Основы и замечания к докладу о влиянии искусственного интеллекта, Интернета вещей и робототехники на безопасность и ответственность Комиссии ЕС перед Европейским парламентом, Советом и Европейским экономическим и социальным комитетом от 19.02.2020

Рейнхольд Бекманн

Аннотация

В статье описывается и анализируется доклад о влиянии искусственного интеллекта, Интернета вещей и робототехники на безопасность и ответственность Комиссии ЕС перед Европейским парламентом, Советом и Европейским экономическим и социальным комитетом 19 февраля 2020 года.

В статье содержится прогноз ожидаемых правовых норм на уровне ЕС на ближайшие несколько лет в области систем искусственного интеллекта (ИИ) и, в частности, в отношении связанных с этим вопросов безопасности и ответственности. В настоящем докладе проводится различие между двумя основными областями регулирования, правилами безопасности продукции и вопросами, касающимися существующих рамок ответственности за цифровые технологии.

Ключевые слова: правила ЕС, интернет вещей; искусственный интеллект, робототехника; правила безопасности продукции, правила ответственности по ИИ-программному обеспечению.

Доклад был опубликован совместно с Белой книгой по искусственному интеллекту – европейской концепцией превосходства и доверия – Комиссией ЕС 19.2.2020.

В настоящем докладе анализируется соответствующая нынешняя правовая база в ЕС. В нем рассматривается вопрос о том, где существуют неопределенности в отношении применения этой правовой базы в связи с конкретными рисками, связанными с системами ИИ и другими технологиями.

В докладе делается вывод о том, что действующее законодательство о безопасности продукции уже поддерживает расширенный подход к защите от всех видов рисков, связанных с продуктом в зависимости от его использования. Однако для обеспечения большей правовой определенности можно было бы включить положения, в которых прямо говорится о новых рисках, связанных с новыми цифровыми технологиями.

Таким образом, можно сказать, что в докладе содержится прогноз ожидаемых правовых норм на уровне ЕС на ближайшие несколько лет в области систем ИИ и, в частности, в отношении связанных с этим вопросов безопасности и ответственности. В настоящем докладе проводится различие между двумя основными областями регулирования, правилами безопасности продукции и вопросами, касающимися существующих рамок ответственности за цифровые технологии.

1. Правила безопасности продукции

Хотя в докладе делается вывод о том, что действующее законодательство о безопасности продукции уже поддерживает расширенную концепцию защиты от всех видов рисков, связанных с продуктом в зависимости от его использования, неясно, каким образом это должно быть достигнуто. Однако для обеспечения большей правовой определенности можно было бы включить положения, в которых прямо касались бы новых рисков, связанных с новыми цифровыми технологиями.

1.1. Автономное поведение некоторых систем ИИ в течение их жизненного цикла может привести к значительным изменениям в продуктах, связанным с безопасностью, которые могут потребовать новой оценки риска. Кроме того, в качестве защитной меры может возникнуть необходимость обеспечить контроль человека на этапе проектирования на протяжении всего жизненного цикла продуктов и систем ИИ.

1.2. Явные обязательства для производителей можно также рассматривать, когда это уместно, в отношении рисков для психической безопасности пользователей (например, при работе с человекоподобными роботами).

1.3. Законодательство ЕС о безопасности продукции может включать как конкретные требования для устранения рисков безопасности, связанных с неверными данными на этапе проектирования, так и механизмы обеспечения хранения качества данных на протяжении всего использования продуктов и систем ИИ.

1.4. Вопрос о непрозрачности систем на основе алгоритмов – возможность самостоятельного обучения и самостоятельного повышения производительности некоторых продуктов ИИ – можно было бы решить путем установления требований к транспарентности.

1.5. В случае самостоятельного программного обеспечения, которое позиционое или загружается в продукт после его разработки, существующие требования, возможно, потребуется адаптировать и уточнить, если программное обеспечение имеет последствия для безопасности.

1.6. С учетом растущей сложности цепочек поставок в новых технологиях положения, в соответствии с которых сотрудничество между экономическими операторами в цепочке поставок и пользователями является обязательным, могут также способствовать правовой определенности.

2. Правила ответственности

Характеристикиновых цифровых технологий, таких как ИИ, могут бросить вызов некоторым аспектам существующих механизмов ответственности и снизить их эффективность. Некоторые из этих особенностей могут затухать отследить ущерб до того или иной лица, что потребуется в соответствии с большинством национальных правил для того, чтобы сделать претензии о вине. Это может значительно увеличить расходы для пострадавшей стороны и затмить и доказать ответственность претензий к субъектам, не производителям.

2.1. Лица, которым, должно быть, был причинен ущерб в результате использования систем ИИ, будут пользоваться такой же защитой, как и лица, пострадавшие от других технологий. В то же время необходимо иметь достаточно возможностей для дальнейшего развития технологических инноваций.

2.2. Следует тщательно рассмотреть все варианты, предусмотренные для достижения этой цели, включая возможную поправку к Директиве об ответственности за продукцию и возможную дальнейшую целевую гармонизацию законов о национальной ответственности. Например, Комиссия предлагает представить замечания по вопросу о том, может ли и в какой степени необходимо смягчить последствия сложности путем изменения правил бремени доказывания ущерба, причиненного функционированием заявок на ИИ, как это предусмотрено национальными правилами поведения.

2.3. В свете вышеуказанных замечаний в отношении рамок ответственности Комиссия приходит к выводу о том, что в дополнение к возможной адаптации этого существующего законодательства может потребоваться новое законодательство, конкретно нацеленное на ИИ, для адаптации правовой базы ЕС к текущим и ожидаемым технологическим и коммерческим изменениям.

В «Белой книге» в качестве возможных дополнительных нормативных пунктов определены следующие области.

- **Чёткое юридическое определение ИИ**

Здесь следует использовать риск-основанный подход, т.е. должны быть приложения для ИИ с высоким или низким риском. В этой связи усилия по регулированию должны быть сосредоточены на тех приложениях с высоким риском, с тем, чтобы не привести к непропорционально высоким издержкам для МСП.

Критериями для класса риска должен быть вопрос о том, используется ли приложение ИИ в секторе, где в связи с характером типичных видов деятельности следует ожидать значительных рисков. Второй критерий заключается в том, используется ли приложение ИИ в секторе, в котором следует ожидать значительных рисков.

- **Ключевые функции**

Требования к приложениям для ИИ высокого риска могут относиться к следующим ключевым особенностям: данные обучения, данные и хранение записей, информация, которая будет представлена, надежность и точность, человеческий надзор,

особые требования к определенным приложениям ИИ, например приложения для удаленной биометрической идентификации.

- **Адресаты**

Многие актеры вовлечены в жизненный цикл системы ИИ. К ним относятся разработчик, оператор и, возможно, другие субъекты, такие как производитель, дилер, импортер, поставщик услуг, профессиональный или частный пользователь. Комиссия считает, что в будущем в правовом поле ответственность за отдельные обязательства должна нести организация, наилучшим образом способная управлять потенциальными рисками. Например, разработчики ИИ могут лучше всего управлять рисками, связанными с этапом разработки, в то время как их способность контролировать риски на этапе эксплуатации может быть более ограниченной.

Комиссия считает необходимым, чтобы требования распространялись на всех соответствующих экономических операторов, предлагающих продукты или услуги на основе ИИ в ЕС, независимо от того, установлены они в ЕС или нет.

- **Соблюдение и обеспечение соблюдения**

Given высокий риск того, что некоторые приложения ИИ представляют в целом, Комиссия считает, на данном этапе, что объективная оценка соответствия ex-ante будет необходима для проверки и обеспечения того, чтобы некоторые из вышеупомянутых обязательных требований для приложений высокого риска были выполнены. Оценка соответствия ex-ante может включать процедуры тестирования, проверки или сертификации. Это может включать обзор алгоритмов и наборов данных, используемых на этапе разработки.

- **Управление**

Европейская структура управления ИИ в форме основы для сотрудничества между компетентными национальными органами необходима для того, чтобы избежать раздробленности обязанностей, укрепить потенциал государств-членов и обеспечить, чтобы Европа постепенно оснащалась потенциалом, необходимым для тестирования и сертификации продуктов и услуг на основе ИИ.

3. Заключение

Несмотря на то что соображения, сделанные Комиссией ЕС в Белой книге и в докладе о влиянии искусственного интеллекта на адаптацию правовых национальных различных нормативных актов, касающихся искусственного интеллекта, все еще находятся на весьма неспецифической стадии и все еще находятся в середине политической дискуссии, можно констатировать следующее.

1) При адаптированном или дополнительном правовом регулировании на уровне ЕС в отношении вопросов безопасности продукции (т.е. требований к доступу на рынки), а также в отношении реорганизации вопросов ответственности в связи с системами ИИ можно с определенной уверенностью предположить, что это произойдет в течение ближайших нескольких лет.

2) Особенно поставщики ИИ должны быть готовы к тому, что алгоритм должен быть прозрачным, проверяемым и, наконец, соответствовать определенным сертификационным требованиям. Кроме того, безусловно, следует ожидать расширенной ответственности и, следовательно, ответственности поставщика ИИ, которая выходит за рамки известных масштабов ответственности за продукцию, например в том, что касается ответственности за цепочки поставок и сложные продукты. В результате это будет связано только с измененными, более транспарентными процессами разработки и расширенной ответственностью, т.е. значительно более высокими расходами на соответствующее страховое покрытие.

Рейнхольд Бекманн является юристом и преподавателем, специализирующимся в области интернет-права и международного ИТ-права. Его внимание сосредоточено на консультировании компаний, например, BASF Digital Farming в Германии, о том, как обеспечить соответствие GDPR. Это также включает в себя международные аспекты защиты данных. Райнхольд Бекманн также является лектором по ИТ-праву и докладчиком на международных конференциях по вопросам GDPR. Например, по приглашению Академии наук в Москве в 2018 г. и в качестве единственного в мире эксперта по правовым вопросам на крупнейшей в мире конференции по искусственному интеллекту ODSC в Бостоне в апреле 2020 г. После изучения права в Мюнстере Рейнхольд Бекманн более 20 лет работал в индустрии корпоративного программного обеспечения, главным образом для североамериканских поставщиков программного обеспечения, чтобы возглавить свои европейские организации.

ESSENTIALS AND REMARKS ON THE REPORT ON THE IMPACT OF ARTIFICIAL INTELLIGENCE, THE INTERNET OF THINGS AND ROBOTICS ON SECURITY AND LIABILITY OF THE EU COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE OF 19.2.2020

Abstract

The article describes and analyses the report on the impact of artificial intelligence, the Internet of Things and robotics on security and liability of the EU Commission to the European Parliament, the Council and the European Economic and Social Committee published of 2/19/2020.

The article provides an outlook on the expected legal regulations at EU level for the next few years in the field of AI systems and there in particular regarding the associated security and liability issues. Here, the report distinguishes between two main areas of regulation, product safety regulations and questions regarding the existing liability frameworks for digital technologies.

Key words: EU-regulations, Internet of Things; AI, Robotic; product safety regulations, liability regulations on AI-software,

Authors Bio:

RA Reinhold Beckmann is a lawyer and lecturer specialized in internet law and international IT law. His focus is on advising companies, e.g. BASF Digital Farming in Germany, on how to ensure GDPR compliance. This also includes international aspects of data protection. Reinhold Beckmann is also a lecturer on IT law and a speaker at international conferences on GDPR issues. E.g. at the invitation of the Academy of Sciences in Moscow in 2018 and as the only legal expert at the world's largest conference on artificial intelligence of the ODSC in Boston April 2020. After studying law in Münster, Reinhold Beckmann worked for more than 20 years in the enterprise software industry, mainly for North American software vendors to lead their European organisations.