УДК 34 **DOI: 10.34670/AR.2021.35.70.011**

Этический аспект применения цифровых технологий в правоохранительной сфере

Шушеначев Алексей Викторович

Аспирант,
Сибирский федеральный университет,
660041, Российская Федерация, Красноярск, просп. Свободный, 79;
e-mail: ashushenachev@inbox.ru

Назаров Александр Дмитриевич

Доктор юридических наук,
заведующий кафедрой, профессор кафедры,
Сибирский федеральный университет,
660041, Российская Федерация, Красноярск, просп. Свободный, 79;
e-mail: goncharovatm@yandex.ru

Аннотация

Внедрение цифровых технологий в сферу деятельности правоохранительных органов порождает ряд проблем этического характера, в частности несанкционированное использование персональных данных, предубежденность алгоритмов, стигматизацию и др. Использование цифровых технологий полицией и другими правоохранительными структурами не только создает новые возможности в процессе обеспечения безопасности, но и предстает – явно или потенциально – как инструмент попрания гражданских свобод и прав человека. т.е. формирования социальных ярлыков, основанных на корреляции между теми или иными преступными проявлениями (либо отрицательными качествами) и отдельным человеком или общностью, на этой основе формируется множество стереотипов. Так, стигматизация, основанная на использовании алгоритмов искусственного интеллекта для предсказания совершения преступления отдельным лицом, может подтолкнуть его к такого рода акту, став, по сути дела, дополнительным фактором риска. Авторы данной статьи выделяют ряд подходов к решению возникающих в сфере правоприменения этических проблем, направленных на минимизацию возможных негативных последствий: обеспечение прозрачности технологий, баланса интересов сторон, повышение уровня правового регулирования применения цифровых технологий и т.д. Подобные негативные тенденции могут быть минимизированы при наличии эффективного – как общественного, так и государственного – контроля. Соответственно, проблемы этического характера, возникающие в правоохранительной сфере, могут быть адекватно и удовлетворительно разрешены в ходе совершенствования современных технологий, эффективного общественного контроля и адекватного правового регулирования.

Для цитирования в научных исследованиях

Шушеначев А.В., Назаров А.Д. Этический аспект применения цифровых технологий в правоохранительной сфере // Вопросы российского и международного права. 2021. Том 11. № 11А. С. 113-120. DOI: 10.34670/AR.2021.35.70.011

Ключевые слова

Цифровизация, искусственный интеллект, этика, права и свободы личности, цифровые технологии, правоохранительная сфера.

Введение

В последние десятилетия на повестку дня выходят процессы цифровизации правоохранительной деятельности. Это явление, будучи пока, по сравнению со сферой услуг или медициной, менее масштабным, сопряжено, тем не менее, с рядом проблем этического порядка. Использование цифровых технологий полицией и другими правоохранительными структурами не только создает новые возможности в процессе обеспечения безопасности, но и предстает – явно или потенциально – как инструмент попрания гражданских свобод и прав человека.

По мнению В.С. Овчинского, «…внедрение цифровых технологий в полицейскую деятельность во многом обусловлено необходимостью противостоять преступному миру, который все лучше вооружается. Криминальный мир активно использует последние достижения четвертой промышленной революции: технологии блокчейна, дроны, ИИ и т.п., а последствия преступлений становятся все более масштабными и тяжелыми, что необходимо учитывать в работе полиции. К современным полицейским структурам предъявляется новое требование – быть открытыми и прозрачными для граждан. Применение цифровых технологий позволяет полиции более эффективно выполнять свои прямые функции, а также повысить доверие граждан и снизить вероятность коррупции».

Основная часть

Следственный комитет РФ формирует в составе своего Главного следственного управления новый отдел – по расследованию киберпреступлений и преступлений в сфере высоких технологий. Эффективно противодействуя преступной деятельности в различных сферах (в том числе в кибернетической), правоохранительные органы должны оперативно реагировать на инновации в области цифровых технологий, своевременно их осваивая. Одним из приоритетов здесь является сбор и обработка массивов данных, многие из которых накапливаются уже сейчас, но не обрабатываются и не используются. В этом аспекте на повестку дня выходит так называемая «предиктивная деятельность» полиции, основанная на стратегии предсказания и последующего предотвращения преступлений с использованием искусственного интеллекта (ИИ).

Этические аспекты такого рода деятельности так или иначе связаны скорее с социальными, нежели с информационными технологиями, а именно с методами сбора информации и принятия решений, касающихся граждан, входящих в «группу риска», – тех, для кого искусственный интеллект предсказывает большую вероятность преступления.

На Западе полицейские службы и судебные органы активно разрабатывают и используют отдельные элементы цифровизации и целые системы ИИ (рис. 1). По данным Е.С. Лариной и Н.

Жолквера, «более чем в 70 странах полицейские на практике используют те или иные виды предиктивной аналитики …

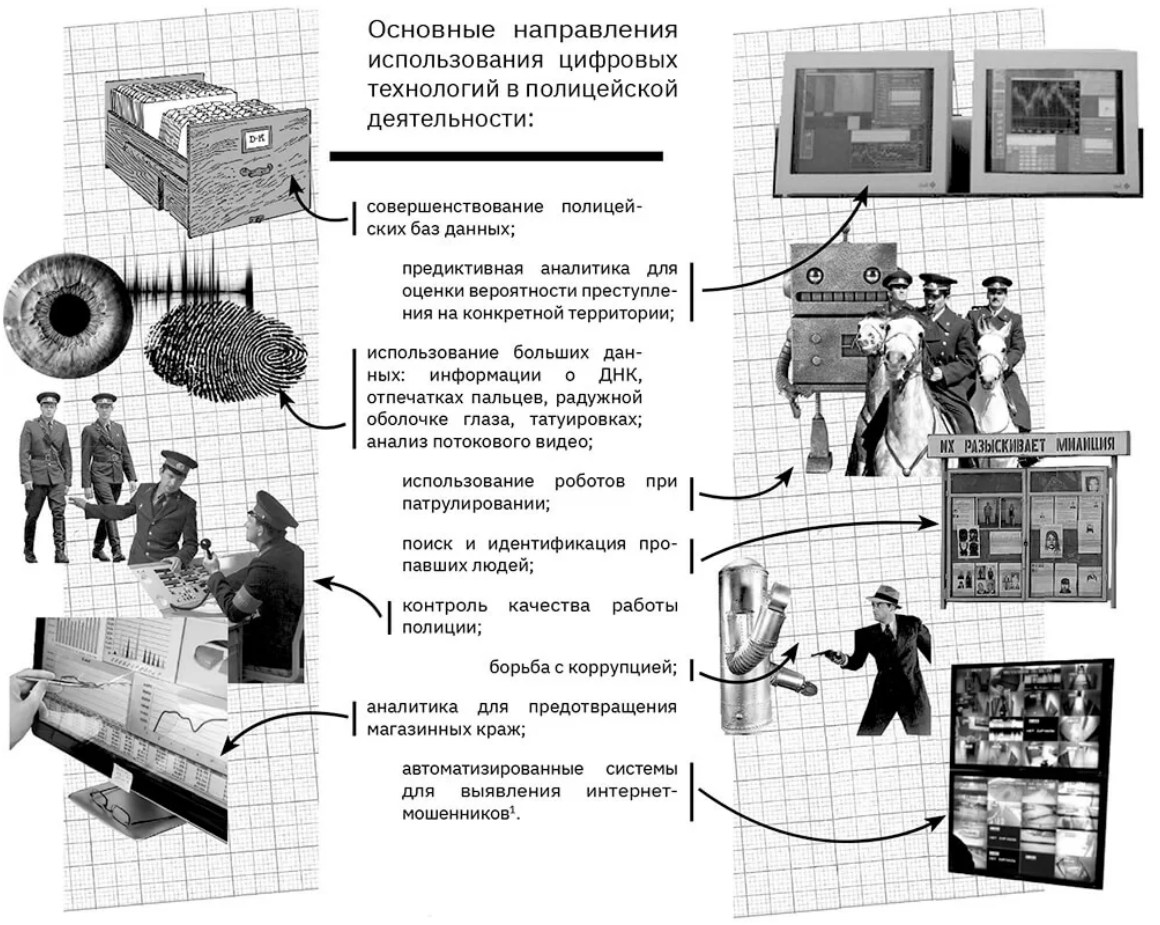

Рисунок 1 – Цифровые технологии в полиции

Помимо узконаправленных систем ИИ, для полицейской работы создаются универсальные комплексные системы, помогающие при расследовании и предотвращении преступлений» [Жолквер, www; Ларина, Овчинский, 2018].

В числе последних необходимо упомянуть систему ePOOLICE, разработанную в 2013 г. по заказу ЕС и способную сканировать содержание сайтов и электронной переписки, а также оперативную информацию с целью выявления признаков активности организованных преступных группировок; она способна также оценить вероятность совершения преступления. В процессе анализа используется информация разных форматов: тесты, видео, содержание социальных сетей, финансовые данные и т.п.

Необходимо подчеркнуть, что этические проблемы, связанные с применением в полицейской деятельности тех или иных цифровых технологий, являются следствием как несовершенства последних, так и собственно человеческим фактором. Одной из принципиальных проблем в этом аспекте, как и в ряде иных областей, является так называемая «предубежденность алгоритмов».

В частности, В.С. Овчинский утверждает, что «…в социологии существует мнение, что все базы данных, сведения для которых собраны в процессе конкретных действий полицейских, например досмотров на улицах, содержат предубеждения. Кроме того, криминальная

статистика не отражает реальный уровень преступлений, а лишь указывает, о каком количестве преступлений стало известно государству, и представляет только ряд социальных характеристик конкретного сообщества (стратификацию, интенсивность и близость взаимодействий и т. д.). Опора на собранные таким образом данные может приводить к неправильным прогнозам, злоупотреблениям по отношению к меньшинствам и группам с низким социальным статусом. Особенно опасно то, что такие прогнозы будут легитимированы, поскольку считается, что технологии объективны, точны и не подвержены влиянию человеческого фактора» [Овчинский, www].

В последнее десятилетие такого рода программы разрабатывались в США. Здесь стоит упомянуть, в частности, программу COMPAS, созданную в Массачусетском технологическом институте в 2014 г.

Эта программа должна была помочь судьям в процессе выработки и принятия решений относительно освобождения того или иного лица под залог либо помещения его под стражу; она использовалась в судах США до тех пор, пока не было выявлено, что ее алгоритм «…априори уменьшает шансы на освобождение для латиноамериканцев, находящихся в стране нелегально, и афроамериканцев с низким доходом» [там же]. Несмотря на статистическую обоснованность предсказаний системы (представители указанных этнических групп действительно чаще нарушали условия освобождения под залог), «расистский уклон» алгоритма вынудил правоохранительные органы США отказаться от ее использования.

Другой опасностью, связанной с цифровизацией деятельности правоохранительных органов, является стигматизация, т.е. формирование социальных ярлыков, основанных на корреляции между теми или иными преступными проявлениями (либо отрицательными качествами) и отдельным человеком или общностью: на этой основе формируется множество стереотипов. Так, стигматизация, основанная на использовании алгоритмов искусственного интеллекта для предсказания совершения преступления отдельным лицом, может подтолкнуть его к такого рода акту, став, по сути дела, дополнительным фактором риска.

По мнению гражданских активистов в США, цифровые системы, вырабатывающие свои решения, основываясь на территориальных данных (социальный состав населения, его плотность, расположение различных учреждений, транспортных узлов и пр.), формируют предубежденность по отношению к жителям неблагополучных районов. Соответственно, прогностическая деятельность полиции способна существенно ухудшить отношения между правоохранителями и населяющими эти территории общинами.

Другая этическая проблема, связанная с цифровизацией деятельности правоохранительных органов, – несанкционированное использование персональных данных. Чаще всего речь идет о видеонаблюдении и слежке, а также контроле над социальными сетями (программно-аналитические системы, ориентированные на автоматическое слежение за социальными сетями, а также семантический анализ тех или иных сообщений) [Ларина, Овчинский, 2018].

Порой для целей расследования полицией используются сведения, предоставляемые коммерческими организациями (банки, телекоммуникационные компании, такси, биллинговые системы и проч.).

В.С. Овчинский говорит о том, что «…практика запросов в компанию Google о местонахождении пользователя впервые была использована федеральными агентами в 2016 году в Северной Каролине и с тех пор распространилась по всей стране. База данных Sensorvault хранит подробные записи о местонахождении сотен миллионов устройств по всему миру за последние десять лет, инструмент обслуживания бизнес-процессов компании Google

постепенно превращается в цифровую сеть для правоохранительных органов. По запросу полиции Google выгружает из Sensorvault информацию об устройствах, отвечающих заданным параметрам. Эта практика вызывает опасения и критику общественности и юристов. Орин Керр, профессор права в Университете Южной Калифорнии, считает, что конфиденциальность невиновных людей, попадающих в поле зрения полиции благодаря цифровым технологиям, – это новая правовая проблема, которую следует решать» [Овчинский, www].

В дополнение к вышесказанному отметим ряд иных актуальных аспектов проблемы, требующих последующего изучения и обсуждения.

Во-первых, имеет место связь процессов внедрения искусственного интеллекта и иных цифровых технологий с численностью полицейских формирований. В ряде структур (в частности, банковских) цифровизация заметно сокращает штат сотрудников; в полиции может сложиться иная ситуация. В процессе усложнения и расширения системы видеонаблюдения объем информации, получаемой полицией и касающейся противоправных действий, требующих уголовно-процессуальной оценки, может существенно возрасти. При этом придется расширять штат экспертов, дознавателей, следователей, оперативных работников.

Во-вторых, подчеркнем расхождение этических рекомендаций, относящиеся к внедрению искусственного интеллекта в полиции, с одной стороны, и в судебной системе – с другой. Несмотря на то, что в принятых в последнее время нормативных документах такого рода ограничения и рекомендации как для судебной системы, так и для полиции одинаковы, специфика их деятельности вынуждает варьировать этическую составляющую. В частности, если принцип прозрачности судебных баз данных возражений не вызывает, то для оперативных данных полиции степень прозрачности может быть существенно ограничена, что, безусловно, связано с уровнем секретности информации и возможными негативными последствиями для ее источников и иных лиц – подозреваемых, обвиняемых и потерпевших.

В-третьих, выделим императив, которым должны руководствоваться сотрудники полиции в процессе сбора информации с использованием средств искусственного интеллекта.

Как полагает Овчинский, здесь «…важен консенсус между полицией и гражданским обществом в отношении целей использования этих данных. Если речь идет о предотвращении и раскрытии терроризма, коррупции, других преступлений, то такой консенсус достижим. Собранная информация будет использоваться для прогнозирования преступных действий на основе соответствующих криминологических и криминалистических критериев. Если же информация станет основанием для ограничения прав и свобод граждан, для построения рейтингов социального кредита, то полиция и гражданское общество вряд ли придут к согласию» [там же].

И наконец, выделим ряд подходов к решению возникающих в сфере правоприменения этических проблем, направленных на минимизацию возможных негативных последствий.

Необходимо обеспечить достаточную степень прозрачности используемых цифровых технологий; использовать возможности искусственного интеллекта в процессе выявления вредных стереотипов; обеспечить баланс интересов всех сторон, так или иначе вовлеченных в процесс внедрения цифровых технологий, –общества, государства и отдельных граждан; предусмотреть достаточный уровень правового регулирования применения цифровых технологий в деятельности органов правоохранительной системы.

Цифровые технологии в деятельности полиции должны внедряться и использоваться под контролем государства и общества. Гражданин должен иметь доступ к своим персональным данным, контролировать их хранение и использование. К сожалению, недостаточное

нормативное регулирование и неравномерный доступ различных групп населения к цифровым технологиям пока не позволяют реализовать этот принцип ни в одной стране. В этом плане правоохранителям еще предстоит создать эффективную систему надзора за использованием средств искусственного интеллекта – как со стороны государства, так и общественных организаций. Задачи такой системы – обеспечение верификации данных для алгоритмов искусственного интеллекта, в равно и предупреждение возможного превышения полномочий со стороны правоохранителей.

Ряд исследователей подчеркивает, что «…в МВД России внимательно относятся к рекомендациям Управления ООН по наркотикам и преступности (United Nations Office on Drugs and Crime), Международного научно-исследовательского института ООН по вопросам преступности и правосудия, его подразделения – Центра искусственного интеллекта и робототехники (UNICRI Centre for Artificial Intelligence and Robotics), Глобального инновационного центра Интерпола, а также Европола. Вопросы применения ИИ в работе полиции неоднократно рассматривались на межведомственных конференциях («Большие данные на службе полиции», 4 декабря 2018 года, Москва; «Искусственный интеллект на службе полиции», 8 ноября 2019 года, Москва, в обоих случаях организаторы – Академия управления МВД России, Главный информационно-аналитический центр МВД России)» [Овчинский, www].

В качестве образца основополагающего нормативного документа в рассматриваемой сфере предлагается, в частности, Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях Европейской комиссии по эффективности правосудия [Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях, www]. Этот документ содержит принципиальные положения в области использования искусственного интеллекта и больших данных, отмечая в то же время необходимость соблюдения прав и свобод личности, декларированных в соответствующих конвенциях Евросоюза.

В частности, в хартии провозглашаются следующие принципы «использования ИИ в судебной и правоохранительной системах» [там же]:

1. «Уважение фундаментальных прав личности». Основные права личности в процессе создания и использования технологий искусственного интеллекта не должны нарушаться.

2. «Недопустимость дискриминации». Дискриминация отдельных групп населения или целых социальных слоев, возможная в ходе применения ряда статистических методов в процессе обработки больших данных, должна блокироваться.

3. «Обеспечение качества и безопасности алгоритмов». В процессе применения больших данных необходимо исследовать их содержание, источники и структуру; при этом необходимо учитывать не только прямые статистические корреляции, но и косвенные факторы, используя, в частности, математические модели междисциплинарного происхождения. Лица, связанные со следствием и судопроизводством, всегда должны понимать, на чем основаны выводы искусственного интеллекта, предлагаемые в качестве автоматизированного экспертного мнения.

4. «Прозрачность систем ИИ». Искусственный интеллект может быть использован как в правоохранительных, так и в судебных структурах лишь при условии прозрачности больших исходных данных.

Заключение

Представляется очевидным то, что, в процессе цифровизации правоохранительные органы применяют все более усложняющиеся технологии, способные представлять потенциальную

опасность для информационной безопасности общества и отдельных граждан, а также норм общественной морали. Подобные негативные тенденции могут быть минимизированы при наличии эффективного – как общественного, так и государственного – контроля. Соответственно, проблемы этического характера, возникающие в правоохранительной сфере, могут быть адекватно и удовлетворительно разрешены в ходе совершенствования современных технологий, эффективного общественного контроля и адекватного правового регулирования.

Библиография

1. Антопольский А.А. Правовое регулирование информационных объектов // Проблемы информатизации. 1999. № 3.
2. Вехов В.Б. и др. Цифровая криминалистика. М.: Юрайт, 2021. 417 с.
3. Городов О.А. Основы информационного права России. СПб.: Юридический центр Пресс, 2003.
4. Громов Г.Р. Очерки информационной технологии. М.: ИнфоАрт, 1993. 331 с.
5. Европейская этическая хартия об использовании искусственного интеллекта в судебных системах и окружающих их реалиях. URL: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4.
6. Жолквер Н. Predictive Policing: как в Германии пытаются предсказывать преступления. URL: https://www.dw.com/ru/predictive-policing.
7. Копылов В.А. Информационное право. 2-е изд. М.: ЮРИСТЪ, 2002. 512 с.
8. Копылов В.А. Информационное право: вопросы теории и практики. М., 2003. 621 с.
9. Ларина Е.С., Овчинский В.С. Искусственный интеллект. Большие данные. Преступность. М.: Книжный мир, 2018. 410 с.
10. Овчинский В.С. Этика цифровых технологий в полиции. URL: https://ethics.cdto.center/7_4.

Ethical issues of using the digital technologies in law enforcement

Aleksei V. Shushenachev

Postgraduate,
Siberian Federal University,
660041, 79 Svobodnyi ave., Krasnoyarsk, Russian Federation;
e-mail: ashushenachev@inbox.ru

Aleksandr D. Nazarov

Doctor of Law,
Head of the department, Professor of the department,
Siberian Federal University,
660041, 79 Svobodnyi ave., Krasnoyarsk, Russian Federation;
e-mail: goncharovatm@yandex.ru

Abstract

The introduction of digital technologies into the sphere of law enforcement agencies generates a number of ethical problems, in particular, unauthorized use of personal data, bias algorithms, stigmatization, etc. The use of digital technologies by the police and other law enforcement agencies not only creates new opportunities in the process of ensuring security, but also appears – explicitly or potentially – as an instrument of violation of civil liberties and human rights. i.e., the formation

of social labels based on the correlation between certain criminal manifestations (or negative qualities) and an individual or community: many stereotypes are formed on this basis. Thus, stigmatization based on the use of artificial intelligence algorithms to predict the commission of a crime by an individual can push him to this kind of act, becoming, in fact, an additional risk factor. The article identifies a number of approaches to solving ethical problems arising in the field of law enforcement, aimed at minimizing possible negative consequences. The authors consider these problems and suggest ways to overcome them: ensuring transparency of technologies, balancing the interests of the parties, increasing the level of legal regulation of the use of digital technologies, etc. Such negative trends can be minimized in the presence of effective – both public and state – control. Accordingly, ethical problems arising in the law enforcement sphere can be adequately and satisfactorily resolved in the course of improving modern technologies, effective public control and adequate legal regulation.

For citation

Shushenachev A.V., Nazarov A.D. (2021) Eticheskii aspekt primeneniya tsifrovykh tekhnologii v pravookhranitel'noi sfere [Ethical issues of using the digital technologies in law enforcement]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 11 (11A), pp. 113-120. DOI: 10.34670/AR.2021.35.70.011

Keywords

Digitalizing, artificial intellect, ethics, human rights and freedoms, digital technologies, law enforcement.

References

1. Antopol'skii A.A. (1999) Pravovoe regulirovanie informatsionnykh ob"ektov [Legal regulation of information objects]. *Problemy informatizatsii* [Problems of informatization], 3.
2. *Evropeiskaya eticheskaya khartiya ob ispol'zovanii iskusstvennogo intellekta v sudebnykh sistemakh i okruzhayushchikh ikh realiyakh* [European Charter of Ethics on the Use of Artificial Intelligence in Judicial Systems and the Realities Surrounding Them]. Available at: https://rm.coe.int/ru-ethical-charter-en-version-17-12-2018-mdl-06092019-2-/16809860f4 [Accessed 16/10/2021].
3. Gorodov O.A. (2003) *Osnovy informatsionnogo prava Rossii* [Fundamentals of information law in Russia]. Saint Petersburg: Yuridicheskii tsentr Press Publ.
4. Gromov G.R. (1993) *Ocherki informatsionnoi tekhnologii* [Essays on information technology]. Moscow: InfoArt Publ.
5. Kopylov V.A. (2002) *Informatsionnoe parvo* [Information law], 2nd ed. Moscow: YuRIST"" Publ.
6. Kopylov V.A. (2003) *Informatsionnoe pravo: voprosy teorii i praktiki* [Information law: questions of theory and practice]. Moscow.
7. Larina E.S., Ovchinskii V.S. (2018) *Iskusstvennyi intellekt. Bol'shie dannye. Prestupnost'* [Artificial intelligence. Big data. Crime]. Moscow: Knizhnyi mir Publ.
8. Ovchinskii V.S. *Etika tsifrovykh tekhnologii v politsii* [Ethics of digital technologies in the police]. Available at: https://ethics.cdto.center/7_4 [Accessed 22/10/2021].
9. Vekhov V.B. et al. (2021) *Tsifrovaya kriminalistika* [Digital forensics]. Moscow: Yurait Publ.
10. Zholkver N. *Predictive Policing: kak v Germanii pytayutsya predskazyvat' prestupleniya* [Predictive Policing: how they try to predict crimes in Germany]. Available at: https://www.dw.com/ru/predictive-policing [Accessed 12/10/2021].