

УДК 34**Правомерность вмешательства в частную жизнь работника:
подход Европейского Союза****Дружинин Максим Игоревич**

Магистр информационного права,
Санкт-Петербургский государственный университет,
199034, Российская Федерация, Санкт-Петербург, Университетская наб., 7/9;
e-mail: Druzhinin@mail.ru

Пагов Астемир Жиросланович

Магистр информационного права,
Санкт-Петербургский государственный университет,
199034, Российская Федерация, Санкт-Петербург, Университетская наб., 7/9;
e-mail: Druzhinin@mail.ru

Аннотация

Статья посвящена исследованию допустимости вмешательства работодателя в частную жизнь работника сквозь призму правовых подходов в юрисдикции Европейского Союза. На основе анализа ключевых решений ЕСПЧ рассматривается применение критерия неприкосновенности права на приватность и необходимость поиска баланса между правами работника и законными интересами работодателя. Особое внимание уделяется влиянию нормативных актов Европейского Союза, включая GDPR и AI Act, на регулирование цифрового мониторинга и использования ИИ на рабочем месте. В статье аргументируется, что традиционные концепции защиты данных, основанные на целостности и прозрачности, не обеспечивают должной защиты в условиях управления трудовыми ресурсами с использованием современных информационных технологий, в условиях структурной уязвимости работника в трудовых правоотношениях.

Для цитирования в научных исследованиях

Дружинин М.И., Пагов А.Ж. Правомерность вмешательства в частную жизнь работника: подход Европейского Союза // Вопросы российского и международного права. 2025. Том 15. № 5А. С. 193-202.

Ключевые слова

Персональные данные, Европейский Союз, Права работников, Информационные технологии, ЕСПЧ.

Введение

В статье анализируется правомерность вмешательства работодателя в частную жизнь работника через призму подходов Европейского союза и Европейского суда по правам человека. Особое внимание уделено критерию «обоснованного ожидания неприкосновенности частной жизни» и практике его применения в делах *Halford*, *Copland*, *Bărbulescu* и других. Рассматриваются ограничения, налагаемые на мониторинг и сбор персональных данных согласно GDPR и новому Регламенту ЕС по искусственному интеллекту (AI Act 2024/1689). Освещаются риски, связанные с использованием высокорискованных ИИ-систем на рабочем месте, и актуальные пробелы в российском и европейском трудовом праве. Делается вывод о необходимости учета структурной неравномерности трудовых отношений при разработке эффективных правовых механизмов информационной защиты работника, способных противостоять росту цифрового контроля и алгоритмического управления трудом.

Основное содержание

В современном мире затруднительно говорить об абсолютной конфиденциальности по причине развития информационных технологий, дающих любому человеку доступ к практически любой информации, находящуюся во «Всемирной паутине» [Ильин, Всемирная паутина, [www](#)]. С течением времени общество осознало необходимость защиты информации, особенно персональных данных. Работодатель является одним из субъектов, обрабатывающих персональные данные работников. Осуществляя в соответствии с Налоговым кодексом РФ функции налогового агента [Хохлов и др., Трудовое право России, 2020], работодатель обязан иметь информацию о дате рождения работника, реквизитах документа, удостоверяющего личность работника-налогоплательщика, полном адресе постоянного места жительства работника, идентификационном номере налогоплательщика — физического лица, а также информацию, на основании которой производятся налоговые вычеты.

В представленном примере понятна целесообразность получения работодателем доступа к этой информации. Однако работодатель в силу своей доминирующей позиции в трудовых отношениях может получить доступ к иным персональным данным работников. Обработка тех данных, которые не указаны непосредственно в законе и не необходимы для исполнения трудового договора, может свидетельствовать о нарушении права работника на уважение частной жизни.

На международном уровне в Европейском суде по правам человека (далее - ЕСПЧ) рассматривалась проблема вмешательства в частную жизнь работника в рамках ст. 8 Конвенции о защите прав человека и основных свобод (далее - ЕКПЧ), устанавливающей в первом пункте суть гарантий на уважение частной жизни, а во втором общие условия и конкретные основания ограничений представленных прав и свобод [Европейская конвенция о защите прав человека, [www](#)]. Однако, прежде чем перейти к анализу решений ЕСПЧ, имеющих исключительную важность для темы настоящей статьи, авторы считают важным рассмотреть понятие неприкосновенности частной жизни.

Концепция частной жизни (*privacy*) получила развитие в научной работе известных американских юристов Самюэля Д. Варрена и Луи Брэндайса “*The Right to Privacy*” 1890 года, в котором приватность определяется как право быть свободным от внешнего воздействия [The Right to Privacy, 1890]. Позднее это право было названо в судебной практике США «началом всех субъективных прав» [Public Utilities Commission v. Pollak, 1952]. Разумеется, столь широкая

концепция требует высокого уровня формальной определенности, которого можно достичь посредством разработки соответствующих критериев. Таковым стал критерий «обоснованного ожидания неприкосновенности частной жизни» (*reasonable expectation of privacy*), впервые упомянутый в судебном решении *Katz v. United States* 1967 года американским судьей Джоном Маршаллом Харланом, рассматривавшим дело о вмешательстве в частную жизнь истца агентами ФБР, прослушивавшими его разговоры в телефонной будке. Основываясь на казуальном толковании Четвертой поправки Конституции США [Constitution of the United States, 1789], судья предложил два стандарта для определения обоснованного ожидания неприкосновенности: человек должен иметь реальное (субъективное) ожидание сохранения конфиденциальности частной жизни в той или иной ситуации, и при этом общество должно быть готовым признать это ожидание разумным [*Katz v. United States*, 1967]. Европейский суд по правам человека при рассмотрении дел в рамках ст.8 ЕКПЧ стал применять критерий «обоснованного ожидания неприкосновенности частной жизни» уже с конца двадцатого столетия.

Первым примером установления ЕСПЧ «обоснованного ожидания неприкосновенности частной жизни» стало дело *Halford v. the United Kingdom*, в котором заявительнице, работавшей в полиции в качестве помощника главного констебля, была поставлена прослушка на оба находящихся в ее личном кабинете телефона, а как известно телефонные звонки, сделанные из служебных помещений, могут охватываться понятием «частная жизнь» по смыслу пункта 1 статьи 8 ЕКПЧ [ECtHR, *Malone v. The United Kingdom*, 1984]. Суд посчитал, что у нее были разумные ожидания в отношении конфиденциальности звонков, которые, кроме того, были подкреплены рядом факторов, а именно, что не было никаких свидетельств того, что заявительнице, как пользователю внутренней телекоммуникационной системы, действующей в штаб-квартире полиции, было сделано какое-либо предупреждение о том, что звонки, сделанные с помощью этой системы, будут подлежать прослушке [ECtHR, *Halford v. United Kingdom*, 1997]. ЕСПЧ придерживался сходной позиции и приводил такую же аргументацию в ряде аналогичных дел (*Copland v. the United Kingdom* [ECtHR, *Copland v. the United Kingdom*, 2007], *Peev v. Bulgaria* [ECtHR, *Peev v. Bulgaria*, 2007], *Köpke v. Germany* [ECtHR, *Köpke v. Germany*, 2010]).

Зарубежными и отечественными исследователями отмечается, что рассмотрение Европейским судом по правам человека дел по ст. 8 ЕКПЧ, касающихся интересов работников, через призму «обоснованного ожидания неприкосновенности частной жизни» зависит от конкретных обстоятельств и контекста вмешательства. Т.е. обоснованность ожиданий работника должна определяться в зависимости от природы и обоснованности вмешательства, а также того, был ли работник проинформирован о том, что возможно вмешательство в его право на уважение частной жизни [Сыченко, 2015]. В упомянутом деле *Köpke v. Germany* ЕСПЧ отметил, что «обоснованное ожидание неприкосновенности частной жизни» является значительным фактором при определении нарушения, но не всегда решающим, ибо под решающим фактором стоит понимать необходимость поиска баланса между защитой права работника на уважение частной жизни и правом работодателя на уважение собственности и законного интерес в обеспечении бесперебойного функционирования своей компании. В деле *Libert v. France* ЕСПЧ не использовал критерий обоснованного ожидания невмешательства и признал, что доступ работодателя к файлам, размещенным на рабочем компьютере работника, не является нарушением права на уважение частной жизни. Суд признал, что вмешательство было направлено на обеспечение защиты «прав других лиц», т.е. в данном случае работодателя, который может законно желать обеспечить использование работниками предоставленных в их

распоряжение компьютерных средств для выполнения своих обязанностей в соответствии с их договорными обязательствами и применимыми правилами. Было установлено, что работодатель имеет законный интерес в обеспечении бесперебойного функционирования компании, и что это может быть сделано путем создания механизмов для проверки того, что его работники выполняют свои профессиональные обязанности надлежащим образом и с необходимой тщательностью [ECtHR, *Libert v. France* (588/13), 2018].

Отдельно хотелось бы отметить, что при повсеместной интеграции систем искусственного интеллекта немаловажным остается вопрос защиты прав и законных интересов работников, как наименее защищенной стороны в трудовых правоотношениях. Предлагается рассмотреть нормы европейского закона об искусственном интеллекте (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence) (далее – AI act).

Нормы ЕС о применении искусственного интеллекта на рабочем месте формируют новый феномен цифровых трудовых прав: они требуют прозрачности, оценки рисков и человеческого контроля над алгоритмами, а также закрепляют процессуальные гарантии (информирование, объяснение решений, коллективное вовлечение). Эти положения укладываются в общую европейскую тенденцию — переход от классической модели «работодатель-работник» к регулированию цифрового управления трудом и дополняют уже принятые отраслевые акты, например, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (далее – GDPR) регулирующий обработку персональных данных в Европейском Союзе, создавая более целостную систему защиты работника.

В частности, AI act подразумевает обязанность работодателя уведомить работников, если он развёртывает программное обеспечение, содержащее высокорисковую модель искусственного интеллекта в корпоративную систему, что предусматривает статья 26 параграф 7. Согласно параграфу 4 приложения 3 к AI Act высокорискованными признаются все системы искусственного интеллекта, используемые при приеме на работу и оценке кандидатов, а также предназначенные для использования с целью принятия решений, влияющих на условия трудовых отношений, на продвижение или прекращение трудовых договорных отношений, на распределение задач на основе индивидуального поведения или личных качеств. Следовательно, практически все системы искусственного интеллекта, применяемые в отношениях с работниками будут относиться к высокорискованной категории. Однако данный подход не является чем-то новым, напротив в Российском законодательстве, в пункте 6 части 1 статьи 86 ТК РФ достаточно продолжительное время содержится положение о запрете обработки персональных данных работников исключительно автоматизированным способом, если такая обработка свидетельствует о принятии решений, затрагивающих интересы работников. В то же время AI act предусматривает право работника (или любого иного субъекта) на объяснение решений, основанных преимущественно на выводах высокорискованных моделей искусственного интеллекта, при условиях, если эти решения затрагивают права и законные интересы субъекта. Немаловажным является и ограничение, предусмотренное пунктом f параграфа 1 статьи 5 AI act, подразумевающее полный запрет на эксплуатацию систем, позволяющим определять эмоциональное состояние работник, м самым блокируется предиктивная оценка лояльности сотрудников.

Традиционные подходы к защите данных работников, основанные на принципах прозрачности, согласия и доступа к информации (как в GDPR), фундаментально не защищают

слабую сторону в трудовых отношениях, поскольку они игнорируют структурную субординацию работников и логику алгоритмических систем управления, большинство из которых используется в сфере кадрового менеджмента [Филипова, 2023]. Эффективная защита требует прямого запрета вредных практик, а не просто их освещения. Работники не являются автономными субъектами – в отличие от тех же потребителей цифровых сервисов, работники юридически подчинены работодателям и не могут свободно отказаться от информационного контроля без потери средств к существованию. Законодательство, регулирующее информационные технологии должно следовать модели традиционного трудового права, при котором вводился бы полноценный запрет на использование систем, прямо нарушающих права работников (например, право на время труда и отдыха). В этой связи, в Европейском Союзе, где номинально, действуют «прогрессивные законы» регулирующие отношения в цифровой среде, в работники, в действительности, остаются уязвимыми перед новыми формами контроля, которые подрывают базовые принципы справедливого труда.

Говоря о GDPR, важно отметить, что он не является инновационным и всеохватывающим нормативным актом в области защиты прав работников на приватность. Несмотря на широкое признание Общего регламента по защите данных как «золотого стандарта» в сфере защиты персональных данных, регламент создает фрагментированную систему защиты, недостаточно учитывает специфику трудовых отношений и не обеспечивает эффективную защиту от современных технологий мониторинга работников [Buckley, Caulfield, Becker, 2024.].

Главная проблема GDPR в контексте трудовых отношений кроется в статье 88, которая оставляет регулирование обработки персональных данных работников на усмотрение государств-членов. Согласно данной статье, «государства-члены могут посредством закона или коллективных соглашений предусматривать более конкретные правила для обеспечения защиты прав и свобод в отношении обработки персональных данных работников в контексте трудовых отношений.

Это создает парадоксальную ситуацию: регламент, призванный гармонизировать правовое регулирование в ЕС, сознательно допускает фрагментацию в одной из наиболее важных сфер - трудовых отношениях. Как отмечают исследователи, «правила защиты данных в контексте трудовых отношений далеки от гармонизированных, последовательных и всеобъемлющих. Эта фрагментация исходит из самого GDPR» [Zhang, 2023. – С. 1-6].

Современные технологии мониторинга за действиями работников развиваются значительно быстрее правового регулирования. Алгоритмические системы управления персоналом, использование ИИ для оценки производительности и биометрические системы контроля создают новые вызовы, которые не были предусмотрены авторами GDPR. В то же время отсутствуют эффективные превентивные механизмы, которые могли бы предотвратить нарушения до их совершения. Система оценки воздействия на защиту персональных данных (DPIA), предусмотренная статьей 35 GDPR теоретически должна выполнять эту функцию, но на практике она часто формальна и неэффективна.

Особо остро стоит вопрос с технологиями искусственного интеллекта: рассмотренные выше положения положения AI Act прямо указывают на необходимость информирования работников и их представителей о внедрении таких систем, а также на обязательность регистрации и строгих процедур оценки риска. Однако главной гарантией защиты остается добросовестность владельца системы и механизм саморегуляции разработчиков, что порождает существенные риски реальной уязвимости персонала. Более того, эти и другие технологии не обеспечивают прозрачности в процессе сбора и обработки данных, что увеличивает риски для конфиденциальности и снижает осведомленность субъектов данных об этих рисках.

Знаковым, по мнению авторов, является решение по делу *Bărbulescu v. Romania* о доступе работодателя к личной переписке работника, отправленной с использованием технических средств работодателя. В решении Большой Палаты ЕСПЧ разработал дополнительные критерии для выявления вмешательства в частную жизнь работника:

Был ли сотрудник уведомлен о вероятности того, что работодатель может принять меры по контролю переписки, а также об осуществлении таких мер. Хотя на практике работников можно уведомлять различными способами, в зависимости от фактических обстоятельств каждого дела в уведомлении обычно должен быть ясно указан характер контроля, а само уведомление направлено заранее;

Степень контроля со стороны работодателя и степень вмешательства в частную жизнь работника. В этом отношении следует учитывать уровень контроля в данной области, а также вопрос о том, ограничен ли контроль по времени и по количеству лиц, которые могут ознакомиться с его результатами;

Указал ли работодатель законные причины для обоснования контроля. Более «глубокое» проникновение в частную жизнь работника требует более серьезных обоснований;

Было ли возможно установить систему контроля, основанную на менее агрессивных методах и мерах проникновения в частную жизнь человека. В связи с этим с учетом конкретных обстоятельств каждого дела должна проводиться оценка того, могла ли поставленная работодателем цель быть достигнута с меньшим проникновением в частную жизнь работника;

Последствия контроля для работника, в отношении которого он осуществляется. Следует учитывать, в частности, использование работодателем результатов контроля, и были ли они применены для достижения заявленной цели осуществленной меры;

Были ли работнику обеспечены надлежащие гарантии, особенно если контроль со стороны работодателя был связан с вмешательством в частную жизнь. Данные гарантии могут быть выражены, среди прочего, в форме предоставления затронутым такими мерами работникам или представителям работников информации о введении и степени контроля, подачи заявления о применении такой меры в независимый орган власти либо обеспечения возможности обжалования [ECtHR, *Bărbulescu v. Romania* (61496/08), 2017].

Представленные выше критерии имеют исключительную ценность для России.

В соответствии со ст. 86 ТК РФ, работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни, кроме случаев, непосредственно связанных с трудовыми отношениями, когда работодатель вправе получать и обрабатывать такие данные с письменного согласия работника [Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ, [www](#)], которое согласно ст. 9 Федерального закона от 27.07.2006 «О персональных данных» № 152-ФЗ (далее - Закон о персональных данных) должно быть конкретным, предметным, информированным, сознательным и однозначным [Федеральный закон "О персональных данных" от 27.07.2006 № 152-ФЗ, [www](#)].

При мониторинге правоприменения по проблематике вмешательства работодателя в частную жизнь работника мотивированных судебных решений в пользу первого больше в абсолютном процентном соотношении. Например, судам достаточным считается наличие общего согласия на обработку персональных данных «спрятанного» в правилах внутреннего трудового распорядка организации для признания такого контроля законным, что напрямую противоречит вышеуказанным положениям как статьи 9 Закона о персональных данных, так и статьи 86 ТК РФ. В основном, судьи рассматривают осуществление видеозаписи или иного контроля за работником как право работодателя требовать от работников исполнения ими своих трудовых

обязанностей и соблюдения правил внутреннего трудового распорядка в соответствии со ст. 22 ТК РФ [Решение Привокзального районного суда г. Тулы от 26.06.2017 по делу № 2-502/2017]. Правоприменители встают на сторону работодателя, когда последний утверждает, что объектом видеосъемки является не фиксация обстоятельств их частной жизни, а осуществление контроля за надлежащим выполнением ими своих трудовых обязанностей [Решение Центрального районного суда г. Сочи от 21.02.2013 по делу № 2-780/2013].

Стоит отметить, что единственное найденное судебное решение, где суд признал незаконность видеосъемки, связано с несоответствием использования полученных видеозаписей тем целям, которые были заявлены в подписанном работником соглашении. В целом, стоит отметить преобладание формального подхода к рассмотрению аналогичных дел, выражающихся в игнорировании доводов работников на нарушение работодателем права на личную неприкосновенность частной жизни, предусмотренной ст. 22 Конституции РФ [Конституция РФ, www].

Заключение

В заключение хотелось бы отметить, что мотивировка решений Европейского суда по правам человека о нарушении права работника на тайну частной жизни должна иметь большую ценность не только для исследователей представленной проблематики, но и для правоприменителей. Применение теста «обоснованного ожидания неприкосновенности частной жизни» кажется разумным и справедливым при системном толковании права работника на уважение частной жизни и права работодателя на осуществление контроля за действиями работника в течение рабочего времени.

Вместе с тем, такие акты, как GDPR и особенно AI Act, задают новые стандарты правовой защиты, формируя основу цифровых трудовых прав. Однако существующая фрагментированность правового регулирования и дефицит эффективного надзора в условиях институционального неравенства участников трудовых отношений ограничивают реальную защиту работника. Для обеспечения справедливого и устойчивого баланса необходим значительный сдвиг от процедурных гарантий к содержательным запретам вредоносных практик.

Библиография

1. Ильин, В. Д. Всемирная паутина // Большая российская энциклопедия. – [Электронный ресурс]. – [сайт]. – URL: https://bigenc.ru/technology_and_technique/text/3923747 (дата обращения: 28.04.2025)
2. Налоговый кодекс РФ (часть первая) от 31.07.1998 № 146-ФЗ – [Электронный ресурс]. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 28.04.2025)
3. Трудовое право России в 2 т. Том 1. Общая часть : учебник для вузов / Е. Б. Хохлов [и др.] ; ответственный редактор Е. Б. Хохлов, В. А. Сафонов. — 8-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 231 с.
4. Европейская конвенция о защите прав человека и основных свобод // Council of Europe – [Электронный ресурс]. – [сайт]. – URL: <https://www.coe.int/ru/web/compass/the-european-convention-on-human-rights-and-its-protocols> – (дата обращения: 28.04.2025).
5. Warren S. D., Brandeis L. The Right to Privacy // Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.
6. Public Utilities Commission v. Pollak, 343 U. S. 451 (1952). [Electronic resource]. // Justia – US Supreme Court. – [Site]. URL: <https://supreme.justia.com/cases/federal/us/343/451/> – (accessed: 03.05.2025)
7. Constitution of the United States (1789) [Electronic resource]. // United States Senate. – [Site]. URL: https://www.senate.gov/civics/constitution_item/constitution.htm?utm_content=buffer05951#:~:text=Written%20in%201787%2C%20ratified%20in,exists%20to%20serve%20its%20citizens. (accessed: 28.04.2025)
8. Katz v. United States, 389 U.S. 347 (1967) [Electronic resource]. // Justia – US Supreme Court. – [Site]. URL:

- <https://supreme.justia.com/cases/federal/us/389/347/> – (accessed: 30.04.2025)
9. ECtHR, *Malone v. The United Kingdom* (8691/79) 2.8.1984 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: <http://hudoc.echr.coe.int/rus?i=001-57533> – (accessed: 28.04.2025)
 10. ECtHR, *Halford v. United Kingdom* (20605/92) 25.06.1997 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: <http://hudoc.echr.coe.int/eng?i=002-8996> – (accessed: 28.04.2025)
 11. ECtHR, *Copland v. the United Kingdom* (62617/00) 3.4.2007 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: <http://hudoc.echr.coe.int/rus?i=001-79996> – (accessed: 29.04.2025)
 12. ECtHR, *Peev v. Bulgaria* (64209/01) 26.07.2007 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: <http://hudoc.echr.coe.int/eng?i=001-119832> (accessed: 29.04.2025)
 13. ECtHR, *Köpke v. Germany* (420/07) 5.10.2010 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: <http://hudoc.echr.coe.int/eng?i=001-101536> - (accessed: 29.04.2025)
 14. Сыченко, Е.В. Прослушивание рабочего телефона, обыск служебных помещений и съёмка работника на видео: практика Европейского суда по правам человека // Административное право. 2015. № 1. С. 77-82.
 15. ECtHR, *Libert v. France* (588/13) 22.02.2018 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: <http://hudoc.echr.coe.int/eng?i=002-12007> - (accessed: 30.04.2025)
 16. ECtHR, *Bărbulescu v. Romania* (61496/08) 5.9.2017 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: <http://hudoc.echr.coe.int/eng?i=001-177082> – (accessed: 30.04.2025)
 17. «Трудовой кодекс Российской Федерации» от 30.12.2001 № 197-ФЗ (ред. от 30.04.2021) – [Электронный ресурс]. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.04.2025)
 18. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ – [Электронный ресурс]. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 30.04.2025)
 19. Решение Привокзального районного суда г. Тулы от 26 июня 2017 г. по делу № 2-502/2017 – [Электронный ресурс]. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 1.05.2025)
 20. Решение Ленинского районного суда г. Ярославля по делу № 2-1688/2018 от 27 марта 2019 г. – [Электронный ресурс]. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 01.05.2025)
 21. Апелляционное определение Московского городского суда от 10.09.12 г. по делу № 11-20012 – [Электронный ресурс]. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 01.05.2025)
 22. Решение Центрального районного суда г. Сочи от 21 февраля 2013 г. по делу № 2-780/2013 // сайт Центрального районного суда г. Сочи – [Электронный ресурс]. – [сайт]. – URL: <http://sochi-centralny.krd.sudrf.ru/> (дата обращения: 02.05.2025)
 23. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с поправками) – [Электронный ресурс]. – Доступ из справ.-правовой системы «Консультант Плюс» (дата обращения: 02.05.2025)

Legitimacy of Employee Privacy Interference: The European Union's Approach

Maksim I. Druzhinin

Master of Information Law,
Saint Petersburg State University,
199034, 7/9 Universitetskaya Naberezhnaya, Saint Petersburg, Russian Federation;
e-mail: Druzhinin@mail.ru

Astemir Zh. Pagov

Master of Information Law,
Saint Petersburg State University,
199034, 7/9 Universitetskaya Naberezhnaya, Saint Petersburg, Russian Federation;
e-mail: Druzhinin@mail.ru

Abstract

The article examines the permissibility of employer interference in employee private life through the lens of legal approaches in the European Union jurisdiction. Through analysis of key

Druzhinin M.I., Pagov A.Zh.

ECtHR decisions, it explores the application of privacy rights inviolability criteria and the need to balance employee rights with legitimate employer interests. Special attention is given to the impact of EU regulatory instruments, including the GDPR and AI Act, on workplace digital monitoring and AI utilization. The authors argue that traditional data protection concepts based on integrity and transparency prove insufficient in employment contexts involving modern information technologies, particularly given employees' structural vulnerability in labor relations.

For citation

Druzhinin M.I., Pagov A.Zh. (2025) *Pravomernost' vmeshatel'stva v chastnuyu zhizn' rabotnika: podkhod Evropeyskogo Soyuza* [Legitimacy of Employee Privacy Interference: The European Union's Approach]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 15 (5A), pp. 193-202.

Keywords

Personal data, European Union, Employee rights, Information technologies, ECtHR.

References

1. Ilyin, V. D. The World Wide Web // The Great Russian Encyclopedia. – [Electronic resource]. – [website]. – URL: // https://bigenc.ru/technology_and_technique/text/3923747 (date of request: 04/28/2025)
2. The Tax Code of the Russian Federation (part one) dated 07/31/1998 No. 146-FZ – [Electronic resource]. – Access from the help.-Consultant Plus legal system(date of application: 04/28/2025)
3. Labor law of Russia in 2 volumes. Volume 1. General part : textbook for universities / E. B. Khokhlov [et al.] ; executive editor E. B. Khokhlov, V. A. Safonov. — 8th ed., revised and add. Moscow: Yurait Publishing House, 2020. 231 p.
4. The European Convention for the Protection of Human Rights and Fundamental Freedoms // Council of Europe – [Electronic resource]. – [website]. – URL: // <https://www.coe.int/ru/web/compass/the-european-convention-on-human-rights-and-its-protocols> – (date of access: 04/28/2025).
5. Warren S. D., Brandeis L. The Right to Privacy // Harvard Law Review, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.
6. Public Utilities Commission v. Pollak, 343 U.S. 451 (1952). [Electronic resource]. // Justia – US Supreme Court. – [Site]. URL: <https://supreme.justia.com/cases/federal/us/343/451/> – (accessed: 03.05.2025)
7. Constitution of the United States (1789) [Electronic resource]. // United States Senate. – [Site]. URL: https://www.senate.gov/civics/constitution_item/constitution.htm?utm_content=buffer05951#:~:text=Written%20in%201787%2C%20ratified%20in,exists%20to%20serve%20its%20citizens. (accessed: 28.04.2025)
8. Katz v. United States, 389 U.S. 347 (1967) [Electronic resource]. // Justia – US Supreme Court. – [Site]. URL: <https://supreme.justia.com/cases/federal/us/389/347/> – (accessed: 30.04.2025)
9. ECtHR, Malone v. The United Kingdom (8691/79) 2.8.1984 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: <http://hudoc.echr.coe.int/rus?i=001-57533> – (accessed: 28.04.2025)
10. ECtHR, Halford v. United Kingdom (20605/92) 25.06.1997 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: <http://hudoc.echr.coe.int/eng?i=002-8996> – (accessed: 28.04.2025)
11. ECtHR, Copland v. the United Kingdom (62617/00) 3.4.2007 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: <http://hudoc.echr.coe.int/rus?i=001-79996> – (accessed: 29.04.2025)
12. ECtHR, Peev v. Bulgaria (64209/01) 26.07.2007 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: - <http://hudoc.echr.coe.int/eng?i=001-119832> (accessed: 29.04.2025)
13. ECtHR, Köpke v. Germany (420/07) 5.10.2010 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: <http://hudoc.echr.coe.int/eng?i=001-101536> - (accessed: 04/29/2025)
14. Sychenko, E.V. Tapping a work phone, searching office premises and filming an employee on video: the practice of the European Court of Human Rights // Administrative Law. 2015. No. 1. pp. 77-82.
15. ECtHR, Libert v. France (588/13) 22.02.2018 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: <http://hudoc.echr.coe.int/eng?i=002-12007> - (accessed: 30.04.2025)
16. ECtHR, Bărbulescu v. Romania (61496/08) 5.9.2017 [Electronic resource]. // HUDOC – European Court of Human Rights. – [Site]. URL: <http://hudoc.echr.coe.int/eng?i=001-177082> – (accessed: 30.04.2025)
17. "Labor Code of the Russian Federation" dated 30.12.2001 No. 197-FZ (as amended on 30.04.2021) – [Electronic resource]. – Access from the help.-Consultant Plus legal system(date of application: 30.04.2025)
18. Federal Law "On Personal Data" dated 27.07.2006 No. 152-FZ – [Electronic resource]. – Access from the help.-

Consultant Plus legal system(date of application: 30.04.2025)

19. The decision of the Privokzalny District Court of Tula dated June 26, 2017 in case No. 2-502/2017 – [Electronic resource]. – Access from the help.-Consultant Plus legal system(date of application: 1.05.2025)
20. Decision of the Leninsky District Court of Yaroslavl in case No. 2-1688/2018 dated March 27, 2019 – [Electronic resource]. – Access from the help.-Consultant Plus legal system(date of application: 05/01/2025)
21. The Moscow City Court's Appeal ruling of 09/10/12 in case No. 11-20012 – [Electronic resource]. – Access from the help.-Consultant Plus legal system(date of application: 05/01/2025)
22. The decision of the Central District Court of Sochi dated February 21, 2013 in case no. 2-780/2013 // the website of the Central District Court of Sochi – [Electronic resource]. – [website]. – URL: // <http://sochi-centralny.krd.sudrf.ru/> (date of reference: 05/02/2025)
23. "The Constitution of the Russian Federation" (adopted by popular vote on 12/12/1993 with amendments) – [Electronic resource]. – Access from the help.-Consultant Plus legal system(date of application: 05/02/2025)