), где все преступления происходят в сетях, отличающихся только степенью виртуальности/воплощенности.

Более того, все вопросы, возникающие при использовании этой технологии, не являются чисто техническими, а затрагивают широкий спектр научных и ненаучных областей, и ее безопасное использование невозможно обеспечить без междисциплинарного подхода.

Искусственный интеллект обладает огромным потенциалом для использования в целях достижения социального благополучия и устойчивого развития. Несмотря на то, что он может решить многие важнейшие социальные проблемы человечества, его применение также вызывает обеспокоенность в связи с нарушением прав человека, таких как право на свободу выражения мнений, право на неприкосновенность частной жизни, защиту данных, отсутствие дискриминации. Технологии на основе ИИ открывают широкие возможности, если они разрабатываются с соблюдением универсальных норм, этики и стандартов, а также опираются на ценности, основанные на правах человека и принципах устойчивого развития. Например, надежный и прозрачный искусственный интеллект может стать эффективным средством для устранения неравенства в образовательном процессе, поскольку с его помощью можно создавать программы, адаптированные к потребностям учащихся, и повышать скорость обучения.

Кроме того, искусственный интеллект может сыграть важную роль в сфере правосудия, создавая автоматизированные судебные системы, а также в области юриспруденции в целом. Например, в сфере уголовного правосудия использование систем искусственного интеллекта для оказания помощи в проведении расследований и автоматизации процессов принятия решений уже применяется во многих судебных системах по всему миру.

В контексте зарождающейся техноэтики отсутствует (или, скорее, находится в процессе формирования) идея о том, что эта неофициальная норма, основанная на убеждениях людей, поможет квалифицировать действия в сети как девиантные или криминальные.

Моральные ценности машин с искусственным интеллектом слишком часто не соответствуют более широким человеческим ценностям. Чтобы примирить их между собой, человек должен добиться господства над обеими и поставить первые (ценности машин) на службу вторым (человеческим ценностям). ИИ не может отвечать за моральное несовершенство человека. Через «зеркало искусственного интеллекта», которое является полезным диагностическим инструментом для общества, люди могут узнать больше о его недостатках и ограничениях, а также о новых открытиях и решениях, которые он предлагает. Будущее искусственного интеллекта и человеческого общества будет решаться не за людей, а самими людьми.

Список литературы

Aas, K. F. (2007). Beyond the desert of the real: Crime control in a virtual(ised) reality. In Y. Jewkes (Ed.), *Crime Online* (pp. 160–177). Portland, Oregon: Willan Publishing.

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6), 1665–1687. https://doi.org/10.1108/intr-10-2019-0400

Bayern, S. (2016). The implications of modern business–entity law for the regulation of autonomous systems. *European Journal of Risk Regulation*, *7*(1), 297–309. http://dx.doi.org/10.1017/S1867299X00005729

Baym, N. K. (2015). *Personal Connections in the Digital Age*. England: Polity, Cambridge.

Berendt, B. (2019). AI for the common good?! Pitfalls, challenges, and ethics pen-testing. *Paladyn, Journal of Behavioral Robotics*, *10*, 44–65. https://doi.org/10.1515/pjbr-2019-0004

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *IEEE Access*, *10*, 77110–77122. https://doi.org/10.1109/access.2022.3191790

Boddington, P. (2017). *Towards a Code of Ethics for Artificial Intelligence*. Oxford: Springer International Publishing.

Broadhurst, R., Maxim, D., Brown, P., Trivedi, H., & Wang, J. (2019). Artificial Intelligence and Crime. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.3407779

Brown, S. (2006a). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, *10*(2), 223–244. https://doi.org/10.1177/1362480606063140

Brown, S. (2006b). Virtual criminology. In E. McLaughlin, & J. Muncie (Eds.), *The Sage Dictionary of Criminology* (pp. 224–258). London: Sage.

Bunge, M. (1977). Towards a Technoethics. *Monist*, *60*(1), 96–107.

Caldwell, M., Andrews, J. T., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 1–13. https://doi.org/10.1186/s40163-020-00123-8

Castells, M. (1996). *The Rise of the Network Society*. Oxford, England: Blackwell.

Castells, M. (2001). *The Internet Galaxy*. Oxford, England: Oxford University Press.

Coeckelbergh, M. (2019). Artificial Intelligence: some ethical issues and regulatory challenges. *Technology and regulation*, *2019*, 31–34. https://doi.org/10.26116/techreg.2019.003

Danaher, J. (2022). Techno-optimism: an analysis, an evaluation and a modest defence. *Philosophy & Technology*, *35*(54), 8. https://doi.org/10.1007/s13347-022-00550-2

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-022-09457-y

Dignum, V. (2019). *Responsible artificial intelligence: how to develop and use AI in a responsible way*. Cham, Switzerland: Springer Nature Switzerland AG.
Dilek, S., Cakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *IJAIA*, *6*(1), 21–39. https://doi.org/10.5121/ijaia.2015.6102
Goldsmith, A., & Brewer, R. (2014). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112–130. https://doi.org/10.1177/1362480614538645
Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, *10*(2), 243–249. https://doi.org/10.1177/a017405
Greenfield, A. (2017). *Radical Technologies*. London: Verso.
Haraway, D. (1987). A manifesto for Cyborgs: Science, technology, and socialist feminism in the 1980s. *Australian Feminist Studies*, *2*(4), 1–42. https://doi.org/10.1080/08164649.1987.9961538
Haraway, D. (1991). *Simians, Cyborgs and Women: The Reinvention of Nature*. London: Free Association Books.
Hayward, K., & Maas, M. (2020). Artificial intelligence and crime: A primer for criminologists. *Crime Media & Culture*, *17*(2), 1–25. https://doi.org/10.1177/1741659020917434
Hayward, K. (2012). Five spaces of cultural criminology. *British Journal of Criminology*, *52*(3), 441–462. https://doi.org/10.1093/bjc/azs008
Heller, P. B. (2012). Technoethics: The Dilemma of Doing the Right Moral Thing in Technology Applications. *International Journal of Technoethics (IJT)*, *3*(1), 14–27. https://doi.org/10.4018/jte.2012010102
Hibbard, B. (2015). *Ethical Artificial Intelligence*. WI, USA: Madison.
Hoanca, B., & Mock, K. J. (2020). Artificial intelligence-based cybercrime. In *Encyclopedia of criminal activities and the deep web* (pp. 36–51). IGI Global.
Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209
Ionescu, B., Ghenescu, M., Răstoceanu, F., Roman, R., & Buric, M. (2020). Artificial intelligence fights crime and terrorism at a new level. *IEEE MultiMedia*, *27*(2), 55–61. https://doi.org/10.1109/mmul.2020.2994403
Jaishankar, K. (2008). Space transition theory of cybercrimes. In F. Schmallager, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). New Jersey: Prentice Hall.
Johnson, D. G., & Verdicchio, M. (2017). Reframing AI discourse. *Minds and Machines*, *27*(4), 575–590. https://doi.org/10.1007/s11023-017-9417-6
Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape. *ACM Computing Surveys*, *53*(1), 1–34. https://doi.org/10.1145/3372823
King, T. C., Aggarwal, N., Taddeo, M. & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, *26*(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0
Lash, S. (2002). *Critique of Information*. London: Sage.
Latour, B. (1993). *We Have Never Been Modern*. Cambridge, Massachusetts: Harvard University Press.
Lee, C. S., & Chua, Y. T. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, *70*(9), 2250–2277. https://doi.org/10.1177/00111287231180093
Li, S. T., Kuo, S. C., & Tsai, F. C. (2010). An intelligent decision-support model using FSOM and rule extraction for crime prevention. *Expert Systems with Applications*, *37*(10), 7108–7119. https://doi.org/10.1016/j.eswa.2010.03.004
Lin, Y. L., Chen, T. Y., & Yu, L. C. (2017). Using machine learning to assist crime prevention. *Proceedings of 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, 1029–1030. https://doi.org/10.1109/iiai-aai.2017.46
LoPucki, Lynn M. (2017, April 17). *Algorithmic Entities. Washington University Law Review (Forthcoming)*, 95. UCLA School of Law, Law-Econ Research Paper No. 17-09.
Luppicini, R. (2008). The Emerging Field of Technoethics. In R. Luppicini, & R. Adell (Eds.), *Handbook of Research on Technoethics*. IGI Global books. https://doi.org/10.4018/9781605660226.ch001
Lupton, D. (2015a). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality*, *17*(4), 440–453. https://doi.org/10.1080/13691058.2014.920528
Lupton, D. (2015b). *Digital Sociology*. 1st ed. London & New York: Routledge.
McAllister, A. (2018). Stranger than science fiction: the rise of A.I. interrogation in the dawn of autonomous robots and the need for an additional protocol to the U.N. convention against torture. *Minnesota Law Review*, *101*, 2527–2573.

McClendon, L., & Meghanathan, N. (2015). Using machine learning algorithms to analyze crime data. *MLAIJ*, *2*(1), 1–12. https://doi.org/10.5121/mlaij.2015.2101

Mielke, C. J., & Chen, H. (2008). Botnets, and the cybercriminal underground. *Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI 2008)*, 206–211. https://doi.org/10.1109/isi.2008.4565058

Müller, V. C. (2020). Ethics of artificial intelligence and robotics. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy*. Stanford, CA: Metaphysics Research Lab. Stanford University.

Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: high confidence predictions for unrecognizable images. *Proceedings of the IEEE conference on computer vision and pattern recognition,* 7–12 June, 427–436. https://doi.org/10.1109/cvpr.2015.7298640

Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a crime. *Proceedings of ACM SIGSAC Conference*, 1528–1540. https://doi.org/10.1145/2976749.2978392

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? *International Journal for Crime, Justice and Social Democracy*, *6*(2), 17–33. https://doi.org/10.5204/ijcjsd.v6i2.355

van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578–595. https://doi.org/10.1093/bjc/azv009

Wang, X. (2020, April). Criminal law protection of cybersecurity considering AI-based cybercrime. *Journal of Physics: Conference Series*, *1533*(3), 032014. https://doi.org/10.1088/1742-6596/1533/3/032014

Williams, R. (2017). *Lords select committee, artificial intelligence committee, written evidence (AIC0206)*.

Wood, M. A. (2016). Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's[19] technological unconscious. *Theoretical Criminology*, *21*(2), 1–18. https://doi.org/10.1177/1362480616643382

Yar, M. (2012). Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime, Media, Culture*, *8*(3), 245–260. https://doi.org/10.1177/1741659012443227

Zardiashvili, L., Bieger, J., Dechesne, F., & Dignum, V. (2019). AI ethics for law enforcement. *Delphi*, *2*(4), 179–185. https://doi.org/10.21552/delphi/2019/4/7

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

Сведения об авторе

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

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.81 / Криминология
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 30 апреля 2024 г.
Дата одобрения после рецензирования – 15 мая 2024 г.
Дата принятия к опубликованию – 25 сентября 2024 г.
Дата онлайн-размещения – 30 сентября 2024 г.

Research article
UDC 34:004:349.2:004.8
EDN: https://elibrary.ru/mqtnqg
DOI: https://doi.org/10.21202/jdtl.2024.32

New Approaches to Researching AI Crime: Institutionalization of Digital Criminology

Fotios Spyropoulos

Philips University, Nicosia, Cyprus
Spyropoulos Law Firm, Athens, Greece

Keywords

artificial intelligence,
crime,
criminal deed,
cybercrime,
digital criminology,
digital society,
digital technologies,
ethics,
law,
technoethics

Abstract

Objective: the article deals with modern scientific approaches to the "digital society", identifies new criminological perspectives, such as that of digital criminology in an ever-changing hybrid world, in the scientific study of the potential use of AI by criminals, including what is referred to here as AI crime.

Methods: this article is an essay commonly used in humanities and social sciences, as the author aims to present provocative arguments to encourage readers to rethink AI issues in relation to criminality in the "hybrid world" based on a non-systematic literature review. The arguments should be supported by relevant references to "digital criminology" and its non-binary way of thinking in favour of a techno-social approach.

Results: the era of divided perspectives is coming to an end, and it's time for synergies, especially at the interdisciplinary level. The «mirror of artificial intelligence» can help identify flaws and solutions, ensuring the future of AI and human society is decided by the people. In a digital society, technology is integrated into people's lives, including crime, victimization, and justice. Digital technologies blur the boundaries between online and offline realities, creating a human-technological hybrid world where crimes occur in virtual networks. AI has potential for social good and Sustainable Development Goals, but concerns about human rights violations need to be addressed. Multidisciplinary approaches are needed to ensure safe use, address education inequalities, enhance justice, and identify online behavior as deviant or criminal. In the context of emerging technoethics, the idea that this unofficial norm, derived from a popular belief, will be the 'touchstone' for characterising online mediated behaviour as deviant/crimninal, is missing - or rather in the process of being formed.

Scientific novelty: the author aims to provide some insightful thoughts on formulating the right questions and interesting reflections from a technoethical perspective on the phenomenon of the use of information and communication technologies for criminal purposes under the catalytic influence of AI, recognising the social challenges arising from technological disruption (e.g. prediction and prevention through the transformation of policing, increased surveillance and criminal justice practises) in "digital society".

Practical significance: some of the initial ideas of this theoretical material can be used in the elaboration of proposals for amendements and additions to the current crime legislation, as well as in pedagogical activity, especially in the implementation of educational courses or modules on crime in the context of the digital transformation of society.

For citation

Spyropoulos, F. (2024). New Approaches to Researching AI Crime: Institutionalization of Digital Criminology. *Journal of Digital Technologies and Law, 2*(3), 636–656. https://doi.org/10.21202/jdtl.2024.32

References

Aas, K. F. (2007). Beyond the desert of the real: Crime control in a virtual(ised) reality. In Y. Jewkes (Ed.), *Crime Online* (pp. 160–177). Portland, Oregon: Willan Publishing.

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*, *30*(6), 1665–1687. https://doi.org/10.1108/intr-10-2019-0400

Bayern, S. (2016). The implications of modern business–entity law for the regulation of autonomous systems. *European Journal of Risk Regulation*, *7*(1), 297–309. http://dx.doi.org/10.1017/S1867299X00005729

Baym, N. K. (2015). *Personal Connections in the Digital Age*. England: Polity, Cambridge.

Berendt, B. (2019). AI for the common good?! Pitfalls, challenges, and ethics pen-testing. *Paladyn, Journal of Behavioral Robotics*, *10*, 44–65. https://doi.org/10.1515/pjbr-2019-0004

Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. *IEEE Access*, *10*, 77110–77122. https://doi.org/10.1109/access.2022.3191790

Boddington, P. (2017). *Towards a Code of Ethics for Artificial Intelligence*. Oxford: Springer International Publishing.

Broadhurst, R., Maxim, D., Brown, P., Trivedi, H., & Wang, J. (2019). Artificial Intelligence and Crime. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.3407779

Brown, S. (2006a). The criminology of hybrids: Rethinking crime and law in technosocial networks. *Theoretical Criminology*, *10*(2), 223–244. https://doi.org/10.1177/1362480606063140

Brown, S. (2006b). Virtual criminology. In E. McLaughlin, & J. Muncie (Eds.), *The Sage Dictionary of Criminology* (pp. 224–258). London: Sage.

Bunge, M. (1977). Towards a Technoethics. *Monist*, *60*(1), 96–107.

Caldwell, M., Andrews, J. T., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 1–13. https://doi.org/10.1186/s40163-020-00123-8

Castells, M. (1996). *The Rise of the Network Society*. Oxford, England: Blackwell.

Castells, M. (2001). *The Internet Galaxy*. Oxford, England: Oxford University Press.

Coeckelbergh, M. (2019). Artificial Intelligence: some ethical issues and regulatory challenges. *Technology and regulation*, *2019*, 31–34. https://doi.org/10.26116/techreg.2019.003

Danaher, J. (2022). Techno-optimism: an analysis, an evaluation and a modest defence. *Philosophy & Technology*, *35*(54), 8. https://doi.org/10.1007/s13347-022-00550-2

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-022-09457-y

Dignum, V. (2019). *Responsible artificial intelligence: how to develop and use AI in a responsible way*. Cham, Switzerland: Springer Nature Switzerland AG.
Dilek, S., Cakır, H., & Aydın, M. (2015). Applications of artificial intelligence techniques to combating cyber crimes: A review. *IJAIA*, *6*(1), 21–39. https://doi.org/10.5121/ijaia.2015.6102
Goldsmith, A., & Brewer, R. (2014). Digital drift and the criminal interaction order. *Theoretical Criminology*, *19*(1), 112–130. https://doi.org/10.1177/1362480614538645
Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, *10*(2), 243–249. https://doi.org/10.1177/a017405
Greenfield, A. (2017). *Radical Technologies*. London: Verso.
Haraway, D. (1987). A manifesto for Cyborgs: Science, technology, and socialist feminism in the 1980s. *Australian Feminist Studies*, *2*(4), 1–42. https://doi.org/10.1080/08164649.1987.9961538
Haraway, D. (1991). *Simians, Cyborgs and Women: The Reinvention of Nature*. London: Free Association Books.
Hayward, K., & Maas, M. (2020). Artificial intelligence and crime: A primer for criminologists. *Crime Media & Culture*, *17*(2), 1–25. https://doi.org/10.1177/1741659020917434
Hayward, K. (2012). Five spaces of cultural criminology. *British Journal of Criminology*, *52*(3), 441–462. https://doi.org/10.1093/bjc/azs008
Heller, P. B. (2012). Technoethics: The Dilemma of Doing the Right Moral Thing in Technology Applications. *International Journal of Technoethics (IJT)*, *3*(1), 14–27. https://doi.org/10.4018/jte.2012010102
Hibbard, B. (2015). *Ethical Artificial Intelligence*. WI, USA: Madison.
Hoanca, B., & Mock, K. J. (2020). Artificial intelligence-based cybercrime. In *Encyclopedia of criminal activities and the deep web* (pp. 36–51). IGI Global.
Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, *35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209
Ionescu, B., Ghenescu, M., Răstoceanu, F., Roman, R., & Buric, M. (2020). Artificial intelligence fights crime and terrorism at a new level. *IEEE MultiMedia*, *27*(2), 55–61. https://doi.org/10.1109/mmul.2020.2994403
Jaishankar, K. (2008). Space transition theory of cybercrimes. In F. Schmallager, & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). New Jersey: Prentice Hall.
Johnson, D. G., & Verdicchio, M. (2017). Reframing AI discourse. *Minds and Machines*, *27*(4), 575–590. https://doi.org/10.1007/s11023-017-9417-6
Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape. *ACM Computing Surveys*, *53*(1), 1–34. https://doi.org/10.1145/3372823
King, T. C., Aggarwal, N., Taddeo, M. & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, *26*(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0
Lash, S. (2002). *Critique of Information*. London: Sage.
Latour, B. (1993). *We Have Never Been Modern*. Cambridge, Massachusetts: Harvard University Press.
Lee, C. S., & Chua, Y. T. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, *70*(9), 2250–2277. https://doi.org/10.1177/00111287231180093
Li, S. T., Kuo, S. C., & Tsai, F. C. (2010). An intelligent decision-support model using FSOM and rule extraction for crime prevention. *Expert Systems with Applications*, *37*(10), 7108–7119. https://doi.org/10.1016/j.eswa.2010.03.004
Lin, Y. L., Chen, T. Y., & Yu, L. C. (2017). Using machine learning to assist crime prevention. *Proceedings of 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI)*, 1029–1030. https://doi.org/10.1109/iiai-aai.2017.46
LoPucki, Lynn M. (2017, April 17). *Algorithmic Entities. Washington University Law Review (Forthcoming)*, 95. UCLA School of Law, Law-Econ Research Paper No. 17-09.
Luppicini, R. (2008). The Emerging Field of Technoethics. In R. Luppicini, & R. Adell (Eds.), *Handbook of Research on Technoethics*. IGI Global books. https://doi.org/10.4018/9781605660226.ch001
Lupton, D. (2015). Quantified sex: a critical analysis of sexual and reproductive self-tracking using apps. *Culture, Health & Sexuality*, *17*(4), 440–453. https://doi.org/10.1080/13691058.2014.920528
Lupton, D. (2015). *Digital Sociology*. 1st ed. London & New York: Routledge.
McAllister, A. (2018). Stranger than science fiction: the rise of A.I. interrogation in the dawn of autonomous robots and the need for an additional protocol to the U.N. convention against torture. *Minnesota Law Review*, *101*, 2527–2573.

McClendon, L., & Meghanathan, N. (2015). Using machine learning algorithms to analyze crime data. *MLAIJ*, *2*(1), 1–12. https://doi.org/10.5121/mlaij.2015.2101

Mielke, C. J., & Chen, H. (2008). Botnets, and the cybercriminal underground. *Proceedings of IEEE International Conference on Intelligence and Security Informatics (ISI 2008)*, 206–211. https://doi.org/10.1109/isi.2008.4565058

Müller, V. C. (2020). Ethics of artificial intelligence and robotics. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy*. Stanford, CA: Metaphysics Research Lab. Stanford University.

Nguyen, A., Yosinski, J., & Clune, J. (2015). Deep neural networks are easily fooled: high confidence predictions for unrecognizable images. *Proceedings of the IEEE conference on computer vision and pattern recognition,* 7–12 June, 427–436. https://doi.org/10.1109/cvpr.2015.7298640

Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a crime. *Proceedings of ACM SIGSAC Conference*, 1528–1540. https://doi.org/10.1145/2976749.2978392

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? *International Journal for Crime, Justice and Social Democracy*, *6*(2), 17–33. https://doi.org/10.5204/ijcjsd.v6i2.355

van der Wagen, W., & Pieters, W. (2015). From cybercrime to cyborg crime: botnets as hybrid criminal actor-networks. *British Journal of Criminology*, *55*(3), 578–595. https://doi.org/10.1093/bjc/azv009

Wang, X. (2020, April). Criminal law protection of cybersecurity considering AI-based cybercrime. *Journal of Physics: Conference Series*, *1533*(3), 032014. https://doi.org/10.1088/1742-6596/1533/3/032014

Williams, R. (2017). *Lords select committee, artificial intelligence committee, written evidence (AIC0206)*.

Wood, M. A. (2016). Antisocial media and algorithmic deviancy amplification: Analysing the id of Facebook's[1] technological unconscious. *Theoretical Criminology*, *21*(2), 1–18. https://doi.org/10.1177/1362480616643382

Yar, M. (2012). Crime, media and the will-to-representation: Reconsidering relationships in the new media age. *Crime, Media, Culture*, *8*(3), 245–260. https://doi.org/10.1177/1741659012443227

Zardiashvili, L., Bieger, J., Dechesne, F., & Dignum, V. (2019). AI ethics for law enforcement. *Delphi*, *2*(4), 179–185. https://doi.org/10.21552/delphi/2019/4/7

[1] The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation

Author information

Fotios Spyropoulos – PostDoc, PhD, Associate Professor of Criminal Law & Criminology, Faculty of Law, Philips University; Senior Partner of Spyropoulos Law Firm
Address: 4-6 Lamias Street, 2001, P.O. Box 28008, Nicosia, Cyprus; Alexandras Avenue 81, 11474, Athens, Greece
E-mail: fspyropoulos@gmail.com
ORCID ID: https://orcid.org/0000-0001-5950-3583
Google Scholar ID: https://scholar.google.com/citations?user=iKQYLWoAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – April 30, 2024
Date of approval – April 15, 2024
Date of acceptance – September 25, 2024
Date of online placement – September 30, 2024