

УДК 343.98

Установление лица, подлежащего уголовной ответственности, при использовании искусственного интеллекта в преступной деятельности¹

Шагапов Исаак Равильевич, аспирант, Уфимский университет науки и технологий, isa.shagapow@gmail.com

В статье рассматривается вопрос об установлении лица, подлежащего уголовной ответственности, при совершении преступления с использованием искусственного интеллекта. Обосновывается, что распространение интеллектуальных цифровых систем изменяет механизм преступного поведения и усложняет традиционное понимание субъекта преступления, поскольку общественно опасный результат нередко опосредуется программным решением, действующим без непосредственного контроля человека в момент реализации. Раскрываются основные подходы к определению круга лиц, подлежащих ответственности, анализируются трудности установления причинной связи, вины и роли каждого участника в общей цепи противоправного поведения. Отмечается значение специальных знаний при исследовании программного кода, журналов регистрации событий, цифровых следов и иных материалов, позволяющих индивидуализировать вклад разработчика, оператора, пользователя и иных лиц.

Ключевые слова: субъект преступления, уголовная ответственность, искусственный интеллект, цифровые следы, специальные знания, расследование преступлений, доказательства.

Цифровое развитие общественных отношений привело к появлению новых способов совершения преступлений, при которых общественно опасный результат достигается не только непосредственными действиями лица, но и посредством использования программных систем, способных выполнять заранее заданные команды, перерабатывать массивы данных и воспроизводить решения без постоянного участия человека. В таких делах вопрос о том, кто именно подлежит уголовной ответственности, перестает быть формальным и приобретает самостоятельное значение для всего процесса доказывания.

Проблема установления субъекта преступления в данной сфере связана не с отказом уголовного права от его базовых положений, а с усложнением фактической картины деяния. Л. В. Санина и В. В. Коломинов справедливо отмечают, что искусственный интеллект уже выступает не только инструментом цифрового развития, но и средством совершения преступных посягательств, что придает расследованию таких деяний повышенную сложность [1, с. 355]. В этой связи правоприменитель сталкивается с необходимостью разграничить роль лица, разработавшего систему, лица, обеспечившего ее функционирование, и лица, использовавшего ее для достижения противоправного результата.

Действующая уголовно-правовая доктрина исходит из того, что субъектом преступления является физическое вменяемое лицо, достигшее установленного законом возраста. Эта конструкция сохраняет силу и применительно к делам, в которых использованы интеллектуальные цифровые системы. И. Н. Мосечкин обращает внимание на то, что попытки рассматривать искусственный интеллект в качестве самостоятельного субъекта уголовной ответственности наталкиваются на непреодолимое препятствие, поскольку такая система не обладает ни виной, ни способностью осознавать общественную опасность совершаемого деяния [2, с. 461].

При этом формальное сохранение классического понятия субъекта преступления не снимает основных затруднений следственной и судебной практики. Когда противоправный результат наступает после работы автономного алгоритма, причинная связь между действиями конкретного лица и наступившими последствиями может быть скрыта сложной технической цепочкой. На уровне фактических обстоятельств преступление нередко выглядит как

результат совместного участия нескольких лиц, каждое из которых вносит собственный вклад в создание, настройку, обучение, запуск и использование цифровой системы.

Именно поэтому в научной литературе получила распространение позиция, согласно которой в делах данной категории необходимо исследовать не отвлеченную связь лица с программой, а его конкретную роль в механизме преступления. З. И. Хисамова и И. Р. Бегишев связывают уголовно-правовую оценку таких деяний с необходимостью разграничения ответственности разработчика, пользователя и иных участников цифрового процесса, если их действия находятся в причинной связи с преступным результатом и охватываются соответствующей формой вины [3, с. 564]. Такой подход представляется наиболее пригодным для практики, поскольку он позволяет не разрушать традиционную конструкцию субъекта преступления и одновременно учитывать специфику интеллектуальных технологий.

Сложность квалификации усиливается в тех случаях, когда цифровая система изначально создавалась для правомерных целей, а противоправный результат возник уже на стадии ее последующего использования либо модификации. При такой модели уголовно-правовое значение приобретают не только свойства самой программы, но и характер предшествующих действий лица, его осведомленность о функциональных возможностях системы и направленность воли на достижение запрещенного законом результата. П. М. Морхат, анализируя правовые проблемы применения искусственного интеллекта, обоснованно подчеркивает, что правовая оценка должна строиться с учетом режима использования соответствующей системы и пределов контроля за ее функционированием [4, с. 63].

Отсюда вытекает еще одно важное положение. В делах о преступлениях с использованием искусственного интеллекта нельзя ограничиваться установлением факта применения цифрового средства. Для признания лица субъектом преступления необходимо доказать, что именно оно определило преступную направленность использования системы, осознавало возможные последствия такого применения и реально влияло на достижение преступного результата. В противном случае возникает риск подмены до-

¹ Научный руководитель: Аминев Фарит Гизарович — профессор кафедры криминалистики, Уфимский университет науки и технологий, доктор юридических наук, профессор.

казывания ссылкой на саму технологию, тогда как уголовная ответственность всегда требует индивидуализации поведения конкретного лица.

Практика показывает, что наиболее сложными являются ситуации, в которых участвуют несколько лиц, действия которых разделены по времени и содержанию. Один субъект создает программную архитектуру, другой осуществляет ее техническую настройку, третий обеспечивает массив данных для обучения, четвертый использует итоговую систему для распространения ложной информации, фишинговых сообщений, дипфейков или иного противоправного контента. В. А. Тирранен отмечает, что преступления с использованием искусственного интеллекта отличаются удаленным способом совершения, высокой скоростью воспроизводства противоправного результата и трансграничным характером, что существенно осложняет выявление лица, подлежащего ответственности [5, с. 10].

Особого внимания заслуживает модель так называемой цепочки ответственности, поскольку именно она позволяет связать уголовно-правовую оценку с реальной цифровой архитектурой преступления. Когда общественно опасный результат возникает как следствие последовательных действий нескольких лиц, задача следствия состоит в разграничении самостоятельного исполнения, соучастия, посредственного причинения и иных форм причастности. Для этого требуется установить, кто определял функциональные пределы системы, кто снимал ограничения, кто обеспечивал незаконный доступ к данным, кто инициировал использование программы в преступных целях, кто извлекал из этого выгоду. Без такой детализации сам вопрос о субъекте преступления остается недоказанным.

Необходимо учитывать и то обстоятельство, что интеллектуальные цифровые системы способны воспроизводить результат, который внешне выглядит самостоятельным, хотя в действительности он заранее обусловлен параметрами, заложенными человеком. В процессуальном смысле это означает, что исследование субъективной стороны нельзя сводить к последнему действию пользователя. Суду и следователю требуется установить, на какой стадии возник преступный умысел, в чьих действиях он выразился и какое лицо обладало реальной возможностью предотвратить наступление общественно опасных последствий. В делах такой категории вопрос о субъекте тесно связан с вопросом о пределах контроля над системой и с объемом осознания лицом ее противоправного потенциала.

Дальнейшее развитие практики невозможно без более активного использования судебной экспертизы. Именно экспертное исследование позволяет не предполагать, а доказывать, кем, когда и в каком режиме использовалась программа, какие изменения внеслись в ее код, какие данные были задействованы и могли ли полученные результаты быть достигнуты без участия конкретного лица. В этой части специальные знания выполняют не вспомогательную, а фактически определяющую функцию, поскольку без них установление субъекта преступления в условиях применения искусственного интеллекта может остаться на уровне вероятностных предположений.

При таких обстоятельствах особое значение приобретают специальные знания. Без исследования программного кода, цифровых

следов, журналов событий, параметров запуска системы, последовательности внесения изменений и характера обмена данными установить роль каждого участника зачастую невозможно. В делах, связанных с созданием и распространением дипфейков, значение имеет не только итоговый контент, но и происхождение исходных файлов, порядок их обработки, признаки использования генеративных моделей и сведения о последующем распространении материала. А. Г. Исакова и А. В. Осин указывают, что исследование технологии создания дипфейков позволяет выявлять признаки вмешательства и тем самым приближает правоприменителя к установлению конкретного виновного лица [6, с. 235].

Следственная практика в настоящее время опирается на общие процессуальные средства: осмотр, обыск, выемку электронных носителей, получение сведений у операторов связи и хостинг-провайдеров, назначение компьютерно-технических экспертиз, допросы разработчиков, администраторов и пользователей. Эти средства сохраняют свое значение, однако в делах рассматриваемой категории они требуют более точной ориентации на цифровую структуру деяния. Для установления субъекта преступления необходимо исследовать не только конечный результат работы системы, но и всю цепь действий, предшествовавших его наступлению.

В научной плоскости это означает необходимость перехода от упрощенного вопроса о том, может ли искусственный интеллект быть субъектом преступления, к более точному вопросу о том, какое лицо должно признаваться субъектом в условиях опосредованного причинения вреда через цифровую систему. При таком подходе искусственный интеллект не занимает место субъекта преступления, а рассматривается как средство, усложняющее механизм деяния и требующее дополнительной доказательственной работы. Уголовно-правовая оценка сохраняет личный характер, но криминалистическая сторона расследования становится значительно более сложной.

Не меньшее значение имеет и вопрос о совершенствовании законодательства. Правоприменительная практика уже нуждается в более четком закреплении подходов к атрибуции деяния при использовании интеллектуальных систем, а также в уточнении правил оценки роли разработчика, оператора, пользователя и иных участников цифрового процесса. Потребность в такой конкретизации обусловлена задачами единообразного применения норм Общей части УК РФ, а также необходимостью более точной правовой реакции на деяния, связанные с незаконным оборотом данных, неправомерным воздействием на компьютерную информацию, распространением дипфейков и иными формами цифровой преступности.

Рассматриваемая проблема не может быть решена за счет одной только уголовно-правовой квалификации. Она требует соединения норм материального права, процессуальных средств доказывания и специальных знаний, позволяющих восстановить фактический механизм деяния. В этом состоит главный вывод: лицо, подлежащее уголовной ответственности, должно устанавливаться не по признаку формальной связи с системой искусственного интеллекта, а по доказанному вкладу в достижение преступного результата, подтвержденному материалами дела и проверенному в процессуальном порядке.

Примечания

1. Санина Л. В., Коломинов В. В. Особенности расследования мошенничества, совершенные с помощью искусственного интеллекта // Право и государство: теория и практика. 2024. N 8.
2. Мосечкин И. Н. Искусственный интеллект и уголовная ответственность: проблемы становления нового вида субъекта преступления // Вестник Санкт-Петербургского университета. Право. 2019. Т. 10. N 3.

3. Хисамова З. И., Бегишев И. Р. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты // Всероссийский криминологический журнал. 2019. Т. 13. N 4.
4. Морхат П. М. К вопросу о специфике правового регулирования искусственного интеллекта и о некоторых правовых проблемах его применения в отдельных сферах // Закон и право. 2018. N 6.
5. Тирранен В. А. Преступления с использованием искусственного интеллекта // Развитие территорий. 2019. N 3.
6. Исакова А. Г., Осин А. В. Применение искусственного интеллекта в расследовании преступлений с использованием технологии «диффейк» // Вестник науки. 2024. Т. 3. N 1.

English version

Establishing the person subject to criminal liability in cases involving the use of artificial intelligence in criminal activity

Shagapov Isaak Ravil'evich, postgraduate, Ufa University of Science and Technology

This article examines the issue of identifying the person subject to criminal liability when a crime is committed using artificial intelligence. It is argued that the spread of intelligent digital systems is transforming the mechanism of criminal conduct and complicating the traditional understanding of the subject of a crime, since the socially dangerous result is often mediated by a software-based decision operating without direct human control at the moment of its implementation. The article outlines the main approaches to determining the range of persons subject to liability and analyzes the difficulties involved in establishing causation, guilt, and the role of each participant in the overall chain of unlawful conduct. It also emphasizes the importance of specialized knowledge in the examination of source code, event logs, digital traces, and other materials that make it possible to individualize the contribution of the developer, operator, user, and other persons.

Keywords: subject of a crime, criminal liability, artificial intelligence, digital traces, specialized knowledge, crime investigation, evidence.