Правовые подходы к определению понятия «машинное обучение»

Фокина Софья Антоновна
аспирант кафедры информационного права и цифровых технологий МГЮА О.Е. Кутафина, sofia.fokina@icloud.com

В статье рассматриваются проблемы правового понимания и регулирования машинного обучения (МО) как ключевой технологии современного этапа цифровизации и искусственного интеллекта (ИИ). Отмечается переход от создания цифровой инфраструктуры к её интеллектуализации и автономной работе, что порождает новые риски и вызовы для права. Анализируются научные подходы к определению МО, включая позиции В. Б. Наумова, Д. Фагелла, Е. В. Кондратенок и С. Н. Макареня, и делается вывод об отсутствии единой дефиниции. Исследуется российское законодательство: Национальная стратегия развития ИИ до 2030 года, Федеральный закон «Об информации, информационных технологиях и о защите информации», ГОСТ Р 71476–2024. Рассматривается зарубежный опыт: Закон об ИИ в ЕС, подходы Франции, США, Японии и КНР. Обосновывается необходимость нормативной детализации понятия МО, закрепления специального правового режима обучающих данных, требований к их происхождению и качеству, а также обеспечения баланса интересов. Указывается и альтернативная позиция о регулировании ИИ в целом без излишней фрагментации.
Ключевые слова: машинное обучение, искусственный интеллект, правовое регулирование, цифровизация, обучающие данные, правовая определённость, нормативная дефиниция, сравнительное правоведение, AI Act, риски, информационное право.

Современный этап технологического развития характеризуется переходом от точечной цифровизации к глубокой интеграции технологий во все сферы жизни. Если ранее речь шла о создании цифровой инфраструктуры, то сегодня фокус сместился на ее интеллектуализацию и способность к автономной работе. Ключевую роль в этом новом качестве цифровой среды играет искусственный интеллект (далее – ИИ), который трансформирует не только бизнес-процессы, но и сами принципы общественного взаимодействия.

Технологии ИИ, став ключевым элементом современной цифровизации, проникли практически во все сферы жизни общества и государства. Фундаментом большинства этих технологий является машинное обучение (далее – МО). Однако стремительное и повсеместное внедрение МО порождает новые риски и вызовы, требующие немедленного правового реагирования. Основная проблема заключается в том, что динамичное развитие и внутренняя сложность технологий на основе МО затрудняют фиксацию их сущности и границ в правовом поле. В связи с этим возникает насущная необходимость в комплексном анализе подходов к пониманию и регулированию МО как в российской, так и в зарубежной правовой практике.

В научной среде отсутствует единый подход к определению понятия «МО», на наш взгляд, это обуславливается отсутствием четко очерченной нормативно-правовой регламентации такого понятия. Например, по мнению В. Б. Наумова, МО представляется в виде одной из ключевых технологий будущего, которая повсеместно внедряется во все сферы жизнедеятельности общества [9, с. 219-231]. При этом сам автор не интерпретирует техническую составляющую такого понятия, а соглашается с тем определением, которое было разработано американским разработчиком программного обеспечения SAS: «МО – метод анализа данных, в основу которого заложена идея о возможности обучения алгоритмов, путем анализа данных, выводя из них определенные закономерности, и принятие решений на основе сделанных выводов с минимальным вовлечением человека» [10]. При этом, автор выделяет конкретные способы реализации МО: контролируемое – основанное на подражании существующим явлениям и процессам; обучение с подкреплением – оптимизация имеющихся данных; неконтролируемое обучение – самостоятельное использование алгоритмов системой последовательно. Д. Фагелл определяет МО как науку, в основе которой заложено обучение компьютеров действиям и обучению как человек, с постепенным самосовершенствованием и автономией, в конечном результате получая наблюдения и взаимодействие в реальном мире [11]. Е.В Кондратенок и С.Н. Макареня в свих исследованиях определяют, что МО является подразделом ИИ, который имеет междисциплинарный характер, и может обучаться самостоятельно за счет накопленного опыта [8]. Исходя из представленных определений мы можем сделать вывод о том, что в научной среде рассматриваемое понятие интерпретируется различным образом, единого подхода на сегодняшний день не выработано, и такой подход в унифицированном виде может быть сформулирован только на законодательном уровне, для возможности одинакового применения на практике.

Необходимость в правовом определении понятия и сущности МО, продиктована необходимостью обезопасить общество и государство от неправомерного использования и осуществления МО, в том числе в преступных целях. В Российской Федерации до 2019 года понятие МО не было четко сформулировано на законодательном уровне, государство предприняло такую попытку в Национальной стратегии развития ИИ на период до 2030 года [6], однако, прямо такое понятие все еще не очерчено, но некоторые его границы устанавливаются. Так, например, в п. 6 Указа сформулировано, что посредством МО информационные системы самостоятельно формируют правила и находят решение на основе анализа зависимостей, используя исходные наборы данных (без предварительного составления человеком перечня возможных решений), что позволяет говорить о появлении ИИ. В п. 8 закреплены характерные особенности МО, в частности, законодатель относит к ним необходимость введения релевантного, корректного и репрезентативного набора данных, также результаты МО могут быть подвергнуты человеком сомнению и отменены. На наш взгляд, данная характеристика имеет принципиальное значение, поскольку включение в соответствующий массив несоответствующих сведений способно повлечь нарушение кон-

ституционных прав и свобод человека, содержать признаки дезинформации или недостоверности, а также включать незаконные данные, в том числе персональные данные. Кроме того, использование в таком контексте произведений, охраняемых авторским правом, без должных оснований может рассматриваться как неправомерное распространение авторского контента. Вследствие этого возможность оспаривания, признания недействительным или отмены соответствующего результата представляется оправданной и обоснованной в правовой плоскости.

Интересным представляется и тот факт, что на уровне законодательства понятие МО вне границ прямого правового регулирования, однако, основные направления зафиксированы в так называемых внутренних актах государственного планирования, на уровне стратегических документов. При этом отдельные аспекты функционирования МО также находят свое отражение в действующем информационном законодательстве, например, принципы перечисленные в ст. 3 ФЗ «Об информации, информационных технологиях и о защите информации» [5], в гражданском законодательстве, регулирующем право интеллектуальной собственности, однако, можно резюмировать, что единое и полное нормативно-правовое регулирование рассматриваемой области отсутствует. Вместе с тем, несмотря на отсутствие нормативного закрепления понятия МО в действующем законодательстве, определённые шаги по формализации понятийного аппарата предпринимаются в смежной сфере технического регулирования. В частности, в 2024 году был принят ГОСТ Р 71476–2024 (ИСО/МЭК 22989:2022) «Искусственный интеллект. Концепции и терминология искусственного интеллекта», в котором МО определяется как «процесс оптимизации параметров модели с помощью вычислительных методов таким образом, чтобы поведение модели отражало данные и/или опыт» [7]. Стандарт также включает смежные термины, в том числе «алгоритм машинного обучения» и «модель машинного обучения», что позволяет говорить о формировании минимально необходимой терминологической базы. Вместе с тем, указанный стандарт относится к категории документов добровольного применения и не обладает статусом нормативного правового акта, в связи с чем сохраняется неопределённость в части обязательности правоприменения указанных дефиниций в юридическом контексте.

В целом МО представляется как класс методов ИИ, в основе которого лежит способность алгоритмов автоматически выявлять скрытые закономерности, и строить аналитические модели на основе обучающих данных. Ключевая особенность МО заключается в том, что логика принятия решений не задаётся человеком в виде явных инструкций, а формируется в процессе обучения на примерах.

В Европейском союзе для унификации правового регулирования ИИ, включая гармонизацию ключевых определений и понятий, был принят основополагающий документ — «Закон об искусственном интеллекте» (The AI Act) [3]. При этом само понятие МО четко не сформулировано, однако, из содержания документа следует, что МО представляется как совокупность методов и подходов, которые позволяют ИИ выявлять закономерности и составлять прогнозы на основе данных. Отсутствие единого подхода в документе ЕС приводит к тому, что принципы должны быть учтены при использовании ИИ, и внедрены в национальное законодательство государств-членов ЕС, однако, из-за отсутствия четкого толкования определения «МО», составляющего основу функционирования ИИ подходы к интерпретации такого понятия в национальном праве государств, могут быть различны, либо отсутствовать в целом. Так, например, во Франции в статье L. 122-5-3 Кодекса интеллектуальной собственности имеется определение понятия «интеллектуальный анализ текста и данных», который раскрывается как использование автоматизированного метода анализа текстов и данных в цифровой форме [1]. Фактически, мы можем говорить о том, что в ЕС единый подход к определению такого понятия и его границ на законодательном уровне отсутствует, большее внимание уделено основным принципам функционирования ИИ, основным элементом которого является МО.

В США на уровне федерального законодательства подход к определению понятия «МО» в контексте применения ИИ также не сформирован, оно представляется одним из составляющих ИИ, и к нему применяются общие законодательные нормы, регулирующие ИИ. В связи с особенностью англо-саксонской правовой семьи, на основе которой построена правовая система США, МО определяется в судебных прецедентах, косвенно. Например, в некоторых судебных решениях Федеральная торговая комиссия делает упор на использование алгоритмов и автоматизированных решений, к которым мы можем отнести и МО. При этом, например, в штате Нью-Йорк МО характеризуется как автоматизированный инструмент с раскрытием алгоритмов и аудитом, в таком случае, такие инструменты могут применяться для найма сотрудников, а если алгоритмы не раскрыты и не был проведен аудит, то использование таких автоматизированных инструментов запрещается (Local Law 144) [2]. То есть, мы также можем указать на отсутствие единого подхода к пониманию МО, наличие некоторых его прообразов в прецедентах и на уровне законодательства отдельных штатов, однако, базовое закрепление в нормативно-правовых актах отсутствует.

Япония является одной из стран, в которых был сформирован законодательный подход к закреплению функционирования ИИ, однако, МО также не характеризуется как отдельная категория, и представляется частью концепции технологий связанных с функционированием ИИ. В законодательстве Японии под технологиями, связанными с ИИ, понимаются технологии, необходимые для реализации функций, которые заменяют интеллектуальные способности человека, касающиеся восприятия, рассуждения и суждения, посредством искусственных способов, а также технологии информационных систем, которые используют эти технологии для обработки введённой информации и генерации вывода результатов [4].

В КНР в законодательстве упоминаются «обучающиеся алгоритмы», при этом, их четкая характеристика не закреплена.

Таким образом, в современных правовых системах, включая российскую, МО как правило не выделяется в качестве самостоятельной правовой категории. Это обуславливает отсутствие единообразия в правоприменительной практике и допускает различную интерпретацию понятия либо как элемента ИИ, либо как автономного объекта. Вместе с тем обоснованным представляется подход, в соответствии с которым МО требует нормативной детализации. Его правовое определение может способствовать снижению рисков злоупотреблений и обеспечить большую юридическую определённость. С этой точки зрения отдельное регулирование могло бы закрепить общеобязательные принципы, аналогичные международным пактам, и тем самым способствовать формированию единой правовой позиции на глобальном уровне.

Особое значение в контексте правового регулирования приобретают обучающие данные как основа алгоритмических решений. Представляется целесообразным нормативно закрепить их специальный правовой режим, включающий требования к происхождению и качеству данных, фиксации источников, процедурам подготовки и соблюдению ограничений, установленных в отношении охраняемой информации. Это позволило бы устранить правовую неопределённость, повысить доверие к алгоритмическим решениям и обеспечить баланс интересов всех участников процесса.

В то же время существует позиция, согласно которой регулирование должно охватывать ИИ в целом без излишней фрагментации. Такая точка зрения опирается на традицию целостного подхода в праве и учитывает возможные сложности правоприменения при избыточной детализации. Вопрос о нормативном выделении МО требует дальнейшего обсуждения и соотнесения с международной практикой и национальными особенностями.

Литература

1. Code de la propriété intellectuelle (Intellectual Property Code). Version consolidée au 2025 [Электронный ресурс]. – Режим доступа: https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006069414/ (дата обращения: 25.09.2025).

2. New York City. Local Law No. 144 of 2021: Automated Employment Decision Tools [Электронный ресурс]. – Режим доступа: https://www.nyc.gov/assets/dca/downloads/pdf/about/LegalCompliance/144-AEDT.pdf (дата обращения: 25.09.2025).

3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts [Электронный ресурс]. – Режим доступа: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689 (дата обращения: 26.09.2025).

4. Zakon o sodejstvii issledovaniju, razrabotke i ispol'zovaniju tehnologij, svjazannyh s iskusstvennym intellektom: принят 13.06.2024 г. // Japanese Law Translation. URL: https://www.noandt.com/publications/publication20250306-1/ (дата обращения: 28.09.2025).

5. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ // Российская газета, N 165, 29.07.2006

6. Указ Президента РФ от 10.10.2019 № 490 (ред. от 15.02.2024) «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Официальный интернет-портал правовой информации. 11.10.2019. № 0001201910110003.

7. ГОСТ Р 71476–2024 (ISO/IEC 22989:2022). Искусственный интеллект. Концепции и терминология искусственного интеллекта [Электронный ресурс]. – Режим доступа: https://www.garant.ru/files/7/7/1799577/natsionalniy_standart_rf_gost_r_71476_2024_iso_mek_22989_2022_iskusstvenniy_inte.pdf (дата обращения: 29.11.2025)

8. Кондратенко Е. В. Машинное обучение как инструмент анализа данных [Электронный ресурс] / Е. В. Кондратенко, С. Н. Макаренко. – Минск : БНТУ, 2022. – Режим доступа: https://rep.bntu.by (дата обращения: 28.09.2025).

9. Наумов В. Б. Правовые проблемы машинного обучения / В. Б. Наумов, Е. В. Тытюк // Образование и право. – 2020. – № 6. – С. 219–231.

10. SAS Institute. Machine Learning: What it is and why it matters [Электронный ресурс]. – Режим доступа: https://www.sas.com/en_us/insights/analytics/machine-learning.html (дата обращения: 25.09.2025).

11. Towards data science. Machine Learning Introduction: A Comprehensive Guide [Электронный ресурс]. – Режим доступа: https://towardsdatascience.com/machine-learning-introduction-a-comprehensive-guide-af6712cf68a3 (дата обращения: 25.09.2025).

Legal approaches to the definition of "machine learning"

Fokina S.A.

Moscow State Law University O.E. Kutafina

The article discusses the problems of legal understanding and regulation of machine learning (MO) as a key technology of the modern stage of digitalization and artificial intelligence (AI). The transition from the creation of digital infrastructure to its intellectualization and autonomous operation is noted, which creates new risks and challenges for the law. The article analyzes scientific approaches to the definition of MO, including the positions of V. B. Naumov, D. Fagell, E. V. Kondratenok and S. N. Makarenya, and concludes that there is no single definition. The Russian legislation is being investigated: National Strategy for the Development of AI until 2030, Federal Law "On Information, Information Technologies and Information Protection", GOST R 71476-2024. Foreign experience is considered: the Law on AI in the EU, the approaches of France, the USA, Japan and China. The necessity of normative specification of the concept of MO, consolidation of a special legal regime for training data, requirements for their origin and quality, as well as ensuring a balance of interests is substantiated. An alternative position on regulating AI in general without excessive fragmentation is also indicated.

Keywords: machine learning, artificial intelligence, legal regulation, digitalization, learning data, legal certainty, normative definition, comparative law, AI Act, risks, information law.

References

1. Code de la propriété intellectuelle (Intellectual Property Code). Consolidated version as of 2025 [Electronic resource]. – Available at: https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006069414/ (accessed: 25.09.2025).
2. New York City. Local Law No. 144 of 2021: Automated Employment Decision Tools [Electronic resource]. – Available at: https://www.nyc.gov/assets/dca/downloads/pdf/about/LegalCompliance/144-AEDT.pdf (accessed: 25.09.2025).
3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts [Electronic resource]. – Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689 (accessed: 26.09.2025).
4. Act on the Promotion of Research, Development, and Use of Technologies Related to Artificial Intelligence: adopted on 13 June 2024 // Japanese Law Translation. URL: https://www.noandt.com/publications/publication20250306-1/ (accessed: 28.09.2025). 5. Federal Law No. 149-FZ of July 27, 2006, "On Information, Information Technologies, and Information Protection" // Rossiyskaya Gazeta, No. 165, July 29, 2006.
6. Decree of the President of the Russian Federation No. 490 of October 10, 2019 (as amended on February 15, 2024), "On the Development of Artificial Intelligence in the Russian Federation" (including the "National Strategy for the Development of Artificial Intelligence for the Period up to 2030") // Official Internet Portal of Legal Information. October 11, 2019. No. 0001201910110003.
7. GOST R 71476–2024 (ISO/IEC 22989:2022). Artificial Intelligence. Concepts and Terminology of Artificial Intelligence [Electronic resource]. – Access mode: https://www.garant.ru/files/7/7/1799577/natsionalniy_standart_rf_gost_r_71476_2024_iso_mek_22989_2022_iskusstvenniy_inte.pdf (accessed: November 29, 2025).
8. Kondratenko, E. V., & Makarenko, S. N. (2022). Machine Learning as a Tool for Data Analysis [Electronic resource]. – Minsk: BNTU. – Access mode: https://rep.bntu.by (accessed: September 28, 2025). 9. Naumov V. B., Tytyuk E. V. Legal Issues of Machine Learning // Education and Law. – 2020. – No. 6. – pp. 219–231.
10. SAS Institute. Machine Learning: What it is and why it matters [Electronic resource]. – Available at: https://www.sas.com/en_us/insights/analytics/machine-learning.html (accessed: 25.09.2025).
11. Towards Data Science. Machine Learning Introduction: A Comprehensive Guide [Electronic resource]. – Available at: https://towardsdatascience.com/machine-learning-introduction-a-comprehensive-guide-af6712cf68a3 (accessed: 25.09.2025).