9. Постановление Губернатора Приморского края от 18.03.2020 N 21-пг (ред. от 05.02.2021) "О мерах по предотвращению распространения на территории Приморского края новой коронавирусной инфекции (COVID-2019)" // Приморская газета. Спецвыпуск. 2020. N 22(1756).
10. Защита деловой репутации в случаях ее диффамации или неправомерного использования (в сфере коммерческих отношений): научно-практическое пособие / Д.В. Афанасьев, А.С. Вороженич, М.Е. Глазкова и др.; под общ. ред. М.А. Рожковой. М: Статут, 2015. 270 с.
11. Илесанми М.А. Пандемии и проблема ограничения прав человека // Юрист. 2018. N 8. С. 59 - 65.
12. Конвенция о защите прав человека и основных свобод (Заключена в г. Риме 04.11.1950) (с изм. от 13.05.2004) // Бюллетень международных договоров. 2001. N 3.
13. Международный пакт о гражданских и политических правах (Принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-ом пленарном заседании Генеральной Ассамблеи ООН) // Бюллетень Верховного Суда РФ. 1994. N 12.

Коростиев А.А.

Использование камер наблюдения в целях сохранения общественного правопорядка

*Дальневосточный федеральный университет
(Россия, Владивосток)*

doi: 10.18411/lj-03-2021-228

idsp: ljjournal-03-2021-228

*Научный руководитель
Рабец А.П.*

Аннотация

Развитие средств видеотехники и их удаленная связь с облачными серверами, в результате которой в определенном месте хранятся гигабайты (если не терабайты) информации, с одной стороны позволяет обществу контролировать процессы, протекающие в повседневной жизни и пресекать готовящиеся или же выявлять совершенные правонарушения, а с другой стороны открывает возможности внедрения в такие неподготовленные автоматизированные системы злоумышленников для реализации своих противоправных замыслов. Автор приходит к выводу, что для обеспечения эффективной защиты систем охраны и наблюдения, необходимо провести комплекс мероприятий и разработать механизм специальных защитных мер по недопущению вмешательства посторонних лиц к таким автоматизированным системам.

Ключевые слова: охранные системы наблюдения, несанкционированный доступ, скрытая съемка, терроризм, частная жизнь, идентификация правонарушителя.

Abstract

The development of video equipment and their remote connection with cloud servers, as a result of which gigabytes (if not terabytes) of information are stored in a certain place, on the one hand, allows society to control the processes taking place in everyday life and to suppress preparations or to reveal committed offenses, and on the other the parties open up opportunities for intruders into such unprepared automated systems to implement their illegal plans. The author comes to the conclusion that in order to ensure effective protection of security and surveillance systems, it is necessary to carry out a set of measures and develop a mechanism for special protective measures to prevent unauthorized persons from interfering with such automated systems.

Keywords: security surveillance systems, unauthorized access, covert filming, terrorism, privacy, identification of the offender.

Оборудования, фиксирующие на протяжении времени определенное состояние окружающей среды, различаются по своей направленности: так, если для уличных видеокamer основным назначением является охрана общественных интересов и правопорядка в определенном районе (улице) города, то если затрагивать придомовые

и приквартирные камеры наблюдения, тогда следует говорить о защите прежде всего частных, личных интересов граждан, проживающих в соответствующих зданиях.

Как правило, уличные видеокамеры наблюдения используют для нескольких целей, включая охрану правопорядка и выявления преступлений, совершенных вне жилых либо производственных зданий. При этом, по мнению С.В. Расторопова, городская инфраструктура становится умнее и более подключенной. Это обеспечивает города источниками информации в реальном времени, начиная от традиционных камер безопасности до смарт-ламп, которые ИИ (искусственный интеллект) может использовать для обнаружения преступлений. С помощью ИИ собранные данные могут быть использованы для обнаружения выстрелов и определения места, откуда раздался выстрелы [1].

В работе приводится пример использования американской компанией ShotSpotter наработки по выявлению местоположения выстрела благодаря технологии триангуляции. Однако все же, данная технология с применением звуковых сенсоров не учитывает ситуации, при которой лицо будет использовать различные приборы по снижению звука выстрелов (оружейный глушитель, дозвуковые патроны и т.д.). Более того, в центральных районах таких крупных городов, как Мумбаи (Индия), Нью-Йорк (США), Шанхай (Китай) средний уровень шума достигает показателей в 100 децибел и выше [2], что сравнимо с взлетающим самолетом в 300 метрах от слушателя. При такой ситуации, не составит труда произвести, сливающийся с окружающей средой, выстрел, подгадав, к примеру, момент звона колоколов церкви, громкого информационного радиооповещения (или нахождения в близости у автомобильной пробки, с многочисленными звуковыми сигналами значительной громкости).

Возможно, в будущем, как достаточно наглядно было показано в научно-фантастическом телесериале «Черное зеркало» (2 сезон 4 серия – «Белое рождество»), технологии достигнут такого уровня развития, что позволит без труда предупреждать, выявлять и пресекать готовящиеся преступления. Однако в настоящее время на такое остается лишь надеяться.

Следующей проблемой использования видеокамер наружного наблюдения является вопрос о самой их защищенности. По данным исследований, эксперты утверждают, что уровень защищенности IP-камер и прочих "умных" устройств находится на чудовищно низком уровне, и эта проблема до сих пор системно не решена [3]. По такой логике, злоумышленник, владея необходимой технической оснасткой и специальными знаниями, запросто сможет подключиться к определенному количеству видеокамер и разом их отключить на определенный промежуток времени для реализации своих противоправных замыслов.

Для недопущения таких случаев представляется необходимым, разработчикам соответствующих устройств наблюдения, предусмотреть механизмы по защите от несанкционированного доступа (Protection from unauthorized acces). Камеры видеонаблюдения должны быть оснащены системой защиты от несанкционированного физического и электронного доступа к их системам и механизмам.

На сегодняшний день понятие и признаки несанкционированных действий в отношении систем наблюдения, а также меры по их предотвращению предусмотрены национальным государственным стандартом [13]. В частности, для максимально возможного уровня защиты информации систем телевизионной охраны (СОТ) – предусматривается обязательная установка пароля (число знаков которого обязательно должно быть не меньше шести, и при его вводе не должны отображаться символы) и его шифрование специальными средствами.

Что касается «бытового» использования видеокамер, например собственниками многоквартирных домов, то и здесь также имеются свои особенности. Как подчеркивают О.В. Кириченко и Е.В. Накушнова, на данный момент в российском федеральном законодательстве отсутствует отдельный нормативный акт, посвященный

процессу организации видеонаблюдения в подъездах, лифтах и других объектах общего имущества в многоквартирном доме [4]. При этом авторы приходят к выводу, что установка видеокамер не только на лестничных клетках, но и на подъездах домов, будет способствовать сохранности жилищного фонда, снижению количества случаев вандализма и хулиганских действий, а также повысит уровень раскрываемости преступлений.

Возникает логичный вопрос: допускается ли устанавливать видеокамеры в подъездах, лестничной клетке или непосредственно у входа в определенную квартиру многоквартирного дома (к примеру установка видеодомофона) и не будет ли это являться нарушением права граждан на неприкосновенность частной жизни?

Отвечая на этот вопрос, следует отметить, что установление видеокамеры (videодомофона) в помещении общего пользования в многоквартирном доме не может нарушать право граждан, проживающих в этом доме, на неприкосновенность частной жизни и неприкосновенность жилища, поскольку данный процесс будет осуществлен на территории, не являющейся жилым помещением.

Конституция РФ устанавливает, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (ч. 1 ст. 24).

Жилище неприкосновенно. Никто не вправе проникать в жилище против воли проживающих в нем лиц иначе как в случаях, установленных федеральным законом, или на основании судебного решения (ст. 25 Конституции РФ).

Согласно п. 1 ч. 1 ст. 36 ЖК РФ помещения в жилом доме, не являющиеся частями квартир и предназначенные для обслуживания более одного помещения в данном доме, в том числе межквартирные лестничные площадки, лестницы, лифты, лифтовые и иные шахты, коридоры, технические этажи, чердаки, подвалы, в которых имеются инженерные коммуникации, иное обслуживающее более одного помещения в данном доме оборудование (технические подвалы), являются общим имуществом собственников помещений в многоквартирном доме.

Отсюда следует, что установление видеокамеры в помещении общего пользования в многоквартирном доме, которое не является жилым, не может нарушать право граждан, проживающих в этом доме, на неприкосновенность частной жизни и неприкосновенность жилища.

Как постановил суд в одном из своих решений «при открытии двери каждый собственник квартиры должен разумно допускать возможность, что часть его жилого помещения может обозреваться кем-либо с публичного места и потому не вправе ожидать сохранения в тайне участков квартиры доступных непосредственному обзору с общедоступных публичных мест, коими являются подъездные помещения. В то же время, собственник жилого помещения вправе ожидать, что никто не будет обозревать его помещение путем проникновения в него либо с использованием специальной техники значительно расширяющей границы получаемой информации» [7].

Данный вывод также подтверждается тем фактом, что любой разумный гражданин не будет демонстрировать в подъезде или на лестничной площадке те стороны своей личной жизни, которые он не желает делать достоянием окружающих.

По поводу установки видеодомофона над или сбоку двери квартиры, то здесь даже не обязательно получать согласие всех жильцов, поскольку данная процедура не является действием по использованию общедомового имущества, требующего согласия долевых собственников в смысле положений ч. 4 ст. 36 ЖК РФ [5]. При том, что зачастую у видеодомофонов даже нет функции по ведению записи [6,8].

А вот при использовании скрытых видеокамер – возникают вопросы уже этического характера. На данный момент никакого вида ответственности за использование скрытых видеокамер не установлено (за исключением угроз

распространения записи, полученной в результате такой съемки при вымогательстве – данные действия уже напоминают состав преступления, со всеми вытекающими).

В одном из судебных решений по поводу использования скрытой камеры было указано: «... ведение видеозаписи (в том числе скрытой камерой) в местах, очевидно и явно открытых для общего посещения и не исключенных в силу закона или правового обычая от использования видеозаписи, является элементом самозащиты гражданского права, что соответствует статье 12 ГК РФ и корреспондирует часть 2 статьи 45 Конституции Российской Федерации, согласно которой каждый вправе защищать свои права и свободы всеми способами, не запрещенными законом» [10]. Более того, суд принял в качестве доказательства такую видеосъемку.

Не вдаваясь в исключения, стоит заметить, что по общему правилу, Закон об оперативно-розыскной деятельности (ст. 6) запрещает обычным гражданам и юридическим лицам устанавливать и использовать скрытые видеокамеры (технические средства для негласного визуального наблюдения) [9]. Также, не допускается использования скрытых видеокамер, поскольку такие действия, направленные на получение информации о частной жизни, будут противоречить ст. 23, 24 Конституции РФ.

Но как только речь заходит о государственных и общественных интересах, приведенные выше формулировки о запрете сбора «частной» и «личной» информации отходят на второй план. Так, согласно Закону о СМИ (ст. 51), журналист вправе не только вести скрытую съемку, но и распространять полученные в результате ее осуществления материалы и информацию при соблюдении ряда условий: 1) если это не нарушает конституционных прав и свобод человека и гражданина; 2) если это необходимо для защиты общественных интересов и приняты меры против возможной идентификации посторонних лиц; 3) если демонстрация записи производится по решению суда [11].

Особенно актуально данное правомочие, в ходе освещения журналистами актов терроризма и контртеррористических операций. Более комплексно данный подход был рассмотрен в ряде международно-правовых актов Совета Европы, среди которых Рекомендация Парламентской Ассамблеи Совета Европы N 1706 (2005) "СМИ и терроризм" (Рекомендация N 1706) и Декларация о свободе выражения мнений и информации в СМИ в контексте борьбы с терроризмом от 2 марта 2005 г., принятая Комитетом министров Совета Европы (Декларация о СМИ в контексте терроризма) [12].

Рекомендация N 1706 предписывает государствам "воздерживаться от запрещения или даже необоснованного ограничения под предлогом борьбы с терроризмом публикации в СМИ информации и мнений о терроризме, а также о реакции государственных властей на террористические акты и угрозы" (п. III ст. 10). Схожая норма содержится и в Декларации о СМИ в контексте терроризма. По мнению А.А. Смирнова, данное предписание блокирует введение государством каких-либо ограничительных мер в отношении деятельности СМИ (при освещении последними террористических актов).

До тех пор, пока съемка (в том числе и скрытая) будет необходима для защиты государственных и общественных интересов, данный процесс с точки зрения действующего законодательства будет признан правомерным. Другое дело касается использования и распространения видеоматериалов при реализации противоправного поведения отдельно взятых лиц. Тут уже будут вступать в действия нормы иного (т.е. публичного) права – ст. 13.11 КоАП, ст. 137 УК РФ и т.д.

1. Расторопов С.В. Использование искусственного интеллекта для предупреждения и выявления преступлений (мировой опыт) // Международное публичное и частное право. 2020. N 5. С. 40 - 43.

2. Самые шумные города мира, 16.10.2020 // [Электронный ресурс] URL: <https://zen.yandex.ru/media/mapmaniac/samye-shumnye-goroda-mira-5fa7b73047a34812ced4bd49> (дата обращения: 04.03.2021).
3. Кондрашин М. "Черные лебеди" информационной безопасности // Банковское обозрение. 2018. N 10. С. 92 - 93.
4. Кириченко О.В., Накушнова Е.В. Права и обязанности граждан - собственников жилых помещений в многоквартирных домах: учебное пособие. М.: Юстицинформ, 2019. 636 с.
5. Апелляционное определение Краснодарского краевого суда от 05.06.2012 по делу N 33-10078-12 // [Электронный ресурс] Доступ из справ.-правовой системы «КонсультантПлюс».
6. Апелляционное определение Московского городского суда от 24.04.2017 по делу N 33-15750/2017 // [Электронный ресурс] Доступ из справ.-правовой системы «КонсультантПлюс».
7. Апелляционное определение Санкт-Петербургского городского суда от 15.08.2017 N 33-15909/2017 по делу N 2-1049/2017 // [Электронный ресурс] Доступ из справ.-правовой системы «КонсультантПлюс».
8. Решение Кунцевского районного суда города Москвы от 07.06.2016 по делу N 2-2569/2016 // [Электронный ресурс] Доступ из справ.-правовой системы «КонсультантПлюс».
9. Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 30.12.2020) "Об оперативно-розыскной деятельности" // Собрание законодательства РФ. 1995. N 33. ст. 3349.
10. Решение Арбитражного суда Приморского края от 29 марта 2016 г. по делу N А51-22036/2015 // [Электронный ресурс] Доступ из справ.-правовой системы «КонсультантПлюс».
11. Закон РФ от 27.12.1991 N 2124-1 (ред. от 30.12.2020) "О средствах массовой информации" (с изм. и доп., вступ. в силу с 01.01.2021) // Российская газета. 1992. N 32.
12. Смирнов А.А. Европейские стандарты правового регулирования освещения терроризма в СМИ // Административное право и процесс. 2014. N 1. С. 71 - 74.
13. ГОСТ Р 51558-2014. Национальный стандарт Российской Федерации. Средства и системы охраняемые телевизионные. Классификация. Общие технические требования. Методы испытаний (утв. и введен в действие Приказом Росстандарта от 22.10.2014 N 1371-ст) (ред. от 31.10.2019) // [Электронный ресурс] Доступ из справ.-правовой системы «КонсультантПлюс».

Кузнецова В.А., Кайралиева Д.В., Поздняков Д.А.

Реализация презумпции невиновности в российском уголовном судопроизводстве

*ФГБОУ ВО Поволжский институт управления «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации»
(Россия, Саратов)*

doi: 10.18411/lj-03-2021-229

idsp: ljjournal-03-2021-229

Аннотация

В статье рассматриваются принцип презумпции невиновности в уголовном судопроизводстве в целом и основные проблемы его реализации в современном мире.

Ключевые слова: принцип презумпции невиновности, обвиняемый, подозреваемый, доказательства.

Abstract

The article examines the principle of the presumption of innocence in criminal proceedings in general and the main problems of its implementation in the modern world.

Key words: principle of the presumption of innocence, accused, suspect, evidence.

Принцип презумпции невиновности определяет характер отношений между государством, его органами, должностными лицами и гражданами, с одной стороны, и лицом, против которого выдвинуты обвинения в преступлении, – с другой. От характера правового закрепления и непосредственной реализации данного принципа зависит, возможно ли говорить о неприкосновенности личности, а также соблюдении основных конституционных прав личности. Данный принцип нормативно закреплён как в Конституции, так и непосредственно в Уголовно-процессуальном кодексе Российской Федерации. Но для определения его действия имеет решающее значение не только нормативное закрепление, но и его реализация. Этим обусловлена актуальность и значимость проведения научных исследований реализации презумпции невиновности в российском уголовном судопроизводстве.