Т. В. Радченко,
кандидат юридических наук,
МИРЭА – Российский технологический университет

РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМЕ УГОЛОВНО-ПРАВОВЫХ И УГОЛОВНО-ПРОЦЕССУАЛЬНЫХ ОТНОШЕНИЙ

Аннотация. Статья посвящена исследованию искусственного интеллекта на современном этапе развития информационных технологий в России и допустимости его применения на досудебной стадии уголовного процесса. Основная цель заключается в анализе состояния современных информационных систем, использующих искусственный интеллект, возможностях и перспективах их применения в процессе доказывания и оценки доказательств, проведении отдельных следственных действий, составлении процессуальных документов следователем. Подчеркнута необходимость разработки четкого, строгого и эффективного правового режима использования технологии искусственного интеллекта в процессуальной деятельности органов предварительного расследования.

Ключевые слова: цифровизация, искусственный интеллект, правовой режим, защита информации, биометрия, уголовная ответственность, расследование преступлений

THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE SYSTEM OF CRIMINAL LEGAL AND CRIMINAL PROCEDURE RELATIONS НАЗВАНИЕ СТАТЬИ НА АНГЛИЙСКОМ ЯЗЫКЕ

Abstract. The article is devoted to the study of artificial intelligence at the present stage of development of information technologies in Russia. A definition is given on the admissibility of its application at the pre-trial stage of criminal procedure. The main goal is to analyze the state of modern information systems that use artificial intelligence. Showing the possibilities and prospects for the use of artificial intelligence in proving and evaluating evidence, in individual investigative actions, in the preparation of procedural documents by the investigator. It's necessary to develop a clear, strict and effective legal order for the use of artificial intelligence in the procedural activities of the preliminary investigation bodies.

Keywords: Digital transformation, Artificial intelligence, Legal order, Information security, Biometrics, Criminal liability, Crime investigation

Развитие информационных технологий и цифровизация большинства направлений деятельности в современной России стремительно меняет привычный образ экономических отношений и способствует построению системы цифровой экономики как наиболее оптимальной среды применения электронных технологий.

Сегодня цифровизация охватила все сферы и направления общественной жизнедеятельности. Польза цифровизации очевидна. Обладая уникальным инструментарием – искусственным интеллектом, она повышает скорость и эффективность обработки и передачи информации, оптимизируя производственные и технологиче-

ские процессы, уменьшая трудозатраты, и в целом, делая нашу жизнь более удобной. Посредством особых свойств современных компьютерных программ – возможности к обучению, генерации сложных нейронных сетей, способных систематизировать большие объемы данных по заданным параметрам, разрешаются многие сложные задачи.

Нормативная дефиниция искусственного интеллекта как «комплекса технологических решений, позволяющего имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека», закреплена в Национальной стратегии развития искусственного интеллекта на период до 2030 года [1], которая указывает на необходимость «адаптации нормативного регулирования в части, касающейся взаимодействия человека с искусственным интеллектом, и выработки соответствующих этических норм», однако без избыточного регулирования, способного замедлить темп развития и внедрения технологических решений.

Искусственный интеллект – система сложных алгоритмов, которые имитируют когнитивные функции человека. В решении многих задач подобные программы давно перешагнули человеческий интеллект: в части системы распознавания текстов, перевода текстов, распознавания речи. Однако нам не всегда известно, каким образом происходит анализ этих данных, работает ли алгоритм с учетом всех условий и параметров, заложенных разработчиками, насколько исключены ошибки и погрешности при использовании. Будет ли конечный результат объективным.

Глубокие нейронные сети принимают решения не на основе известных алгоритмов, и в ряде случаев проанализировать как они выбирают решение невозможно. Непрозрачность этого алгоритма ведет к тому, что прогноз и проверку результатов осуществить нельзя. И в этом кроется опасность тотального использования искусственного интеллекта, потенциально возрастающая.

Любая компьютерная программа, созданная на основе искусственного интеллекта, сегодня не эффективна даже на 99 %, имеет погрешности, выдает ошибки. Так, современные программы защиты информации эффективны в среднем на 80 % и это отличный результат. Но представим, что искусственный интеллект активно используется в социальной и правоохранительной сферах: для постановки диагноза больному, производит профессиональный отбор сотрудников или квалифицирует преступления. Возможность совершения ошибки при этом колеблется в пределах 20 % случаев, что недопустимо. В каждой из этих ситуаций мы столкнемся с крайне негативными последствиями, влекущими применения мер юридической ответственности.

В связи с вышесказанным актуальным представляется вопрос места искусственного интеллекта в системе правовых отношений и уголовно-процесуальных правоотношений, в частности.

С одной стороны технологии искусственного интеллекта могут выступать в качестве средства оптимизации и повышения эффективности деятельности органов предварительного расследования. Поскольку, реализация уголовно-правовых отношений возможна только в процессуальной форме в соответствии с нормами

УПК РФ представляется возможным в рамках данной работы затронуть сферу уголовно-процессуальных отношений, а именно проведение отдельных следственных действий: допроса и очной ставки, в которых дословная фиксация информации допрашиваемого лица максимально важна. Представляется, что использование искусственного интеллекта при проведении этих следственных действий вполне оправдано и позволит повысить эффективность отображения и сохранения информации при переводе записи голоса в текстовый формат. Это позволит избежать формальных ошибок и неточности изложении при традиционных способах составления протокола следователем.

Фиксацию информации, которая потенциально может иметь доказательственное значение также возможно осуществлять с помощью искусственного интеллекта. Так, использование биометрических систем распознавания лица облегчило работу по пресечению и раскрытию преступлений. Однако в ряде случаев полученные данные требуют всесторонней скрупулезной и качественной проверки на достоверность. В частности, информация, полученная с камер видеонаблюдения, обладающих технологией распознавания лица, не может быть признана прямым и единственно достаточным доказательством, а должна быть проверена и подтверждена иными доказательствами по делу, оцениваемыми в совокупности.

Кроме того, указанная биометрическая информация поступает в хранилища персональных данных и содержит подробные данные о человеке, его внешности, биометрических параметрах, местах нахождения, круге общения, предпочтениях и о многом другом, что позволяет составить характеристику конкретного человека. При этом наблюдается крупномасштабный рост накопления информации в системах устройств прослушивания, анкетирования, тестирования, опросов, видеонаблюдения, в действиях на сайтах. Данные, позволяющие идентифицировать личность, превращаются в товар, который можно продать. Подобная информация может быть использована как в благих целях, например, для ускорения оформления документов, получения услуг, отслеживания преступников, но также с противоправными намерениями: для слежки, компрометации, умаления и дискредитации чести и достоинства, нарушения неприкосновенности частной жизни.

Центром экспертной аналитики InfoWatch был произведен анализ статистики незаконного распространения конфиденциальной информации в последние годы. Так, в 2019 г. было зафиксировано 395 случаев утечек данных из российских фирм и государственных учреждений. Объем кажется небольшим в масштабах страны, но, если возможно получить даже такую малую часть, значит, есть потенциальная возможность украсть и другие данные. [2] В последующие годы количество подобных инцидентов продолжало возрастать. Современные масштабы сбора и использования персональных данных хорошо иллюстрирует цитата Эрика Шмидта, возглавляющего Alphabet: «Постепенно вы, как реальный человек, будете интересовать мир все меньше и меньше, а значение вашего цифрового аватара, наоборот, станет неуклонно повышаться, поскольку он очень многое о вас может сказать. Всех будет интересовать ваша цифровая копия, которая хранится в облаках, а не вы. При этом важно понимать, что все

мы будем абсолютно прозрачны для цифрового мира… это ключевой тренд на ближайшие годы» [3].

Сегодня остро стоит проблема создания эффективного и детализированного правового режима, регулирующего использование технологии распознавания лиц как одного из направлений биометрии. Она внедряется практически повсеместно, и активно используется правоохранительными органами при раскрытии и расследовании преступлений в качестве доказательства.

Однако на сегодня не существует систем защиты биометрической информации. Пока их нет, использование этой информации в целях доказывания требует осторожности и тщательной проверки, поскольку в отличие от логинных систем, где информацию можно поменять, в биометрической системе это абсолютно невозможно. Поскольку биометрическая информация на порядок чувствительнее любой другой, то и системы защиты должны быть на порядок выше: даже 1 % ошибок в их работе – это катастрофа, когда чужое лицо распознается как ваше или ваше лицо не распознается. Обе эти ошибки существуют и до сих пор, эффективность работы биометрических систем измеряется процентами, а для по-настоящему эффективной работы, по мнению специалистов должна измеряться 10-тысячными долями процента.

Стремительное развитие информационного общества привело к отставанию в детальном правовом обеспечении данной сферы. При формировании правовых норм, направленных на регулирование применения технологии распознавания лиц, а также использование персональных данных, важное значение имеет определение закономерностей и перспектив развития, анализ законодательной стратегии и тактика правоприменительной практики в этой сфере. Исследуемая проблема требует нового концептуального подхода, исходя из возникающих угроз и в связи с трудностями определения правовой природы указанных информационных феноменов.

Представляется, что сегодня использование искусственного интеллекта затруднительно при осуществлении аналитических мероприятий, требующих высокой степени анализа и оценки всех обстоятельств совершенного деяния. Речь идет о процессе уголовно-правовой квалификации, которая невозможна, на наш взгляд, только с помощью искусственного интеллекта. Каждое преступление помимо признаков элементов состава обладает также и особыми индивидуальными свойствами, учитывать которые должен и искусственный интеллект. Слишком высока в этом процессе роль правоприменителя, его аналитические способности, умение систематизировать и структурировать информацию и на основании этого соотносить обстоятельства совершенного деяния, признакам элементов состава преступления. Очевидно, что каждое противоправное, преступное деяние обладает индивидуальными свойствами, при этом ни одна программа, использующая свойства искусственного интеллекта, не обладает такой широкой вариативностью как человеческий разум. Кроме того, точность и правильность результатов квалификации, осуществляемой искусственным интеллектом, потребует от пользователя внесения исходных данных, а это только затруднит работу следователя/дознавателя, сделает ее наоборот более рутинной.

Подводя итог сказанному, следует отметить, что проблема нормативного закрепления правовой регламентации использования искусственного интеллекта при осуществлении процессуальных действий при осуществлении предварительного расследования требует незамедлительного решения. Основной целью при этом должна стать не попытка заменить человеческий разум компьютерной программой, использующей искусственный интеллект, а оказание помощи правоприменителю в проведении отдельных следственных и процессуальных действий, фиксации материалов расследования в целях оптимизации и повышения эффективности деятельности.

Список литературы

1. Указ Президента Российской Федерации от 10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации». URL: http:// Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 11.10.2019, «Собрание законодательства РФ», 14.10.2019, № 41, ст. 5700 (дата обращения: 19.02.2022).

2. Утечки данных. Россия. 2019 год. Аналитический центр Infowatch. URL: https://www.infowatch.ru/analytics/reports/27614 (дата обращения: 19.02.2022).

3. Четверикова О. Цифровой тоталитаризм. Как это делается в России? – М.: Книжный мир. 2019 // URL: https://iknigi.net/avtor-olga-chetverikova/183838-cifrovoy-totalitarizm-kak-eto-delaetsya-v-rossii-olga-chetverikova/read/ (дата обращения: 19.02.2022).

В. В. Ровнейко,
кандидат юридических наук, доцент,
Удмуртский государственный университет

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОЦЕНКИ «КРАЖИ ИДЕНТИФИКАЦИИ»

Аннотация. Статья посвящена анализу такого понятия как «кража идентификации» и проблемам уголовно-правовой оценки деяний, которые посягают на безопасность цифровой личности. Введение экспериментальных правовых режимов, реализация «пилотных проектов» в «регуляторных песочницах» выявляют новые виды рисков, которые должны быть минимизированы. Так, один из проектов, связанный с использованием биометрических персональных данных при предоставлении банковских услуг, был запущен как регулятивная «песочница» Банка России. Однако «пилот» не взлетел из-за серьезных рисков подделки биометрических данных и документов. Неправомерное использование чужих персональных данных для получения выгоды является «кражей идентификации». Определение понятия «кража идентификации» с учетом положений российского законодательства нуждается в существенной коррекции. Уголовно-правовые средства позволяют рассматривать в качестве основания уголовной ответственности за «кражу идентификации» составы различных преступлений, предусмотренных в УК РФ (например,