УДК 349.23

Кулагина Анна Владиславовна
Московский государственный университет имени М.В. Ломоносова
Юридический факультет
Россия, Москва
ankulagina5895@gmail.com
Kulagina Anna
Moscow State University named after M.V. Lomonosov
Faculty of Law
Russia, Moscow

ВИДЫ КОНТРОЛЯ ЗА ПОВЕДЕНИЕМ РАБОТНИКОВ

Аннотация: в данной статье автор рассматривает наиболее часто применяемые способы контроля работодателя за поведением работников во время исполнения их трудовых обязанностей. Отдельно анализируется правомерность, обоснованность и моральная допустимость используемых методов, их соотношение с принципом неприкосновенности частной жизни, особое внимание уделяется актуальной российской и зарубежной судебной практике.

Ключевые слова: контроль, дисциплина труда, правомерность, принцип неприкосновенности, частная жизнь.

TYPES OF MONITORING OF EMPLOYEE BEHAVIOUR

Annotation: In this article, the author examines the most commonly used methods of employer's control over the conduct of employees during the performance of their employment duties. The legitimacy, justification and moral permissibility of the used methods, their correlation with the principle of privacy are analyzed separately; special attention is paid to the current Russian and foreign judicial practice.

Key words: control, labour discipline, lawfulness, principle of inviolability, privacy.

В современном мире работники все чаще подвергаются использованию многообразных методов и средств контроля за их поведением на рабочих местах. Мотивация работодателей весьма проста и понятна: они заинтересованы в получении максимальной прибыли, эффективном расходовании ресурсов и минимизации издержек, выраженных в том числе в выплате заработной платы работникам.

Поскольку цифровая трансформация современного общества является неизбежным процессом, то неумолимо приближается применение все новых способов контроля и господство так называемого «капитализма наблюдения» - иными словами, коммерциализированного и широко распространенного сбора и хранения данных корпорациями. Одним из самых заметных проявлений цифровизации в трудовом праве считается возможность работодателей осуществлять контроль и наблюдение за работниками с помощью самых разнообразных устройств, варьирующихся от *«от программного обеспечения для совместной работы до виртуального персонального ассистента, от компьютерных сетей до систем распознавания лиц»* [1, p. 107].

По данным исследования сервиса интернет – рекрутмента HeadHunter, около 27% работодателей используют программное обеспечение в качестве средства контроля [2]. А примерно 50% отечественных компаний следят за своими сотрудниками при помощи DLP-программ (технологии и технические устройства, обрабатывающие проходящие через них данные и предотвращающие утечку конфиденциальной информации) и систем учета рабочего времени [3]. Такие впечатляющие статистические значения дают основания полагать, что антиутопия Дж. Оруэлла «1984», красной нитью которой считается тотальный и всеобъемлющий контроль, не является такой нереалистичной.

Для доказывания факта наличия состава дисциплинарного проступка, обеспечения техники безопасности и иных соображений работодатель может

использовать следующие способы контроля: видеонаблюдение, прослушивание телефонных звонков, мониторинг электронной почты и активности работника за компьютером, GPS-наблюдение, контроль за постами и аккаунтами в социальных сетях и иные способы. Рассмотрим указанные методы подробнее.

1. Прослушивание телефонных звонков. В этом случае работодатель устанавливает специальные устройства слежения на телефонную линию. Чаще всего данная мера применяется для оценки качества обслуживания клиентов, степень уважительности и вежливости общения работников, чья трудовая функция непосредственно связана с большим количеством звонков и общением. При этом личные телефоны прослушивать запрещается, у работодателя есть подобные полномочия только в отношении корпоративных телефонов и сим-карт, что должно быть закреплено в ЛНА, например, о порядке использования корпоративной мобильной связи [4]. Более того, в последнее время многие компании при начале разговора добавляют фразу: «В целях улучшения качества обслуживания разговор будет записан». Упоминание данной фразы необходимо в силу того, что такие разговоры с высокой степенью вероятности включают в себя персональные данные. Именно поэтому в соответствии со статьей 9 Федерального закона о «О персональных данных» продолжение лицом разговора после такого предупреждения может рассматриваться как фактическое согласие на обработку его персональных данных. В российской судебной практике есть интересный пример признания расшифровки телефонных переговоров в качестве доказательства совершения дисциплинарного проступка. Так, сотрудник отдела МВД сообщал сведения о пострадавших от преступления и их родственниках третьим лицам по телефону. Суд пришел к выводу, что прослушка являлась законной и правомерной и свидетельствовала о наличии проступка и ущербе репутации сотрудников органов внутренних дел [5].

2. GPS-наблюдение. Данный вид наблюдения позволяет контролировать скорость передвижения водителей и местонахождение иных лиц, чья работа

связана с частыми разъездами. Эти системы могут также использоваться для предотвращения различных коллективных действий со стороны работников, если будет установлено, что они собираются в определенных местах [6, p. 482]. Первое дело, связанное с вопросом правомерности мониторинга GPS, рассматривалось в Нью-Йорке. В деле Каннингем против Департамента труда штата Нью-Йорк (2013 NY Slip Op 04838) работник был подвергнут дисциплинарному наказанию на основании доказательств, полученных с помощью устройства слежения GPS, установленного на его личном автомобиле [7]. Наниматель подозревал, что работник возвращался из командировок раньше, чем указывал в отчетах, и решил установить устройство слежения. Суд признал, что причина установления слежки была обоснованной и разумной. Однако суд также постановил, что такой способ контроля был излишне навязчивым, наниматель следил за передвижениями даже в не рабочее время. А когда работник находился в отпуске, работодатель не предпринял усилий для того, чтобы избежать чрезмерного контроля и убрать средства слежения. Итог решения заключался в том, что в целом подобная мера допустима, однако долгосрочное и постоянное отслеживание с помощью GPS является существенным вторжением в частную жизнь. Российская правоприменительная практика также идет по пути признания результатов GPS-наблюдения в качестве доказательств при соблюдении принципа неприкосновенности личности и обязательного уведомления о ведении наблюдения [8].

3. Мониторинг электронной почты (в том числе личных переписок). Этот вид мониторинга характеризуется выявлением случаев корпоративной утечки информации, совершения правонарушений, профилактикой неблагоприятной атмосферы в коллективе [9]. Подобный контроль встречается довольно часто: опрос, проведенный Американской ассоциацией менеджмента, показывает, что 84% американских работодателей разработали политику использования электронной почты, а примерно 43% в той или иной форме осуществляют мониторинг [10]. Одним из хрестоматийных примеров такого

мониторинга представляется дело «Барбулеску против Румынии», рассмотренное ЕСПЧ [11]. В названном кейсе сотрудник в рабочих целях общался с клиентами посредством расширения почты - Yahoo Messenger. Однако Барбулеску также вел беседы со своими родственниками, в том числе личного характера. Эти действия привели к тому, что в ходе проверки корпоративного мессенджера работодатель уличил работника в нарушении политики компании и уволил его. Изначально ЕСПЧ постановил, что работодатель действовал в пределах своих полномочий в соответствии с политикой компании. Тем не менее впоследствии решение было изменено из-за отсутствия справедливого баланса интересов: Большая палата ЕСПЧ признала, что право работника на неприкосновенность частной жизни было нарушено, его не предупредили о ведении наблюдения и такой способ был в достаточной степени навязчивым.

4. Контроль за использованием сети Интернет и пользованием рабочим компьютером. Для такого вида контроля наниматель может устанавливать специальные программы для отслеживания рабочего времени (TimeTracko), для мониторинга использования различных приложений и URL – адресов. Одним из самых излюбленных способов наблюдения можно назвать «кейлоггер». Его смысл заключается в регистрации и запоминании всех нажатий клавиш работником, что позволяет узнать, какие запросы и сообщения были напечатаны, даже если история браузера или письмо не сохранились. Помимо этого, в 2007 году Европейский суд по правам человека по делу Копланд против Соединенного Королевства вынес постановление от 03.04.07 № 62617/00 (Copland v. United Kingdom), в котором пришел к выводу, что работодатель не может контролировать использование компьютера и сети Интернет работников, если не соблюден ряд условий. В этом деле заявительница работала в британском колледже личным помощником директора. Вскоре на ее компьютер было установлено средство контроля за электронной почтой и интернетом. По утверждению работодателя, это было

сделано для того, чтобы убедиться в том, что она не использует оборудование колледжа в личных целях. При этом правила и регламентация подобного наблюдения урегулированы не были. В ходе рассмотрении дела ЕСПЧ сделал логичный вывод о том, что *«электронные сообщения, отправленные с работы, должны быть защищены аналогичным образом, как и информация, полученная в результате мониторинга личного использования интернета»* [12]. Таким образом, наблюдение за Копланд было признано незаконным.

5. Контроль за постами и аккаунтами в социальных сетях. Этот вид мониторинга появился относительно недавно в связи со все большим распространением новых технологий и возможности освещения рабочих проблем на широкую аудиторию. Практика проверки и мониторинга аккаунтов в социальных сетях стала абсолютно обыденной. Более того, опрос CareerBuilder отразил, что 57% работодателей не заинтересованы в собеседовании с кандидатами, если они не видят их в социальных сетях [13]. Несмотря на то, что социальные сети стели неотъемлемой частью жизни многих людей и местом, где есть возможность выразить свои мысли и поделиться размышлениями, все же возникают прецеденты с привлечением к дисциплинарной ответственности за посты и фотографии. В частности, тринадцать стюардесс авиакомпании Virgin Airlines разместили в своих профилях информацию об отсутствии необходимых мер безопасности на борту и общую неудовлетворенность работой в компании [14, с. 87]. Интересно, что в США суды подтвердили иной подход, а именно в 2012 году рассматривалось дело *Элинг против Монмута-Ocean Hospital Service Corp* [15]. Решение приравняло записи на стене Facebook к сообщениям, защищаемым Законом о сохраненных сообщениях. Он запрещает несанкционированный доступ к частным электронным сообщениям и предусматривает уголовное наказание.

Совершенно справедливо выделяют отдельно стоящий блок вопросов о допустимости ведения наблюдения за дистанционными работниками и лицами, занятыми на интернет-платформах. Отдельные сторонники данного подхода

утверждают, при нетипичных формах занятости, подразумевающих под собой взаимодействие механизмов, алгоритмов или машин с одной стороны и человека с другой, использование средств контроля позволяет работодателям заботиться о соблюдении норм охраны труда и передавать соответствующие заключения руководству (к примеру, степень усталости для корректировки рабочего графика и др.) [16, с. 83]. Однако данная позиция не отражает основной особенности такого вида контроля. Главное отличие заключается в том, что на электронных платформах применяется алгоритмический контроль и делегирование контроля клиентам, потребляющим услугу, оба этих метода неразрывно связаны и дополняют друг друга.

Если рассматривать в качестве примера платформу по предоставлению услуг такси Uber, то в первую очередь после окончания поездки водителя оценивает клиент. В специальном приложении потребитель по своему личному усмотрению ставит оценки в соответствии с определенными критериями, затем эти данные отправляются к агрегатору платформы. При этом, чем ниже рейтинг водителя, тем меньше заказов ему поступает и тем меньше его заработок. Более того, суды признают не только делегированный контроль клиентов, но и алгоритмический контроль платформ. Так, в 2017 году трибунал по трудовым спорам в Великобритании обнаружил примеры контроля, реализуемого Uber. В частности, особое внимание было обращено на тот момент, когда водитель отклоняется от предложенного алгоритмом маршрута, исполнитель был обязан объяснить свое решение и обосновать выбор другого пути [17]. Иными словами, уровень мониторинга за такого работника становится намного выше, чем был когда-либо [18].

Для работников, занятых дистанционно, зачастую применяются средства контроля, управляемые искусственным интеллектом. К примеру, компания Crossover предоставляет системы Workmart Productivity Tool для мониторинга удаленных работников. Эта программа делает скриншоты компьютеров через определенные промежутки времени, а также собирает иные данные. Затем

собранная информация передается менеджеру и вышестоящему начальству для оценки, насколько рационально и эффективно работник использовал рабочее время [19].

Таким образом, целесообразно отметить, что общим условием применения всех вышеуказанных средств контроля является обязательное уведомление работников о намерении внедрить средства контроля, получение их согласия на проведение таких мер и неукоснительное обеспечение мер безопасности и сохранности персональных данных.

Список литературы:

1. Aloisi A., Gramano E. Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring, and Regulatory Issues in the EU Context // Special Issue of Comparative Labor Law & Policy Journal, "Automation, Artificial Intelligence and Labour Protection" / ed. by V. De Stefano. 2019. Vol. 41. No. 1.

2. 27% работодателей контролируют своих сотрудников в рабочее время с помощью специального ПО [Электронный ресурс] // URL: https://www.vedomosti.ru/management/articles/2022/10/31/948100-kontroliruyut-svoih-sotrudnikov-s-pomoschyu-spetsialnogo-po (дата обращения – 24.02.2023).

3. Доверяй, но проверяй: когда слежка за сотрудниками просто необходима [Электронный ресурс] // URL: https://habr.com/ru/post/560364/ (дата обращения – 24.02.2023).

4. «Слежка» работодателя за работниками по закону [Электронный ресурс] // URL: https: www.advgazeta.ru/ag-expert/advices/slezhka-rabotodatelya-za-rabotnikami-po-zakonu/ (дата обращения - 24.02.2023).

5. Определение Первого кассационного суда общей юрисдикции от 17.02.2020 № 88-4351/2020 [Электронный ресурс] // URL: https://cloud.consultant.ru/cloud/cgi/online.cgi?req=doc&rnd=FhMGzA&base=KSOJ001&n=6539#rfIcDUTsWJa0XeIA (дата обращения - 24.02.2023).

6. De Stefano, Valerio. 2015. “The rise of the ‘just-in-time workforce’: On-demand work, crowdwork and labour protection in the ‘gig-economy” // Comparative Labor law and Policy Journal 37(3): P. 471-514.

7. Matter of Cunningham v New York State Dept. of Labor [Электронный ресурс] // URL: https://case.lawmemo.com//ny/cunningham1.htm (дата обращения - 24.02.2023).

8. Определение Седьмого кассационного суда общей юрисдикции от 30.07.2020 г. № 88-11180/2020. [Электронный ресурс] // URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=KSOJ007&n=12725#yIO1EUT0RkPhqNn31 (дата обращения - 24.02.2023).

9. Employee Email Monitoring: Your Guide to Tools & Software [Электронный ресурс] // URL: https://www.intradyn.com/employee-email-monitoring/ (дата обращения - 24.02.2023).

10. American Management Association. (2007). AMA/ePolicy 2007survey of electronic monitoring & surveillance survey [Электронный ресурс] // URL: http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf (дата обращения - 24.02.2023).

11. Постановление ЕСПЧ от 05.09.2017 г. "Дело "Бэрбулеску (Barbulescu) против Румынии" [Электронный ресурс] // URL:https://cloud.consultant.ru/cloud/cgi/online.cgi?req=doc&cacheid=4188565DE4C31A1CC9123876BE886EC9&mode=multiref&SORTTYPE=0&BASENODE=g1&base=ARB&n=518148&dst=1000000001&rnd=tfbYuA#wt7XGUTqOfTodvyn/ (дата обращения - 24.02.2023).

12. Постановление ЕСПЧ от 03.04.2007 г. "Дело "Копланд (Copland) против Соединенного Королевства" (жалоба N 62617/00) [Электронный ресурс] //
URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=43155#gs1jJUTOqmtbujsf2/ (дата обращения - 24.02.2023).

13. Is It Legal To Monitor The Social Media Accounts Of Employees? // [Электронный ресурс] URL: https://www.theonespy.com/is-it-discriminatory-to-monitor-your-employees-social-media-accounts/ (дата обращения - 24.02.2023).

14. Офман Е. М. Мониторинг поведения работников в социальных сетях: возможности и пределы работодателя // Ex jure. 2020. №1. С. 85-94.

15. Ehling v. Monmouth-Ocean Hosp. Serv. Corp. // [Электронный ресурс] URL: https://jolt.law.harvard.edu/digest/ehling-v-monmouth-ocean-hosp-serv-corp (дата обращения - 24.02.2023).

16. Серегина Л. В. Обеспечение прав граждан на охрану труда в условиях инновационного развития экономики // Журнал российского права. 2021. Т. 25. № 3. С. 76-92.

17. Uber B. V., Uber London LTD, Uber Britania LTD v. Mr Y. Aslam, Mr J. Farrar, Mr R. Dawson and Others. Appeal No. UKEAT/0056/17/DA [Электронный ресурс]//URL:https://assets.publishing.service.gov.uk/media/5a046b06e5274a0ee5a1f171/Uber_B.V._and_Others_v_Mr_Y_Aslam_and_Others_UKEAT_0056_17_DA.pdf (дата обращения - 24.02.2023).

18. Sprague, Robert. 2015. “Worker (Mis)Classification in the Sharing Economy: Trying to Fit Square Pegs in Round Holes.” Journal of Labor and Employment Law 53: P. 53-76.

19. Crossover is hiring around the world. [Электронный ресурс] // URL: https://www.crossover.com/worksmart/#worksmartproductivity-Too (дата обращения - 24.02.2023).