ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНТЕРНЕТ ВЕЩЕЙ

https://doi.org/10.5281/zenodo.13777343

Мухитдинов Жахонгир Фахриддин угли
доктор философии по юридическим наукам (PhD),
соискатель Ташкентского государственного юридического университета,
Ташкент, Узбекистан

Аннотация. *Данная статья посвящена комплексному анализу правового регулирования интернета вещей (IoT) в глобальном контексте. В работе рассматриваются ключевые аспекты нормативно-правовой базы IoT, включая защиту персональных данных, обеспечение кибербезопасности, вопросы интеллектуальной собственности. В заключение обсуждаются тенденции развития правового регулирования IoT и необходимость международного сотрудничества в этой области.*

Ключевые слова: *Интернет вещей, персональные данные, кибербезопастность, интеллектуальная собственность.*

LEGAL REGULATION OF THE INTERNET OF THINGS

Mukhitdinov Jakhongir Fakhriddin ugli
Doctor of Philosophy in Legal Sciences Independent researcher
at Tashkent State University of Law, Tashkent, Uzbekistan

Abstract. *This article provides a comprehensive analysis of the legal regulation of the Internet of Things (IoT) in a global context. The paper examines key aspects of the IoT regulatory framework, including personal data protection, cybersecurity, and intellectual property issues. In conclusion, trends in the development of IoT legal regulation and the need for international cooperation in this field are discussed.*

Keywords*: internet of things, personal data, cybersecurity, intellectual property.*

В современную эпоху цифровизации и технологического прогресса интернет вещей (IoT) становится неотъемлемой частью нашей повседневной жизни и экономики. Этот феномен, представляющий собой сеть взаимосвязанных устройств, способных собирать, обрабатывать и обмениваться данными без непосредственного участия человека, открывает новые горизонты для инноваций и повышения качества жизни. Однако вместе с многочисленными преимуществами IoT приносит и ряд серьезных вызовов, особенно в сфере правового регулирования. Возникает острая необходимость в создании адекватной нормативно-правовой базы, способной

обеспечить безопасное и этичное использование технологий интернета вещей, защитить права пользователей и стимулировать дальнейшее развитие отрасли.

Правовое регулирование интернета вещей представляет собой комплексную и многогранную проблему, затрагивающую различные аспекты законодательства: от защиты персональных данных и обеспечения кибербезопасности до вопросов интеллектуальной собственности. По мере того как IoT все глубже проникает в различные сферы жизни общества, законодатели и регуляторы по всему миру сталкиваются с необходимостью адаптировать существующие правовые нормы и создавать новые, учитывающие специфику этих технологий.

В контексте глобального характера интернета вещей особую важность приобретает международное сотрудничество и гармонизация законодательства различных стран. В то же время, национальные особенности и приоритеты также играют значительную роль в формировании правового ландшафта IoT. Анализ подходов к регулированию интернета вещей в различных юрисдикциях, таких как США, Европейский Союз, Китай и Узбекистан, позволяет выявить как общие тенденции, так и уникальные черты, характерные для каждого региона.

Одним из ключевых аспектов правового регулирования IoT является защита персональных данных. Устройства интернета вещей генерируют, собирают и обрабатывают огромные объемы информации, часто включающей чувствительные персональные данные пользователей. В этой связи особую актуальность приобретают вопросы обеспечения конфиденциальности и контроля над данными. Европейский Союз, являющийся пионером в области защиты персональных данных, установил высокие стандарты в этой сфере с принятием Общего регламента по защите данных (GDPR) в 2018 году. Согласно GDPR, компании, работающие с данными граждан ЕС, обязаны обеспечивать прозрачность обработки данных, получать явное согласие пользователей на сбор и использование их персональной информации, а также предоставлять им возможность удаления или переноса своих данных[1].

В США подход к защите данных в контексте IoT носит более фрагментированный характер. На федеральном уровне отсутствует единый всеобъемлющий закон о защите персональных данных, аналогичный GDPR. Вместо этого регулирование осуществляется через комбинацию отраслевых законов, таких как Закон о переносимости и подотчетности медицинского страхования (HIPAA) для медицинских данных, и инициатив отдельных штатов. Например, Калифорнийский закон о защите конфиденциальности потребителей (CCPA), вступивший в силу в 2020 году, устанавливает строгие требования к компаниям, собирающим персональные данные

[1] Weber, R.H. (2015) “Internet of Things: Privacy issues revisited”, Computer Law & Security Review, 31(5), pp. 618-627.

жителей Калифорнии, включая право потребителей знать, какая информация о них собирается и как она используется[2].

Китай, в свою очередь, принял Закон о кибербезопасности в 2017 году и Закон о защите персональных данных в 2021 году, которые устанавливают строгие правила для компаний, работающих с данными китайских граждан. Эти законы требуют локализации данных и получения разрешения регулирующих органов на трансграничную передачу определенных типов информации, что создает дополнительные сложности для международных IoT-компаний, работающих на китайском рынке[3].

Узбекистан, стремясь не отставать от глобальных тенденций в сфере цифровизации, в 2019 году принял закон «О персональных данных», который устанавливает основные принципы и требования к обработке персональных данных. Хотя этот закон не содержит специфических положений, касающихся IoT, он создает базовую правовую основу для защиты данных в контексте развития цифровых технологий в стране.

Анализируя различные подходы к защите данных в контексте IoT, можно выделить общую тенденцию к усилению контроля над сбором и использованием персональной информации. Однако существуют значительные различия в степени и методах регулирования. Если ЕС и Китай склонны к более жесткому и централизованному подходу, то США предпочитают более гибкое и отраслевое регулирование. Эти различия создают определенные сложности для глобальных IoT-компаний, вынужденных адаптировать свои продукты и практики к требованиям различных юрисдикций.

Другим критически важным аспектом правового регулирования интернета вещей является обеспечение кибербезопасности. IoT-устройства, зачастую обладающие ограниченными вычислительными ресурсами и работающие в условиях минимального контроля со стороны пользователей, представляют собой привлекательную мишень для киберпреступников. Атаки на IoT-системы могут иметь серьезные последствия, от нарушения работы критической инфраструктуры до компрометации личных данных миллионов пользователей.

Анализируя различные подходы к обеспечению кибербезопасности IoT, можно отметить общую тенденцию к ужесточению требований и повышению ответственности производителей и операторов IoT-систем. Однако существуют значительные различия в методах регулирования: от обязательной сертификации устройств до установления общих принципов безопасности. Эти различия создают

[2] Carsten, P. (2019) “California’s new privacy law: What it means for businesses and consumers”, Reuters, 12 December. Available at: https://www.reuters.com/article/us-usa-privacy-california-idUSKBN1YG1CT (Accessed: 15 September 2024).
[3] Kshetri, N. (2017) “The evolution of the internet of things industry and market in China: An interplay of institutions, demands and supply”, Telecommunications Policy, 41(1), pp. 49-67.

определенные сложности для глобальных IoT-компаний, вынужденных адаптировать свои продукты и практики к требованиям различных юрисдикций.

Еще одним важным аспектом правового регулирования интернета вещей являются вопросы интеллектуальной собственности. IoT-системы часто включают в себя множество запатентованных технологий, программного обеспечения с открытым исходным кодом и проприетарных алгоритмов. Это создает сложную экосистему интеллектуальной собственности, в которой возникают вопросы о праве собственности на генерируемые данные, патентоспособности IoT-изобретений и лицензировании технологий.

В США патентное ведомство (USPTO) сталкивается с вызовом определения патентоспособности IoT-изобретений в свете решения Верховного суда по делу Alice Corp. v. CLS Bank International, которое установило более строгие критерии для патентования программного обеспечения и бизнес-методов. Это решение оказало значительное влияние на патентование IoT-технологий, многие из которых основаны на сочетании аппаратного и программного обеспечения[4].

В Европейском Союзе вопросы интеллектуальной собственности в контексте IoT регулируются как на уровне ЕС, так и на национальном уровне. Европейское патентное ведомство (EPO) разработало специальные руководства по патентованию изобретений, связанных с искусственным интеллектом и IoT. Эти руководства призваны обеспечить баланс между защитой инноваций и предотвращением чрезмерно широких патентов, которые могут препятствовать развитию отрасли[5].

В Китае, где наблюдается бурное развитие IoT-технологий, государство активно поддерживает патентование в этой области. Китайское патентное ведомство (CNIPA) предоставляет ускоренную процедуру рассмотрения заявок на патенты в области IoT и других перспективных технологий. Это способствует быстрому росту числа патентов в сфере интернета вещей, что укрепляет позиции Китая как одного из мировых лидеров в этой области[6].

В Узбекистане, где развитие IoT находится на начальном этапе, вопросы интеллектуальной собственности в этой сфере пока не получили специфического регулирования. Однако общие положения законодательства об интеллектуальной собственности создают базовую правовую основу для защиты IoT-изобретений.

Анализируя различные подходы к регулированию интеллектуальной собственности в сфере IoT, можно отметить общую тенденцию к адаптации существующих правовых норм к специфике новых технологий. При этом

[4] Menell, P.S. (2019) “Economic analysis of network effects and intellectual property”, Berkeley Technology Law Journal, 34, pp. 219-284.
[5] Giannopoulou, A. (2021) “Algorithmic systems: the consent is in the detail?”, Internet Policy Review, 10(1),
pp. 1-19.
[6] Kshetri, N. (2017) “The evolution of the internet of things industry and market in China: An interplay of institutions, demands and supply”, Telecommunications Policy, 41(1), pp. 49-67.

наблюдаются значительные различия в степени готовности правовых систем разных стран к вызовам цифровой эпохи. Эти различия могут создавать как барьеры, так и возможности для развития IoT-технологий в глобальном масштабе.

Отдельного внимания заслуживает вопрос регулирования ответственности за ущерб, причиненный устройствами и системами интернета вещей. С ростом числа подключенных устройств и их интеграцией в критически важные системы, от автономных транспортных средств до медицинского оборудования, вопрос о том, кто несет ответственность в случае сбоя или неправильного функционирования IoT-устройства, становится все более актуальным.

В США вопросы ответственности за продукцию традиционно регулируются на уровне штатов, что создает определенные сложности в случае с IoT-устройствами, которые часто функционируют в рамках глобальных сетей. Некоторые штаты, такие как Калифорния, начали разрабатывать специфическое законодательство для регулирования ответственности за автономные транспортные средства, которые можно рассматривать как одно из наиболее сложных приложений IoT. На федеральном уровне обсуждается необходимость создания единых стандартов ответственности для IoT-устройств, но пока эти обсуждения не привели к принятию конкретных законов[7].

В Европейском Союзе вопросы ответственности за продукцию регулируются Директивой об ответственности за качество продукции (Product Liability Directive), принятой еще в 1985 году. Однако в свете развития IoT-технологий Европейская комиссия инициировала пересмотр этой директивы. В 2020 году был опубликован отчет экспертной группы по ответственности и новым технологиям, в котором рекомендуется адаптировать существующее законодательство к специфике IoT и других новых технологий. В частности, предлагается расширить понятие «продукта» для включения программного обеспечения и цифровых услуг, а также пересмотреть концепцию «дефекта» применительно к самообучающимся системам[8].

В Китае вопросы ответственности за IoT-устройства регулируются в рамках общего законодательства о качестве продукции и защите прав потребителей. При этом в последние годы наблюдается тенденция к ужесточению ответственности производителей за качество и безопасность продукции, что также затрагивает сферу IoT. В 2021 году были приняты новые правила управления сетевой безопасностью подключенных транспортных средств, которые устанавливают строгие требования к производителям и операторам таких систем[9].

[7] Chatzipanagiotis, M. and Leloudas, G. (2020) “Automated vehicles and third-party liability: A European perspective”, University of Illinois Journal of Law, Technology & Policy, 2020(1), pp. 109-199.
[8] European Commission (2020) Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics. Brussels: European Commission.
[9] Kshetri, N. (2017) “The evolution of the internet of things industry and market in China: An interplay of institutions, demands and supply”, Telecommunications Policy, 41(1), pp. 49-67.

В Узбекистане, как и в других странах СНГ, вопросы ответственности за продукцию регулируются общими положениями гражданского законодательства и законодательства о защите прав потребителей. Специфического регулирования для IoT-устройств пока не разработано, что может создавать определенные правовые неопределенности в случае причинения ущерба такими устройствами.

Анализируя различные подходы к регулированию ответственности за IoT-устройства, можно отметить общую тенденцию к пересмотру существующих норм ответственности за продукцию с учетом специфики новых технологий. При этом наблюдаются значительные различия в степени готовности правовых систем разных стран к вызовам цифровой эпохи. Эти различия могут создавать как риски, так и возможности для развития глобального рынка IoT.

Подводя итоги анализа правового регулирования интернета вещей, можно сделать следующие выводы:

Правовое регулирование IoT представляет собой комплексную и многогранную проблему, затрагивающую различные аспекты законодательства: от защиты персональных данных и обеспечения кибербезопасности до вопросов интеллектуальной собственности.

Наблюдается общая тенденция к усилению регулирования в сфере IoT, особенно в аспектах защиты данных и обеспечения безопасности. При этом регуляторы сталкиваются с вызовом найти баланс между стимулированием инноваций и защитой прав пользователей.

Существуют значительные различия в подходах к регулированию IoT в разных странах, что отражает различия в правовых системах, политических приоритетах и культурных ценностях. Эти различия создают определенные сложности для глобальных IoT-компаний, вынужденных адаптировать свои продукты и практики к требованиям различных юрисдикций.

Важную роль в регулировании IoT играют не только законы, но и мягкое право – руководства, стандарты и этические принципы, разрабатываемые как государственными органами, так и индустриальными ассоциациями.

Многие аспекты регулирования IoT находятся в стадии формирования, и ожидается, что в ближайшие годы будут приняты новые законы и нормативные акты, адаптирующие правовые системы к вызовам цифровой эпохи.

Ключевым вызовом для регуляторов является необходимость создания гибких и адаптивных правовых рамок, способных учитывать быстрое развитие технологий и появление новых бизнес-моделей в сфере IoT.

Международное сотрудничество и гармонизация законодательства различных стран становятся все более важными для обеспечения эффективного регулирования глобального рынка IoT.

В заключение можно отметить, что правовое регулирование интернета вещей находится на этапе активного формирования и развития. По мере того как IoT все

глубже проникает в различные аспекты нашей жизни, важность адекватного правового регулирования этой сферы будет только возрастать. Ключевой задачей для законодателей и регуляторов в ближайшие годы будет создание правовых рамок, способных обеспечить баланс между стимулированием инноваций, защитой прав пользователей и обеспечением общественной безопасности в эпоху повсеместного интернета вещей.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Carsten, P. (2019) “California's new privacy law: What it means for businesses and consumers”, Reuters, 12 December. Available at: https://www.reuters.com/article/us-usa-privacy-california-idUSKBN1YG1CT.

2. Chatzipanagiotis, M. and Leloudas, G. (2020) “Automated vehicles and third-party liability: A European perspective”, University of Illinois Journal of Law, Technology & Policy, 2020(1), pp. 109-199.

3. European Commission (2020) Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics. Brussels: European Commission.

4. Giannopoulou, A. (2021) “Algorithmic systems: the consent is in the detail?”, Internet Policy Review, 10(1), pp. 1-19.

5. Kshetri, N. (2017) “The evolution of the internet of things industry and market in China: An interplay of institutions, demands and supply”, Telecommunications Policy, 41(1), pp. 49-67.

6. Menell, P.S. (2019) “Economic analysis of network effects and intellectual property”, Berkeley Technology Law Journal, 34, pp. 219-284.

7. Weber, R.H. (2015) “Internet of Things: Privacy issues revisited”, Computer Law & Security Review, 31(5), pp. 618-627.