IoT-регулирование и статус данных

Карен КАЗАРЯН,
директор по аналитике АНО «Цифровая экономика»

Данные принято подразделять на генерируемые устройствами (machine generated-data) и людьми (human-generated data). Генерируемые устройствами данные создаются в автоматическом режиме без участия человека. К ним относятся, в частности, системные журналы различных операционных систем и ПО, телекоммуникационные данные. Наиболее яркий пример – данные, полученные от устройств Интернета вещей, бизнес-модель которого предусматривает автоматический сбор данных с помощью датчиков, сенсоров, носимых устройств и т. д. с целью мониторинга, повышения качества предоставляемых услуг или пользовательского опыта. Рассмотрим подходы к определению правового статуса данных на примере опыта разных стран.

Данные особой ценности

К данным Интернета вещей, представляющим особую ценность для развития экономики данных, IBM относит:

- данные о местонахождении человека или объекта, полученные посредством использования технологий GPS, Wi-Fi и т. п.;
- данные о состоянии окружающей среды (температура, давление, влажность, скорость ветра и т. п.);
- данные о состоянии отдельных компонентов устройства и параметрах его функционирования (диагностическая информация, данные мониторинга процессов работы и др.);
- данные о состоянии живого организма, полученные с носимых устройств (пульс, температура, кровяное давление и т. д.);
- данные о перемещении или расположении объекта в пространстве (показания акселерометра и т. п.).

Промышленные данные в большой степени – продукт применения технологий Интернета вещей на промышленных предприятиях (индустриальный Интернет вещей, или IIoT), где сбор информации о работе устройств посредством различных датчиков, сенсоров и т. д. и ее последующая обработка позволяют компании приобрести объективные и точные данные о состоянии предприятия. Полученная информация может быть использована для предотвращения простоев, поломок оборудования, сокращения внепланового техобслуживания и сбоев в управлении цепочками поставок, благодаря чему предприятие может функционировать более эффективно.

Под данными, генерируемыми устройствами (промышленными данными), понимаются данные, которые создаются без вмешательства человека посредством вычислительных процессов, приложений, сервисов, сенсоров, программного обеспечения либо оборудования и т. п. Такие данные могут относиться к персональным, если отвечают критериям идентифицируемости. В подобном случае к их обработке будут применяться положения законодательства о защите персональных данных. Если данные полностью обезличены (анонимизированы) либо изначально не имели идентифицирующего свойства, то они не признаются персональными и могут обрабатываться без соблюдения требований к защите персональных данных.

Инициативы Еврокомиссии

Европейский Союз – одна из основных юрисдикций, которая рассчитывает на масштабное применение технологий Интернета вещей и данных, созданных без участия человека. В Сообщении Европейской Комиссии 2017 г. «Построение европейской экономики данных» отдельное внимание уделено вопросам определения правового статуса данных, генерируемых устройствами.

Для обсуждения Еврокомиссия предложила следующие возможные варианты достижения обозначенных целей регулирования:

- стимулирование разработки технических решений для обмена данными и идентификации их источников. Для повышения доверия к системе обмена и обеспечения

прослеживаемости необходимы надежные и стандартизированные протоколы с целью идентификации источников данных. Открытые стандартизированные API-интерфейсы могут способствовать развитию экосистемы разработчиков приложений и алгоритмов, заинтересованных в данных, которые хранятся в компаниях, а также помочь частным компаниям и государственным органам определять различные типы хранящихся у них данных и коммерциализировать их повторное использование;
– признавая необходимость выработки новых подходов к регулированию договорных отношений в области обработки данных, для снятия правовых барьеров для малых и средних предприятий и уменьшения дисбаланса в переговорных позициях с сохранением принципа свободы договора, Еврокомиссия предложила разработать шаблоны контрактов, которые включили бы в себя лучшие практики в сфере оборота данных;
– предоставление свободного доступа органам публичной власти к данным, генерируемым без участия человека, при наличии общего интереса (например, в целях повышения эффективности государственного управления, здравоохранения и т. п.), а также в научных и статистических целях;
– в целях правового определения принадлежности прав на данные предложено закрепить «право производителя данных» (data producer's right), которое предоставляет возможность использовать и предоставлять другим лицам право использования неперсональных данных, генерируемых устройствами. В качестве правообладателя может выступать лицо, являющееся собственником, или лицо, использующее устройство, оснащенное соответствующими сенсорами, на свой экономический риск.

При этом необходимо включить в разрабатываемые шаблоны контрактов правовые обязательства поставщика услуг обеспечивать переносимость данных клиента для облегчения процесса смены поставщика. Рекомендуется разработать систему прав на переносимость неперсональных данных, по аналогии с правами, закрепленными в ст. 20 GDPR в отношении персональных данных, а также стандарты переносимости данных с учетом отраслевой специфики на основе экспериментального подхода с вовлечением всех заинтересованных сторон.

Оборот неперсональных данных

Регламент 2018/1807 об основах свободного обмена неперсональными данными внутри ЕС, вступивший в силу 28 мая 2019 г., концентрируется на трех аспектах оборота неперсональных данных:
– обеспечение свободного трансграничного перемещения неперсональных данных внутри ЕС посредством ограничения возможности стран – членов ЕС устанавливать требования по локализации данных на уровне национального законодательства. Подобные требования допустимы только по соображениям национальной безопасности с соблюдением принципа пропорциональности (ст. 4);
– стимулирование переносимости данных посредством внедрения кодексов поведения и иных инструментов саморегулирования с целью предоставления пользователям возможностей для беспрепятственной смены провайдеров информационных услуг (ст. 6);
– сохранение действия требований по обеспечению безопасности, которые уже применяются к лицам, хранящим и обрабатывающим данные, в случае обработки данных за пределами ЕС или в облаках (п. 34 Преамбулы);
– обеспечение беспрепятственного доступа органов публичной власти к неперсональным данным для выполнения их контрольно-надзорных функций (ст. 5).

Американский опыт

Необходимость регулирования Интернета вещей достаточно длительный период активно обсуждалась в США. Однако единого федерального закона, который относился бы к данной сфере, до недавнего времени не было. Ситуация изменилась в декабре 2020 г. с принятием Закона о совершенствовании кибербезопасности Интернета вещей. Документ устанавливает минимальные стандарты безопасности для устройств Интернета вещей, находящихся под контролем правительства США. В законе рассматриваются вопросы использования таких устройств, способы управления и обслуживания, система отчетности об уязвимостях. Требования закона и сопутствующих ему стандартов, которые разработаны Национальным институтом стандартов и технологий США (NIST), распространяются на всех разработчиков и поставщиков устройств Интернета вещей и соответствующих услуг структурам федерального правительства.

IoT Act охватывает разработку, управление, настройку и установку исправлений для устройств IoT, гарантируя, что кибербезопасность остается в центре внимания на протяжении всего жизненного цикла.

Основные требования Закона включают в себя:
– обязательство NIST опубликовать стандарты надлежащего применения устройств Интернета вещей для федеральных органов власти. Помимо прочего, в них должны быть описаны требования к безопасности таких устройств. Стандарты предполагается пересматривать раз в пять лет. NIST также должен будет при участии представителей промышленности и научных кругов разработать процедуры получения и публикации информации об уязвимостях в устройствах Интернета вещей;
– обязанность подрядчиков и субподрядчиков, участвующих в государственных проектах, сообщать о новых уязвимостях и устранять их по мере

возникновения. NIST, в свою очередь, должен разработать руководство по раскрытию и устранению уязвимостей устройств Интернета вещей;
- необходимость разработки политик и принципов информационной безопасности федеральных органов, согласованных со стандартами и принципами NIST;
- пересмотр положения о федеральных закупках;
- соответствие подрядчиков и субподрядчиков стандартам NIST, запрет на заключение или продление контрактов с подрядчиками, не соответствующими стандартам (начиная с декабря 2022 г.).

Уже в декабре 2020 г. NIST представил четыре документа, которые в совокупности составляют руководство для производителей устройств Интернета вещей и для федеральных агентств, использующих такие устройства. В частности, до вступления Закона в силу в декабре 2022 г. организациям предстояло сделать следующее:
- производители должны изучить руководства и стандарты и разработать соответствующую им документацию для устройств. Также необходимо спланировать разработку процессов публичной отчетности об уязвимостях устройств и повышения их безопасности;
- федеральные подрядчики должны идентифицировать информационные системы, использующие устройства Интернета вещей, и предусмотреть пути выполнения рекомендаций и стандартов NIST, в том числе посредством соответствующей адаптации спецификаций устройств, процессов выбора поставщиков и контрактных требований;
- организации, не являющиеся федеральными подрядчиками, должны учитывать влияние стандартов и рекомендации NIST на соблюдение ими законов о кибербезопасности, требующих разумных мер безопасности для защищенной информации в зависимости от сценариев использования.

Принятие закона оказало косвенное влияние на частные компании, использующие устройства Интернета вещей, поскольку у них есть выбор между приобретением устройств и систем, соответствующих федеральным требованиям, и приобретением не столь защищенных с точки зрения закона устройств.

Китайский правовой ландшафт

В Китае развитие рынка Интернета вещей – одно из важнейших направлений государственной политики в области инновационного развития. В 2013 г. Государственный совет Китая выпустил Руководство по развитию Интернета вещей, в котором IoT назван технологией нового поколения, способной фундаментально улучшить жизнь и условия труда людей.

Несмотря на это, отдельный правовой ландшафт для Интернета вещей в Китае отсутствует. Как один из ключевых сегментов с точки зрения национальной безопасности, телекоммуникационной сектор в Китае находится под пристальным вниманием властей. И требования, относящиеся к телекоммуникационному сегменту, отчасти распространяются на сферу Интернета вещей, однако применимость данных правил зависит от конкретных сценариев использования IoT-устройств.

Министерство промышленности и информатизации КНР выпустило Положение о защите личной информации пользователей электросвязи и Интернета, вступившие в силу 1 сентября 2013 г. Документ предъявляет ряд требований к сбору и использованию персональных данных операторами связи. В то же время Закон о кибербезопасности Китая предусматривает принятие технических и других необходимых мер для обеспечения стабильной работы сетей, эффективного реагирования на инциденты, связанные с безопасностью сетей, предотвращения незаконных и преступных действий, а также поддержания целостности, конфиденциальности и доступности сетевых данных со стороны операторов сетей и поставщиков сетевых услуг (включая операторов связи).

Регуляторным направлением, связанным непосредственно с областью Интернета вещей в Китае, является стандартизация. Министерство промышленности и информатизации КНР в январе 2021 г. выпустило проект Рекомендаций по разработке базовых стандартных систем безопасности для Интернета вещей. Проект предполагает разработку системы базовых стандартов для Интернета вещей, к 2025 г. ожидается разработка еще более 30 стандартов, направленных на повышение уровня безопасности межотраслевых приложений Интернета вещей.

Безбарьерная регуляторная среда

В России с 2021 г. обсуждаются вопросы регулирования оборота промышленных данных и данных Интернета вещей. Если три года назад возможное регулирование обсуждалось, в основном, в контексте безопасности и ужесточения принципов оборота, то в рамках работы над Стратегией развития искусственного интеллекта в России больше говорят о снятии регуляторных барьеров, препятствующих использованию промышленных данных в обучении моделей ИИ и внедрении сервисов на основе анализа больших данных на предприятиях.

В центре внимания также снятие ограничений на сбор и обработку промышленных данных, в том числе в облаках, решение вопросов безопасной передачи промышленных данных, возникновения прав на них, а также публикации отдельных видов промышленных данных.

Аналогичные ограничения на промышленные данные можно найти и в отраслях строительства, ЖКХ, транспорта. Комплексное решение указанных регуляторных барьеров необходимо для успешной реализации национального проекта «Экономика данных и цифровая трансформация государства» в России. ■