DOI: http://dx.doi.org/10.21686/2411-118X-2022-1-7-14

# Особенности развития правового регулирования технологий искусственного интеллекта в Евросоюзе

**Т. Э. Зульфугарзаде**
кандидат юридических наук, доцент, доцент кафедры гражданско-правовых дисциплин РЭУ им. Г. В. Плеханова.
Адрес: ФГБОУ ВО «Российский экономический университет имени Г. В. Плеханова», 117997, Москва, Стремянный пер., д. 36.
E-mail: zulfugarzade.te@rea.ru

# Features of the Development of Legal Regulation of Artificial Intelligence Technologies in the European Union

**T. E. Zulfugarzade**
PhD of Law, Associate Professor, Associate Professor of the Department of Civil Legal Disciplines of the PRUE.
Address: Plekhanov Russian University of Economics, 36 Stremyanny Lane, Moscow, 117997, Russian Federation.
E-mail: zulfugarzade.te@rea.ru

**Аннотация**

В статье приведены основные результаты исследования особенностей развития правового обеспечения технологий искусственного интеллекта (ИИ) в Евросоюзе с учетом морально-этических норм, обязательных для соблюдения в ЕС. Предметом исследования послужили отношения, возникающие между разработчиками, производителями и распространителями технологий ИИ, с одной стороны, и пользователями (физлицами и организациями) указанных технологий – с другой. В качестве основных методов познания при проведении исследования были использованы логический, сравнительный, эмпирический, аналитический, историко-правовой, описательный и др. Научную новизну исследования составили выводы, в соответствии с которыми, предложенный Еврокомиссией регламент по регулированию ИИ представляет собой пока только дополнение к многоцелевой программе цифрового законодательства, которую Евросоюз анонсировал пошагово, начиная с 2019 г. Комиссией осознанно позиционируется это регулирование ИИ как мера защиты европейских ценностей от менее скрупулезных разработчиков ИИ в КНР. Несмотря на ряд вышеперечисленных недостатков, проанализированный Проект Регламента является всеобъемлющим, продуманным началом правотворческого и законодательного процесса в Европе и может стать основой для глобального сотрудничества в покрытии общей нормативно-правовой сетью важных новых и инновационных технологий. При этом постепенное сближение европейского и американского подходов к регулированию ИИ в ближайшие годы может привести к созданию ЕС и США Совета по торговле и технологиям, а также выработке совместного соглашения о регулировании ИИ. Тем не менее США пока не выразили свою готовность признать сформулированное Евросоюзом определение ИИ системой высокого уровня рисков, а также разработанные в ЕС детализированную систему оценки соответствия и подход к всеобъемлющему регулированию ИИ. В связи с этим представляется целесообразным перенести вышеозначенные подходы, выработанные в ЕС, на государства – члены ЕАЭС с последующей их консолидацией с правилами Евросоюза, что позволит создать евразийскую систему безопасности ИИ, которая впоследствии может перерасти в универсальную систему, например, под эгидой ООН.

**Ключевые слова:** гражданское право, акт, закон, регламент, этика, мораль, дипфейк, зловредность, инновационный, технологии, собственность, продукция, воздействие, осторожность, безопасность, ответственность, программа.

**Abstract**

The article presents the main results of the study of the peculiarities of the development of legal support for artificial intelligence (AI) technologies in the European Union, taking into account the moral and ethical standards required to be observed in the EU. The subject of the study was the relations arising between developers, manufac-

turers and distributors of AI technologies, on the one hand, and users (individuals and organizations) in the field of using these technologies, on the other. Logical, comparative, empirical, analytical, historical-legal, descriptive, etc. were used as the main methods of cognition during the research. The scientific novelty of the study was the conclusions, according to which, the regulation on AI regulation proposed by the European Commission is so far only an addition to the multi-purpose program of digital legislation, which the European Union announced step by step, starting in 2019. The Commission consciously positions this AI regulation as a measure to protect European values from less scrupulous AI developers in China. Despite a number of the above shortcomings, the analyzed draft regulation is a comprehensive, thoughtful beginning of the law-making and legislative process in Europe and can become the basis for global cooperation in covering a common regulatory network of important new and innovative technologies. At the same time, the gradual convergence of European and American approaches to AI regulation in the coming years may lead to the creation of the EU and the US Council on Trade and Technology, as well as the development of a joint agreement on AI regulation. Nevertheless, the US has not yet expressed its readiness to recognize the definition of AI formulated by the European Union as a high-risk system, as well as the detailed conformity assessment system developed in the EU and the approach to comprehensive regulation of AI. In this regard, it seems appropriate to transfer the above-mentioned approaches developed in the EU to the EAEU member states with their subsequent consolidation with the rules of the Euro-Union, which will allow creating a Eurasian AI security system, which can later grow into a universal system, for example, under the auspices of the UN.

**Keywords***:* civil law, act, law, regulation, ethics, morality, deepfake, malignity, innovative, technology, property, products, impact, caution, safety, responsibility, program.

Не только позитивные, но и нередко негативные последствия широкого внедрения инновационных технологий искусственного интеллекта (ИИ) [3. – С. 224] в различные сферы социально-экономической деятельности объективно предопределяют необходимость совершенствования правового регулирования, направленного прежде всего на гармонизацию правовых норм в сфере ИИ с морально-этическими подходами [1. – С. 85], обеспечивающими надлежащий контроль за ними [2. – С. 39], а также качественное и безопасное
[6. – С. 24] использование таких технологий в профессиональной деятельности и в повседневной жизни. В этой связи полагаем необходимым обратиться к рассмотрению Проекта нового Евррегламента в области ИИ, предложенного и опубликованного 21 апреля 2021 г.

В процессе проведения настоящего исследования были сделаны основные выводы по содержательной части Проекта Регламента ЕС по регулированию искусственного интеллекта (ИИ)[1], который стал прямым вызовом распространенному в Кремниевой долине (США) мнению, что законодателям следовало бы оставить в покое новые, особенно инновационные технологии [8].

В исследуемом Проекте Регламента изложена детализированная регуляторная структура, в которой запрещаются некоторые сферы применения ИИ такие как, в частности, регулирование систем ИИ с высокими уровнями рисков и поверхностным регулированием с меньшими уровнями. Принятие этого Регламента, по нашему мнению, потребует от поставщиков и пользователей систем ИИ с высокими уровнями рисков соблюдения правил применения и управления «данными документации (документационному обеспечению) и делопроизводства, прозрачности и предоставления информации пользователям, человеческого надзора, высокого качества, надежности, точности и безопасности»[2]. Его главным новшеством, изложенным в Белой книге по ИИ[3], является требование провести

[1] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. COM/2021/206 Final. 21.04.2021. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206/ (дата обращения: 31.01.2022).

[2] Новый регламент ЕС в области искусственного интеллекта (ИИ). – URL: https://uisgda.com/ru/novyj-reglament-es-v-oblasti -iskusstvennogo-intellekta-ii.html/ (дата обращения: 31.01.2022).

[3] European Commission (2020d). White Paper on Artificial Intelligence - a European Approach, Consultation. – URL: https://ec.europa.eu/info/law/better-regulation/have-your-say/

предварительную оценку системы искусственного интеллекта с высокими уровнями рисков прежде, чем они могут быть предложены на рынке или введены в эксплуатацию. Дополнительное важное нововведение – обеспечить постмаркетинговый мониторинг системы, для того чтобы обнаружить проблемы при использовании и устранить таковые [7].

Предмет регулирования исследуемого документа предопределяет, что расширенное определение ИИ в этом нормативном правовом акте будет охватывать программное обеспечение, включающее машинное обучение, и ранее введенное определение понятия (дефиницию) ИИ, а также традиционные статистические методы, которые длительное время использовались для создания моделей кредитного рейтинга или повторяющихся событий и явлений (рецидивизма). Несмотря на то что документ покрывает пользователей систем ИИ, он в основном ориентирован на поставщиков, т. е. на организации, которые их разрабатывают, размещают на рынке либо вводят в эксплуатацию для собственного использования. Юрисдикция этого Регламента распространяется на поставщиков систем ИИ в ЕС независимо от их местонахождения, на пользователей таких систем, расположенных в ЕС, а также на поставщиков и пользователей, находящихся за пределами ЕС в тех случаях, когда производимая этой системой продукция используется в ЕС. В результате эффективность таких тестов потенциально расширит сферу действия этого нормативного правового акта на организации, которые используют системы ИИ для обработки данных о гражданах Евросоюза, но не представлены на рынке в ЕС.

Рассматриваемый Проект Регламента предусматривает целый ряд запретов. Так, в частности, запрещается применение систем ИИ, причиняющих или способных (могущих) «причинить физический или психологический вред посредством использования подсознательных методов или эксплуатации уязвимостей определенной группы лиц из-за их возрастных, физических или умственных недостатков»[1]. Также системам ИИ запрещается выдавать рейтинги социального доверия для их использования госорганами в общих целях. Регламент предусматривает «исключение использования систем удаленной биометрической идентификации в реальном времени, таких как распознавание лиц в общедоступных местах для достижения правоохранительных целей»[2], так как это неблагоприятным образом может сказаться на системе предупреждения и профилактики правонарушений и преступлений в целом.

Перечисленные запреты, возможно, будут императивными предписаниями и потому, по нашему мнению, к моменту принятия этого документа большая часть таковых запретов будет либо полностью устранена, либо таковые запреты будут смягчены целым рядом оговорок. При этом немаловажно отметить, что перечисленные запреты сфокусированы на манипулятивных или своекорыстных системах ИИ с целью устранения из них так называемых темных паттернов (манипулятивных технологий, подталкивающих пользователей приобретать, например, товары по завышенным ценам), которые в том числе могут быть направлены на то, чтобы обманом сподвигнуть (подтолкнуть) или даже заставить пользователей принимать противоречащие их собственным интересам решения, например, разглашать больше личных данных, чем это необходимо для получения доступа к тому или иному онлайн-сервису или сетевой информации.

По замыслу правотворцев к обязанностям правоохранительных органов должно быть отнесено определение и выявление фактов того, является ли система ИИ эксплуатирующей или манипулятивной, поэтому эффект от этого запрета будет зависеть от последующих его регулирующих действий. Запрет на выдачу социальных рейтингов (рейтингов социального доверия) предположительно станет предупреждением о том, что традиционные европейские ценности не приемлют и даже отвергают системы, подобные разрабатываемым и реализуемым в КНР.

initiatives/12270-White-Paper-on-ArtificialIntelligence-a-European-Approach/public-consultation/ (дата обращения: 31.01.2022).

[1] Новый регламент ЕС в области искусственного интеллекта (ИИ). – URL: https://uisgda.com/ru/novyj-reglament-es-v-oblasti -iskusstvennogo-intellekta-ii.html/ (дата обращения: 31.01.2022).

[2] Там же.

Кроме того, предлагаемые правила позволили бы пользоваться системами удаленной биометрической идентификации для поиска таких жертв преступлений, как, например, пропавшие дети, а также предотвращения угроз террористических актов, криминальных нападений, выявления или преследования за серьезные правонарушения и преступления, обеспечения надлежащих средств защиты, включая предварительное судебное или административное разрешение возникающих споров и конфликтов. Предполагаемые запреты, как отчасти указано выше, не распространяются на использование правоохранительными органами систем распознавания лиц в базах данных, собранных ранее изображений или видеозаписей, что является препятствием для обеспечения бе-зопасности, прежде всего личности, а также общества и государства в целом.

Такого рода компромиссы, предусмотренные в Проекте Регламента, с одной стороны, вызовут недовольство ряда сторонников защиты гражданских прав и свобод, а с другой – будут способствовать обеспечению безопасности государств – членов ЕС, прежде всего в сфере предупреждения террористических угроз и иных тяжких и особо тяжких преступлений. Например, французские власти могли бы использовать технологию распознавания лиц для поиска на железнодорожных вокзалах и в аэропортах подозреваемых исламских радикалов из Северной Африки, грозящих привести в действие взрывное устройство. Кроме того, исследуемый Проект Регламента может в последующем позволить полиции государств – членов ЕЭС использовать «системы распознавания лиц для постфактумной идентификации подозреваемых, как это сделало ФБР после беспорядка в Капитолии»[1] и на постоянной основе реализуют сотрудники правоохранительных органов Российской Федерации в московском метрополитене и на других крупных транспортных узлах по всей стране.

Так, изучение правил для систем ИИ с высокими уровнями рисков позволило выявить, что к системам ИИ высокого риска относятся объекты, предназначенные для использования в качестве компонентов для обеспечения безопасности продукции, которая уже регулируется действующим законодательством ЕС, включая машинное оборудование, игрушки и медицинские устройства. Кроме того, в Регламенте прямо определены отдельные системы ИИ как высокорисковые. В список высокого риска входят системы ИИ, используемые при удаленной биометрической идентификации в обеспечение безопасности критически важных (в том числе, информационных) инфраструктур, т. е. объектов критической информационной инфраструктуры (КИИ), в воспитательных и образовательных целях, в целях трудоустройства (обеспечения занятости населения), права на получение социальных (общественных) льгот, кредитной истории (кредитного рейтинга) и диспетчеризации экстренных (оперативных) служб. Высокорисковыми считаются также некоторые системы ИИ, используемые в правоохранительных органах при иммиграционном контроле и отправлении правосудия.

Рассматриваемый Проект Регламента в общих чертах предписывает применение такого вида программы управления, которую финансовые регуляторы в США определили для моделей финансового анализа деятельности компаний. В этом документе должным образом отмечается, что приведенные правила являются современными для многих добросовестных операторов и основаны на Принципах этики группы экспертов Еврокомиссии[2].

Поставщики систем ИИ обязаны устанавливать в них надлежащие средства управления данными, а практики – использовать актуальные, репрезентативные, свободные от ошибок и полные базы данных. Они должны предоставить техническую документацию для того, чтобы продемонстрировать, что их система ИИ соответствует установленным правилам. Документация должна содержать в себе общее описание системы ИИ, ее базовые (основные) элементы, в которые в обязательном порядке

[1] Новый регламент ЕС в области искусственного интеллекта (ИИ). – URL: https://uisgda.com/ru/novyj-reglament-es-v-oblasti -iskusstvennogo-intellekta-ii.html/ (дата обращения: 31.01.2022).

[2] Ethics Guidelines for Trustworthy AI. European Commission. 8 March 2021. – URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai/ (дата обращения: 31.01.2022).

включены данные о валидации (корректности) и тестировании, информация о работе такой системы (показатели о ее точности).

При этом системы ИИ высокого риска должны быть в достаточной степени прозрачными. Это требуется для того, чтобы пользователи могли понимать и контролировать, как работает такая система. Представленная информации должна включать в себя показатели уровня точности, надежности, общую логику и выбор ее конструкции, при каких обстоятельствах ее можно использовать без риска для безопасности ее эксплуатацию, а также описание данных, необходимых для обучения применения системы ИИ.

Дополнительно определено, что разработка системы ИИ с высоким уровнем рисков должна осуществляться в соответствии с требованием, согласно которому пользователи получают возможность надлежащим образом контролировать их, а также предотвращать либо минимизировать потенциальные риски. Конструктивные особенности таких систем ИИ должны позволять (не препятствовать) пользователям-физлицам избегать чрезмерной зависимости от выходных данных, присущих системе ИИ, называемой предвзятостью автоматизации, которая может быть вызвана личными предпочтениями и игнорированием человеком-пользователем даже верной информации, и разрешать назначенному контролеру-физлицу блокировать их с помощью кнопки «стоп».

После введения в действие рассматриваемый Регламент потребует от систем ИИ с высокими рисками соблюдения заданного им уровня точности, соответствующего их прямому назначению, и непрерывной работы при их применении. Это потребует от них устойчивости к ошибкам, сбоям или неувязкам, а также к попыткам изменения алгоритмов их применения или производительности третьими сторонами, намеревающимися воспользоваться уязвимостью этой системы.

Ключевым обязательством для поставщиков является «проведение ими оценок соответствия, демонстрирующих, что ИИ-система высокого риска соответствует этим правилам»[1]. Также поставщики систем ИИ, используемых в качестве составных частей (компонентов) в системах обеспечения безопасности потребительских товаров (продукции), подлежащие предварительной оценке соответствия третьей стороной, что определено действующим законодательством ЕС о безопасности продукции, будут обязаны также продемонстрировать соблюдение ими правил, предъявляемых к ИИ рассматриваемым Регламентом. Поставщики автономных систем ИИ с высоким уровнем рисков будут обязаны сами проводить их внутренние испытания (за исключением тех систем ИИ, оценку которых должны проводить независимые третьи стороны), а также должны проводить оценку систем ИИ, используемых для идентификации лиц.

После продажи или введения в эксплуатацию системы ИИ с высоким уровнем рисков, поставщики должны создать систему постмаркетингового мониторинга данных о ее работе, чтобы обеспечить ее постоянное соответствие требованиям рассматриваемого Регламента и при необходимости предпринимать корректирующие воздействия. Системы ИИ, которые продолжают обучаться после их ввода в эксплуатацию, потребуют переоценки их соответствия, если изменения в результате их обучения будут существенными. При этом понятие существенности в рассматриваемом Проекте Регламента не определено. В Проекте Регламента указано: если пользователь такой системы ИИ существенно ее перемодифицирует, тогда уже пользователь, а не поставщик, будет нести ответственность за проведение новой оценки соответствия.

Рассматриваемый Регламент в последующем должен соответствовать представлениям Еврокомиссии в части делегированных ей полномочий по обновлению определения ИИ с учетом развивающихся технологий и представить списки систем ИИ с высоким уровнем риска, в которые должны быть внесены поправки в требования к технической документации. Делегированные действия представляют собой вид административных воздействий,

[1] Новый регламент ЕС в области искусственного интеллекта (ИИ). – URL: https://uisgda.com/ru/novyj-reglament-es-v-oblasti -iskusstvennogo-intellekta-ii.html/ (дата обращения: 31.01.2022).

инициированных и контролируемых Еврокомиссией; они менее обременительны с процедурной точки зрения, чем внесение изменений в законодательство.

При этом регулирование вопросов управления и правоприменения позволило определить, что надзор за соблюдением и исполнением законодательства Евросоюза всегда затруднен из-за присущего ЕС порядка разделения ответственности (главные регулирующие органы ЕС расположены в Брюсселе, национальные – непосредственно в государствах – членах ЕС). Тем не менее схема этого объединения государств, разработанная для ИИ, – нетривиальна. Национальные надзорные органы должны будут взять на себя ведущую роль в осуществлении надзора за рынком продукции систем ИИ, следуя обычной практике ЕС, которая полагается на экспертов, находящихся в столицах каждого из государств-членов.

В свою очередь для государств – членов ЕС не возникает необходимости создания новых специализированных регулирующих органов в области ИИ, так как уже существующие в них госорганы, на которые уже ранее были возложены соответствующие регулирующие (регулятивные) обязанности исходя из других (иных) нормативных правовых актов ЕС, смогут взять на себя задачи по регулированию ИИ. Полномочия этих органов в области ИИ включают в себя расследование рисков здоровью и безопасности или фундаментальных прав, а также приказы компаниям предпринимать корректирующие воздействия, например, удаление с рынка вредоносных систем ИИ. Государство –член ЕС, или Еврокомиссия в целом, может не согласиться с решением, принятым другим государством-членом, автоматически инициировав тем самым процесс консультаций, проводимых в масштабах ЕС, которые могут привести к его отмене.

Национальные надзорные органы обладают доступом ко всей информации, включая документацию и данные, необходимые для обеспечения соблюдения этого законодательства, а также доступ к исходному коду. При необходимости они должны «защищать права интеллектуальной собственности, а также конфиденциальность коммерческой информации или коммерческой тайны, включая исходные коды»[1].

Воссозданный недавно Европейский совет по ИИ[2], скорее всего, в ближайшее время возглавит Еврокомиссия, в составе которой будет не менее чем по одному представителю (с правом голоса) от каждого надзорного органа и Евросовета по защите данных (EDPB). Возможно, со временем EDPB будет наделен правом издавать (выдавать) заключения и детальные указания относительно применения законодательства, касающегося ИИ, осуществлять обмен передовым опытом с заинтересованными, прежде всего профильными организациями, и разрабатывать гармонизированные технические регламенты и стандарты. Тем самым эта комиссия возможно будет играть ведущую роль в управлении системами ИИ на уровне ЕС, в отличие от возглавляемого государствами – членами EDPB. Вместе с тем Еврокомиссия объявила о потенциальных весьма существенных штрафах, выходящих даже за рамки такого важного документа, которым является «Общий Регламент по защите данных» (GDPR)[3]. Государства – члены ЕС могут налагать административные штрафы «в размере до 30 млн евро или 6% от глобального годового корпоративного оборота в зависимости от того, что из них больше, а именно на продающие в запрещенных целях ИИ-системы компании»[4] (например, для определения показателей социального доверия) или которые не отвечают требованиям, предъявляемым к проведению подготовки к их применению. Нарушение других требований повлечет за собой меньшие штрафы, по градуированной шкале. Несмотря на

[1] Новый регламент ЕС в области искусственного интеллекта (ИИ). – URL: https://uisgda.com/ru/novyj-reglament-es-v-oblasti -iskusstvennogo-intellekta-ii.html/ (дата обращения: 31.01.2022).

[2] European Artificial Intelligence Board / Article 56 – Establishment of the European Artificial Intelligence Board. 2022. – URL: https://lexparency.org/eu/52021PC0206/ART_56/ (дата обращения: 31.01.2022).

[3] Регламент ЕС 2016/679 от 27 апреля 2016 г. (General Data Protection Regulation – GDPR) [Электронный ресурс]. 4 June 2021. – URL: https://ec.europa.eu/info/law/law-topic/data-protection_en/ (дата обращения: 31.01.2022).

[4] Новый регламент ЕС в области искусственного интеллекта (ИИ). – URL: https://uisgda.com/ru/novyj-reglament-es-v-oblasti -iskusstvennogo-intellekta-ii.html/ (дата обращения: 31.01.2022).

вышеперечисленные новации правового обеспечения систем ИИ и надежность структуры системы оценки рисков, в рассматриваемом Регламенте содержатся отдельные недостатки. Так, в частности, детальные описания в тексте этого документа изобилуют ссылками на хорошо задокументированные опасения по поводу рисков алгоритмической предвзятости. Тем не менее в тексте Проекта Регламента мало внимания уделено необходимости проведения оценок возможных последствий неправильного использования технологий ИИ.

В Проекте Регламента практически не уделено внимания именно тем субъектам оценок ИИ, которых непосредственно затрагивают системы ИИ. При этом в Регламенте отсутствуют какие-либо общие требования к информированию людей, ставших не по собственной воле объектами алгоритмических оценок и принятия киберрешений. В тексте Проекта Регламента уделено недостаточно внимания так называемой алгоритмической предвзятости (повторяющиеся системные ошибки), что может привести в свою очередь к нарушению прав и охраняемых законом интересов граждан (физлиц) и организаций (юрлиц). При этом предусмотренные Проектом Регламента новые требования, предъявляемые к оценкам соответствия систем ИИ, оказываются попросту встроенными процессами, но не документами, которые могут контролироваться государственными и общественными органами и организациями. При этом в тексте документа неоднократно упоминалась возможность несопоставимости оценок вышеозначенных последствий. Правило управления данными позволяет поставщикам систем ИИ использовать информацию, касающуюся конфиденциальных данных о расовой, половой и этнической принадлежности, для обеспечения мониторинга обнаружения и корректировки алгоритмической предвзятости. Правило устойчивости требует, чтобы некоторые системы ИИ были защищены от возможно предвзятых результатов.
В свою очередь техдокументация системы ИИ должна содержать такие показатели, которые возможно использовать для проведения измерений различного рода потенциально дискриминирующих последствий, а также информацию об ожидаемых (возможных) непредвиденных результатах и источниках возникновения рисков, представляющих реальную угрозу для фундаментальных прав человека и его дискриминации.

Вышеперечисленные несколько абстрактные отсылки в свою очередь не требуют конкретной оценки воздействий на подлежащие защите интересы граждан и организаций. Более того, любые документы, содержащие предвзятую оценку, не должны предоставляться пользователям (физлицам и организациям), представителям общественного контроля или тем, кто потенциально мог бы пострадать от дискриминационных алгоритмов. Она доступна только регулирующим органам по запросу. Напротив, действующее законодательство ЕС четко требует проведения оценок и раскрытия таких систем.

В целом Проект Регламента составляют компании Big Tech (доминирующие в киберпространстве начиная с 2010-х гг. Google, Amazon, Facebook, Apple, а также Microsoft практически неохвачены, несмотря на то, что неоднократно проверялись на предмет неправомерного или чрезмерного использования алгоритмов, управляющих системами ИИ, и являются объектом большинства передовых прикладных исследований в сфере технологий ИИ).
В Проекте Регламента не рассматриваются как высокорисковые алгоритмы, используемые в соцсетях, розничной онлайн-торговле, интернет-магазинах (магазинах приложений), мобильных приложениях (операционных системах). Возможно, что отдельные, используемые в системах отслеживания контекстной рекламы или рекламных рекомендаций алгоритмы, содержащиеся в Этических принципах для ИИ[1], могут быть запрещены в ЕС как манипулятивные (эксплуататорские) практики, методы и методики, для чего, как отмечено ранее, в обязательном порядке потребуется оценка, проводимая регулирующим органом.

Таким образом, в исследуемом документе довольно мало говорится об информации, которая должна быть раскрыта людям, подверженным воздействию систем ИИ. Регламент требует, чтобы люди были

[1] Ethics guidelines for trustworthy AI. 8 April 2019. – URL: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai/. Дата обращения: 31.01.2022 г.

проинформированы о взаимодействии с системой ИИ или когда их эмоции, половая, расовая, этническая принадлежность или сексуальная ориентация распознается этой системой ИИ. Им необходимо сообщать, когда системы так называемого дипфейка (deepfake – склеивание объектов линейной структуры) [4. – С. 19] искусственно создают данные и манипулируют ими, но не в других случаях. Например, людей не следует информировать, о том, что они отсортировываются алгоритмически при определении их права на получение государственных пособий, кредитов, образования или трудоустройства.

В свою очередь наличие в документе требования оценки соответствия, по нашему мнению, недостаточно защищает права пользователей-физлиц, так как оценка соответствия представляет собой процедуру, а не документ. Другими словами, она представляет собой самостоятельную проверку для большинства поставщиков систем ИИ высокого уровня рисков, поэтому в ней отсутствует необходимость предоставления аудиторского отчета для организаций общественного контроля или регулирующего органа государства. Вместо аудиторского отчета система ИИ получает маркировку, указывающую на ее соответствие правилам ЕС. Поставщики систем ИИ обязаны предоставить декларацию соответствия в распоряжение регулирующих органов, но даже это признание о соответствии правилам Евросоюза может быть скрыто от широкой общественности.

Так, в ЕС регулирование ИИ отличается системным подходом, что является более прагматичным. Например, в США такого рода подход к регулированию в сфере ИИ является фрагментарным: ответственность за ИИ делегирована конкретным регулирующим госорганам с общими инструкциями, не допускающими перерегулирования.

Аналогичный подход пока наблюдается и в Российской Федерации. В дальнейшем, возможно, сложившийся в США децентрализованный подход будет несколько усилен и акцентирован на обязательности регулирования ИИ для того, чтобы избежать потенциальных рисков, связанных с повсеместным внедрением технологий ИИ (вероятно, аналогичные изменения будут происходить и в России). При этом немаловажно отметить, что исчерпывающая структура регулирования ИИ в ЕС, включающая в себя горизонтальные, основанные на рисках правила, предварительную оценку соответствия и обязанности по постмаркетинговому мониторингу, в США не будет скопирована, несмотря на то, что в них некоторые города и штаты приняли меры в отношении определенных видов использования ИИ, запретив или строго регулируя системы распознавания лиц.

Завершая исследование отметим, что предложенный Еврокомиссией Регламент по регулированию ИИ представляет собой пока только дополнение к многоцелевой программе цифрового законодательства, которую Евросоюз анонсировал пошагово, начиная с 2019 г. Проекты законодательных актов ЕС о цифровых услугах (DSA)[1], а также о цифровых рынках (DMA)[2] сфокусированы на поведении цифровых платформенных гигантов США, что объясняет, почему это законодательное предложение по регулированию ИИ нацелено на все остальное. Комиссией также осознанно позиционируется это регулирование ИИ как мера защиты европейских ценностей от менее скрупулезных разработчиков ИИ в КНР.

Несмотря на ряд вышеперечисленных недостатков проанализированный Проект Регламента является всеобъемлющим, продуманным началом правотворческого и законодательного процесса в Европе и может стать основой для глобального сотрудничества в покрытии общей нормативно-правовой сетью важных новых и инновационных технологий.

Постепенное сближение европейского и американского подходов к регулированию ИИ в ближайшие годы может привести к созданию ЕС и США Совета по торговле и технологиям, а также выработке совместного соглашения о регулировании ИИ. Тем не менее США пока не выразили готовности признать

[1] The Digital Services Act: ensuring a safe and accountable online environment. 2019. – URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en/ (дата обращения: 31.01.2022).

[2] The Digital Markets Act: Ensuring Fair and Open Digital Markets. 2019. – URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en/ (дата обращения: 31.01.2022).

сформулированное Евросоюзом определение ИИ высокого уровня рисков, а также выработанные в ЕС детализированную систему оценки соответствия и соответствующий подход к всеобъемлющему регулированию ИИ. В этой связи представляется целесообразным перенести вышеозначенные подходы, выработанные в ЕС, на государства – члены ЕАЭС с последующей их консолидацией с правилами Евросоюза, что позволит создать евразийскую систему безопасности использования ИИ, которая впоследствии может перерасти в универсальную систему, например, под эгидой ООН.

**Список литературы**

1. *Ибрагимов Р.С., Сурагина Е. Д., Чурилова Д. Ю.* Этика и регулирование искусственного интеллекта // Закон. – 2021. – № 8. – С. 85–95.

2. *Кирина А.* Искусственный интеллект, контроль и судебные споры // Административное право. – 2021. – № 4. – С. 39–42.

3. *Метелев С. Е.* Оценка инновационного потенциала субъектов рыночной экономики // Опыт, достижения, перспективы торговли и экономики : материалы Международной научно-практической конференции ученых, практиков, аспирантов, магистрантов, студентов. – Омск, 2016. – С. 224–229.

4. *Левушкин А. Н., Тюлин А. В.* Deepfake и системы искусственного интеллекта в парадигме развития цифрового права // Юрист. – 2021. – № 11. – С. 19–24.

5. *Чеховская С. А.* Использование систем искусственного интеллекта для принятия решений: построение системы принципов регулирования // Предпринимательское право. – 2021. – № 1. – С. 24–35.

6. *Madiega T.* Artificial Intelligence Act, 2021. – November 18. – URL: https://epthinktank.eu/2021/11/18/artificial-intelligence-act-eu-legislation-in-progress/ (дата обращения: 31.01.2022).

7. *MacCarthy M., Propp K.* Machines Learn that Brussels Writes the Rules: the EU's New Ai Regulation The Lawfare Institute. 2021. – April 28. – URL: https://www.lawfareblog.com/machines-learn-brussels-writes-rules-eus-new-ai-regulation/ (дата обращения: 31.01.2022).