

Мониторинг международных трендов правового регулирования для развития законодательства в сфере цифровой экономики в России

Ограничение передвижения автономных транспортных средств по дорогам общего пользования, специальные меры для защиты детей в цифровой среде

Мониторинг №4 (Апрель 2024)

Мониторинг подготовлен коллективом экспертов Института экономической политики имени Е. Т. Гайдара (Института Гайдара):

Левашенко А.Д., с.н.с. лаборатории анализа лучших международных практик Института Гайдара;

Гирич М.Г., н.с. лаборатории анализа лучших международных практик Института Гайдара;

Ермохин И.С., н.с. лаборатории анализа лучших международных практик Института Гайдара;

Магомедова О.С., н.с. лаборатории анализа лучших международных практик Института Гайдара;

Малинина Т.А., с.н.с. лаборатории анализа лучших международных практик Института Гайдара

При частичном или полном использовании материалов ссылка на источник обязательна.

«Умею коротко говорить о длинных вещах»

А.П. Чехов

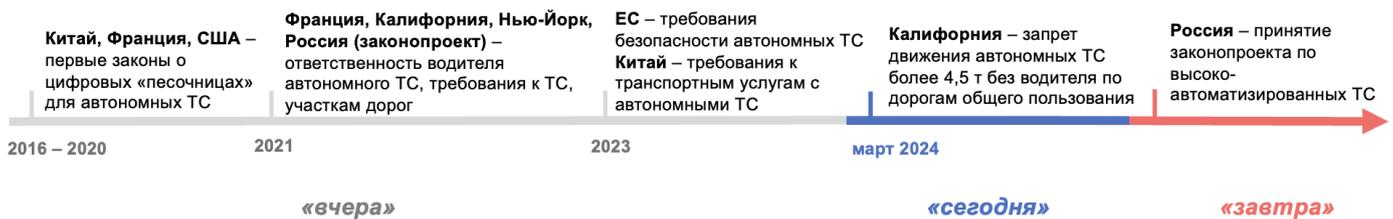
В апреле 2024 г. можно выделить 2 события, которые определяют тренды развития регулирования цифровой экономики.

Тренд №1. Ограничение передвижения автономных транспортных средств по дорогам общего пользования

В апреле 2024 г. в Калифорнии (США) было предложено полностью ограничить движение автономных транспортных средства (далее – ТС) массой более 4,5 т без водителей по дорогам общего пользования. Ряд других стран (Китай, Франция) допускают возможность движения таких ТС, однако при наличии лицензии, соблюдении требований безопасности к участкам дорог и пр.

Тренд

ограничение передвижения автономных транспортных средств на дорогах общего пользования

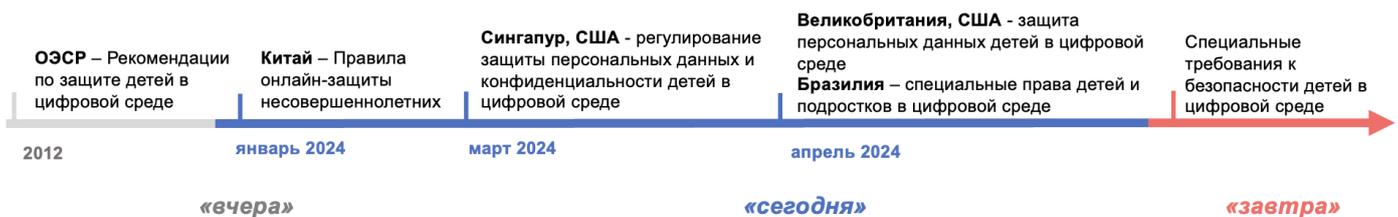


Тренд №2. Специальные меры для защиты детей в цифровой среде

В апреле 2024 г. Великобритания, Бразилия и США одновременно приняли ряд мер для защиты детей и подростков в цифровой среде. С начала 2024 г. Китай и Сингапур уже приняли некоторые из них. Такие меры относятся и к пользователям, и к операторам, предоставляющим онлайн-услуги, включая платформы и соцсети, и выражаются в усилении регулирования: меры против кибербуллинга, мониторинг времени использования цифровых продуктов, минимизация сбора и распространения персональных данных детей.

Тренд

специальные меры для защиты детей в цифровой среде





Ключевые аспекты

1. Ограничение передвижения беспилотных транспортных средств по дорогам общего пользования

В апреле 2024 г. в Калифорнии был предложен законопроект в части ограничения движения ТС массой более 4,5 т без водителей по дорогам общего пользования (фургоны и более тяжеловесные грузовые машины). Законопроект продвигается профсоюзом водителей грузовиков, которые рискуют потерять рабочие места из-за использования беспилотных грузовиков.

Во Франции движение таких беспилотников возможно только по специальным дорогам, в Китае – при наличии удаленного оператора, в большинстве штатов США такому ТС может быть отказано в разрешении на передвижение.

ОЭСР и МТФ¹ используют классификацию автоматизированных транспортных средств, выделяя 6 уровней². С учетом уровня автоматизации определяется, кто берет на себя управление – от частичной автоматизации (уровень 0) до полного автоматизированного управления без водителя по любым дорогам (уровень 5). В ЕС с 2024 года все новые транспортные средства должны оснащаться системами экстренного торможения и удержания на

полосе движения, что фактически делает невозможным покупку нового автомобиля без автоматизации 1 уровня.

Опыт ЕС, США, Китая и Франции

Общая тенденция – выработка требований безопасности для беспилотных ТС 3 и 4 уровня и повышенные требования к ТС 5 уровня:

1) соответствие техническим требованиям к системам, заменяющим управление водителем – сигнализация, рулевое управление, ускорение и торможение (ЕС, Калифорния, Франция);

2) наличие систем информирования в режиме реального времени о состоянии ТС и окружающей местности (ЕС, Франция). Во Франции такие данные используются для анализа аварий – производитель автоматизированного ТС обязан обеспечить доступ к данным;

3) наличие системы контроля водителя, позволяющей оценить, в состоянии ли он взять на себя управление ТС, например, в случае риска аварийной ситуации (ЕС, Франция, Калифорния, Невада). Если водитель не реагирует, ТС должно остановиться (Калифорния);

Таблица – 6 уровней автоматизации ТС

Уровень	Уровень 0	Уровень 1	Уровень 2	Уровень 3	Уровень 4	Уровень 5
Функция контроля	водитель управляет ТС, отдельные функции выполняются автоматизировано			водитель контролирует ТС, только если ТС запрашивает	полностью автоматизированное вождение, водитель может отсутствовать	
	Функции поддержки водителей			Функции автоматизированного вождения		
Как реализуются функции?	выдача предупреждений и мгновенная помощь водителю	поддержка рулевого управления ИЛИ торможения / ускорения	поддержка рулевого управления И торможения / ускорения	водитель берет управление, если ТС запрашивает	автоматизированное управление ТС в любых условиях	
Примеры	– автоматическое экстренное торможение – предупреждение о выезде с полосы движения	– центрирование полосы движения ИЛИ – адаптивный круиз	– центрирование полосы движения И – адаптивный круиз	автоматизация при нахождении водителя за рулем	– передвижение на выделенных дорогах – могут отсутствовать педали и руль	аналогично уровню 4, но ТС может перемещаться без водителя по любым дорогам

¹ Международный транспортный форум

² <https://www.itf-oecd.org/sites/default/files/docs/preparing-infrastructure-automated-vehicles.pdf>

4) определение производителем условий (географических, погодных, дорожных и пр.), при которых может осуществляться автоматизированное управление ТС (Франция);

5) определение условий, при которых автоматизированная система ТС включает аварийный маневр в случае риска столкновения (Франция).

При этом в ЕС для ТС 5 уровня необходимо иметь регистраторы данных о событиях, связанных с передвижением ТС (маршрут, барьеры, риски аварий, данные об управлении и пр.), системы информирования о безопасности других участников дорожного движения (например отсутствие водителя);

6) наличие механизма включения и отключения автоматизированного управления (Калифорния, Нью-Йорк, Невада);

7) соответствие правилам защиты от кибератак, несанкционированных вторжений и ложных команд (Калифорния, Нью-Йорк). В Калифорнии ТС должно иметь отдельный механизм для сбора и хранения данных за 30 секунд до столкновения с чем бы то ни было.

8) маркировка автономных ТС (Китай);

Стоит отметить, что подход Китая несколько отличается от других стран. Там предусмотрено лицензирование услуг общественного пассажирского транспорта и грузового транспорта, оказываемых с использованием ТС 3 – 5 уровней автоматизации. Оператор должен внедрить систему управления эксплуатационной безопасностью, включая безопасность деятельности сотрудников, расследование угроз, управление сетевой безопасностью, планы реагирования на чрезвычайные ситуации.

Чтобы запустить по дорогам такие ТС, страны предъявляют следующие условия:

1) высоко или полностью автоматизированные ТС должны ездить только по специальным выделенным полосам или маршрутам (Франция, Китай), либо производитель должен получить разрешение на использование автоматизированных ТС на дорогах общего пользования (штаты США).

Во Франции назначается специальный оператор таких маршрутов, который осуществляет организацию маршрута, проводит оценку безопасности маршрута в

уполномоченных организациях, получает у префекта разрешение на введение в действие маршрута. В Калифорнии и Неваде отсутствуют выделенные дороги для автоматизированных ТС, однако производители ТС должны получить разрешение на введение в эксплуатацию ТС на дорогах общего пользования (может быть установлено требование обязательного присутствия водителя).

В Китае во время перевозки в автономных ТС должен находиться как минимум оператор (водитель или лицо, отвечающее за безопасность), например, грузовых автономных ТС, а полностью автономные такси с разрешения местных властей в отведенных местах могут эксплуатироваться без водителей, но с удаленным контролем. Один оператор вправе контролировать одновременно не более 3 транспортных средств;

2) производитель должен протестировать автоматизированное ТС на дорогах общего пользования (Калифорния, Нью-Йорк, Невада).

В Китае оператор автономных ТС обязан создать систему гарантий безопасности перевозок перед началом эксплуатации ТС, например, путем подписания соглашения с производителями, инспекторами по безопасности и т.д.;

3) производитель должен иметь страховку на сумму от 5 млн долл. (Калифорния, Невада, Нью-Йорк).

Также устанавливаются требования к дорожным системам/полосам, которые используются для движения автоматизированного ТС:

1) дорожные системы/полосы должны быть спроектированы так, чтобы избежать несчастных случаев (Франция). В Нью-Йорке требуется сертификат разработчика ТС, подтверждающий, что ТС будет более безопасно, чем водитель-человек;

2) иметь системы выявления неисправностей, рисков выхода ТС за пределы выделенной дороги, информирования об этом оператора (Франция);

3) в случае ДТП должен проводиться анализ всех рисков и причин события (Франция, Калифорния, Нью-Йорк).

Во Франции о всех дорожных происшествиях оператор системы

докладывает префекту, в Нью-Йорке и Калифорнии (законопроект) – сообщают производители ТС дорожным органам штата;

4) проводится ежегодный аудит безопасности (Франция).

Что касается ответственности лица, управляющего ТС, то во Франции на водителя не возлагается уголовная ответственность в случае правонарушений, если ТС управляет автоматизированная система (для уровней 3 - 5).

Водитель несет ответственность за ДТП, если: (1) берет на себя управление ТС; (2) не берет на себя управление ТС по запросу автоматизированной системы; (3) водитель не соблюдает предписания правоохранительных органов. Нахождение в состоянии алкогольного опьянения также наказывается. Аналогичный режим ответственности предложен Калифорнией в апреле 2024 г.

В Китае в рамках специальной экономической зоны Шэньчжэнь³ приняты правила ответственности: (1) если ТС управляется водителем – ответственность за аварию несет водитель; (2) если водитель отсутствует – несет владелец или управляющий (оператор) ТС. Если ТС нанесло ущерб из-за неисправности, то компенсацию потерпевшему платит водитель (владелец или оператор), которые далее вправе потребовать возмещение с продавца, изготовителя или дилера ТС.

Опыт России

В России дважды предлагались законы о ВАТС (высокоавтоматизированных транспортных средств) в 2021 г. и 2022 г. (сегодня – действует регулирование только экспериментальных правовых режимов).

В рамках законопроектов предлагалось возложить ответственность за ДТП на владельца ВАТС, при этом бремя доказывания отсутствия вины или вины других участников (оператора, разработчика, дилера) также было возложено на владельца ВАТС. В штатах США и Франции водитель не несет ответственность, если в момент происшествия ТС управлялось автоматизировано. Минтранс заявил о

подготовке обновлений законопроекта в 2024 г.

Постановление Правительства РФ от 09.03.2022 № 309 (экспериментальный правовой режим для ВАТС) также устанавливает требования безопасности: ВАТС должно содержать систему управления, обеспечивающую соблюдение ПДД, осуществлять контроль дорожно-транспортной обстановки, безопасно и предсказуемо взаимодействовать с другими участниками дорожного движения, может диагностировать собственные неисправности и т.д. По каждому ВАТС в рамках ЭПР должен быть застрахован риск ответственности за причинение вреда жизни, здоровью или имуществу других лиц на 10 млн руб.

Владелец (оператор) ВАТС в рамках ЭПР обязан вести постоянный удаленный мониторинг, если ВАТС осуществляет движение без водителя в салоне (только с удаленной маршрутизацией и диспетчеризацией) – регулируется 4 уровень автоматизации ТС.

Таким образом, в России действует ограниченное ЭПР регулирование с возможностью проезда по выделенным дорогам без водителя при условии удаленного мониторинга ТС. В зарубежных странах ответственность за ДТП несет водитель (есть случаи исключения ответственности), тогда как в России – владелец ТС (или изготовитель за недостоверную информацию). При этом неясно, будет ли нести ответственность диспетчер (дистанционно мониторинг состояние ТС) или дилер (осуществляет технический осмотр и ремонт ВАТС), если авария произошла по их вине.

2. Специальные меры для защиты детей в цифровой среде

Опыт Великобритании, США, Китая, Сингапура, ЕС

В апреле 2024 г. в Великобритании опубликованы приоритеты на 2024–2025 гг. по защите персональной информации детей в цифровой среде⁴, а в США внесен проект

³ Правила управления интеллектуальными подключенными ТС 2022 г.

⁴ <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/04/ico-sets-out-priorities-to-protect-childrens-privacy-online/>

закона о защите конфиденциальности данных о детях и подростках онлайн⁵ (еще один законопроект был внесен в марте⁶), в Бразилии принято Постановление по правам детей и подростков в цифровой среде⁷. Кроме того, в январе 2024 г. в Китае⁸ вступили в силу правила онлайн-защиты детей, а в марте 2024 г. в Сингапуре принято руководство о защите персональных данных детей в цифровой среде⁹. Таким образом, налицо тенденция к усилению защиты в цифровой среде детей путем уточнения мер регулирования.

Меры демонстрируют расширение сферы регулирования в части:

а) возраста пользователей (США, Сингапур, Китай, Франция). Например, верификация возраста, ограничение к онлайн услугам / соцсетям в зависимости от возраста, ограничение сбора персональных данных;

б) продуктов: один из законопроектов в США предлагает распространить обязанности по защите несовершеннолетних на поставщиков онлайн- и мобильных приложений.

Меры в разных странах и регионах мира в целом схожи и включают:

1. Запрещенные (например, вовлечение детей в увеличение трафика онлайн-сервиса – Великобритания, США, Китай) и ограниченные практики (например, показ вредного для здоровья контента – Великобритания, Китай; целевой рекламы – Великобритания, США; контроль времени использования сервиса – Китай, Франция).

Вместе с тем подходы к реализации ограничений варьируют от запрещающих в Китае до относительно мягких в Европе и США. Так, в Китае использование онлайн-игр ограничено указанием конкретного времени (например, в выходные), тогда как во Франции предполагается система, регулярно уведомляющая пользователя о продолжительности использования соцсети. В ЕС запрещается использование данных детей для персонализированной рекламы.

Различаются и подходы к родительскому контролю: в Китае для онлайн аудио- и видео-сервисов, соцсетей он обязателен, тогда как в Великобритании это опция, при работе которой поставщик должен информировать об этом ребенка;

2. Повышенные требования к конфиденциальности, в т.ч.:

а) Защита данных заложена на этапе проектирования продукта (Великобритания, Сингапур, Китай, планы ЕС);

б) Оценка воздействия онлайн-защиты (Великобритания, Китай), рисков нарушения прав детей (ЕС) – например, какая именно информация собирается и как именно она используется;

в) Защита данных детей должна распространяться не только на продукты, разработанные специально для детей, но и на другие продукты, к которым дети имеют реальный доступ – соцсети, EdTech, онлайн-игры (США, Сингапур);

г) Отключение по умолчанию геолокации, для ограничения возможности определения местоположения ребенка, например, в соцсетях (Великобритания, США, Сингапур);

д) Соответствующий возрасту язык информации об использовании данных пользователей (Великобритания, Сингапур);

е) Возраст самостоятельного предоставления данных онлайн-сервисам – обычно 13 лет, но в Сингапуре операторы могут устанавливать более высокий возрастной порог, а во Франции для аккаунтов в соцсетях – 15 лет¹⁰;

3. Повышенные требования к сохранности данных, в т.ч. минимизация сбора и распространения данных несовершеннолетних (Великобритания, США, Сингапур, Китай), возможность изменения и удаления таких данных (США, Китай).

Опыт России

В России Закон «О защите детей от информации, причиняющей вред их

⁵ <https://www.congress.gov/bill/118th-congress/house-bill/7890/text?s=1&r=89>

⁶ <https://www.congress.gov/bill/118th-congress/house-bill/7534/text?s=1&r=87>

⁷ <https://www.loc.gov/item/global-legal-monitor/2024-04-14/brazil-rights-of-children-and-adolescents-in-digital-environments-regulated/>

⁸ https://english.www.gov.cn/policies/latestreleases/202310/24/content_WS6537a5d2c6d0868f4e8e095e.html

⁹ <https://www.pdpc.gov.sg/guidelines-and-consultation/2024/03/advisory-guidelines-on-the-pdpc-for-childrens-personal-data-in-the-digital-environment>

¹⁰ <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533>

здоровью и развитию» запрещает распространять среди детей информацию: побуждающую к причинению вреда здоровью или жизни, склоняющую к участию в азартных играх, оправдывающую насилие и жестокость. Определенная информация, например, вызывающая страх или панику, ограничена возрастными категориями. Эти требования распространяются на Интернет. Вместе с тем меры для защиты детей шире

ограничений на распространение информации, в этом смысле Россия отстает от наиболее значимых мировых тенденций. Например, отсутствуют меры против кибербуллинга, отслеживания детей через геолокацию (например, отключение геолокации для аккаунтов детей в соцсетях).