Литература

1. Об угрозе для демократии со стороны экстремистских партий и движений в Европе : резолюция 1344. – 2003 – Режим доступа: https://www.coe.int/t/r/parliamentary_assembly/%5Brussian_documents%5D/%5B2003%5D/%5BSept_2003%5D/Res%201344%20Rus.asp. – Дата доступа: 04.05.2024.
2. Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом. – Режим доступа: https://pravo.by/document/?guid=12551&p0=I00100109. – Дата доступа: 04.05.2024.
3. Декларация о мерах по ликвидации международного терроризма : принята резолюцией 49/60 Генер. Ассамбл., 9 дек. 1994 г. // ООН. – Режим доступа: https://www.un.org/ru/documents/decl_conv/declarations/terrdec1.shtml. – Дата доступа: 04.05.2024.
4. О противодействии экстремизму : Закон Респ. Беларусь, 4 янв. 2007 г., № 203-З : в ред. Закона Респ. Беларусь от 17 июля 2023 г. № 292-З // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.
5. Швайко, Э. Республика Беларусь в системе борьбы с международным терроризмом / Э. Швайко // Законность и правопорядок. – 2021. – № 3. – С. 16–20.

УДК 349.2

ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ В КОНТЕКСТЕ ТРУДОВЫХ ОТНОШЕНИЙ

Д. С. Таболич

Белорусский государственный университет, г. Минск

Научный руководитель Е. В. Мотина

Активное и бессистемное использование нанимателем цифровых технологий для осуществления контроля за поведением работников поднимает проблему готовности трудового законодательства эффективно регулировать трудовые отношения с учетом соблюдения при этом прав и интересов работников. В современных условиях механизм осуществления субъективных прав и исполнения обязанностей работников и нанимателей трансформируется: взаимодействие субъектов трудового права становится все более опосредованным.

Ключевые слова: работник, наниматель, мониторинг, наблюдение, цифровые технологии в сфере труда, трудовые отношения, персональные данные.

USE OF ALGORITHMS IN THE CONTEXT OF LABOUR RELATIONS

D. S. Tabolich

Belarusian State University, Minsk

Science supervisor E. V. Motina

Active and unsystematic use of digital technologies by the employer to control the behavior of employees raises the problem of the readiness of labour legislation to effectively regulate labour relations, taking into account the observance of the rights and interests of employees. In modern conditions, the mechanism of exercising the subjective rights and fulfilling the duties of employees and employers is being transformed: the interaction of subjects of labour law is becoming more and more indirect.

Keywords: employee, employer, monitoring, surveillance, digital technologies in the field of labour, labour relations, personal data.

В современных условиях взаимодействие субъектов трудового права становится все более опосредованным: тенденцией настоящего времени является использование нанимателем цифровых технологий в процессе коллективного труда в целях осуществления контроля за работниками. В основе цифровых технологий лежит алгоритм, использование которого в трудовых отношениях не урегулировано. Активное и бессистемное использование технологий для осуществления контроля за поведением работников поднимает проблему готовности трудового законодательства эффективно регулировать трудовые отношения с учетом соблюдения при этом прав и интересов работников. Применение нанимателем многочисленных и разнообразных технических устройств в целях контроля за поведением работников нередко приводит к вторжению в частную жизнь работников и нарушению их конституционных прав. С юридической точки зрения эти инструменты постоянно собирают, производят, обмениваются и объединяют информацию (данные), которые могут использоваться нанимателем в самых различных целях.

Европейский фонд по улучшению условий труда и жизни (Еврофонд) констатировал наличие важных отличий между контролем и наблюдением со стороны нанимателя за поведением работника: «По сравнению с контролем (мониторингом) поведения работников, который обычно ограничивается сбором информации о деятельности, связанной с работой, наблюдение является более навязчивым и агрессивным, поскольку при его осуществлении нанимателем используются технологии, позволяющие собирать более широкий спектр информации как о трудовой деятельности работника, так и о его (работника) деятельности, не связанной с работой... Хотя практика мониторинга и наблюдения дублирует друг друга, различие между ними позволяет предположить, что в результате наблюдения за работниками возникают более серьезные этические проблемы, связанные с неприкосновенностью частной жизни... Субъекты, которые знают о том, что они находятся под наблюдением большую часть рабочего времени или все время в период выполнения трудовых обязанностей, обязаны соответствующим образом корректировать свое поведение. Все это позволяет предположить, что наблюдение нарушает автономию человека» [4].

Технический прогресс сделал доступным контроль и наблюдение за работниками в режиме реального времени. Теперь наниматели могут доказать факт совершения работниками дисциплинарного проступка различными средствами: видеофиксация поведения и проступка, повлекшего причинение материального ущерба имуществу нанимателя, аудиозапись разговоров, прослушивание совершенных работниками телефонных звонков, GPS- и GPRS-наблюдение, мониторинг электронной почты, записей (постов) аккаунтов в социальных сетях, осуществление взаимодействия с работником путем направления ему юридически значимых документов посредством электронной почты, биочипирование работников.

Очевидно, что трудовое законодательство Республики Беларусь оказалось не готовым в полной мере урегулировать возникшие отношения. Несмотря на наличие Закона «О защите персональных данных» и Рекомендаций об обработке персональных данных в связи с трудовой (служебной) деятельностью, ряд вопросов все еще нуждается в уточнении, конкретизации и урегулировании в целом.

Например, разъяснению подлежит вопрос о правомерности нанимателя требовать от дистанционного работника установить на используемый им в процессе выполнения работы компьютер систему фильтрации веб-трафика. Не урегулирован вопрос защиты работником своих прав, если наниматель ущемляет их чрезмерным контролем, выходящим за рамки дозволенного, хотя критерий «дозволенности» также не определен. Законодательство не дает четкого ответа на вопрос о том, когда

наниматель должен запрашивать согласие работника на использование технологий мониторинга, предполагающих сбор и анализ персональных данных.

Целесообразным представляется адаптировать опыт зарубежных государств в области регулирования данных отношений. Приведем некоторые примеры.

В Германии действует Федеральный закон о защите данных (BDSG). Указывается, что если обработка персональных данных работников осуществляется на основании согласия, при оценке того, имеется ли согласие, должны учитываться зависимость лица, занятого в трудовых отношениях, и обстоятельства, при которых было дано согласие, а также его добровольность. Согласие должно быть дано в письменной или электронной форме, если иная форма не является подходящей из-за особых обстоятельств. Наниматель должен проинформировать работника в текстовой форме о цели обработки данных и его праве на отзыв в соответствии с п. 3 ст. 7 Регламента (ЕС) 2016/679 [3] .

В Финляндии действует Закон о защите приватности в трудовой жизни, которым установлено, что цели и процедуры видеонаблюдения, контроля доступа и иных методов мониторинга сотрудников должны вырабатываться нанимателем совместно с представителями работников. Помимо контроля доступа и видеонаблюдения перечислены такие варианты мониторинга, как мониторинг через интернет или иные внутренние системы, контроль электронной почты или информационной сети, отслеживание местоположения работника. Установлено также, что наниматель обязан утвердить цель и методы мониторинга и ознакомить с ними работников [2].

В Великобритании Законом о регулировании полномочий по расследованию и Правилами о телекоммуникации (перехвате сообщений) 2000 г. нанимателю разрешено контролировать и записывать коммуникации сотрудника в телекоммуникационной системе нанимателя без согласия работника для следующих целей: 1) для установления фактов (например, для предоставления доказательств коммерческих сделок или других деловых контактов в случае возникновения споров); 2) для того чтобы удостовериться в соблюдении регуляторных или саморегулируемых практик или процедур; 3) для того чтобы установить или продемонстрировать стандарты, которые должны быть достигнуты лицами, использующими систему при выполнении своих обязанностей (например, мониторинг звонков клиентов для контроля качества и обучения сотрудников); 4) для предотвращения или выявления преступлений (таких как мошенничество или коррупция); 5) для расследования или выявления несанкционированного использования той или иной телекоммуникационной системы (например, для проверки того, что сотрудники не используют Интернет в целях, запрещенных политикой нанимателя в отношении использования Интернета); 6) для обеспечения эффективной работы системы или в качестве ее неотъемлемой части (например, для защиты системы от вирусов и хакеров, а также для выполнения рутинных перехватов в оперативных целях, таких как резервное копирование).

Наниматель также может отслеживать, но не записывать сообщения:

– которые предназначены для получения сотрудником (независимо от того, получил он их или нет), чтобы определить, относятся ли они к его бизнесу (например, наниматель может проверить голосовую почту сотрудника и ящики входящей электронной почты);

– поступающие на горячую линию, которая предоставляется бесплатно и гарантирует анонимность звонящего (в целях поддержки или защиты сотрудников горячей линии).

Тем не менее мониторинг или запись сообщений для любой из перечисленных выше целей не разрешены, за исключением случаев, когда:

– сообщение относится к деятельности нанимателя или иным образом происходит в ходе этой деятельности;

– рассматриваемая система предназначена для использования полностью или частично, в связи с этим бизнесом;

– наниматель «предпринял все разумные усилия» для информирования «каждого лица, которое может использовать рассматриваемую телекоммуникационную систему» о том, что сообщения, передаваемые через нее, могут быть прослушаны [1].

Таким образом, установлен четкий перечень случаев, в которых допускается мониторинг коммуникаций без согласия сотрудников. Однако работники, а также в ряде случаев и клиенты нанимателя, должны быть уведомлены о прослушивании или просмотре сообщений, осуществляемых в телекоммуникационной системе нанимателя.

Предлагается внести изменения в Закон «О персональных данных» (далее – Закон) в части трудовых отношений; на данный момент Закон содержит лишь положения о том, что согласие субъекта персональных данных на обработку персональных данных при оформлении трудовых (служебных) отношений, а также в процессе трудовой (служебной) деятельности не требуется в случаях, предусмотренных законодательством. При этом речь идет в том числе и о специальных персональных данных. Предлагается дополнить Закон рядом статей, устанавливающих перечень случаев, когда мониторинг допускается без согласия работников, а также случаев, когда получение согласия необходимо, установить ответственность нанимателей при нарушении прав работников при использовании средств контроля, ограничить возможности использования технических средств критерием «допустимости» в целях ограничения степени «вторжения» нанимателя в личную жизнь работника.

Литература

1. Цифровой контроль за сотрудниками (использование технологий мониторинга на рабочем месте). – Режим доступа: https://xn--h1aax.xn--p1ai/news/tsifrovoy-kontrol-za-sotrudnikami-ispolzovanie-tekhnologiy-monitoringa-na-rabochem-meste/. – Дата доступа: 21.04.2024.
2. Act on the Protection of Privacy in Working Life 759/2004. – Mode of access: https://www.finlex.fi/en/laki/kaannokset/2004/en20040759. – Date of access: 21.04.2024.
3. Bundesdatenschutzgesetz. – Mode of access: https://www.gesetze-im-internet.de/bdsg_2018/. – Date of access: 21.04.2024.
4. Employee monitoring and surveillance: The challenges of digitalization / Eurofound, 2020. – Mode of access: https://www.eurofound.europa. eu/sites/default/files/ef_publication/field_ef_document/ef20008en.pdf. – Date of access: 21.04.2024.

УДК 343

АКТУАЛЬНЫЕ СПОСОБЫ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ В СЕТИ ИНТЕРНЕТ

И. Ю. Тимошенко

Учреждение образования «Гомельский государственный технический университет имени П. О. Сухого», Республика Беларусь

Научный руководитель Д. Н. Лемтюгов

В современном мире Интернет играет ключевую роль в повседневной жизни людей, обеспечивая им доступ к информации, услугам и коммуникации. Однако вместе с возможностями, которые предоставляет Интернет, существует и ряд угроз, включая различные виды мошенничества. Мошенничество в сети Интернет является одной из наиболее распространенных и серьезных угроз, с которыми сталкиваются пользователи. Современные