DOI 10.37539/2949-1991.2024.17.6.032

**Хасанова Лилиана Фанисовна**,
преподаватель отделения права,
ГАПОУ Уфимский колледж статистики,
информатики и вычислительной техники,
г. Уфа

# НОВЕЙШИЕ ТЕХНОЛОГИИ И ДЕЯТЕЛЬНОСТЬ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ

**Аннотация:** в современных условиях информационные системы имеют своей целью не просто увеличение эффективности обработки данных и оказание помощи лицу, призванному проанализировать полученную информацию. Соответствующие информационные технологии должны способствовать лицам, профессионально работающими в правовой сфере противостоять негативным «вызовам», которые применяются в цифровом пространстве. На этом фоне неизбежно возникает вопрос о том, что как будут распоряжаться полученным таким образом массивом сведений представители правоохранительных органов. Автор попыталась представить две модели развития подобных ситуаций на примере двух западных государств.

**Abstract:** in modern conditions, information systems have as their goal not just to increase the efficiency of data processing and to help the person, called upon to analyze the information received. Appropriate information technologies should help people who work in the legal field to confront negative “challenges” that are used in the digital space. Against this background, the question inevitably arises as to how the representatives of law enforcement agencies will dispose of the information received in this way. The author tried to present two models of the development of such situations on the example of two Western states. Moreover, all described events refer to 2014.

**Ключевые слова:** правовая сфера, информационные системы, цифровизация, государственный контроль, видеозапись.

**Keywords:** legal sphere, information systems, digitalization, state control, video recording

В современных условиях информационные системы имеют своей целью не просто увеличение эффективности обработки данных и оказание помощи лицу, призванному проанализировать полученную информацию. Соответствующие информационные технологии должны способствовать лицам, профессионально работающими в правовой сфере противостоять негативным «вызовам», которые применяются в цифровом пространстве. На этом фоне неизбежно возникает вопрос о том, что как будут распоряжаться полученным таким образом массивом сведений представители правоохранительных органов. Автор попыталась представить две модели развития подобных ситуаций на примере двух западных государств. Следует отметить, что все описываемые события относятся к 2014 году.

Как показало расследование, проведенное в 2014 г. британской газетой «Guardian», три из четырех крупных сетей мобильной телефонной связи в Великобритании одним нажатием компьютерной мыши предоставляют полиции возможность доступа к записям телефонных разговоров с помощью автоматизированных систем.

EE, Vodafone и Three используют автоматизированные системы, которые передают данные о клиентах в качестве своеобразного «банкомата», как описал этот процесс один из сотрудников телефонной компании.

Эрик Кинг, заместитель директора Privacy International, контролирующего прозрачность деятельности государственных учреждений, подчеркнул: «Если компании

предоставляют данные связи правоохранительным органам на так называемом автопилоте, это все равно, что предоставить полиции прямой доступ (к индивидуальным телефонным счетам)».

Компания O2, напротив, является единственной крупной телефонной сетью, требующей от сотрудников проверять все запросы полиции на получение информации, говорится в сообщении руководства компании.

По закону операторы мобильной связи должны хранить годовые записи разговоров всех своих клиентов, к которым полиция и другие агентства могут получить доступ без ордера на основании спорного Акта о властных полномочиях следствия (Ripa).

Ripa – это закон о перехвате, дающий право на большую часть массового наблюдения посредством использования системы Центра правительственной связи. Недавно закон снова оказался в центре внимания после того, как он был использован для выявления источников получения информации журналистами двух общенациональных газет, Sun и Mail on Sunday.

Документы от поставщиков программного обеспечения и разговоры с персоналом мобильных компаний показывают, насколько автоматизированной стала эта система: «подавляющее большинство» записей, требуемых полицией, доставляется через автоматизированные системы без участия сотрудников какой-либо телефонной компании.

Министерство внутренних дел утверждает, что полученные таким способом данные являются «важным инструментом», а использование Ripa было «необходимым и соразмерным».

Несмотря на заверения политиков в том, что законы Великобритании, требующие ведения телефонными компаниями записей, не будут создавать, в конечном счете, государственную базу данных о частных сообщениях, критики утверждают, что эта практика очень близка к этому. Кинг предупредил, что «широко распространенный автоматический доступ подобного рода» означает, что телекоммуникационная отрасль Великобритании «по существу уже предоставляет правоохранительным органам объединенные базы данных, которых, по их утверждениям, у них не было, когда они настаивали на применении так называемой «хартии следящего».

В автоматизированных системах, используемых телефонными компаниями, полицейские, ищущие записи телефонных разговоров, должны получить разрешение от другого сотрудника той же полиции, который затем вводит данные в онлайн-форму. Это фактически полностью копирует программу US Prism, раскрытую Эдвардом Сноуденом, которая фактически создала «черный вход» для продуктов американских технологических корпораций. В подавляющем большинстве случаев подобная информация затем доставляется без какой-либо дополнительной роли человека.

В одном из документов, подготовленных компанией Charter Systems, которая продает программное обеспечение, используемое полицией для связи с компаниями мобильной связи, объясняется, что автоматизированный процесс экономит 32 минуты человеческого времени на одно приложение. Компания Charter Systems работала в партнерстве с Министерством внутренних дел и Detica (фирмой, занимающейся перехватом данных для служб безопасности и полиции, теперь она называется BAE Systems Applied Intelligence) разработать решение, которое напрямую связано со всеми операторами связи (провайдеры услуг связи, термин, охватывающий телефонные компании)», – говорится в заявлении. В документе поясняется, что система производит «автоматизированное решение для сбора информации в электронном виде. Новое решение экономит время и усилия властей при запросе и получении постоянно растущих объемов данных».

Системы были настолько взаимосвязаны, что в документе, подготовленном компанией Charter, показано, что «сведения могут быть получены из нескольких CSP за один запрос».

Представители общественности, выступающие за сохранение строгой конфиденциальности, гневно отреагировали на детали подобных процессов. «Нам срочно нужно

прояснить, насколько беспрекословными стали отношения между телекоммуникационными компаниями и правоохранительными органами», – сказал Кинг. «Крайне важно, чтобы каждый отдельный ордер на коммуникационные данные независимо проверялся компаниями, которые их получают, и, при необходимости, оспаривался, чтобы гарантировать, что конфиденциальность их клиентов не будет нарушена ненадлежащим образом».

Несколько сетей мобильной связи подтвердили, что большая часть их запросов обрабатывалась без вмешательства человека. «У нас действительно есть автоматизированная система», – сказал представитель EE, крупнейшей сети Великобритании, которая также управляет Orange и T-Mobile. Подавляющее большинство запросов Ripa обрабатывается через автоматизированную систему. Представитель компании также добавил, что система подлежит надзору: ежемесячные отчеты отправляются в правоохранительные органы с запросом данных, а годовые отчеты направляются уполномоченному по перехвату и Министерству внутренних дел.

Представитель Vodafone сказал, что компания обрабатывала запросы аналогичным образом. «Подавляющее большинство уведомлений Ripa, которые мы получаем, обрабатываются автоматически в соответствии со строгими рамками, установленными Ripa и подкрепленными сводом правил», – сказал он. «Даже при ручном процессе мы не можем смотреть за спросом, чтобы определить, разрешено ли оно должным образом».

Представитель Three, которая, как известно, использует в значительной степени автоматизированную систему, сказал, что компания просто соблюдает требования закона. «Мы серьезно относимся как к своим юридическим обязательствам, так и к конфиденциальности клиентов», – сказал он. «Компания работает с правительством и делает не больше и не меньше, чем требуется или разрешено в соответствии с установленной правовой базой».

В отличие от других сетей, O2 заявила, что вручную проверяла все свои запросы Ripa. «У нас есть система обработки запросов, с помощью которой правоохранительные органы могут обращаться к нам со своими запросами», – сказала пресс-секретарь O2. «Все ответы O2 проверяются группой по раскрытию информации, чтобы гарантировать, что каждый запрос является законным, а предоставленные данные соизмеримы с запросом»

Майк Харрис, организатор движения «Не следите за нами», сказал, что автоматизированные системы представляют серьезную угрозу для свободы слова в Великобритании. «Откуда мы знаем, что полиция через новые системы Министерства внутренних дел не отправляет автоматические запросы, раскрывающие источники информации журналистов или даже личные контакты политиков?»

Харрис подчеркнул: «Эдвард Сноуден показал, что и АНБ, и Центр правительственной связи имели доступ к нашей частной информации, хранящейся на серверах. Теперь, когда у полиции тоже есть доступ, когда же парламент встанет и защитит наши основные гражданские свободы?»

Представитель Министерства внутренних дел отказался отвечать на конкретные вопросы об использовании автоматических систем для получения записей звонков, но выступил в защиту использования Ripa силами полиции. «Коммуникационные данные – это абсолютно важный инструмент, используемый полицией и другими ведомствами для расследования преступлений, обеспечения национальной безопасности и защиты населения», – отметил он в своем заявлении. Оно также подчеркнул:

«Эти данные хранятся самими поставщиками услуг связи и могут быть получены только государственными органами в соответствии с Законом о регулировании следственных полномочий 2000 года в каждом конкретном случае и там, где это необходимо и соразмерно.

Получение коммуникационных данных в соответствии с RIPA подлежит строгим гарантиям в соответствии с действующим законодательством и находится под независимым надзором Комиссара по перехвату коммуникационных данных» [1].

В том же 2014 году в Соединенных Штатах Америки произошел также серьезный прорыв в области применения новых технологий правоохранительными органами на федеральном уровне. Причем, речь шла об использовании давно апробированного в других сферах средства фиксации аудио и видео изображения.

Министерство юстиции заявило о том, что ФБР и другим федеральным правоохранительным органам в большинстве случаев потребуются видеозаписи допросов подозреваемых, что фактически будет означать действия федерального правительства в соответствие с практикой, принятой во многих штатах и графствах.

Это одно из самых значительных изменений в ФБР после прихода Джеймса Б. Коми, который в сентябре 2013 г. возглавил бюро. Предшественник г-на Коми, Роберт С. Мюллер и другие должностные лица бюро в свое время выступили против применения видеосъемки, заявив, что записи могут раскрыть тактику допроса агентов и фактически вынудить свидетелей прервать дачу показаний.

В этих условиях ФБР, официальные лица все чаще выступают за процедуру видеозаписи, высказали свою положительную оценку бывшие прокуроры, многие адвокаты также поддержали данное предложение. Пол К. Чарльтон, сказал, что федеральные прокуроры во многом проигрывали дела, потому что не могли представить присяжным заседателям самые убедительные доказательства, доступные им: видеозаписи признаний.

П. К. Чарльтон, адвокат, ныне занимающийся частной практикой, в телефонном интервью отметил: «Самая трудная часть доказывания преступления – это душевное состояние, и это почти всегда достигается с помощью заявления подозреваемого». «Это была неоправданная политика. Я думаю, что это одно из самых значительных улучшений в системе уголовного правосудия за долгое время».

Пол К. Чарльтон подчеркнул, что, занимая в свое время высокий пост, он был особенно обеспокоен тем, что прокуроры, находившиеся под его юрисдикцией, проигрывали дела о сексуальном насилии и преступлениях с применением насилия, а также вынуждены были идти на уступки в виде соглашений о признании вины по менее серьезным обвинениям, – и все потому, что они не могли записывать на пленку подозреваемых. Многие из этих дел были связаны с преступлениями, совершенными в резервациях американских индейцев, где непосредственная юрисдикция принадлежит федеральным властям, а не местным властям, которым, в свою очередь, разрешено записывать показания.

Чарльтон утверждал, что жертвы во многих случаях не получали равного обращения в соответствии с законом, и обвинял в этом политику ФБР. Основы прежней политики были изложены в меморандуме 2006 года генерального юрисконсульта ФБР и разослана 56 местным отделениям бюро. В меморандуме в большинстве случаев запрещалось использование записывающего оборудования во время допросов, поскольку это могло оттолкнуть подозреваемых от разговоров и создавало у присяжных неблагоприятное впечатление о деятельности агентов ФБР.

Новая политика аналогична политике, которую использовали многие прокуратуры штатов и городов, поскольку технология записи стала более доступной и менее дорогой. Он вступила в силу в июле 2014 г. и также распространяется на Бюро по алкоголю, табаку, огнестрельному оружию и взрывчатым веществам, Управление по борьбе с наркотиками и Службу судебных приставов.

«Создание электронной записи гарантирует, что у нас будет объективный отчет о ключевых расследованиях и взаимодействиях с людьми, которые содержатся под стражей в

федеральных учреждениях», – сказал генеральный прокурор Эрик Х. Холдер в видео, размещенном на веб-сайте департамента. «Это позволит нам документально подтвердить, что задержанным лицам предоставлены их конституционно защищенные права».

Холдер также отметил, что новая практика предоставит сотрудникам правоохранительных органов «необходимые материалы, так что они будут иметь четкие и неоспоримые записи важных заявлений и признаний, сделанных лицами, которые были задержаны».

В служебной записке от 12 мая заместитель генерального прокурора Джеймс М. Коул сказал, что видеозапись будет разрешена в период между арестом подозреваемого и первой явкой к судье. В служебной записке говорилось, что аудиозаписи будут разрешены, если видеоустройство недоступно. Он добавил, что должностным лицам следует выполнить просьбу, если подозреваемые просят не вести запись.

В случаях, когда на карту поставлена национальная безопасность и время имеет существенное значение, должностным лицам не нужно будет ждать, пока будет приобретено и установлено записывающее оборудование. Новая политика также поощряет должностных лиц использовать электронную запись во время расследования, например, во время допросов свидетелей.

«Федеральные агенты и прокуроры по всей стране твердо привержены соблюдению надлежащих правовых процедур при неукоснительном и беспристрастном применении закона», – заключил свое выступление Холдер. Он добавил, что новая политика «предоставит проверяемые доказательства того, что наши слова соответствуют нашим делам» [2,14].

Приведенные примеры служат ярким подтверждением необходимости сочетания осторожного и в то же время способного работать на опережение подходов в ежедневной деятельности сотрудников правоохранительных структур по борьбе с преступностью.

*Список литературы:*

1.The Guardian, 2014, October 10th.
2.The New York Times, 2014, May 23th.