

DOI: 10.17803/2542-2472.2025.35.3.027-039

УМНЫЕ ИГРУШКИ И ЦИФРОВОЙ СЛЕД НЕСОВЕРШЕННОЛЕТНИХ: ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Рыжков Дмитрий Игоревич,

руководитель проекта Центра по обеспечению прав молодежи в цифровом пространстве, аспирант кафедры информационного права и цифровых технологий Университета имени О.Е. Кутафина (МГЮА)
125993, Россия, г. Москва, Садовая-Кудринская ул., д. 9
dir1922@yandex.ru

© Рыжков Д. И., 2025

Аннотация. В статье рассматриваются актуальные проблемы правового регулирования цифрового следа несовершеннолетних в условиях стремительного развития цифровых технологий, особенно в контексте использования умных игрушек и интернет-устройств. Проанализированы основные международные и российские подходы к защите персональных данных детей, выявлены правовые риски и пробелы, характерные для современных технологических решений. Особое внимание уделено необходимости комплексного регулирования, которое объединяет законодательные нормы, технические стандарты, эффективный государственный и общественный контроль. Сформулированы предложения по совершенствованию законодательства и практик защиты цифрового следа несовершеннолетних в Российской Федерации с учетом зарубежного опыта.

Ключевые слова: цифровой след; несовершеннолетние; персональные данные; информационная безопасность; умные игрушки; интернет вещей; правовое регулирование; защита детей; конфиденциальность.

Благодарности. Исследование выполнено в рамках программы стратегического академического лидерства «Приоритет-2030».

SMART TOYS AND THE DIGITAL FOOTPRINT OF MINORS: LEGAL REGULATION ISSUES

Dmitriy I. Ryzhkov,

project manager of the Center for Ensuring the Rights of Youth in the Digital Space; Graduate Student, Department of IT and Digital Technologies Law, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation
dir1922@yandex.ru

Abstract. The paper addresses pressing issues in the legal regulation of the digital footprint of minors amid the rapid development of digital technologies, particularly in the context of smart toys and internet-connected devices. It analyzes key international and Russian approaches to protecting children's personal data, identifying legal risks and

gaps inherent in modern technological solutions. Special attention is given to the need for comprehensive regulation that integrates legislative provisions, technical standards, and effective state and public oversight. The authors propose measures to improve legislation and practices for safeguarding the digital footprint of minors in the Russian Federation, taking into account relevant foreign experience.

Keywords: digital footprint; minors; personal data; information security; smart toys; internet of things; legal regulation; child protection; privacy.

Acknowledgements. The study was carried out within the framework of «Priority-2030» Strategic Academic Leadership Program.

Современное общество переживает этап глубокой цифровой трансформации, характеризующийся повсеместным внедрением высокотехнологичных устройств, объединенных в интернет вещей (Internet of Things, IoT)¹. Устройства, оснащенные множеством датчиков и возможностью постоянного подключения к сети Интернет, стремительно заполняют рынок детских товаров, формируя новую реальность «цифрового» детства. При этом умные игрушки — от интерактивных кукол до программируемых роботов — собирают, обрабатывают и передают значительное количество как несовершеннолетних персональных данных, так и персональных данных их родителей, формируя обширный цифровой след².

Мировой рынок игрушек в 2024 г. оценивался в 114,4 млрд долл., при этом потребители отдельных стран наиболее заинтересованы игрушками, которые включают такие функции, как дополненная реальность, виртуальная реальность и искусственный интеллект, сочетая физическую игру с цифровым улучшениями³. Представляется очевидным, что несовершеннолетние являются особо уязвимой категорией пользователей цифровых технологий, поскольку не обладают достаточными компетенциями для защиты своих цифровых прав. В последние же годы всё чаще возникают инциденты безопасности с умными игрушками, что свидетельствует о необходимости комплексного анализа правового регулирования данной сферы⁴.

Структурно рынок умных игрушек подразделяется на несколько основных сегментов. Интерактивные игрушки с элементами искусственного интеллекта обеспечивают персонализированное взаимодействие с ребенком на основе анализа его речевых команд и поведенческих паттернов⁵. Образовательные роботы и конструкторы предназначены для обучения детей основам программирования и STEM-дисциплин. Носимые устройства (умные часы, фитнес-браслеты) отслеживают физическую активность и местоположение ребенка. Устройства для младенцев (умные мониторы, интерактивные игрушки для колыбели) собирают данные о режиме сна, плаче и физиологических показателях.

¹ См.: Интернет вещей. Развитие технологий и оценка возможностей перехода на отечественные решения. М. : АНО «Цифровая экономика», 2024. 134 с. URL: <https://files.data-economy.ru/Docs/IoT-5.pdf> (дата обращения: 30.09.2025).

² См.: Умные игрушки могут собирать данные о ребенке: как защитить семью от слежки // Компьютерра. URL: <https://www.computerra.ru/290335/umnye-igrushki-mogut-sobirat-dannye-o-rebenke-kak-zashhitit-semyu-ot-slezhki/> (дата обращения: 30.09.2025).

³ См.: Размер рынка игрушек — по типу продукта, по мощности, по ценовому диапазону, по использованию, по конечному использованию, по каналу сбыта, прогноз, 2025–2034 гг. // Global Market Insights. URL: <https://www.gminsights.com/ru/industry-analysis/toy-market> (дата обращения: 30.09.2025).

⁴ См.: Smart toy vulnerabilities could let cybercriminals video-chat with kids // Kaspersky. URL: <https://www.kaspersky.com/about/press-releases/smart-toy-vulnerabilities-could-let-cybercriminals-video-chat-with-kids> (дата обращения: 30.09.2025).

⁵ См.: Умный Мишка (Mishka AI) // ICT Moscow. URL: <https://ict.moscow/card/mishka-ai-umnyj-mishka/> (дата обращения: 30.09.2025).

Географически рынок характеризуется доминированием азиатских производителей, прежде всего китайских компаний, которые обеспечивают производство около 80 % всех игрушек в мире⁶. При этом крупнейшими рынками сбыта являются Соединенные Штаты Америки, страны Европейского Союза и Китай. Российский рынок умных игрушек также характеризуется преобладанием импортной продукции⁷.

Устройства Интернета вещей, ориентированные на детскую аудиторию, представляют собой сложные технические системы, интегрирующие разнообразные сенсорные технологии, вычислительные мощности и коммуникационные модули. Как справедливо отмечает Н. В. Кучковская, IoT-устройства собирают значительное число категорий данных, относимых законодательством Российской Федерации к персональным данным⁸.

Игрушки в современном мире могут оснащаться следующими компонентами сбора данных: микрофонами для распознавания речи, камерами для идентификации визуальных паттернов, акселерометрами и гироскопами для отслеживания движений, GPS-модулями для определения геолокации, датчиками приближения, а также радиопередатчиками для обеспечения связи через Wi-Fi или Bluetooth⁹. Данные сенсорные технологии позволяют устройствам непрерывно собирать информацию о физическом окружении ребенка, его поведении, предпочтениях и даже эмоциональном состоянии.

Принципиально важным является то, что большинство современных умных игрушек функционируют не автономно, а в составе распределенной информационной системы. Собранные данные передаются на удаленные серверы, где подвергаются обработке с использованием технологий искусственного интеллекта для персонализации взаимодействия с ребенком. При этом, как отмечают исследователи из Университета Базеля, многие производители не обеспечивают должного уровня шифрования при передаче данных, что создает дополнительные риски их несанкционированного перехвата¹⁰.

Данные, генерируемые умными игрушками, характеризуются исключительной широтой и включают различные категории информации, которые могут быть в том числе отнесены к персональным данным.

Идентификационные данные включают имя ребенка, дату рождения, пол, фотографические изображения, а также сведения о родителях или законных представителях (адреса электронной почты, номера телефонов, платежную информацию)¹¹. Такие категории данных позволяют идентифицировать конкретного несовершеннолетнего пользователя в цифровом пространстве.

Данные о геолокации представляют собой информацию о текущем местоположении ребенка, его перемещениях, посещаемых местах, что в совокупности позволяет

⁶ См.: More toy innovations coming out of China: industry expert // ChinaDaily. URL: <https://www.chinadaily.com.cn/a/201902/19/WS5c6b934ca3106c65c34ea1db.html> (дата обращения: 30.09.2025).

⁷ См.: Таможенное оформление игрушек // URL: <https://sbcargo.ru/poleznaya-informatsiya/tamozhennoe-oformlenie-igrushek/#:~:text=о государственной регистрации.-,Страны-импортеры,игрушки должны проходить радиочастотную экспертизу> (дата обращения: 30.09.2025).

⁸ См.: Кучковская Н. В. Развитие права в области IoT // Вопросы российского и международного права. 2023. Т. 13. № 4А. С. 350–356.

⁹ См.: Умные игрушки от Google смогут управлять оборудованием в доме // Умный дом. URL: <https://dom-automation.ru/umnyj-dom/articles/umnye-igrushki-ot-google-smogut-upravlyat-oborudovaniem-v-dome.html> (дата обращения: 30.09.2025).

¹⁰ См.: Pavliv V., Akbari N., Wagner I. AI-powered smart toys: interactive friends or surveillance devices? // Proceedings of the 14th International Conference on the Internet of Things. Oulu. 2025. P. 172–175.

¹¹ См.: Consumer Notice: Internet-connected Toys Could Present Privacy and Contact Concerns for Children // TowneBank. URL: <https://www.townebank.com/personal/resource/security/digital/internet-toys/> (дата обращения: 30.09.2025).

установить адрес проживания, образовательное учреждение, маршруты передвижения¹². Данные о местоположении относятся к наиболее чувствительной категории информации, поскольку их несанкционированное использование может создавать риски для физической безопасности ребенка.

Кроме того, умные игрушки могут осуществлять сбор голосовых сообщений, содержания разговоров, историю взаимодействия с устройством, предпочтения ребенка, его интересы и увлечения. Интеллектуальный анализ данной категории информации позволяет формировать детальные психологические профили несовершеннолетних, что в дальнейшем используется производителями для таргетированной рекламы и манипулятивных практик¹³. Биометрические данные, получаемые через распознавание лица, голоса, а также анализ эмоциональных реакций, образуют особую категорию собираемой информации, поскольку законодательство о биометрических персональных данных устанавливает более жесткие требования к их сбору, хранению и обработке.

Кроме того, умные игрушки интегрируют передовые технологические решения. Одним из ключевых трендов является использование технологий машинного обучения и обработки естественного языка, что позволяет устройствам адаптироваться к индивидуальным особенностям ребенка, распознавать его эмоциональное состояние и формировать персонализированные ответы. Игрушки типа Hello Barbie от Mattel или Dino от Cognitoys способны поддерживать диалог с ребенком, запоминать предыдущие разговоры и использовать полученную информацию для последующих взаимодействий¹⁴.

Другим значимым направлением является интеграция дополненной реальности и облачных сервисов. Игрушки подключаются к мобильным приложениям родителей, обеспечивая удаленный мониторинг активности ребенка, видеосвязь через встроенные камеры, а также доступ к библиотекам образовательного контента. Технология распознавания лиц позволяет устройствам идентифицировать ребенка и членов его семьи, а системы геолокации обеспечивают постоянное отслеживание местоположения¹⁵.

Однако увеличение числа новых функций умных игрушек сопровождается возрастанием количества рисков в сфере нарушения права на личную и семейную тайны, а также в сфере безопасности данных. Ключевым же риском, связанным с использованием умных игрушек, является угроза конфиденциальности персональных данных несовершеннолетних.

Так, в первую очередь существенная часть производителей интеллектуальных игрушек не обеспечивает должной защиты соединений между устройствами и серверами. Анализ, проведенный экспертами «Лаборатории Касперского», показал, что такие популярные детские устройства, как куклы Cayla и роботы i-Que от компании Genesis Toys, подключаются к смартфонам по протоколу Bluetooth без какой-либо аутентификации и не требуют введения пароля. Это создает условия для

¹² См.: Chinese toymaker accused of violating children's privacy in U.S., products also sold in Canada // CTVNews. URL: <https://www.ctvnews.ca/canada/article/chinese-toymaker-accused-by-us-of-sharing-childrens-data-sells-products-in-canada/> (дата обращения: 30.09.2025).

¹³ См.: Fantinato M., Priscilla de Albuquerque A., Yankson B. A Literature Survey on Smart Toy-related Children's Privacy Risks // Proceedings of the 53rd Hawaii International Conference on System Sciences. Hawaii. 2020. P. 1479–1488.

¹⁴ См.: Pavliv V., Akbari N., Wagner I. AI-powered smart toys: interactive friends or surveillance devices? // Proceedings of the 14th International Conference on the Internet of Things. Oulu. 2025. P. 172–175.

¹⁵ См.: Smart Toys: Navigating fun and security challenges in the digital age // KidsNetGuard. URL: <https://kidsnetguard.com/en/2024/05/09/smart-toys-navigating-fun-and-security-challenges-in-the-digital-age/> (дата обращения: 30.09.2025).

противоправного перехвата аудиоданных и даже позволяет злоумышленникам вести диалог с ребенком через игрушку, используя ее в качестве беспроводной гарнитуры¹⁶.

Во-вторых, системы аутентификации многих устройств характеризуются недостаточной надежностью. Эксперты компании Kaspersky также обнаружили, что в популярном роботе для детей отсутствовала проверка подлинности при генерации токенов видеосессии, что позволяло любому лицу, знающему идентификатор устройства, инициировать видеозвонок ребенку без согласия родителей. Более того, система позволяла полностью захватить родительский аккаунт посредством простого перебора шестизначного одноразового пароля¹⁷.

В-третьих, архитектура облачных хранилищ данных нередко не соответствует современным стандартам информационной безопасности. Инцидент с игрушкой CloudPets в 2017 г. продемонстрировал, что производитель хранил персональную информацию и голосовые записи более чем двух миллионов пользователей в незащищенной базе данных, доступной через Интернет¹⁸. Аналогичная ситуация произошла с компанией VTech, когда в результате кибератаки были скомпрометированы данные 6,4 млн детей и 4,9 млн родителей¹⁹.

Существенную угрозу также представляют манипулятивные практики, основанные на использовании собранных персональных данных. Умные игрушки, оснащенные алгоритмами машинного обучения, способны анализировать предпочтения, эмоциональные реакции и поведенческие паттерны детей с целью формирования профилей для таргетированной рекламы. Как отмечается в руководстве Европейской комиссии по защите несовершеннолетних в цифровой среде, дети часто не обладают достаточной коммерческой грамотностью для распознавания манипулятивных техник и могут быть подвержены нежелательному воздействию²⁰.

Особую озабоченность вызывают механизмы, направленные на формирование аддиктивного поведения. Игрушки могут использовать виртуальные валюты, механизмы т.н. «лутбоксов», системы наград и push-уведомления для стимулирования чрезмерного использования устройства. Директивы Европейского Союза по цифровым услугам требуют, чтобы подобные функции были отключены по умолчанию для несовершеннолетних пользователей²¹.

Помимо цифровых рисков, умные игрушки могут представлять угрозу для физической безопасности детей. Геолокационные функции, встроенные во многие устройства, позволяют отслеживать текущее местоположение и маршруты перемещения ребенка. В случае несанкционированного доступа к этим данным злоумышленники могут получить информацию об адресе проживания, образовательном учреждении и ежедневных перемещениях несовершеннолетнего.

Так, Германия в 2017 г. запретила продажу куклы My Friend Cayla, признав ее устройством скрытого наблюдения, поскольку игрушка могла быть взломана для записи частных разговоров через Bluetooth-соединение без ведома родителей.

¹⁶ См.: Недетские проблемы детских игрушек: как уследить за данными ребенка // Kaspersky daily. URL: <https://www.kaspersky.ru/blog/kids-devices-vulnerabilities/14574/> (дата обращения: 30.09.2025).

¹⁷ См.: Smart toy vulnerabilities can put your child at risk of abuse by strangers // Insomnihack. URL: <https://insomnihack.ch/talks/smart-toy-vulnerabilities-can-put-your-child-at-risk-of-abuse-by-strangers/> (дата обращения: 30.09.2025).

¹⁸ См.: Плюшевые мишки сболтнули лишнего // Газета.ру. URL: https://www.gazeta.ru/tech/2017/03/01/10551011/cloud_pets.shtml?ysclid=mgxq9byrul76011297 (дата обращения: 30.09.2025).

¹⁹ См.: В ходе атаки на VTech скомпрометированы данные 11 млн пользователей // SecurityLab.ru. URL: <https://www.securitylab.ru/news/477140.php?ysclid=mgxqddfpij923546527> (дата обращения: 30.09.2025).

²⁰ См.: Commission publishes guidelines on the protection of minors // Official website of the European Union. URL: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-protection-minors> (дата обращения: 30.09.2025).

²¹ Commission publishes guidelines on the protection of minors.

Аналогичные меры были предприняты в отношении умных часов для детей, которые были запрещены из-за рисков шпионажа²². Отдельные ученые также отмечают, что постоянное отслеживание действий ребенка может негативно влиять на формирование его личности, создавая атмосферу тотального контроля. указывая, что чрезмерная зависимость от умных устройств может препятствовать развитию самостоятельности, творческого мышления и навыков социального взаимодействия²³.

Далее следует обратиться к опыту правового регулирования сбора персональных данных о несовершеннолетних умными игрушками в различных странах.

Так, в Европейском Союзе разработана комплексная система защиты персональных данных несовершеннолетних в контексте использования цифровых технологий. Основопологающим актом является Общий регламент о защите персональных данных (GDPR)²⁴. Статья 8 GDPR устанавливает возраст цифрового согласия в 16 лет с возможностью для государств — членов Европейского Союза снижения данного порога до 13 лет. Для детей младше установленного возраста обработка персональных данных требует получения согласия от родителей и опекунов несовершеннолетнего.

Принципиально важным является признание в GDPR персональных данных детей в качестве особой категории чувствительной информации, требующей повышенного уровня защиты. Так, статья 6(1)(f) GDPR указывает, что законные интересы оператора данных не могут служить основанием для обработки данных детей, что фактически исключает возможность обработки без явного согласия.

В развитие положений GDPR в 2020 г. в Великобритании был издан Кодекс проектирования с учетом возраста (англ. Age-Appropriate Design Code), устанавливающий 15 стандартов для онлайн-сервисов, доступных детям. Среди ключевых требований: высокий уровень конфиденциальности по умолчанию, ограничение геолокационных функций, запрет на использование техник для стимулирования раскрытия персональных данных, требование о проведении оценки рисков для прав детей²⁵.

В дальнейшем, в рамках законодательства Европейского Союза были усилены меры, направленные на защиту прав несовершеннолетних посредством введения дополнительных требований о защите данных несовершеннолетних в рамках Акта о цифровых услугах (англ. Digital Services Act)²⁶. Так, названным Актом установлены конкретные требования для онлайн-платформ, доступных несовершеннолетним: установка приватных настроек по умолчанию, модификация рекомендательных систем для снижения рисков столкновения с вредоносным контентом, расширение возможностей для блокировки пользователей, запрет на скачивание контента,

²² См.: *Apthore N., Varghese S., Feamster N.* Evaluating the Contextual Integrity of Privacy Regulation: Parents IoT Toy Privacy Norms Versus COPPA // The Proceedings of the 28th USENIX Security Symposium. Santa Clara. 2019. P. 123–140.

²³ См.: *Castelli P. R.* Are interactive toys spying on young children // IBSA Foundation for scientific research. URL: <https://www.ibsafoundation.org/en/blog/games-for-children-secretly-collect-data> (дата обращения: 30.09.2025).

²⁴ Регламент № 2016/679 Европейского парламента и Совета Европейского Союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)». Принят в г. Брюсселе 27.04.2016. Неофициальный перевод Е. В. Новиковой // СПС «КонсультантПлюс».

²⁵ См.: Age appropriate design: a code of practice for online services // ICO. URL: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/> (дата обращения: 30.09.2025).

²⁶ См.: Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) // Official Journal of the European Union. 2022. L 277. P. 1–102. URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng> (дата обращения: 30.09.2025).

размещенного несовершеннолетними, отключение функций, способствующих чрезмерному использованию²⁷.

В Соединенных Штатах Америки основным федеральным актом, регулирующим сбор персональных данных детей, является Закон о защите конфиденциальности детей в Интернете (англ. Children's Online Privacy Protection Act, COPPA). COPPA применяется к операторам онлайн-сервисов, деятельность которых ориентирована на детей до 13 лет, либо в случае, если имеются фактические сведения о том, сервис собирает данные от таких детей²⁸.

В июне 2017 г. Федеральная торговая комиссия США прямо указала, что COPPA применяется к устройствам Интернета вещей, включая умные игрушки. Закон требует от операторов: размещения четкой политики конфиденциальности, получения поддающегося проверке родительского согласия до сбора данных, предоставления родителям возможности просматривать и удалять информацию о детях, обеспечения конфиденциальности и безопасности собранных данных²⁹.

Значимым прецедентом применения COPPA к умным игрушкам стало дело компании VTech в 2018 г., когда Федеральной торговой комиссией США был наложен штраф в размере 650 000 долл. за незаконный сбор данных от примерно 5 млн родителей и детей без получения родительского согласия и без обеспечения должной защиты информации³⁰. В 2025 г. Министерство юстиции США подало иск против китайской компании Apitor Technology за нарушение COPPA путем сбора геолокационных данных от детей младше 12 лет через мобильное приложение, связанное с образовательными роботами³¹.

На уровне штатов также принимаются специализированные акты. Так, в штате Калифорния разработан Кодекс проектирования с учетом возраста штата Калифорния (англ. California Age-Appropriate Design Code Act), во многом аналогичный британскому Кодексу проектирования с учетом возраста, который требует от операторов проведения оценки рисков для детей и минимизации сбора данных³². Законодательство названного штата устанавливает более жесткое правовое регулирование в сфере услуг для несовершеннолетних в цифровой среде, чем предусмотрено законодательством Соединенных Штатов Америки.

В законодательстве Китайской Народной Республики также уделяется значительное внимание правовому регулированию защиты персональных данных несовершеннолетних. Базовым актом является Закон о защите персональной информации

²⁷ The Digital Service Act (DSA) explained — What online platforms should do to keep kids and teens safe online // Official website of the European Union. URL: <https://digital-strategy.ec.europa.eu/en/library/digital-service-act-dsa-explained-what-online-platforms-should-do-keep-kids-and-teens-safe-online> (дата обращения: 30.09.2025).

²⁸ Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501–6506 (COPPA). URL: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> (дата обращения: 30.09.2025).

²⁹ См.: Complying with COPPA: Frequently Asked Questions // An official website of the United States government. URL: <https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions> (дата обращения: 30.09.2025).

³⁰ См.: Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act // An official website of the United States government. URL: <https://www.ftc.gov/news-events/news/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated-childrens-privacy-law-ftc-act> (дата обращения: 30.09.2025).

³¹ См.: FTC Takes Action Against Robot Toy Maker for Allowing Collection of Children's Data without Parental Consent // An official website of the United States government. URL: <https://www.ftc.gov/news-events/news/press-releases/2025/09/ftc-takes-action-against-robot-toy-maker-allowing-collection-childrens-data-without-parental-consent> (дата обращения: 30.09.2025).

³² California Assembly Bill 2273 (Age-Appropriate Design Code Act) // California Legislative Information. 2022. URL: <https://legiscan.com/CA/text/AB2273/id/2606836> (дата обращения: 30.09.2025).

(англ. Personal Information Protection Law, PIPL). PIPL признает личные данные детей до 14 лет конфиденциальной информацией, требующей особых мер защиты³³.

Статья 31 PIPL устанавливает, что обработка персональных данных несовершеннолетних до 14 лет допускается только при получении согласия от родителей или иных законных представителей. Операторы обязаны разработать специальные правила обработки персональных данных несовершеннолетних, провести оценку воздействия на защиту персональных данных, а также обеспечить прозрачность обработки. Названный нормативный правовой акт требует от операторов доказывания факта того, что они предприняли все возможные меры для проверки возраста пользователей. Кроме того, в октябре 2021 г. было предложено обязать несовершеннолетних при регистрации в Интернете указывать личные данные родителей и предоставлять их согласие³⁴.

В Российской Федерации правовое регулирование защиты персональных данных несовершеннолетних при использовании умных игрушек находится на стадии формирования и характеризуется фрагментарностью. Базовым актом является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее — Закон о персональных данных), однако данный нормативный правовой акт не содержит специальных положений, учитывающих особенности обработки данных детей³⁵. Согласно положениям Закона о персональных данных, в случае недееспособности субъекта персональных данных согласие на обработку дает его законный представитель. Вместе с тем закон не определяет возраст, с которого субъект может самостоятельно давать согласие на обработку своих данных. Авторы отдельных статей исходят из положений Гражданского кодекса Российской Федерации о дееспособности, однако данный подход не учитывает специфику цифровых отношений³⁶.

Что касается специального регулирования умных игрушек, в России отсутствуют нормативные акты, аналогичные COPPA или британскому Кодексу проектирования с учетом возраста. Технический регламент Таможенного союза «О безопасности игрушек» (ТР ТС 008/2011) устанавливает требования к физической, химической и биологической безопасности игрушек, однако не регулирует вопросы обработки персональных данных³⁷.

В октябре 2025 г. в Государственной Думе Российской Федерации была вынесена на обсуждение концепция законопроекта о введении обязательной психолого-педагогической экспертизы игрушек, изображающих кино- и анимационных персонажей³⁸. Однако данная инициатива направлена на оценку психологического воздействия игрушек и не затрагивает проблематику защиты персональных данных.

С 1 сентября 2025 г. в России введена обязательная маркировка детских игрушек через систему «Честный знак», что обеспечивает прослеживаемость товаров и

³³ См.: Zhang L., Kolling K. Theory and practice: the protection of children's personal information in China // International Data Privacy Law. 2023. № 09. P. 1–16.

³⁴ См.: Возраст цифрового согласия и способы его проверки // Центр правовой помощи гражданам в цифровой среде ФГУП «ГРЧЦ». URL: <https://4people.grfc.ru/analyt-ics-and-legislation/case-studies/voznrast-cifrovogo-soglasiya-i-sposoby-ego-proverki/> (дата обращения: 30.09.2025).

³⁵ Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (ч. 1). Ст. 3451.

³⁶ См.: Может ли несовершеннолетний студент в возрасте от 14 до 18 лет получать на свой расчетный счет компенсацию за питание за время прохождения практики и давать согласие на обработку персональных данных? // Правовест. URL: <https://pravovest.ru/hotnews/faq/192940> (дата обращения: 30.09.2025).

³⁷ ТР ТС 008/2011 Технический регламент Таможенного союза «О безопасности игрушек», утв. решением Комиссии Таможенного союза от 23.09.2011 № 798 // URL: <https://docs.cntd.ru/document/902303210> (дата обращения: 30.09.2025).

³⁸ ВГД хотят бороться с игрушечными «чудовищами с улыбкой» // ТАСС. URL: <https://tass.ru/ekonomika/25303303> (дата обращения: 30.09.2025).

противодействие контрафакту³⁹. С 1 августа 2025 г. вступил в силу межгосударственный стандарт, систематизирующий классификацию игрушек⁴⁰. Однако данные меры носят преимущественно административно-экономический характер и не направлены непосредственно на защиту прав детей в цифровом пространстве.

Российское правовое регулирование в сфере умных игрушек характеризуется значительным отставанием от ведущих зарубежных юрисдикций. Отсутствуют специальные требования к получению родительского согласия, проведению оценки рисков для прав детей, обеспечению конфиденциальности по умолчанию, ограничению сбора и хранения данных. Данные пробелы создают правовую неопределенность и не обеспечивают должного уровня защиты цифровых прав несовершеннолетних. Проведенный сравнительно-правовой анализ убедительно демонстрирует необходимость разработки специализированного правового регулирования умных устройств, предназначенных для детей. Универсальные нормы законодательства о персональных данных, разработанные без учета специфики IoT-технологий и особой уязвимости несовершеннолетних, оказываются недостаточными для эффективной защиты прав несовершеннолетних в цифровом пространстве.

Ключевыми элементами такого специализированного регулирования должны стать: установление повышенных стандартов безопасности для устройств, предназначенных для детей, включая требования по шифрованию данных, аутентификации пользователей и защите от несанкционированного доступа; введение обязательной оценки воздействия на права детей перед вводом умных игрушек товарный оборот; закрепление принципа «конфиденциальности по умолчанию», предполагающего минимизацию сбора данных и максимальные настройки приватности в базовой конфигурации для таких изделий; установление четких требований к получению информированного родительского согласия с использованием надежных методов верификации; запрет на использование манипулятивных техник и таргетированной рекламы в отношении несовершеннолетних пользователей; создание эффективных механизмов надзора и ответственности за нарушение прав детей в цифровой среде. Для правового регулирования в Российской Федерации представляется целесообразным: внести комплексные изменения в Федеральный закон «О персональных данных», устанавливающие особенности обработки данных детей; разработать технический регламент или национальный стандарт, определяющий требования безопасности для умных игрушек и IoT-устройств для детей; создать систему обязательной сертификации умных игрушек с оценкой соответствия требованиям защиты персональных данных. Только комплексный подход, сочетающий правовое регулирование, технические стандарты, эффективный контроль и повышение осведомленности родителей, может обеспечить баланс между инновационным развитием рынка умных игрушек и защитой фундаментальных прав несовершеннолетних на конфиденциальность и безопасность в цифровую эпоху.

³⁹ Обязательная маркировка игр и игрушек для детей до 14 лет стартует уже этой зимой // КонсультантПлюс. Новости. URL: <https://www.consultant.ru/legalnews/28683/> (дата обращения: 30.09.2025).

⁴⁰ ГОСТ 35099-2024. Игрушки. Классификация. Термины и определения. Toys. Classification. Terms and definitions: межгосударственный стандарт: принят Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 31.07.2024 № 175-П) ; дата введения 01.08.2025. М. : Российский институт стандартизации, 2024. URL: <https://docs.cntd.ru/document/1307065829> (дата обращения: 30.09.2025).

БИБЛИОГРАФИЯ

1. В ГД хотят бороться с игрушечными «чудовищами с улыбкой» // ТАСС. — URL: <https://tass.ru/ekonomika/25303303> (дата обращения: 30.09.2025).
2. В ходе атаки на VTech скомпрометированы данные 11 млн пользователей // Security Lab.ru. — URL: <https://www.securitylab.ru/news/477140.php?ysclid=mgxqddfpiq923546527> (дата обращения: 30.09.2025).
3. Возраст цифрового согласия и способы его проверки // Центр правовой помощи гражданам в цифровой среде ФГУП «ГРЧЦ». — URL: <https://4people.grfc.ru/analytics-and-legislation/case-studies/voznrast-cifrovogo-soglasiya-i-sposoby-ego-proverki/> (дата обращения: 30.09.2025).
4. Интернет вещей. Развитие технологий и оценка возможностей перехода на отечественные решения / АНО «Цифровая экономика». — М. : АНО «Цифровая экономика», 2024. — 134 с. — URL: <https://files.data-economy.ru/Docs/IoT-5.pdf> (дата обращения: 30.09.2025).
5. Кучковская Н. В. Развитие права в области IoT // Вопросы российского и международного права. — 2023. — Т. 13. — № 4А. — С. 350–356.
6. Может ли несовершеннолетний студент в возрасте от 14 до 18 лет получать на свой расчетный счет компенсацию за питание за время прохождения практики и давать согласие на обработку персональных данных? // Правовест. — URL: <https://pravovest.ru/hotnews/faq/192940> (дата обращения: 30.09.2025).
7. Недетские проблемы детских игрушек: как уследить за данными ребенка // Kaspersky daily. — URL: <https://www.kaspersky.ru/blog/kids-devices-vulnerabilities/14574/> (дата обращения: 30.09.2025).
8. Обязательная маркировка игр и игрушек для детей до 14 лет стартует уже этой зимой // КонсультантПлюс. Новости. — URL: <https://www.consultant.ru/legalnews/28683/> (дата обращения: 30.09.2025).
9. Плюшевые мишки сболтнули лишнего // Газета.ру. — URL: https://www.gazeta.ru/tech/2017/03/01/10551011/cloud_pets.shtml?ysclid=mgxq9byrul76011297 (дата обращения: 30.09.2025).
10. Размер рынка игрушек — по типу продукта, по мощности, по ценовому диапазону, по использованию, по конечному использованию, по каналу сбыта, прогноз, 2025–2034 гг. // Global Market Insights. — URL: <https://www.gminsights.com/ru/industry-analysis/toy-market> (дата обращения: 30.09.2025).
11. Таможенное оформление игрушек // URL: <https://sbcargo.ru/poleznaya-informatsiya/tamozhennoe-oformlenie-igrushek/#:~:text=о государственной регистрации.,Страны-импортеры,игрушки должны проходить радиочастотную экспертизу> (дата обращения: 30.09.2025).
12. Умные игрушки могут собирать данные о ребенке: как защитить семью от слежки // Компьютерра. — URL: <https://www.computerra.ru/290335/umnye-igrushki-mogut-sobirat-dannye-o-rebenke-kak-zashhitit-semyu-ot-slezhki/> (дата обращения: 30.09.2025).
13. Умные игрушки от Google смогут управлять оборудованием в доме // Умный дом. — URL: <https://dom-automation.ru/umnyj-dom/articles/umnye-igrushki-ot-google-smogut-upravlyat-oborudovaniem-v-dome.html> (дата обращения: 30.09.2025).
14. Умный Мишка (Mishka AI) // ICT Moscow. — URL: <https://ict.moscow/card/mishka-ai-umnyj-mishka/> (дата обращения: 30.09.2025).
15. Age appropriate design: a code of practice for online services // ICO. — URL: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/> (дата обращения: 30.09.2025).
16. Aphore N., Varghese S., Feamster N. Evaluating the Contextual Integrity of Privacy Regulation: Parents» IoT Toy Privacy Norms Versus COPPA // The Proceedings of the 28th USENIX Security Symposium. Santa Clara. — 2019. — P. 123–140.
17. California Assembly Bill 2273 (Age-Appropriate Design Code Act) // California Legislative Information. — 2022. — URL: <https://legiscan.com/CA/text/AB2273/id/2606836> (дата обращения: 30.09.2025).

18. *Castelli P. R.* Are interactive toys spying on young children // IBSA Foundation for scientific research. — URL: <https://www.ibsafoundation.org/en/blog/games-for-children-secretly-collect-data> (дата обращения: 30.09.2025).
19. Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501–6506 (COPPA). — URL: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> (дата обращения: 30.09.2025).
20. Chinese toymaker accused of violating children's privacy in U.S., products also sold in Canada // CTVNews. — URL: <https://www.ctvnews.ca/canada/article/chinese-toymaker-accused-by-us-of-sharing-childrens-data-sells-products-in-canada/> (дата обращения: 30.09.2025).
21. Consumer Notice: Internet-connected Toys Could Present Privacy and Contact Concerns for Children // TowneBank. — URL: <https://www.townebank.com/personal/resource/security/digital/internet-toys/> (дата обращения: 30.09.2025).
22. Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act // An official website of the United States government. — URL: <https://www.ftc.gov/news-events/news/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated-childrens-privacy-law-ftc-act> (дата обращения: 30.09.2025).
23. *Fantinato M., Albuquerque A. P., Yankson B.* A Literature Survey on Smart Toy-related Children's Privacy Risks // Proceedings of the 53rd Hawaii International Conference on System Sciences. Hawaii. — 2020. — P. 1479–1488.
24. More toy innovations coming out of China: industry expert // ChinaDaily. — URL: <https://www.chinadaily.com.cn/a/201902/19/WS5c6b934ca3106c65c34ea1db.html> (дата обращения: 30.09.2025).
25. *Pavliv V., Akbari N., Wagner I.* AI-powered smart toys: interactive friends or surveillance devices? // Proceedings of the 14th International Conference on the Internet of Things. Oulu. — 2025. — P. 172–175.
26. Smart toy vulnerabilities can put your child at risk of abuse by strangers // Insomnihack. — URL: <https://insomnihack.ch/talks/smart-toy-vulnerabilities-can-put-your-child-at-risk-of-abuse-by-strangers/> (дата обращения: 30.09.2025).
27. Smart toy vulnerabilities could let cybercriminals video-chat with kids // Kaspersky. — URL: <https://www.kaspersky.com/about/press-releases/smart-toy-vulnerabilities-could-let-cybercriminals-video-chat-with-kids> (дата обращения: 30.09.2025).
28. Smart Toys: Navigating fun and security challenges in the digital age // KidsNetGuard. — URL: <https://kidsnetguard.com/en/2024/05/09/smart-toys-navigating-fun-and-security-challenges-in-the-digital-age/> (дата обращения: 30.09.2025).
29. *Zhang L., Kolling K.* Theory and practice: the protection of children's personal information in China // International Data Privacy Law. — 2023. — № 09. — P. 1–16.

REFERENCES

1. The State Duma wants to fight toy «monsters with a smile». TASS. Available at: <https://tass.ru/ekonomika/25303303> [Accessed 20.09.2025]. (In Russ.).
2. During the attack on VTech, the data of 11 million users was compromised. Available at: *SecurityLab.ru*. Available at: <https://www.securitylab.ru/news/477140.php?ysclid=mgxqddfp-jq923546527> [Accessed 30.09.2025]. (In Russ.).
3. Age of digital consent and ways to verify it. Center for Legal Assistance to Citizens in the Digital Environment FSUE «GRChTs». Available at: <https://4people.grfc.ru/analytics-and-legislation/case-studies/vozrast-cifrovogo-soglasiya--i-sposoby-ego-proverki/> [Accessed 30.09.2025]. (In Russ.).
4. Internet of Things. Development of technologies and assessment of opportunities for transition to domestic solutions. Moscow: ANO Tsifrovaya ekonomika; 2024. Available at: <https://files.data-economy.ru/Docs/IoT-5.pdf> [Accessed 30.09.2025].
5. *Kuchkovskaya NV.* Development of IoT Law. *Issues of Russian and International Law*. 2023;13(4A):350-356. (In Russ.).

6. Can a minor student aged 14 to 18 receive compensation for food for the duration of the internship and agree to the processing of personal data? Pravovest. Available at: <https://pravovest.ru/hotnews/faq/192940> [Accessed 30.09.2025].
7. Childish problems of children's toys: how to keep track of a child's data. Kaspersky daily. Available at: <https://www.kaspersky.ru/blog/kids-devices-vulnerabilities/14574/> [Accessed 30.09.2025]. (In Russ.).
8. Mandatory labeling of games and toys for children under 14 starts this winter. Consultant Plus. News. Available at: <https://www.consultant.ru/legalnews/28683/> [Accessed 30.09.2025]. (In Russ.).
9. Teddy bears blabbed too much. Gazeta.ru. Available at: https://www.gazeta.ru/tech/2017/03/01/10551011/cloud_pets.shtml?ysclid=mgxq9byrul76011297 [Accessed 30.09.2025]. (In Russ.).
10. Toy Market Size — By Product Type, By Power, By Price Range, By Use, By End-Use, By Distribution Channel, Forecast, 2025–2034. Global Market Insights. Available at: <https://www.gminsights.com/ru/industry-analysis/toy-market> [Accessed 30.09.2025]. (In Russ.).
11. Customs clearance of toys. Available at: <https://sbcargo.ru/poleznaya-informatsiya/tamozhennoe-oformlenie-igrushek/#:~:text=о государственной регистрации,-Страны-импортеры,игрушки должны проходить радиочастотную экспертизу> [Accessed 30.09.2025]. (In Russ.).
12. Smart toys can collect data on a child: how to protect a family from surveillance. Kompyuterra. Available at: <https://www.computerra.ru/290335/umnye-igrushki-mogut-sobirat-dannye-o-rebenke-kak-zashhitit-semyu-ot-slezhki/> [Accessed 30.09.2025].
13. Smart toys from Google will be able to control equipment in the house. Smart Home. Available at: <https://dom-automation.ru/umnyj-dom/articles/umnye-igrushki-ot-google-smogut-upravlyat-oborudovaniem-v-dome.html> [Accessed 30.09.2025].
14. Mishka AI. ICT Moscow. Available at: <https://ict.moscow/card/mishka-ai-umnyj-mishka/> [Accessed 30.09.2025].
15. Age appropriate design: a code of practice for online services. ICO. Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/> [Accessed 30.09.2025].
16. Aphore N, Varghese S, Feamster N. Evaluating the Contextual Integrity of Privacy Regulation: Parents» IoT Toy Privacy Norms Versus COPPA. *The Proceedings of the 28th USENIX Security Symposium*. Santa Clara. 2019;123-140.
17. California Assembly Bill 2273 (Age-Appropriate Design Code Act). California Legislative Information. 2022. Available at: <https://legiscan.com/CA/text/AB2273/id/2606836> [Accessed 30.09.2025].
18. Castelli P. R. Are interactive toys spying on young children // IBSA Foundation for scientific research. Available at: <https://www.ibsafoundation.org/en/blog/games-for-children-secretly-collect-data> [Accessed 30.09.2025].
19. Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501–6506 (COPPA). Available at: <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa> [Accessed 30.09.2025].
20. Chinese toymaker accused of violating children's privacy in U.S., products also sold in Canada. CTVNews. Available at: <https://www.ctvnews.ca/canada/article/chinese-toymaker-accused-by-us-of-sharing-childrens-data-sells-products-in-canada/> [Accessed 30.09.2025].
21. Consumer Notice: Internet-connected Toys Could Present Privacy and Contact Concerns for Children. TowneBank. Available at: <https://www.townebank.com/personal/resource/security/digital/internet-toys/> [Accessed 30.09.2025].
22. Electronic Toy Maker VTech Settles FTC Allegations that it Violated Children's Privacy Law and the FTC Act. An official website of the United States government. Available at: <https://www.ftc.gov/news-events/news/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated-childrens-privacy-law-ftc-act> [Accessed 30.09.2025].

23. Fantinato M, Albuquerque AP, Yankson B. A Literature Survey on Smart Toy-related Children's Privacy Risks. *Proceedings of the 53rd Hawaii International Conference on System Sciences*. Hawaii. 2020;1479-1488.
24. More toy innovations coming out of China: industry expert. ChinaDaily. Available at: <https://www.chinadaily.com.cn/a/201902/19/WS5c6b934ca3106c65c34ea1db.html> [Accessed 30.09.2025].
25. Pavliv V, Akbari N, Wagner I. AI-powered smart toys: interactive friends or surveillance devices? *Proceedings of the 14th International Conference on the Internet of Things*. Oulu. 2025:172-175.
26. Smart toy vulnerabilities can put your child at risk of abuse by strangers. *Insomnihack*. Available at: <https://insomnihack.ch/talks/smart-toy-vulnerabilities-can-put-your-child-at-risk-of-abuse-by-strangers/> [Accessed 30.09.2025].
27. Smart toy vulnerabilities could let cybercriminals video-chat with kids. Kaspersky. Available at: <https://www.kaspersky.com/about/press-releases/smart-toy-vulnerabilities-could-let-cybercriminals-video-chat-with-kids> [Accessed 30.09.2025].
28. Smart Toys: Navigating fun and security challenges in the digital age. KidsNetGuard. Available at: <https://kidsnetguard.com/en/2024/05/09/smart-toys-navigating-fun-and-security-challenges-in-the-digital-age/> [Accessed 30.09.2025].
29. Zhang L, Kolling K. Theory and practice: the protection of children's personal information in China. *International Data Privacy Law*. 2023;09:1-16.