



► Справка МОТ

► Совершенствование права работников на защиту персональных данных

Введение

В данном обзоре рассматривается вопрос о том, как извлечение данных о нашей личной и трудовой жизни влияет на наши возможности трудоустройства, на соотношение сил между руководством и работниками, а также о том, какими правами должны обладать работники в отношении своих данных, чтобы не допустить сужения своих потенциальных возможностей на рынке труда.

Все цифровые устройства извлекают и/или генерируют данные о том, как мы общаемся в социальных сетях, производим оплату кредитными картами, о наших покупательских привычках, какими веб-сайтами

и приложениями мы пользуемся и когда, и в дополнение к этому 14 датчиков в нашем смартфоне собирают данные о местоположении, акустических параметрах и температуре вокруг нас, скорости передвижения и многом другом. Все эти данные используются для составления профиля и выводов о каждом из нас – как о гражданине и как о работнике. Наши профили и прогнозы о нас создаются не только для рекламы, но и для манипулирования мыслями, для информирования о вакансиях, а также для оценки инклюзивности и многообразия рынка труда.

Важно понимать, что извлечение данных может повлиять не только на нашу жизнь и карьеру. По мере накопления данных они используются для сравнения людей или групп по бесконечному множеству других критериев. Например, рейтинги клиентов сопоставляются с особенностями работников, вероятность вступления в профсоюз – с типом друзей. Индекс массы тела – со скоростью выполнения работы. Акцент, почтовый индекс – с воспринимаемой благонадежностью. Алгоритмические системы, используемые для поиска таких корреляций, вероятностей, прогнозов и различий постоянно усложняются по мере экспоненциального роста объема данных. Другими словами, то, что мы делаем, даже не осознавая этого, влияет на жизнь других людей.

Данные в сфере труда

В связи с пандемией COVID-19 тенденция к созданию рабочих мест, основанных на данных, только усилилась. Все цифровые сервисы и системы на рабочих местах извлекают данные о работниках пятью способами:



Прямой сбор данных

у кандидатов на должность, сотрудников,



Профили/наборы данных, приобретенные



Извлечение электронно-цифровых следов



Данные, полученные с помощью датчиков,



Аудио и видео данные

с камер видеонаблюдения, телефонных

- **Прямой сбор:** В резюме содержится много ценной информации, например: о предыдущих работодателях, образовании, возможно, даже досуга и хобби. Работодатели могут напрямую собирать данные о своих клиентах (что они покупают, как часто, какие товары или услуги просматривают в Интернете и т. д.) и сотрудниках (например, как часто они болеют, продолжительность рабочего дня и смены и т. д.).
- **Приобретенные профили данных:** Повсеместно существует множество брокеров данных, чья бизнес-модель заключается в покупке, объединении и продаже наборов данных. К ним относятся агрегированные наборы данных о трафике, данные о «благонадежности» определенных групп людей, кредитные рейтинги, данные о состоянии здоровья и уровне образования в зависимости от географического региона или социально-экономического статуса.
- **Извлечение следов данных:** Когда вы открываете свою рабочую электронную почту или сервер, вы оставляете следы своих действий. В какое время вы вошли в систему, к каким документам обращались? Кроме того, некоторые системы, например Office365, генерируют отчеты о том, насколько вы «продуктивно работаете», «сконцентрированы» и пр. Обращает ли руководство компании внимание на эти показатели?
- **Данные датчиков:** Некоторые компании устанавливают датчики в своих зданиях: эти датчики, размещенные под столом, фиксируют, как часто вы садитесь и встаете из-за стола. Датчики размещаются на дверях, чтобы отслеживать загруженность помещения и наличие свободных мест. Некоторые работники вынуждены использовать ручные сканеры или носимые устройства, например, фитнес-трекеры и системы отслеживания местоположения. Все они генерируют данные, которые используются или могут быть использованы руководством.
- **Аудио и видео данные:** некоторые данные получают с помощью аудиовизуальных систем. Измеряется и оценивается тон голоса и речь сотрудников колл-центров. Прослушиваются звонки с мобильных телефонов. Для определения местоположения и идентификации работников используются системы видеонаблюдения или распознавания лиц. Несмотря на резкую критику, некоторые из этих систем используются для прогнозирования настроения и

эмоционального состояния работников: устали ли они, озабочены, разочарованы, довольны или нервничают?

Независимо от способа получения данных, цифровые системы наблюдения и мониторинга собирают данные о работниках, их действиях или бездействии. Системы мониторинга не новы, но цифровая природа современных систем имеет особые характеристики, которые влияют на отношение профсоюзов к ним. Рассмотрим систему, оснащенную камерами видеонаблюдения и портативными датчиками для контроля объема произведенной продукции работниками завода. *Во-первых*, такую систему невозможно обойти, так как она интегрирована в трудовые процессы и в

оборудование. *Во-вторых*, она осуществляет и собирает большие объемы данных из разных источников. *В-третьих*, сбор данных осуществляется в режиме реального времени, поэтому руководство получает информацию мгновенно. *В-четвертых*, интерактивная система обеспечивает передачу данных и обратную связь в реальном времени – в нашем случае непосредственно в производственном цехе, где на промышленных светодиодных табло приводятся данные о количестве изготовленных изделий каждым работником.

Работодатели могут использовать эти данные для оценки производительности труда и эффективности работы (как бы они ее ни определяли). Например, они могут произвести сложные расчеты вероятности того, что вы выполните поставленные задачи, получите высокую оценку клиентов, будете работать быстро и с энтузиазмом относиться к своей работе. Кроме того, эти данные могут использоваться для прогнозирования, например, вероятности того, что вы скоро покинете компанию, заболите, станете работать медленнее или вступите в профсоюз.

Для чего именно работодатель будет использовать эти данные, зависит от *назначения* внедряемых систем и выполняемого ими анализа данных. В некоторых случаях работники могут дать согласие на извлечение этих данных. Например, работники могут поддержать сбор данных для целей охраны труда во избежание производственного травматизма или для измерения продолжительности рабочего дня, чтобы предотвратить стресс и профессиональное выгорание. Важно, чтобы сотрудники знали и могли влиять на то, будут ли собираться данные, каковы цели сбора данных, как они будут использоваться и что произойдет с этими данными в последующем. В Справке MOT 2 рассматриваются уже выявленные вредные последствия воздействия данных и алгоритмов на работников.

Политэкономия извлечения

данных Хотя работники и работодатели в принципе могли бы договориться о целях извлечения и анализа данных, существуют и другие опасения. В частности, действительно ли мы хотим, чтобы наш труд был превращен в многочисленные измеряющие наше поведение элементы данных, которые могут или не могут быть использованы по назначению? Каким образом восприятие работников не как людей, а скорее как

данные или баллы в сравнении со статистической нормой, может повлиять на права человека и права работников?

Существует широко распространенное выражение «данные – это новая нефть», т.е. это ценный ресурс, который можно добыть, но он будет бесполезным в «сыром», т.е. необработанном, виде. Поэтому данные необходимо анализировать и агрегировать. Они должны стать средством производства, которое можно использовать для создания прибыли в производственных и сервисных цепочках. Такое толкование данных говорит о том, что данные – это товар, который можно покупать и продавать. Из этого следует, что данные работников могут быть монетизированы.

Однако если рассматривать вклад работников в эти средства производства в денежном выражении и требовать на этой основе перераспределения

их добавленной стоимости в пользу самих работников, как это иногда происходит, то это может лишь увековечить и, возможно, даже оправдать превращение труда в товар.

Критики трактовки данных с точки зрения экономической теории утверждают, что данные следует рассматривать с точки зрения власти и прав.

Те, кто собирает данные, получают власть над рынками, конкурентами, гражданами и работниками. Именно их аналитика и их истории в одностороннем порядке контролируют нас как индивидов и манипулируют тем, какие услуги, мнения и продукты предоставляются нам, невзирая на права человека и другие моральные соображения.

Известный автор книги «Эпоха надзорного капитализма» Шосана Зубофф убеждена, что мы должны запретить так называемые «поведенческие фьючерсные рынки»¹. Она имеет в виду торговлю профилями, используемыми для постоянного манипулирования ничем не подозревающими людьми. По ее словам, организаторам процесса сбора данных нужны огромные объемы данных, чтобы обеспечить определенность и уверенность своим клиентам, и им нужны самые разнообразные данные, чтобы их максимально повысить точность их прогнозов и моделей. Это приводит к экономии масштаба и охвата – и, следовательно, к концентрации власти в руках нескольких очень богатых глобальных компаний: Google, Meta, Apple, Amazon, Microsoft, Alibaba и Tencent.

Если сбор данных с экономической точки зрения ограничивается только законом (например, нормативными правовыми актами в области защиты персональных данных), то правозащитный подход требует, чтобы сбор данных производился только при соблюдении более широких прав человека. В 2018 году УВКПЧ опубликовало методическую записку² по правозащитному подходу к данным. Она содержит шесть основных принципов, каждый из которых содержит ряд дополнительных установок:

1. Участие: Участие соответствующих групп населения в работе по сбору данных, включая планирование, сбор, распространение и анализ данных

2. Дезагрегирование данных:

Дезагрегирование данных позволяет пользователям данных получить сопоставимые показатели для сравнения групп населения, а также для

лучшего понимания ситуации по конкретным группам. Для проведения дезагрегирования необходимо осуществить сбор данных с конкретными характеристиками.

3. Самоидентификация: Для целей сбора данных населению, представляющему интерес, должна быть предоставлена возможность самоопределения. Физические лица должны иметь выбор: раскрывать или не раскрывать информацию о своих персональных данных

сбора данных должны предоставлять в открытом доступе точную информацию о своей деятельности, в том числе структуру исследований и методологию сбора данных. Данные, собранные государственными органами, должны быть доступными для широкой общественности

5. Неприкосновенность частной

жизни: Данные, предоставленные организаторам процесса сбора данных, должны быть защищены и храниться в неприкосновенности; необходимо обеспечить строгую конфиденциальность ответов физических лиц и их персональных данных.

6. Подотчетность: Организаторы процесса сбора данных несут ответственность за соблюдение прав человека при осуществлении своей деятельности.

Данные следует использовать, когда необходимо обеспечить подотчетность государств и других субъектов в области соблюдения прав человека

Для работников эти принципы означают, что они имеют право участвовать в процессе сбора своих данных, знать, для каких целей они будут использоваться, что данные являются репрезентативными и, следовательно, недискриминирующими, а также что их права человека всегда соблюдаются. Признаются ли эти права работников в нормативно-правовых актах о защите данных во всем мире?

Регламент о защите персональных данных и работники

Во всем мире нормативные акты, регулирующие защиту данных, касаются обработки персональных данных субъектов данных и, в некоторых случаях, дополнительной информации, позволяющей идентифицировать личность³. По данным UNCTAD, 19% стран мира не имеют нормативно-правовых актов по защите данных⁴. В остальных странах нормативные акты по защите данных работников можно условно разделить на три большие категории. Акты, содержащие конкретные положения относительно данных о работниках (например, Общий регламент ЕС о защите персональных данных – GDPR); акты, содержащие отсылочные положения, как, например, в большинстве стран Африки, Латинской Америки и Азиатско-Тихоокеанского региона; акты, которые прямо исключают работников из сферы охвата (например, Закон штата Калифорния о защите прав потребителей 2018 года – CCPA, а также частично Закон Австралии о конфиденциальности 1988 года⁵).

Большинство нормативных актов по защите данных относятся ко второй категории⁶, где все законодательные требования, связанные с конфиденциальностью данных, распространяются на сбор, обработку, передачу и использование данных работников. Более того, подавляющее большинство стран требуют, чтобы работодатели получали «информированное согласие»⁷ работников на извлечение и использование данных о них. Это противоречит

¹ <https://www.project-syndicate.org/onpoint/surveillance-capitalism-exploiting-behavioral-data-by-shoshana-zuboff-2020-01?barrier=accesspaylog>

² <https://www.ohchr.org/documents/issues/hrindicators/guidancenoteonapproachtoadata.pdf>

³ <https://techgdp.com/blog/difference-between-pii-and-personal-data/>

⁴ <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

⁵ <https://www.lexology.com/library/detail.aspx?g=0f6d20a7-a6b1-4980-aa0e-a98f1d637d38>

⁶ См. обзор в электронной книге: <https://www.mayerbrown.com/ebooks/A-Global-Guide-to-Employee-Data-Privacy/#/spreads/1>

⁷ В GDPR говорится, что согласие должно быть «добровольным, конкретным, информированным и недвусмысленным». Это означает, что субъект данных должен осознавать, что он дает согласие на обработку своих данных добровольно и его нельзя вынуждать давать такое согласие. Пункт 32 – Условия согласия – Общий регламент ЕС о защите персональных данных

некоторыми исключениями⁸ информированное согласие не является правовым основанием для обработки данных работников в соответствии с GDPR.

Третья категория, прямо исключаящая работников из сферы охвата, встречается нечасто, однако в настоящее время в США на рассмотрении находятся несколько законопроектов о защите персональных данных, которые направлены именно на то, чтобы исключить работников из их сферы охвата. В 2019 году законопроект Ассамблеи 25 (AB-25) внес поправки в Закон Калифорнии о защите персональных данных потребителей (CIPA), отменив обязательства работодателей по отношению к жителям Калифорнии, которые являются соискателями работы, сотрудниками, автономными подрядчиками, корпоративными должностными лицами и руководителями⁹. Несмотря на предусмотренные законопроектом AB-25 исключения, работодатели по-прежнему обязаны уведомлять потребителей, в том числе своих работников, а также лиц, ищущих работу, о видах собираемой ими персональной информации и целях ее использования во время или до сбора данных.

В целом, во всем мире нормативные акты по защите данных, за исключением GDPR, не содержат четко определенные права работников на данные. Хотя большинство нормативных актов по защите данных косвенно распространяется и на работников, они также основаны на «информированном согласии» как основы для обработки персональных данных работников. В любом случае, как указано в Регламенте GDPR, работники не могут свободно давать информированное согласие в свете властных отношений между руководством и работниками¹⁰.

Помимо этого, хотя работодатели, согласно требованиям большинства систем защиты персональных данных, обязаны *информировать работников* о собранных данных и целях их сбора, у работников нет права на просмотр, исправление, а также редактирование или удаление собранных данных.

Ни одна из них не соответствует в полной мере принципам УВКПЧ, как описано выше.

Совершенствование права работников на защиту персональных данных

Очевидно, что в большинстве стран и регионов индивидуальные и коллективные права работников на данные определены недостаточно четко. На приведенной ниже схеме представлен жизненный цикл данных в сфере труда от сбора данных до их анализа, хранения и удаления; темы,

которые должны быть известны профсоюзам и по которым они должны вести переговоры, а также права, которыми должны обладать работники. Схема основана на публикации МОТ 1997 года «Защита персональных данных работников». Свод практических правил МОТ¹¹.

Жизненный цикл данных

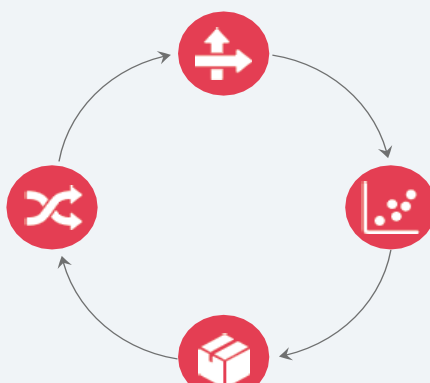
в сфере труда

Сбор данных:

Источники? Знание и доступ профсоюза к ним? Права на опровержение или блокировку?

Удаление данных:

Продаются ли данные? Кому? Удаляются ли данные? Могут ли работники отказать/заблокировать того, кому проданы данные? К ним



относятся наборы данных, статистика, выводы (профили)

Анализ данных:

Используется в сфере производства и управления персоналом. Какие права имеют работники на доступ к

этим данным и сделанным выводам

(профилям)?

Могут ли они возражать против этого и т. д.? Профсоюзы должны четко определить, для чего данные можно использовать, а для чего – нельзя

Хранение данных:

Серверы – где? У кого есть доступ? В какой юрисдикции? Это особенно важно в связи с обсуждением вопросов электронной коммерции в ВТО

⁸ https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-my-employer-require-me-give-my-consent-use-my-personal-data_en

⁹ <https://secureprivacy.ai/blog/ab-25-what-this-ccpa-amendment-means-for-employers-and-employees>

¹⁰ См. Рабочая группа по 29-ой статье. Руководство по согласию в соответствии с Регламентом 201 6/679, стр. 7. <https://ec.europa.eu/newsroom/article29/redirection/document/51030>

¹¹ https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf

Некоторые из требований каждого из четырех этапов, хотя и далеко не все, распространяются на работников в зоне действия европейского Общего регламента о защите данных. Для работников в большинстве других юрисдикций эти права, если они будут согласованы, станут новыми.

Сбор данных

На этапе сбора данных рассматриваются внутренние и внешние инструменты сбора данных; источники данных; информированы ли профсоюзные представители и работники о том, какие инструменты предполагается использовать и имеют ли они право возражать или отказываться от таких инструментов. Извлечение большей части данных происходит скрыто от работника (или гражданина), но на руководство должна быть возложена ответственность за это.

В зоне действия GDPR компании обязаны проводить оценку воздействия на защиту данных (DPIA) при внедрении новых технологий, которые могут быть сопряжены с высоким риском для персональной информации физических лиц. Они также обязаны консультироваться с работниками по этому поводу¹². Однако лишь немногие профсоюзы имеют доступ к таким оценкам или знают о их проведении – профсоюзам следует отстаивать свое право на участие в них.

Анализ данных

На этапе анализа данных профсоюзы должны охватить выявленные пробелы в законодательстве, в частности, отсутствие прав в отношении профилей работников, создаваемых с использованием статистических вероятностей на основе собранных данных. Работники в зоне действия GDPR

имеют право знать, какие профили составлены на основе прямого использования их персональных данных, но у них нет права знать, какие выводы о них строятся без использования их персональных данных¹³. Такие выводы (профили) могут быть использованы для определения оптимального графика работы, заработной платы (если она связана с показателями эффективности) или, в кадровых службах – для определения того, кого нанимать, продвигать по службе или увольнять. Они также могут быть использованы для прогнозирования поведения на основе предыдущих моделей, данных об эмоциях и/или данных об активности.

Доступ к профилям является ключом к расширению прав и возможностей работников и к соблюдению прав человека. Работники должны иметь более полное представление об этих профилях

и иметь к ним доступ, а также право требовать их исправления, блокировки и удаления. Без этих прав не будет никаких «сдержек и противовесов» относительно использования руководством алгоритмических систем, а также дискриминации и предвзятости, которые могут возникнуть на основе этих данных.

На этапе сбора данных профсоюзы могли бы успешно проводить переговоры относительно целей сбора и анализа данных, и четко определять, для чего можно использовать собранные данные, а для чего — нельзя.

Хранение данных

Этап хранения данных важен не в последнюю очередь в связи с торговыми соглашениями и переговорами о потоках данных. Например, в контексте электронной торговли переговоры о «свободном обмене данными» в рамках и вокруг Всемирной торговой организации направлены на лишение любой страны права локализовать данные в пределах территории своей страны. Это может привести к перемещению данных в зоны с более низким уровнем защиты персональных данных и создать риски, поскольку данные работников могут затем быть проданы, перегруппированы и снова проданы без соблюдения политики защиты данных страны происхождения.

Если данные будут свободно распространяться по всему миру, а работники не добьются существенно более широких прав на данные, обеспечиваемых национальным законодательством или коллективными

соглашениями, их доступ к этим данным и контроль над ними станет еще слабее.

Удаление данных

Последний этап — удаление данных. Он связан с этапом хранения, а также и с возможной продажей данных и их наборов, содержащих информацию о

Пример:

В ходе переговоров профсоюз Teamsters в Калифорнии добился того, что данные о местоположении водителей, собранные в целях обеспечения их безопасности, не будут использоваться при оценке

работниках. Профсоюзы должны проявлять бдительность! Речь идет не только об удалении данных, но и о продаже и передаче третьим сторонам наборов данных с соответствующими выводами и профилями. Профсоюзы должны участвовать в переговорах об укреплении и расширении прав на получение информации о том, что и кому передается, для того, чтобы у них была возможность возражать или даже блокировать процесс передачи — это чрезвычайно важно в свете упомянутых выше переговоров по электронной торговле. Кроме того, в соответствии с принципом минимизации данных, принятым в GDPR (статья 5.1с)¹⁴, профсоюзы должны, иметь право, как минимум, требовать удаления наборов данных и выводов/профилей работников, после того как они были использованы по своему первоначальному назначению.

¹² Статья 35 GDPR и мнение № 2/2017 РАБОЧЕЙ ГРУППЫ СТ.29 об обработке данных в сфере труда

¹³ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829

¹⁴ <https://gdpr-info.eu/art-5-gdpr/>

Пример:

Профсоюз работников финансового сектора в Ирландии успешно провел переговоры по двум важнейшим статьям кадровой политики Королевского банка Шотландии. Это:

1. Оговорка о запрете передачи персональных данных работников в коммерческих целях

Банк обязуется не превращать данные сотрудников в товар, предназначенный для продажи или коммерческой деятельности.

2. Уважение неприкосновенность частной жизни и прав человека

Банк обязуется не превращать данные сотрудников в товар, предназначенный для продажи или коммерческой деятельности.

Банк обязуется уважать неприкосновенность частной жизни и права человека работников, закрепленные законом и, в частности, Всеобщей декларацией прав человека ООН и Сводом практических правил МОТ по защите персональных данных работников от 1997 года.

См. пресс-релиз [здесь](#)

Рекомендации

Чтобы защитить права работников на цифровых рабочих местах и предотвратить влияние выводов и профилей (которые часто оказываются неточными) на возможности трудоустройства работников, профсоюзам следует начать решительные переговоры об улучшении прав работников на данные.

Для успешного выполнения этой задачи профсоюзы могут:

- 1.** Обучать членов профсоюза и профсоюзных представителей по вопросам о роли данных на цифровых рабочих местах и в обществе в целом. Это включает в себя полезные рекомендации по использованию цифровых устройств, предоставленных работодателем, и передовой опыт защиты прав работников на неприкосновенность частной жизни в нерабочее время.
- 2.** Рассмотреть возможность создания группы профсоюзных представителей-специалистов по датафикации трудовых процессов и работников. См. также Справку 2.
- 3.** Предусмотреть в профсоюзе наличие специалистов (экспертов по правовым вопросам, команды переговорщиков и организаторов), которые могут поддержать вышеуказанные переговоры.
- 4.** Рассмотреть жизненный цикл данных на рабочем месте с точки зрения прав человека и прав работников.

5. Разработать единую рамочную политику профсоюза в области защиты персональных данных, которая могла бы стать ориентиром для (цифровых) профсоюзных представителей в ходе переговоров. В свете прав человека и в соответствии с жизненным циклом данных на рабочем месте такая политика может охватывать следующие темы:

- а.** Общий принцип: Необходимо обеспечивать достоинство и благополучие работников при использовании на рабочем месте технологий, основанных на данных. Необходимо сформулировать положения и стандарты, предоставляющие работникам свободу выбора в отношении новых технологий; способствующие охране здоровья и безопасности, защите права на объединение в профсоюзы и предотвращение дискриминации и других негативных последствий для работников.
- б.** Работники и/или их представители должны участвовать во всех мероприятиях по оценке воздействия данных и их периодической переоценке.
- с.** Работодатели должны в ясной и доступной форме уведомлять работников обо всех технологиях, основанных на данных, которыми оснащается рабочее место. Уведомления должны содержать понятное описание технологий, типов собираемых данных, назначения этих систем, а также прав и средств защиты, доступных работникам.

d. Минимизация данных:

Работодатели должны собирать данные о работниках только тогда, когда это необходимо и требуется для выполнения работниками своей работы. См. также определение в GDPR <https://gdpr-info.eu/art-5-gdpr/>

e. Работники должны иметь право на доступ к своим данным, их исправление и скачивание. Они должны получать всю необходимую информацию об этих данных, в том числе о том, почему и как они были собраны, были ли сделаны выводы на основе этих данных и если да, то что они собой представляют, и использовались ли эти данные работодателем в качестве основы для принятия решений, связанных с трудовыми отношениями, включая решения о найме. Работодатели несут ответственность за исправление любых неточных данных.

f. Данные работников должны быть защищены, в том числе от неправомерного использования. В частности, работодателям не следует разрешать продавать, выдавать лицензии/дарить или иным образом предоставлять третьим лицам доступ к данным работников; в противном случае соблазн нарушить неприкосновенность частной жизни работников с целью получения денежной выгоды путем продажи персональных данных работников может быть слишком высок.

g. Индивидуальные биометрические и медицинские данные работников никогда не должны передаваться третьим лицам, если это не предусмотрено законом.

h. Работодатели должны использовать системы мониторинга и наблюдения только в узких целях, не наносящих прямого или косвенного ущерба работникам.

i. Изменения в системах мониторинга и наблюдения в связи с технологическими изменениями

на рабочем месте должны быть предметом коллективных переговоров.

j. Технологии, основанные на данных, не должны дискриминировать работников по таким «защищенным характеристикам», как гендер, пол, возраст, инвалидность, брачный статус и статус «гражданского партнерства», беременность и материнство, раса, религия и убеждения.

k. Удаление защищенных характеристик из технологий, основанных на данных, не должно автоматически позволять работодателям обходить другие требования этой рамочной политики. Например, многие работодатели оправдывают продажу или передачу наборов данных, содержащих личные данные работников, тем, что наборы данных обезличены поэтому не могут быть связаны с отдельными работниками. Однако многие исследования показывают, как можно сравнительно легко деанонимизировать наборы данных¹⁵ и тем самым подвергнуть риску идентификационные данные и неприкосновенность частной жизни работников.

6. Будьте бдительны и критически относитесь к попыткам определять данные как товар/ актив или средство производства, а также к рекомендациям по разработке систем перераспределения в пользу работников прибыли, обеспечиваемой данными как фактором производства. Права не должны обмениваться на деньги.

7. Подумайте об этических методах сбора данных о работниках, которые позволили бы опровергнуть результаты анализа, проведенного руководством (см.

Справку 3), и тем самым разрушить монополию работодателя или системы на «истину».

15 https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAlmZ_o2Up5jda586F714qomIzWnAvy7a3pbaQ4D8vXb7WB3oxaA-ZMJHNpXWZM9W0uCR8aCSvyqd-ZGaCWrugvxJ_y7GYlwTuv5Cysn4MvhjGmLmVg4uLwMjspp5cT1epXQCMYLMgIpNizUzEW_MIBPJNEQWiUrQ7tBOTr8VIFXU