



Научная статья

УДК 343.2/.7:343.9:004

EDN: <https://elibrary.ru/zmirlt>

DOI: <https://doi.org/10.21202/jdtl.2023.9>

Цифровые тренды криминологии и уголовного правосудия XXI века

Мехрдад Райеджиан Асли

Институт исследования и развития гуманитарных дисциплин
г. Тегеран, Исламская Республика Иран

Ключевые слова

Алгоритмическая криминология, кибервиктимология, киберкриминология, киберпространство, криминология, риск, уголовное право, уголовное правосудие, цифровизация, цифровые технологии

Аннотация

Цель: определение ключевых трендов развития криминологии и уголовного правосудия в условиях значительного расширения цифровизации и применения современных технологий.

Методы: приоритет аналитического метода в его сочетании с описательным методом обеспечили оптимальный инструментарий для поиска и выявления основных цифровых трендов развития криминологии и уголовного правосудия в XXI веке.

Результаты: выявлена возрастающая зависимость уголовно-правовой науки от развития цифровых технологий, которая приводит к изменению сущности и типов современной преступности, моделей поведения преступников, методов и механизмов контроля и предотвращения преступности в свете требований уголовной политики и уголовного правосудия. Подчеркивается двоякая роль глобального тренда цифровизации, достижения которой используются как органами системы уголовного правосудия (в частности, для контроля, управления и предотвращения преступности), так и преступниками – при осуществлении своих преступных замыслов. Установлено, что существенная трансформация криминологии и уголовного правосудия вызвана в значительной степени резким развитием в XXI веке цифровизации и созданных на ее основе современных технологий, являющихся более эффективными, чем обычные методы традиционной криминологии, такие как количественные и качественные оценки, наблюдения, интервью, опросы и др.

Научная новизна: вводятся новые области уголовно-правового знания и соответствующие им дисциплины, образованные исключительно под влиянием цифровизации, такие как киберкриминология и кибервиктимология; в качестве новейшего направления криминологической науки выделяется алгоритмическая (вычислительная) криминология, основанная на страховом праве и теории рисков.

© Райеджиан Асли М., 2023

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Практическая значимость: учет трендов и положительного опыта, полученного в области цифровизации, обуславливает успешное решение задач, связанных с противодействием преступности, трансформацию подходов к содержанию, целям и методологии прикладной криминологии и уголовного правосудия. Глобальный мегатренд цифровизации существенно меняет облик уголовно-правовой науки, задает новые теоретические и прикладные направления ее развития. Своевременное обновление и адаптирование знаний, умений и навыков согласно достижениям цифровизации позволит криминологии и уголовному правосудию соответствовать задачам нового тысячелетия.

Для цитирования

Райеджиан Асли, М. (2023). Цифровые тренды криминологии и уголовного правосудия XXI века. *Journal of Digital Technologies and Law*, 1(1), 235–250. <https://doi.org/10.21202/jdtl.2023.9>

Содержание

Введение

1. Теория риска в контексте цифровизации

1.1. Административная криминология в свете требований предотвращения преступности

1.2. Управление рисками и страховое право в свете проблемы рецидивизма

2. Киберкриминология и виктимология

2.1. Возникновение киберкриминологии в качестве объяснения этиологии киберпреступности

2.2. Необходимость кибервиктимологии для противодействия киберпреступности и виктимизации

3. Алгоритмическая, или вычислительная, криминология

Выводы

Введение

Цифровизация определяется как «интеграция цифровых технологий в повседневную жизнь во всех сферах, где это возможно» (Ochs & Reinmann, 2018). Также ее определяют как применение цифровых технологий для изменения труда в целях создания ценности путем использования новых прогрессивных технологий, развития цифровых сетей и гигантского цифрового потока информации (Scuotto et al., 2019; Cho et al., 2021; Moneva et al., 2022; Khan et al., 2020; van de Weijery & Moneva, 2022; Sampson, 2014). Цифровизация может быть реализована как процесс трансформации чего-либо в цифровую форму, возникающую при использовании цифровых технологий для усовершенствования процессов (Cabada García et al., 2022; Abubotain & Chamakiotis, 2020; Lallie et al., 2021; Okutan & Çebi, 2019; Solak & Topaloglu, 2015).

Учитывая вышеуказанные определения, цифровизация может найти применение во многих областях науки, включая, в частности, гуманитарные и общественные дисциплины. При этом уголовно-правовые дисциплины относятся к тем областям гуманитарных и общественных наук, в которых цифровизация может сыграть значительную роль. Два основных направления исследований в уголовно-правовой науке, которые испытали особенно сильное влияние цифровизации и развития технологий в последние десятилетия, – это криминология и уголовное правосудие.

По сравнению с 1980–1990-ми годами в области криминологии появились новые подходы и теории, связанные с развитием общественных наук и критического знания, которые привели к созданию критической криминологии и других современных тенденций в этой науке. В начале XXI века криминология и уголовное правосудие начали развиваться в свете цифровизации и технологий, особенно компьютеризации. Таким образом, в этих областях возникло несколько тенденций и даже новых направлений науки. Три из которых рассматриваются в данной статье, а именно: теория управления рисками и страховое правосудие – тенденция, появившаяся в последние десятилетия прошлого века; киберкриминология и кибервиктимология, а также алгоритмическая, или вычислительная, криминология, возникшая за два десятилетия третьего тысячелетия.

В широком смысле, учитывая вышеуказанные определения, роль и положение цифровизации в криминологии и уголовном правосудии описываются концепциями и теориями, берущими начало в возникновении криминологии. Автор делает попытку обнаружить и показать самые значимые примеры и проявления тех концепций и теорий, которые могут продемонстрировать процесс цифровизации этих двух важнейших направлений уголовно-правовой науки через их достижения за два десятилетия XXI века. Соответственно, в данной статье выделены три основные части. В первой части речь идет об управлении рисками как криминологической теории, связанной со страховым правом и исследуемой в контексте цифровизации. Во второй части два новых раздела уголовно-правовой науки – киберкриминология и кибервиктимология – рассматриваются в свете компьютерных наук. Третья часть посвящена алгоритмической, или вычислительной, криминологии, развившейся за последние два десятилетия в рамках криминологии и уголовного правосудия.

1. Теория риска в контексте цифровизации

Риск – важнейшее ключевое понятие нескольких разделов криминологии, включая функционирование системы уголовного правосудия, модели предотвращения преступности и криминальную этиологию, базирующуюся на теории рационального выбора (O'Malley, 2009). Прежде чем стать центральным объектом науки уголовного правосудия, риск изучался в рамках классической криминологии с точки зрения рационального выбора при преступном поведении. Такая точка зрения предполагает, что криминальное поведение дает преступникам преимущество и основывается на их свободно принимаемых решениях. Однако ранее было показано, что эта теория применима лишь к определенным типам преступлений – так называемым утилитарным преступлениям, при которых преступное поведение направлено на получение выгоды (McLaughlin & Muncie, 2019).

1.1. Административная криминология в свете требований предотвращения преступности

Независимо от применимости теории рационального выбора к определенным типам преступлений, она используется для объяснения ситуационного, или оппортунистического, предотвращения преступлений. Эта модель предотвращения преступлений возникла в рамках «административной криминологии» в 1980-е гг. Она определяется как направление криминологии, фокусирующееся на повышении эффективности системы уголовного правосудия, в частности, путем ситуационного, или оппортунистического, предотвращения преступлений (Halder, 2021). Постулируя, что преступники действуют рационально и обдуманно, административная криминология рассматривает преступление как событие, в котором роли преступника и жертвы и другие обстоятельства являются компонентами преступного поведения (McLaughlin & Muncie, 2019). Согласно теоретическим и прикладным положениям криминологии и уголовного правосудия, административная криминология базируется на этиологической точке зрения, которая носит название «криминология преступного поведения». Эта точка зрения берет начало в европейском (особенно французском) подходе к изучению преступности. Как указывает французский криминолог Raymond Gassin, криминология преступного поведения включает в себя теорию совершения действия, которая объясняет преступное поведение как процесс, в ходе которого формируется поведение от намерения до самого акта (Gassin, 1990). Таким образом, эта теория учитывает преступный расчет как существенный элемент административной криминологии. Преступный расчет предполагает, что преступник действует на основе рациональной оценки. Поэтому для контроля и предотвращения преступности необходим ряд технико-технологических инструментов и средств измерения. Они составляют модель ситуационного, или оппортунистического, предотвращения преступлений, которая включает такие средства и методы, как системы видеонаблюдения и охранной сигнализации.

Введя административную криминологию как новое направление уголовной этиологии и уголовной политики, криминологические исследования перешли к оценке рисков в системе уголовного правосудия.

1.2. Управление рисками и страховое право в свете проблемы рецидивизма

На раннем этапе оценка риска имела критическое значение для клинического прогнозирования и судебной экспертизы. В то же время она использовалась для работы с факторами риска с этиологической точки зрения (Pritchard et al., 2014). Сегодня оценка риска получила новую трактовку в рамках страхового права. Страховое право – это подход в криминологии, возникший из сферы страхования. Он предполагает использование компьютерного программного обеспечения (McLaughlin & Muncie, 2019) и представляет собой теоретическую модель на основе концепций и методов, сходных со страховой математикой (Bosworth, 2005).

Распространение этой модели в уголовном праве произошло благодаря актуарному статистическому моделированию рисков, т. е. в рамках страховой отрасли (Metcalf, 2004). В криминологии и уголовном правосудии страховое право использует расчетные методы, которые формируют основу для уголовной политики, в частности, в области коррекции и пенитенциарной системы. Таким образом, это одна

из моделей уголовного правосудия, в рамках которой реабилитация как механизм уголовных санкций получает новую интерпретацию через вероятностное исчисление и статистические распределения для управления заключенными, особенно в тюремной системе. В свете этого подхода управление заключенными осуществляется на основе технологий и практики оценки рисков (McLaughlin & Muncie, 2019). Ярким примером служит использование таких мер и средств, как пробация, при управлении рисками в приложении к проблеме рецидивизма опасных, в частности сексуальных, преступлений. Например, сегодня суды в США используют компьютерные программы, чтобы предсказать вероятность повторения преступления в будущем. Этот метод внедряется как в процесс принятия судебных решений, так и в тюремную систему. Рассматривая такие переменные, как точность и справедливость, критики заявляют, что компьютерная программа может демонстрировать расовую предвзятость, особенно в пользу белых по сравнению с чернокожими (Dressel & Farid, 2018).

На уровне профилактики в аспекте ситуационного, или оппортунистического, предотвращения преступлений управление рисками связано с теми методами сокращения уровня преступности (McLaughlin & Muncie, 2019), которые используют технологии и стратегии снижения возможностей для совершения преступлений в отношении их организации и сопутствующих обстоятельств. Как писал один из основателей новой пенологии Feeley, «страховое правосудие стремится предсказать будущее преступное поведение человека, в настоящий момент осужденного системой уголовного правосудия, а затем применить к нему меры, снижающие его возможности для совершения будущих преступлений» (Feeley, 2004). Типичным примером могут служить США, где применяются различные меры оценки рисков, основанные на страховом праве. Одним из значимых методов оценки риска является метод COMPAS – профилирование осужденного преступника для управления альтернативными санкциями. Этот метод используется с 1998 г. для оценки более миллиона лиц в системе уголовного правосудия. При этом с 2000 г. используется компонент прогнозирования рецидивизма из шкалы COMPA (шкала риска рецидивизма). Эта компьютерная программа предсказывает риск совершения преступления лицом в течение двух лет с момента оценки на основании личных демографических данных и уголовного прошлого (Dressel & Farid, 2021). Данный метод оценки риска позволил концептуализировать «прогнозирование совершения преступлений» в качестве ключевого понятия криминологии и уголовного правосудия. Это понятие относится к рецидивизму (повторению преступления), которое играет важную роль в контроле преступности. Используя методы и технологии, позволяющие предсказать преступления, можно достичь более адекватных результатов применения мер уголовного правосудия.

Сегодня ученые признают, что инструменты управления рисками и оценки рисков, применяемые для предотвращения и прогнозирования преступлений, достойны более пристального внимания со стороны юристов и судебных органов¹. Таким образом, можно утверждать, что необходимо создать юриспруденцию рисков для судей и других органов уголовного правосудия (например, прокуратуры).

¹ A Primer on Risk Assessment Instruments for Legal Decision-Makers. Vanderbilt Law School. https://law.vanderbilt.edu/academics/academic-programs/criminal-justice-program/Primer_on_Risk_Assessment.pdf

2. Киберкриминология и виктимология

Широкое использование технологий и Интернета в современном мире, особенно с наступлением третьего тысячелетия, выдвинуло на первый план их криминальные аспекты во всех сообществах. Одним из основных аспектов развития технологий и Интернета являются киберпреступность и виктимизация. Эта проблема привлекает внимание криминологов уже несколько десятилетий. Результатом такого внимания стало развитие киберкриминологии и виктимологии.

2.1. Возникновение киберкриминологии в качестве объяснения этиологии киберпреступности

Киберкриминология – это одно из новейших направлений междисциплинарных исследований в уголовно-правовой науке, которое объединило достижения уголовного правосудия и компьютерных наук для изучения углубляющихся проблем компьютерной преступности. С развитием технологий и науки преступность и преступное поведение также изменились. Следовательно, необходимо пересмотреть теории и типологии преступности на основе этого развития. Это означает, что киберпреступность и преступники изменяются с течением времени, осваивая новую деятельность, получая новый опыт и совершенствуя навыки (Jahankhani, 2018). Киберпреступность определяется как преступная деятельность с использованием технологий и цифровизации. Она включает незаконные деяния и действия, в том числе доступ к информации, перехват или повреждение данных, вмешательство в работу компьютерных систем или устройств и т. д. Обычно киберпреступность подразделяют на преступления, связанные с информацией, и преступления, связанные с компьютерными сетями. Киберкриминология позволяет узнать, каким образом компьютеры можно использовать для совершения преступлений и какие преступления можно совершить с помощью компьютера. Как указывают некоторые авторы, «интегрированный характер Интернета и преступлений, совершаемых с его помощью, привели к экстренной необходимости анализировать киберпреступность иначе, чем другие виды преступлений» (Maheshwari, 2021).

С исторической точки зрения, начиная с 1990-х гг. криминологи обратили внимание на то, что киберпространство стало новой площадкой для совершения преступлений. Это пошатнуло парадигму классической криминологии, которая оказалась неспособна объяснить новые формы девиаций, преступлений и социального контроля в киберпространстве. Как писал основатель киберкриминологии Jaishankar, «криминология потерпела поражение в исследовании феномена киберпреступности и не смогла вовремя признать важность киберпространства в изменении природы и масштаба преступности и виктимизации» (Jaishankar, 2007). Он ввел киберкриминологию как отдельную дисциплину, чтобы объяснить и проанализировать преступления, совершаемые в Интернете. Как междисциплинарное направление, киберкриминология является областью исследований на стыке между компьютерными науками и криминологией. Jaishankar определяет киберкриминологию как «науку о причинах преступлений, совершаемых в киберпространстве, и их влияние на физический мир» (Jaishankar, 2007). В книге «Изучение преступлений и преступного поведения в Интернете с помощью киберкриминологии», вышедшей под редакцией Jaishankar, он объясняет, почему он ввел киберкриминологию как отдельную

дисциплину, изучающую киберпреступность с точки зрения общественных наук, и выделил отдельный корпус знаний для рассмотрения киберпреступности отдельно от компьютерно-технической экспертизы (Jaishankar, 2011). Будучи первопроходцем в области киберкриминологии, Jaishankar внес большой вклад в развитие теории перехода пространства для объяснения причин совершения преступлений в киберпространстве (Jaishankar, 2011). Согласно его теории, перемещение людей из физического пространства в киберпространство и наоборот происходит по-разному. Другими словами, люди действуют и ведут себя по-разному, перемещаясь из физического пространства в киберпространство (Jaishankar, 2007).

Рассматривая место киберкриминологии в дискурсе общественных и уголовно-правовых наук, некоторые ученые признают, что «хотя киберкриминология – это развивающаяся область криминологии, которая еще не получила адекватного внимания от классической криминологии, будущее обещает огромные перспективы этой новой дисциплине. По мере того, как виртуальные сообщества и электронные племена будут распространяться по киберпространству, а уровень преступности будет повышаться, киберкриминология получит толчок к развитию и свою долю внимания. Она будет по-прежнему активно искать ответы на фундаментальные вопросы о контекстах и причинах преступности в киберпространстве, как и пути достижения общественного порядка» (Ndubuez, 2019).

2.2. Необходимость кибервиктимологии для противодействия киберпреступности и виктимизации

Наряду с развитием киберкриминологии, необходимость общественно-правового взгляда на виктимизацию в киберпространстве определила появление параллельного направления исследований – кибервиктимологии. Этот термин был предложен индийскими криминологами-виктимологами К. Jaishankar и Debarati Halder для изучения виктимизации в Сети и выработки практических решений данной проблемы (Jaishankar, 2020; Halder, 2022).

В книге «Кибервиктимология: новое направление виктимологии XXI века» Jaishankar пишет: «Примечательно, что некоторые ученые не воспринимают виктимизацию от киберпреступности как новую форму виктимизации, а некоторые отказываются признавать их общие черты. В любом случае многие страны борются с виктимизацией от киберпреступности с помощью своих обычных законов, не создавая особых законов. Эти новые явления позволили изучать кибервиктимизацию с различных точек зрения. Я подчеркиваю необходимость выделить особое направление виктимологии, то есть кибервиктимологию, для изучения киберпреступности с точки зрения жертв/виктимизации, так как я убежден, что виктимизация от киберпреступности является новой формой виктимизации. В данной главе мы обсудим формирование нового направления виктимологии, называемого кибервиктимологией» (Jaishankar, 2020).

Как показал Jaishankar, виктимизация от киберпреступности является новой формой виктимизации (Jaishankar, 2020). Общим для киберкриминологии и виктимологии является изучение различных аспектов виктимизации от киберпреступности. Индийский коллега этого исследователя, Halder, также утверждает, что характеристики различных групп жертв составляют профиль жертв киберпреступности. Одним из важнейших результатов кибервиктимологии является открытие эффектов

киберпреступлений на различные слои общества. Иными словами, даже индивидуальная кибервиктимизация может повлечь за собой значительный ущерб для другого члена общества (Halder, 2022).

Что касается вопросов цифровизации и новых технологий, киберкриминология и виктимология привлекают наше внимание к Интернету и киберпространству, которые трансформировали жизнь и повседневную деятельность миллионов людей. В то же время эти новые направления общественных и уголовно-правовых наук показали, что Интернет и новые технологии как явления современного мира часто используются недобросовестно (Jaishankar, 2020). Другими словами, Интернет и киберпространство могут сыграть двоякую роль, предоставляя преступникам возможности для их противозаконной деятельности. Что касается различных форм и функций технологий, связанных с Интернетом и киберпространством, исследователи рассматривают преступления и преступную деятельность в них или посредством их, включая компьютерные преступления, цифровые преступления, преступления в сфере информационных технологий, интернет-преступления, виртуальные преступления, электронную преступность, сетевую преступность (Jaishankar, 2020).

Таким образом, нет сомнений, что Интернет и современные технологии играют важную роль в киберпреступности и защите от нее². И все же криминологически-виктимологическая точка зрения не должна игнорироваться в этом отношении, поскольку эти технологии могут предоставлять новые возможности для совершения преступлений и виктимизации онлайн и офлайн.

3. Алгоритмическая, или вычислительная, криминология

Третье направление цифровизации в криминологии, которое мы обсудим в данной статье, возникло под влиянием математики и компьютерных наук. Алгоритмическая криминология и вычислительная криминология – это синонимичные термины, обозначающие данное новое направление, которое связывает криминологию и компьютерные науки. Оно также включает прикладную математику как компьютерные симуляции преступного поведения (Berk, 2013). В свете математики и компьютерных наук криминологические теории получают новый импульс для объяснения вопросов преступности и охраны правопорядка. В то же время существенную роль в вычислительной криминологии играет статистика. Кроме страхового права, основанного на теории управления рисками и оценки риска, вычислительная криминология применяется в сфере правоприменения и системе уголовного правосудия. Она также используется для моделирования и симулирования преступных событий, таких как терроризм или киберпреступления, в сложной обстановке. Вычислительная криминология применяется посредством использования вычислительной топологии и алгоритмов, дающих информацию для теории картины преступления (Brantingham, 2011). Это направление решает задачи криминологии с помощью прикладной математики, компьютерных наук и криминологии. Прикладные методы в этой области включают составление алгоритмов, поиск данных, разработку структур данных и программного обеспечения (Harris, 2014).

² Don't Forget Victimology as a Cybersecurity Strategy. <https://www.secureworks.com/blog/dont-forget-victimology-as-a-cybersecurity-strategy>

Наряду с практическими и прикладными задачами, необходимость эмпирических исследований в криминологии, обусловленная поиском этиологии и причин преступности, требует алгоритмического подхода, в частности, для прогнозирования преступлений. Эта концепция связана с проблемой рецидивизма, которая является одной из важнейших в криминологических дискуссиях и теориях. Профилактика рецидивизма – главная цель криминологических санкций и механизмов вынесения приговора, таких как probation и условное освобождение. Эти механизмы связаны с переменной оценки риска в криминологии, что обсуждалось ранее. Они требуют тщательного изучения и точной оценки возможности рецидивизма и соответствия осужденного критериям участия в указанных программах. Прогнозирование совершения преступления занимает особое место в этих процессах изучения и оценки. Используемые при этом алгоритмические методы являются более эффективными, чем обычные методы исследования традиционной криминологии, такие как количественные и качественные оценки, наблюдения, интервью, опросы и др.

В целом преступность развивается по тем же закономерностям, что и неправомерное поведение (Brantingham, 2011). Следовательно, точное понимание этих закономерностей будет зависеть от использования современных методов и механизмов, которые применяются в алгоритмической, или вычислительной криминологии.

Выводы

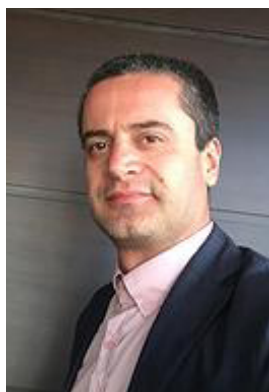
Современные технологии, Интернет и киберпространство изменили природу, типы и обстоятельства преступлений и преступников, а также инструменты контроля над ними. Новые формы преступности (например, киберпреступность) представляют более серьезную угрозу и опасность для всех слоев общества. Эта реальность значительно влияет на технологии контроля и предотвращения преступности, что в свою очередь приводит к появлению новых форм преступности. Рассматривая эти изменения в третьем тысячелетии, необходимо радикально изменить подходы к содержанию, целям, а особенно методологии криминологии, чтобы успешно разрешать проблемы и справляться с задачами, связанными с преступностью. Соответственно, криминология должна обновиться в форме различных дисциплин и разделов дисциплин, чтобы соответствовать задачам нового тысячелетия. Три направления криминологии и уголовного правосудия, обсуждавшиеся в этой статье, обнаруживают взаимосвязи и взаимовлияние друг на друга. Общим элементом их взаимодействия является цифровизация, которая ознаменовала появление современных направлений криминологии в последние десятилетия. С точки зрения взаимодействия механизмы управления рисками и оценки рисков в свете страхового права требуют использования и развертывания алгоритмической, или вычислительной, криминологии. Более того, киберкриминология и виктимология, как еще один новый тренд в этой основной дисциплине уголовно-правовой науки, явились результатом требования и запроса компьютерных наук и киберпространства по отношению к киберпреступности, киберпреступникам и их жертвам.

Список литературы

- Abubotain, F., & Chamakiotis, P. (2020). FinTech in the Saudi Context. *Advanced MIS and Digital Transformation for Increased Creativity and Innovation in Business*, 188–208. <https://doi.org/10.4018/978-1-5225-9550-2.ch009>
- Berk, R. (2013). Algorithmic criminology. *Security Informatics*, 2(1). <https://doi.org/10.1186/2190-8532-2-5>
- Bosworth, M. (2005). Actuarial justice. In *Encyclopedia of prisons & correctional facilities* (Vol. 1, pp. 12–14). SAGE Publications, Inc. <https://dx.doi.org/10.4135/9781412952514.n5>
- Brantingham, P. L. (2011). Computational Criminology. *2011 European Intelligence and Security Informatics Conference*. <https://doi.org/10.1109/eisic.2011.79>
- Cabada García, M. J., Quezada Ramírez, S. I., Negrete Gómez, G. A., Villarreal Serrano, E., Colín García, D. L., Villar Cantón, C., Baca Luna, A., Díaz Villanueva, P. D., & Segura-Azuara, N. D. (2022). Social Media Campaign as a Tool for Patient Education of Disease Prevention and Health Promotion: Digital Health Campaign on Osteoporosis Knowledge. In M. Lopez (Ed.), *Advancing Health Education With Telemedicine* (pp. 183–208). IGI Global. <https://doi.org/10.4018/978-1-7998-8783-6.ch010>
- Cho, Y., DioGuardi, S., Nickell, T., & Lee, W. (2021). Indirect cyber violence and general strain theory: Findings from the 2018 Korean youth survey. *Children and Youth Services Review*, 121, 105840. <https://doi.org/10.1016/j.childyouth.2020.105840>
- Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, 4(1). <https://doi.org/10.1126/sciadv.aao5580>
- Dressel, J., & Farid, H. (2021). The Dangers of Risk Prediction in the Criminal Justice System. *MIT Case Studies in Social and Ethical Responsibilities of Computing*. <https://doi.org/10.21428/2c646de5.f5896f9f>
- Feeley, Malcolm M. (2004). Actuarial justice and the modern state. *Punishment, Places and Perpetrators*, 78–93. <https://doi.org/10.4324/9781843924760>
- Gassin R. (1990). *Criminologie*. Paris: Dalloz.
- Halder, D. (2021). *Cyber Victimology: Decoding Cyber-Crime Victimisation* (1st ed.). Routledge.
- Harris, P. (2014). *Computational Analysis and Public Policy of Criminology* (First). Koros Press Limited.
- Jahankhani, Hamid (2018). *Cyber Criminology*. Springer Nature Switzerland AG. <https://doi.org/10.1007/978-3-319-97181-0>
- Jaishankar, K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal. *CERN European Organization for Nuclear Research – Zenodo*. <https://doi.org/10.5281/zenodo.18276>
- Jaishankar, K. (2008). Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, 1, 7–9. <https://doi.org/10.5281/zenodo.18792>
- Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. CRC Press: Taylor & Francis Group.
- Jaishankar, K. (2020). Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology. In *An International Perspective on Contemporary Developments in Victimology*, pp. 3–19. https://doi.org/10.1007/978-3-030-41622-5_1
- Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention*, 148, 105837. <https://doi.org/10.1016/j.aap.2020.105837>
- Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, 102248. <https://doi.org/10.1016/j.cose.2021.102248>
- Maheshwari, R. (2021). Changing Paradigms of Victimization in Cybercrimes: An Analysis, *International Journal of Law Management & Humanities*, 4(3), 2871–2883.
- McLaughlin, E., & Muncie, J. (2019). *The Sage Dictionary of Criminology*. Sage: EBooks.
- Metcalf, C. (2004). Managing Risk and the Causes of Crime. *Criminal Justice Matters*, 55(1), 8–42. <https://doi.org/10.1080/09627250408553585>
- Moneva, A., Leukfeldt, E. R., Van De Weijer, S. G., & Miró-Llinares, F. (2022). Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective. *Computers in Human Behavior*, 126, 106984. <https://doi.org/10.1016/j.chb.2021.106984>
- Ndubuez, P. N. (2019). Cyber Criminology and the Quest for Social Order in Nigerian Cyberspace, *The Nigerian Journal of Sociology and Anthropology*, 14(1), 32–48.
- O'Malley, Pat (2009). Risk and Criminology. *Legal Studies Research Paper*, 9(87), 1–29.

- Ochs, T., & Riemann, U. A. (2018). IT Strategy Follows Digitalization. *Encyclopedia of Information Science and Technology* (4th ed., pp. 873–887). <https://doi.org/10.4018/978-1-5225-2255-3.ch075>
- Okutan, A., & Çebi, Y. (2019). A Framework for Cyber Crime Investigation. *Procedia Computer Science*, 158, 287–294. <https://doi.org/10.1016/j.procs.2019.09.054>
- Pritchard, A. A., Blanchard, A. J. E., & Douglas, K. S. (2014). Risk Assessment. *Criminology*. <https://doi.org/10.1093/obo/9780195396607-0095>
- Sampson, F. (2014). Cyberspace. *Cyber Crime and Cyber Terrorism Investigator's Handbook*, 1–10. <https://doi.org/10.1016/b978-0-12-800743-3.00001-3>
- Scuotto, V., Serravalle, F., Murray, A., & Viassone, M. (2019). The Shift Towards a Digital Business Model. *Women Entrepreneurs and Strategic Decision Making in the Global Economy*, 120–143. <https://doi.org/10.4018/978-1-5225-7479-8.ch007>
- Solak, D., & Topaloglu, M. (2015). The Perception Analysis of Cyber Crimes in View of Computer Science Students. *Procedia – Social and Behavioral Sciences*, 182, 590–595. <https://doi.org/10.1016/j.sbspro.2015.04.787>
- van de Weijer, S. G., & Moneva, A. (2022). Familial concentration of crime in a digital era: Criminal behavior among family members of cyber offenders. *Computers in Human Behavior Reports*, 8, 100249. <https://doi.org/10.1016/j.chbr.2022.100249>

Сведения об авторе



Мехрдад Райеджиан Асли – доктор наук, доцент Института исследования и развития гуманитарных дисциплин

Адрес: 1463645851, Исламская Республика Иран, г. Тегеран, мост Ядегар, шоссе Аль-Ахмад

E-mail: m.rayejian@samt.ac.ir

ORCID ID: <https://orcid.org/0000-0003-0693-1888>

Web of Science Researcher ID:

<https://www.researchgate.net/profile/Mehrdad-Rayejian-Asli>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57195374005>

Google Scholar ID: <https://scholar.google.com/citations?user=WKgazNEAAAAJ>

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

История статьи

Дата поступления – 13 декабря 2022 г.

Дата одобрения после рецензирования – 18 января 2023 г.

Дата принятия к опубликованию – 6 марта 2023 г.

Дата онлайн-размещения – 10 марта 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.9>

Digital Trends of Criminology and Criminal Justice of the 21st Century

Mehrdad Rayejian Asli

Institute for Research and Development in the Humanities (SAMT),
Tehran, Iran

Keywords

Cyber criminology,
cyber victimology,
cyber space,
criminology,
criminal law,
criminal justice,
digitalization,
digital technologies,
risk

Abstract

Objective: to define the key trends in the development of criminology and criminal justice under significant broadening of digitalization and using modern technologies.

Methods: the priority of analytical method combined with descriptive method provided an optimal set of tools for searching and revealing the main digital trends in the development of criminology and criminal justice in the 21st century.

Results: the growing dependence was revealed between criminal-legal science and digital technologies, which leads to the change in essence and types of contemporary criminality, models of criminals' behavior, methods and mechanism of crime control and prevention in the light of requirements of criminal policy and justice. The dual role of the global digitalization trend is highlighted, the achievements of which are used both by the agencies of criminal justice system (in particular, for crime control, management and prevention) and criminals when implementing their criminal intents. It was determined that the essential transformation of criminology and criminal justice is largely caused by a dramatic development of digitalization in the 21st century, as well as by the modern technologies created on its basis, which appear to be more effective than the standard methods of traditional criminology, including quantitative and qualitative estimations, observation, interviews, polls, etc.

Scientific novelty: new spheres of criminal-legal knowledge are introduced, as well as the corresponding disciplines formed exclusively under the influence of digitalization, such as cyber criminology and cyber victimology; algorithmic (computational) criminology, based on actuarial justice and the theory of risks, is highlighted as the most recent trend in criminological science.

Practical significance: the account of trends and positive experience gained in the sphere of digitalization determines the successful solution of the tasks associated with crime counteraction, transformation of approaches to the content, goals and

© Rayejian Asli M., 2023

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

methodology of applied criminology and criminal justice. The global megatrend of digitalization essentially changes the appearance of the criminal-legal science, sets the new theoretical and applied directions of its development. Timely upgrade and adaptation of knowledge, skills and capabilities in compliance with the achievements of digitalization will allow criminology and criminal justice to correspond to the tasks of the new millennium.

For citation

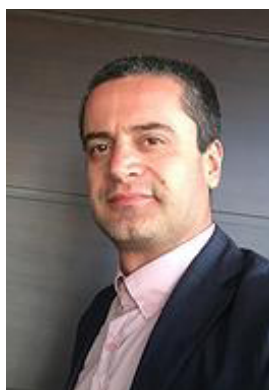
Rayejian Asli, M. (2023). Digital Trends of Criminology and Criminal Justice of the 21st Century. *Journal of Digital Technologies and Law*, 1(1), 235–250. <https://doi.org/10.21202/jdtl.2023.9>

References

- Abubotain, F., & Chamakiotis, P. (2020). FinTech in the Saudi Context. *Advanced MIS and Digital Transformation for Increased Creativity and Innovation in Business*, 188–208. <https://doi.org/10.4018/978-1-5225-9550-2.ch009>
- Berk, R. (2013). Algorithmic criminology. *Security Informatics*, 2(1). <https://doi.org/10.1186/2190-8532-2-5>
- Bosworth, M. (2005). Actuarial justice. In *Encyclopedia of prisons & correctional facilities* (Vol. 1, pp. 12–14). SAGE Publications, Inc. <https://dx.doi.org/10.4135/9781412952514.n5>
- Brantingham, P. L. (2011). Computational Criminology. *2011 European Intelligence and Security Informatics Conference*. <https://doi.org/10.1109/eisic.2011.79>
- Cabada García, M. J., Quezada Ramírez, S. I., Negrete Gómez, G. A., Villarreal Serrano, E., Colín García, D. L., Villar Cantón, C., Baca Luna, A., Díaz Villanueva, P. D., & Segura-Azuara, N. D. (2022). Social Media Campaign as a Tool for Patient Education of Disease Prevention and Health Promotion: Digital Health Campaign on Osteoporosis Knowledge. In M. Lopez (Ed.), *Advancing Health Education With Telemedicine* (pp. 183–208). IGI Global. <https://doi.org/10.4018/978-1-7998-8783-6.ch010>
- Cho, Y., DioGuardi, S., Nickell, T., & Lee, W. (2021). Indirect cyber violence and general strain theory: Findings from the 2018 Korean youth survey. *Children and Youth Services Review*, 121, 105840. <https://doi.org/10.1016/j.childyouth.2020.105840>
- Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, 4(1). <https://doi.org/10.1126/sciadv.aao5580>
- Dressel, J., & Farid, H. (2021). The Dangers of Risk Prediction in the Criminal Justice System. *MIT Case Studies in Social and Ethical Responsibilities of Computing*. <https://doi.org/10.21428/2c646de5.f5896f9f>
- Feeley, Malcolm M. (2004). Actuarial justice and the modern state. *Punishment, Places and Perpetrators*, 78–93. <https://doi.org/10.4324/9781843924760>
- Gassin R. (1990). *Criminologie*. Paris: Dalloz.
- Halder, D. (2021). *Cyber Victimology: Decoding Cyber-Crime Victimization* (1st ed.). Routledge.
- Harris, P. (2014). *Computational Analysis and Public Policy of Criminology* (First). Koros Press Limited.
- Jahankhani, Hamid (2018). *Cyber Criminology*. Springer Nature Switzerland AG. <https://doi.org/10.1007/978-3-319-97181-0>
- Jaishankar, K. (2007). Cyber Criminology: Evolving a novel discipline with a new journal. *CERN European Organization for Nuclear Research – Zenodo*. <https://doi.org/10.5281/zenodo.18276>
- Jaishankar, K. (2008). Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, 1, 7–9. <https://doi.org/10.5281/zenodo.18792>
- Jaishankar, K. (2011). *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. CRC Press: Taylor & Francis Group.
- Jaishankar, K. (2020). Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology. In *An International Perspective on Contemporary Developments in Victimology* (pp. 3–19). https://doi.org/10.1007/978-3-030-41622-5_1

- Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Chen, Y. (2020). Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions. *Accident Analysis & Prevention*, 148, 105837. <https://doi.org/10.1016/j.aap.2020.105837>
- Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, 105, 102248. <https://doi.org/10.1016/j.cose.2021.102248>
- Maheshwari, R. (2021). Changing Paradigms of Victimization in Cybercrimes: An Analysis, *International Journal of Law Management & Humanities*, 4(3), 2871–2883.
- McLaughlin, E., & Muncie, J. (2019). *The Sage Dictionary of Criminology*. Sage: EBooks.
- Metcalf, C. (2004). Managing Risk and the Causes of Crime. *Criminal Justice Matters*, 55(1), 8–42. <https://doi.org/10.1080/09627250408553585>
- Moneva, A., Leukfeldt, E. R., Van De Weijer, S. G., & Miró-Llinares, F. (2022). Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective. *Computers in Human Behavior*, 126, 106984. <https://doi.org/10.1016/j.chb.2021.106984>
- Ndubuez, P. N. (2019). Cyber Criminology and the Quest for Social Order in Nigerian Cyberspace, *The Nigerian Journal of Sociology and Anthropology*, 14(1), 32–48.
- O'Malley, Pat (2009). Risk and Criminology. *Legal Studies Research Paper*, 9(87), 1–29.
- Ochs, T., & Riemann, U. A. (2018). IT Strategy Follows Digitalization. *Encyclopedia of Information Science and Technology* (4th ed., pp. 873–887). <https://doi.org/10.4018/978-1-5225-2255-3.ch075>
- Okutan, A., & Çebi, Y. (2019). A Framework for Cyber Crime Investigation. *Procedia Computer Science*, 158, 287–294. <https://doi.org/10.1016/j.procs.2019.09.054>
- Pritchard, A. A., Blanchard, A. J. E., & Douglas, K. S. (2014). Risk Assessment. *Criminology*. <https://doi.org/10.1093/obo/9780195396607-0095>
- Sampson, F. (2014). Cyberspace. *Cyber Crime and Cyber Terrorism Investigator's Handbook*, 1–10. <https://doi.org/10.1016/b978-0-12-800743-3.00001-3>
- Scuotto, V., Serravalle, F., Murray, A., & Viassone, M. (2019). The Shift Towards a Digital Business Model. *Women Entrepreneurs and Strategic Decision Making in the Global Economy*, 120–143. <https://doi.org/10.4018/978-1-5225-7479-8.ch007>
- Solak, D., & Topaloglu, M. (2015). The Perception Analysis of Cyber Crimes in View of Computer Science Students. *Procedia – Social and Behavioral Sciences*, 182, 590–595. <https://doi.org/10.1016/j.sbspro.2015.04.787>
- van de Weijer, S. G., & Moneva, A. (2022). Familial concentration of crime in a digital era: Criminal behavior among family members of cyber offenders. *Computers in Human Behavior Reports*, 8, 100249. <https://doi.org/10.1016/j.chbr.2022.100249>

Author information



Mehrdad Rayejian Asli – Assistant Professor of Institution for Research and Development in the Humanities (SAMT); Deputy of Research in the UNESCO Chair for Human Rights, Peace and Democracy, Tehran, Iran

Address: 1463645851, SAMT Organization, Al-e-Ahmad Highway, Yadegar Bridge, Tehran, Iran

E-mail: m.rayejian@samt.ac.ir

ORCID ID: <https://orcid.org/0000-0003-0693-1888>

Web of Science Researcher ID:

<https://www.researchgate.net/profile/Mehrdad-Rayejian-Asli>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57195374005>

Google Scholar ID: <https://scholar.google.com/citations?user=WKgazNEAAAAJ&hl=en>

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Article history

Date of receipt – December 13, 2022

Date of approval – January 18, 2023

Date of acceptance – March 6, 2023

Date of online placement – March 10, 2023