Никитенко Илья Викторович
доктор юридических наук, профессор
профессор кафедры уголовного права и криминологии
ДВЮИ МВД России им. И.Ф. Шилова;
профессор ДВФ РГУП им. В.М. Лебедева
г. Хабаровск
ORCID: 0009-0006-7406-7998
Researcher ID: KJM-5058-2024
dfvnii@mail.ru

МЕХАНИЗМ ПРЕСТУПНОГО ПОВЕДЕНИЯ В УГОЛОВНО-ПРОТИВОПРАВНЫХ ДЕЯНИЯХ С ИСПОЛЬЗОВАНИЕМ ГЕНЕРАТИВНЫХ ТЕХНОЛОГИЙ

Аннотация: *статья содержит краткую аналитику особенностей моделирования механизма преступного поведения при совершении уголовно-противоправных деяний с использованием криминогенного потенциала электронно-информационных технологий способных генерировать новую информацию в электронно-цифровой форме (digital content).*

Ключевые слова: *генеративные технологии, дипфейки, контент, криминогенные факторы, механизм преступного поведения, цифровой обман.*

Nikitenko Ilya Viktorovich
Doctor of Law, Professor
Professor of the Department of Criminal Law and Criminology
Far Eastern Law Institute of the Ministry of Internal Affairs of Russia named after I.F. Shilov;
Professor at the Far Eastern Federal University
Khabarovsk
ORCID: 0009-0006-7406-7998
Researcher ID: KJM-5058-2024
dfvnii@mail.ru

THE MECHANISM OF CRIMINAL BEHAVIOR IN CRIMINALLY-OFFENSIVE ACTS USING GENERATIVE TECHNOLOGIES

Abstract: *the article contains a brief analysis of the features of modeling the mechanism of criminal behavior in committing criminally-offensive acts using the criminogenic potential of electronic and information technologies capable of generating new information in electronic and digital form (digital content).*

Keywords: *generative technologies, deepfakes, content, criminogenic factors, mechanism of criminal behavior, digital deception.*

Исследуя особенности криминологического моделирования механизма преступного поведения в уголовно-противоправных деяниях с использованием генеративных технологий, целесообразно сосредоточить внимание, на тех объективных факторах, которые влияют на формирование преступной заинтересованности и решимости совершения различных преступлений, в которых криминогенный потенциал подобных технологий имеет определяющее значение.

Экстраполируя же естественнонаучное понимание механизма на человеческое поведение, в общем, и преступное поведение в частности, можно констатировать, что эти явления, как правило, рассматриваются через призму взаимодействия объективных факторов и соответствующих этим факторам субъективных процессов личности, что само по себе весьма логично, так как осознанное поведение индивида представляет собой субъективное отображение объективной реальности [7, с. 42 – 50].

Экстраполируя же естественнонаучное понимание механизма на человеческое поведение, в общем, и преступное поведение в частности, можно констатировать, что эти явления, как правило, рассматриваются через призму взаимодействия объективных факторов и соответствующих этим факторам субъективных процессов личности, что само по себе весьма логично, так как осознанное поведение индивида представляет собой субъективное отображение объективной реальности [3, с. 42 – 50].

Но прежде, стоит напомнить, какие именно преступления имеются в виду. Так, в экспертном сообществе, сложилось устойчивое мнение, что большинство из преступлений, совершаемых через криминальное применение генеративных возможностей нейросетевых технологий, совершаются посредством так называемого – «цифрового обмана».

К наиболее распространённым формам цифрового обмана относят: дипфейки (цифровое клонирование образов и звуков), генерацию фальшивых голосовых сообщений, фишинговые сайты и тому подобное [2, с. 26 – 41].

Не ставя задачу, вновь истолковать содержание указанных терминов, в обобщённом виде можно представить, что перечисленные формы цифрового обмана, не что иное, как преднамеренное использование вновь созданного (синтезированного) контента для введения в заблуждение потенциальной жертвой преступного посягательства.

Можно предположить, что уголовную ответственность за совершение преступлений с использованием генеративных возможностей нейросетевых технологий, должны нести те лица, которые непосредственно взаимодействовали с соответствующей программой при постановке задач в преступных целях. Вероятно и то, что подобное злонамеренное использование рассматриваемых технологий должно следовать из конкретных формулировок, используемых при постановке ранее упомянутых задач.

Основываясь на материалах правоприменительной практики по делам о мошенничествах с использованием нейросетевых технологий можно прийти к выводу, что в адресованном к генеративному ИИ запросе можно не увидеть прямой и непосредственной связи с объективной стороной преступления, в котором используется вновь сгенерированный контент [1].

Так, например, сам процесс формулирования и размещения в нейросетевых чатах запросов можно расценивать лишь как приготовление к тому или иному преступлению.

Судя по материалам отечественной и зарубежной правоприменительной практики по средством цифрового обмана, кроме наиболее распространённого – «цифрового мошенничества», могут быть совершены любые преступления, в которых ложное восприятие объективной реальности способствует достижению преступного результата, на который рассчитывает преступник. Кроме наиболее распространённых преступлений против собственности (преимущественно, мошенничества, кражи, причинения имущественного

ущерба путём обмана или злоупотребления доверием), цифровой обман может быть использован в любых преступлениях в которых цифровой обман является средством реализации преступных намерений. Это, прежде всего, преступления связанные: с распространением заведомо ложной, порочащей и иной, способной причинить существенный вред, либо создать угрозу причинения такого вреда, интересам личности, общества и государства, информации.

Несомненно, что эффективное противодействие таким преступлениям возможно при условии формировании чёткого представления о механизме формирования и реализации преступных намерений. Вместе с этим стоит обратить внимание на завершающие компоненты в механизме преступного поведения рассматриваемых деяний, такие как, оценивание преступного результата и выбор возможных вариантов посткриминального поведения.

С опорой на накопленные теоретические и прикладные знания о криминологической парадигме механизма преступного поведения, логично предположить, что посредством анализа объективных и субъективных криминогенных факторов которые влияют на развитие индивидуальной преступной деятельности в умышленном деянии, можно смоделировать механизм преступного поведения относительно любого умышленного преступления. Относительно же преступлений с использованием нейросетевых технологий, необходимо акцентировать внимание на ряд особенностей в реализации их объективной стороны, которые существенно отличают эти деяния от иных умышленных преступлений, имеющих сопоставимые признаки.

Очевидно, что преступники использующие «цифровой обман» для реализации преступных намерений не контактируют с потенциальными жертвами непосредственно, как это имеет место при совершении обычных преступлений, объективная сторона которых так же состоит из обмана или злоупотребления доверием, но в обычной, не связанной с использованием цифрового контента форме. И как уже отмечалось в общетеоретической части

работы, подобное опосредованное взаимодействие преступников и жертв значительно повышает скрытность и осложняет выявление первых, что существенно повышает возможности избежать уголовного преследования. Это же в свою очередь, способствует формированию стойкого убеждения безнаказанности и мнимой отстранённости от преступных событий, которые происходят вне традиционных причинно-следственных связей. Известно, что многие из рассматриваемых преступлений совершаются с использованием так называемых – «чат ботов», специальных программ которые в режиме «инкогнито», совершают телефонные звонки относительно неопределённого круга лиц, по принципу «случайной выборки». Однако, подобный способ выявления потенциальных жертв, среди случайных абонентов, значительно расширяет криминальный потенциал телефонных мошенников и других преступников, использующих подобные цифровые технологии. Кроме этого, подобные программные комплексы способны анализировать значительные объёмы сведений, выявляя слабые места в системах обеспечения информационной безопасности для получения доступа к персональным данным.

Массовость, скрытность, безнаказанность и широкая вариативность реализации криминальных задач при совершении преступлений с использованием нейросетевых технологий существенно влияет на механизм преступного поведения при совершении таких уголовно-противоправных деяний. Есть основания полагать, что эти криминогенные факторы значительно усиливают влияние на формирование преступной мотивации и решимости совершать рассматриваемые деяния. При этом первый из компонентов механизма индивидуального преступного поведения, а именно, потребность в совершении рассматриваемых преступлений может оставаться неизменной, в виду органичной взаимосвязи с коренными причинами (детерминантами) тех или иных преступлений, без относительно способов их совершения.

Факторы, влияющие на формирование потребности совершить обычное мошенничество, также как и его аналога с применением ранее упомянутого «цифрового обмана» могут быть схожими. Это, прежде всего, связанно с тем, что потребность совершения любого корыстного преступления вызвана стремлением удовлетворить индивидуальные материальные запросы за счёт противоправного присвоения чужого имущества. Это же можно сказать в отношении иных преступлений, совершение которых может быть связанно с применением нейросетевых технологий (преступления против личности, общественного порядка и общественной безопасности, государственной власти и т.д.).

Известно, что потребность совершения упомянутых преступлений формируется под влиянием фундаментальных криминогенных факторов вне зависимости от средств либо способов их совершения. Так например, факторы, влияющие на формирование потребности совершить преступления против жизни и здоровья (зависть, ревность, месть) не зависят от того как именно будут реализованы преступные намерения. Однако известно и то, что часто в качестве отягчающих ответственность обстоятельств рассматриваются те преступные способы и средства, которые способны повысить общественную опасность преступных деяний. Очевидно, что целенаправленное использование криминальных возможностей генеративных технологий при совершении тех или иных преступлений может рассматриваться с позиций усиление мер уголовной ответственности.

Список источников:

1. Бодров Н.Ф., Лебедева А.К. Анализ судебной практики установления обстоятельств в случаях противоправного распространения генеративного контента, созданного с омощью технологий искусственного интеллекта // Юридические исследования. 2024. № 1.
2. Бодров Н.Ф., Лебедева А.К. Понятие дипфейка в российском праве, классификация дипфейков и вопросы их правового регулирования // Юридические исследования. 2023. № 11. С.26-41.

3. Никитенко И. В. Механизм преступного поведения как криминологическая парадигма: теоретическое и прикладное значение // Вестник Дальневосточного юридического института МВД России им. И.Ф. Шилова: № 3 (68), 2024. – Хабаровск. С. 42 – 50