DOI 10.37882/2223–2974.2023.04.14

ЗАЩИЩЕННОСТЬ ОБЪЕКТОВ СОБСТВЕННОСТИ ОТ ПРЕСТУПНОСТИ И ОЦЕНКА НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ ЛИЧНОСТИ

PROTECTION OF PROPERTY OBJECTS FROM CRIME AND ASSESSMENT OF PRIVACY

V. Kowalewski

Summary. The article proves that the digitalization of society and the consequences of the fourth technological revolution require a revision and updating of standards in the field of ensuring human rights and freedoms. The author solves the main question: how to guarantee human rights and ensure the security of personal data in the context of developing digital relations, including ensuring the security of architectural objects and territories.

Keywords: human rights, security of architectural projects, privacy, personal freedom, digital technologies.

Ковалевский Владимир Евгеньевич
Аспирант, Юго-Западный государственный университет
kovalevski27@mail.ru

Аннотация. В статье доказывается, что цифровизация общества и последствия четвертой технологической революции требуют пересмотра и актуализации стандартов в области обеспечения прав и свобод человека. Автором решается главный вопрос: как гарантировать права человека и обеспечить безопасность личных данных в условиях развивающихся цифровых отношений, в том числе обеспечивающих защищенность объектов собственности и градостроительной застройки территории.

Ключевые слова: права человека, защищенность собственности, архитектурный облик цифровой защиты объектов собственности и территории, неприкосновенность частной жизни личности, цифровые технологии.

Цель и предмет работы

Цель работы заключается в поиске баланса между безопасностью и свободой личности в условиях цифровизации. Предмет работы — опыт России в обеспечении архитектурной защищенности объектов с помощью цифровых технологий.

Введение

XXI век характеризуется повсеместным внедрением цифровых технологий и переводом всех процессов жизнедеятельности из офлайн режима в режим онлайн. С помощью инновационных технологий правоохранительными органами обеспечивается защита личности и собственности от преступных посягательств. На государственном уровне многих стран активно разрабатывают стратегии по адаптации законов об использовании современных цифровых технологий. Основные проблемы, однако, заключаются в том, что, с одной стороны, предлагаемые стратегии обеспечивают безопасность и защищенность объектов, а с другой — накладывают тотальный контроль над обществом. Исходя из этого, в условиях цифровизации общества возникает необходимость в создании согласованных, глобальных и всеобъемлющих правовых гарантий, включая надежные гарантии обеспечения частной жизни и свободы личности. В последнее время наблюдается значительный прогресс в развитии указанного научного направления, в том числе со стороны автора исследования [15–19], однако на уровне практического обеспечения защиты частной жизни от систем видеонаблюдения еще существуют проблемы, требующие своего решения.

Обзор литературы. О правовых и этических последствиях бесконтрольного распространения технологий электронного распознавания лица пишет М.А. Михайлов, подчеркивая, что право на частную жизнь входит в прямое противоречие с принимаемыми мерами и неизбежно влечет его ограничение [1, с. 81].

Н.А. Барановым отмечается, «в общественно-политической практике появился термин «цифровой тоталитаризм», под которым понимается тотальный цифровой контроль с помощью видеокамер, гаджетов, цифровых приложений, программ искусственного интеллекта за поведением и действиями человека для дальнейшего выстраивания его рейтинга в обществе. Опасность вторжения государства и общества в частную жизнь человека в условиях цифровизации не уменьшается, а напротив, возрастает. Всевластие органов безопасности и связанные с этим ограничения прав и свобод человека является проблемой не только авторитарных обществ, но и демократических государств» [2, с. 117].

«Если раньше человек как сложная система биологических алгоритмов, уникальных жизненных процессов,

Рис. 1. Рейтинг умных крупнейших городов в 2021 году [6]

субъективных поведенческих моделей и эмоциональных реакций выступал «черным ящиком» — отмечает М. Каку, подразумевая под «черным ящиком» внутренние процессы, неизвестные внешнему наблюдателю,— то с развитием гуманитарных и социальных наук он стал открытой и управляемой системой» [3, с. 223].

А. Гринфилд справедливо разъясняет, что «алгоритмы разрабатываются сторонами, которые не отвечают ни перед кем, кроме своих клиентов и заказчиков, а инструменты, которые они производят, почти никогда не оцениваются по другим критериям, кроме минимального: достаточно, чтобы все видели, что они работают. Мы должны понимать, что происходит на самом деле: беспрецедентное вторжение небольшой группы частных и никому не подотчетных лиц в структуры возможностей и распределение шансов в жизни» [4, с. 330].

Метод и методология проведения работы

В основу исследования легли как общенаучные (анализ, синтез, индукция, дедукция), так и частно-научные методы познания (формально-логический, формально-юридический, сравнительно-правовой, статистический, диалектический). Комплексный подход заключался в использовании при написании статьи не только наук юридического профиля (уголовное право, криминология), но и иных отраслей знаний (психология, архитектура, социология, философия, информационная безопасность и др.).

Результаты работы

Существующее в настоящее время строительство жилых комплексов предполагает наличие всей необходимой охранной инфраструктуры и всего необходимого для безопасного проживания. Архитектурный фактор в данном случае предполагает повышение уровня безопасности и снижение преступности. Предупреждение преступлений против собственности является одной из важнейших задач правоохранительных, и в первую очередь органов внутренних дел.

Заместитель Министра строительства и жилищно-коммунального хозяйства Российской Федерации К.А. Михайлик отметил: «Перед нами стоит огромная задача — к 2030 году построить 120 млн. кв. м. жилья. Но самое важное — сделать это жилье не только доступным, но и обеспечить должный уровень комфорта. И одним из ключевых инструментов реализации поставленной цели является цифровизация отрасли. Все лучшее, что делается в любом отраслевом направлении, должно находить отражение в повседневной жизни человека. Это именно то, чего позволяет достигнуть применение цифровых решений. Именно поэтому мы ведем постоянную работу по совершенствованию ведомственного проекта «Умный город». А основная задача всех участников отрасли — подсказать нам, что еще нужно учесть в этой работе» [5].

В этой связи во многих городах России уже сделан уклон на обеспечение безопасности с помощью цифровых технологий. Так, в большинстве городов функционирует городская система видеонаблюдения, состоящая из тысяч камер, установленных во дворах, подъездах, парках, школах, дорогах и других объектах, требующих мер безопасности. Во многих городах работают сервисы АПК «Безопасный город» и «Умный дом», обеспечивающие круглосуточное видеонаблюдение и предусматривающие другие меры защиты от посягательства на архитектурный объект.

С целью обеспечения безопасности разрабатываются и внедряются отдельные алгоритмы нейросетей.

Рис. 2. Системы «Безопасный город» и «Умный дом» (слева направо)

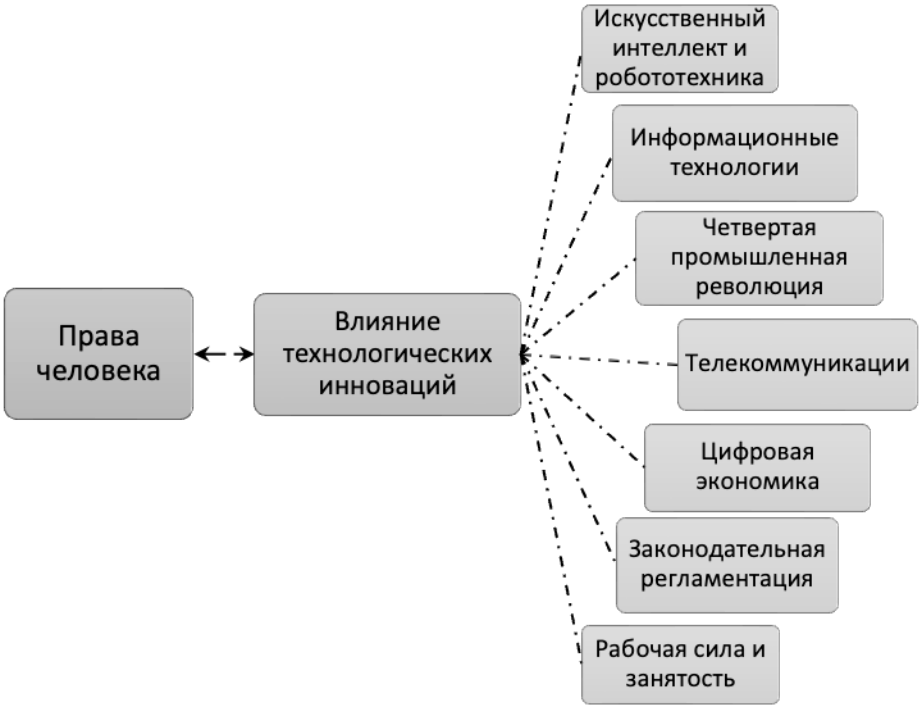

Рис. 3. Влияние технологических инноваций на права человека

Например, система распознавания лиц FindFace позволяет сравнивать пары лиц и проводить поиск по базе в 1,5 млрд. лиц менее чем за 0,3 секунды с точностью 99% [7]. В 2022 году в ряде регионов функционирует система распознавания силуэтов людей, которая актуальна в случаях, когда не удается распознать лицо.

По подсчетам TelecomDaily «сейчас в стране установлено почти 13,5 млн. камер. На каждую тысячу россиян приходится почти 100 камер наблюдения. Агентство выяснило, что большая часть камер в России (58,7%) установлена коммерческими организациями с целью обеспечения безопасности, предотвращения краж и преступлений» [8].

Пожалуй, каждый россиянин хоть раз задумывался о необходимости установки частной охранной системы во дворе, подъезде или даже на лестничной площадке собственного дома для защиты своей собственности, но останавливался из-за нежелания устанавливать круглосуточный контроль за собственной жизнью, доступный сторонним лицам и организациям.

Страхи и сомнения жителей небеспочвенны. Так, «скандал, связанный с программой PRISM, разразившийся с подачи Эдварда Сноудена, показал, насколько ограничена сфера частной жизни. Как выяснилось, американское Агентство национальной безопасности собрало более 97 млрд. телефонных разговоров и электронных сообщений. К сбору информации были привлечены многие известные компании, все делалось без уведомления и согласия пользователей» [9]. При этом камеры городского наблюдения уже считаются обыденностью, «глазами современного большого города».

Выводы, обсуждение и заключения. Проблема полноценной реализации и безопасности прав и свобод человека в цифровую эпоху требует особого внимания.

Как отмечают Е.С. Ларина, В.С. Овчинский, в условиях возрастающих амбиций государства в сфере контроля виртуального пространства особое внимание приобретают вопросы, касающиеся обеспечения неприкосновенности частной виртуальной жизни граждан, тайны переписки, телефонных переговоров, свободы слова в интернете и др. [10, с. 112].

Ярким примером проявления цифрового тоталитаризма является Китай — лидер инновационного развития цифровых технологий и первая страна, внедрившая систему социального рейтинга, предусматривающая «систему оценки отдельных граждан или организаций по различным параметрам, значения которых получаются с помощью инструментов массового наблюдения и использующих технологию анализа больших данных» [11].

«По логике правительства Китая данная система направлена не на ущемление прав граждан, а лишь на ущемление привилегий. Так, низкий социальный рейтинг ведет не к тому, что у тебя отнимут кусок хлеба или лишат свободы, а к тому, что ты не получишь кредит на льготных условиях, не продадут билет со скидкой на скоростной поезд или самолёт или откажут в поездке за границу» [12, с. 381].

Если брать за основу мнение о том, что для государства контроль над обществом куда важнее, чем контроль над отдельной личностью при нормальных условиях её поведения [13 с. 317], то все принимаемые государством меры по обеспечению безопасности архитектурных объектов с помощью цифровых технологий не кажутся проблемой.

Современный человек не должен делать выбор между безопасностью и свободой, поскольку они одинаково важны для комфортного уровня жизни каждого.

Однако государство должно четко дать понять всем правоохранительным структурам и организациям, разрабатывающим и использующим в своей деятельности цифровые технологии, затрагивающие личные данные третьих лиц, что цель такого направления одна — обеспечение безопасности населения, объектов и территории. Все принимаемые и внедренные государством меры не являются средством достижения контроля над обществом.

Сложность возникает в том, что как сообщает начальник отдела городского видеонаблюдения Департамента информационных технологий города Москвы Д.А. Головин, «около 10000 сотрудников органов исполнительной власти и 6 тыс. представителей правоохранительных органов могут просматривать видео в реальном времени и изучать архивы записей на рабочих местах и с мобильных устройств» [14], и нет никаких гарантий, что личные данные не будут использованы не по назначению в других противоречащих государственному замыслу целях.

Таким образом, сделан обоснованный вывод о том, что используемые цифровые технологии, в том числе искусственный интеллект, необходимо применять под жестким государственным и общественным контролем. Для этого в системе МВД РФ следует создать специальный орган по осуществлению мониторинга и анализа полученной видео и фото информации, а на уровне органов прокуратуры межведомственную комиссию с участием общественных наблюдателей для оценки и выработки решений в области использовании систем «Безопасный или умный город», решения которой будут основой для защиты частной жизни человека и баланса интересов общества.

ЛИТЕРАТУРА

1. Михайлов М.А. Правовые и этические аспекты распространения и использования систем идентификации человека путем электронного распознавания лица / М.А. Михайлов // Проблемы получения и использования доказательственной и криминалистически значимой информации: материалы Международной научно-практической конференции, Мисхор (Большая Ялта), 26–27 сентября 2019 года.— Мисхор (Большая Ялта): Общество с ограниченной ответственностью «Издательство Типография «Ариал», 2019, с. 79–82.
2. Баранов Н.А. Цифровые технологии на службе человека и государства: поиск приоритетов / Н.А. Баранов // Теории и проблемы политических исследований, 2020, Т. 9, № 3А, с. 117–127.

3. Гринфилд А. Радикальные технологии: устройство повседневной жизни. — М.: Издательский дом «Дело» РАНХиГС, 2018. 424 с.
4. Каку М. Будущее разума. 4-е изд. — М.: Альпина нон-фикшн, 2018. 646 с.
5. Минстрой России обозначил ключевые направления для развития «Умных городов» в 2022 году [Электронный ресурс]. — Режим доступа: — https://minstroyrf.gov.ru/press/minstroy-rossii-oboznachil-klyuchevye-napravleniya-dlya-razvitiya-umnykh-gorodov-v-2022-godu-/.
6. Результаты оценки хода и эффективности цифровой трансформации городского хозяйства Российской Федерации (IQ городов) по итогам 2021 года [Электронный ресурс]. — Режим доступа: — https://minstroyrf.gov.ru/docs/224339/?sphrase_id=1829573.
7. Обеспечение общественной безопасности [Электронный ресурс]. — Режим доступа: — https://ntechlab.ru/cases/raspoznavanie-lits-dlya-obshhestvennoj-bezopasnosti/.
8. Эксперты назвали Россию третьей в мире по числу камер видеонаблюдения [Электронный ресурс]. — Режим доступа: — https://www.rbc.ru/technology_and_media/25/12/2020/5fe5862d9a7947bc3af51a67.
9. Глаза большого города [Электронный ресурс]. — Режим доступа: — https://www.kommersant.ru/doc/2253867.
10. Ларина Е.С., Овчинский В.С. Искусственный интеллект. Большие данные. Преступность. — М.: Книжный мир, 2018. 416 с.
11. Материал из «Википедии — свободной энциклопедии» [Электронный ресурс]. — Режим доступа: — https://ru.wikipedia.org/wiki/Ротшильд,_Натан_Майер.
12. Ковалевский В.Е. Анализ использования цифровых технологий управления обществом в Китае для практики предупреждения корыстных преступлений против собственности в России // Вопросы российского и международного права, 2022, Т. 12, № 9А, с. 378–386.
13. Протченко А.В. Тотальный контроль в цифровизации: положительные и отрицательные стороны // Скиф. Вопросы студенческой науки,2020, № 12 (52), с. 314–317.
14. Безопасность и комфорт: как работает городская система видеонаблюдения [Электронный ресурс]. — Режим доступа: — https://vc.ru/story/47136-bezopasnost-i-komfort-kak-rabotaet-gorodskaya-sistema-videonablyudeniya.
15. Желудков М.А., Ковалевский В.Е. Критический взгляд на теорию самоактуализации с позиции анализа системных потребностей личности корыстного преступника // Право: история и современность. — 2021. — № 4 (17). — С.122.
16. Желудков М.А. Реализация новой технологии цифрового контроля QR-кодов в предупреждении городской преступности // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. — 2022. — № 1. — С.15.
17. Желудков М.А. Обоснование необходимости адаптации деятельности правоохранительных органов к условиям цифровой трансформации преступной среды // LEX RUSSICA. — 2021. — № 4 (173). — С. 64.
18. Желудков М.А., Орцханова Т.М. Мошеннические действия в сфере финансовой поддержки жилищно-коммунального хозяйства в субъектах РФ: проблемы квалификации // Право: история и современность. — 2020. — № 2 (11). — С.69.
19. Желудков М.А., Ковалевский В.Е. Историко-правовой анализ «Русской Правды» как наиболее древнего правового источника формирования особых способов территориальной защиты от корыстной преступности // Современное право. — 2019. — № 6. — С.135–139.

Журнал «Современная наука: актуальные проблемы теории и практики»