

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЕС

И БУДУЩЕЕ ТЕХНОЛОГИЧЕСКОЙ КОНКУРЕНЦИИ



ГРИНЯЕВ СЕРГЕЙ НИКОЛАЕВИЧ

МОСКВА • 2026

Сергей Гриняев

**Цифровая трансформация
ЕС и будущее
технологической конкуренции**

«Автор»

2026

Гриняев С.

Цифровая трансформация ЕС и будущее технологической конкуренции / С. Гриняев — «Автор», 2026

Книга посвящена цифровой трансформации Европейского союза как проекту экономической модернизации, политической интеграции и технологической субъектности. Она прослеживает путь ЕС от стратегии Единого цифрового рынка к программе «Цифровое десятилетие — 2030», анализирует регулирование платформ, данных и искусственного интеллекта, развитие сетей, облаков, суперкомпьютеров, полупроводников и цифрового государства. Особое внимание уделено национальным моделям, человеческому капиталу, социальному неравенству, кибербезопасности, оборонным технологиям и зависимости Европы от США, Китая и азиатских цепочек поставок. Показано, что ЕС добился значительной нормативной и институциональной силы, однако сталкивается с фрагментацией рынка, дефицитом кадров, слабым масштабированием компаний и внешними технологическими зависимостями. Книга адресована исследователям, студентам, государственным служащим и всем, кто стремится понять связь цифровизации, суверенитета, прав человека и геополитики.

© Гриняев С., 2026

© Автор, 2026

Содержание

Введение. Европа перед цифровым зеркалом	5
Часть I. Стратегия и институты	10
Часть II. Право и регулирование	22
Конец ознакомительного фрагмента.	30

Цифровая трансформация ЕС и будущее технологической конкуренции

Введение. Европа перед цифровым зеркалом

Европейский союз привык описывать себя языком ценностей: свобода, достоинство личности, закон, солидарность. В XXI веке к этому перечню добавилось ещё одно слово — **цифровой суверенитет**. Оно звучит почти как термин из дипломатического словаря, но относится к самым обыденным вещам: к смартфону в кармане, банковскому приложению, навигатору, медицинской карте, промышленному роботу, спутниковому сигналу и беспилотнику.

Когда человек открывает интернет-магазин, общается в социальной сети или пользуется облачным хранилищем, он редко думает о том, где физически находятся серверы, кто владеет программным кодом, по каким правилам собираются его данные и кто может отключить услугу в критический момент. Однако для современного государства эти вопросы перестали быть техническими деталями. Они стали вопросами власти, безопасности и экономического будущего.

Цифровая трансформация — это не просто переход от бумаги к экрану. Это изменение способа, которым общество производит товары, управляет городами, лечит людей, ведёт войну, получает образование и принимает политические решения. В цифровой эпохе особое значение приобретают не только природные ресурсы, заводы и вооружения, но и данные, вычислительные мощности, алгоритмы, сети связи, микроэлектроника и специалисты, умеющие всем этим управлять.

Европейский союз вступил в эту эпоху с сильными и слабыми сторонами. Его сильная сторона — огромный рынок, высокий уровень образования, развитая промышленность, мощная научная школа и способность создавать правила, которые вынуждены учитывать даже крупнейшие мировые корпорации. Слабая сторона — раздробленность. Европа состоит из десятков национальных экономик, правовых систем, языков, промышленных традиций и технологических стратегий. Там, где Соединённые Штаты могут опираться на гигантские частные цифровые платформы, а Китай — на сочетание государственной воли, внутреннего рынка и промышленного масштаба, Европейский союз вынужден постоянно согласовывать интересы государств-членов, бизнеса, профсоюзов, регионов и общественных организаций.

Именно поэтому европейская цифровая политика напоминает одновременно лабораторию, парламент и верфь. В лаборатории создаются новые технологии. В парламенте спорят о правах человека, конкуренции и приватности. На верфи пытаются собрать сложное судно — европейскую цифровую систему, способную плыть в бурных водах глобальной конкуренции.

Для России этот опыт важен не потому, что его следует механически копировать. Напротив, он ценен как пример того, какие возможности и ограничения возникают, когда крупное политико-экономическое пространство стремится уменьшить внешнюю зависимость, не разрушая при этом связь науки, промышленности, общества и государства.

Российская Федерация сталкивается с близкими по характеру задачами, хотя решает их в иных условиях. Это развитие собственной микроэлектроники, программного обеспечения, телекоммуникационной инфраструктуры, облачных платформ, искусственного интеллекта, средств киберзащиты и систем управления критически важными объектами. Это также подготовка кадров, защита данных граждан, обеспечение технологической независимости и сохранение возможности самостоятельно определять правила развития в условиях внешнего давления.

Европейский пример позволяет увидеть несколько принципиальных обстоятельств.

Во-первых, цифровой суверенитет нельзя получить простым принятием закона. Закон может установить правила, но не создаст сам по себе процессор, операционную систему, центр обработки данных или школу инженеров. Суверенитет вырастает из длительной связи науки, образования, производства, инвестиций и государственного планирования.

Во-вторых, зависимость редко бывает абсолютной. Ни одна крупная страна или объединение не производит у себя все необходимые компоненты цифровой цивилизации. Речь идёт не об изоляции, а о способности выбирать: иметь критически важные компетенции, диверсифицировать поставки, контролировать наиболее уязвимые звенья и не позволять внешним силам диктовать условия развития.

В-третьих, цифровая независимость не сводится к замене одного иностранного продукта другим. Если национальная система строится только на импортозамещении, но не производит собственных исследований, стандартов, архитектур и конкурентоспособных решений, то она остаётся зависимой — пусть и от другого поставщика.

В-четвёртых, цифровая среда неизбежно затрагивает вопрос о человеке. Чем больше решений передаётся алгоритмам, тем важнее становятся вопросы ответственности, справедливости, прозрачности и контроля. Может ли гражданин узнать, почему ему отказали в кредите? Кто отвечает за ошибку медицинской системы с искусственным интеллектом? Где проходит граница между защитой общества и избыточным наблюдением? Эти вопросы одинаково важны для Европы, России и всего мира.

Книга, которую читатель открывает, посвящена не просто европейским программам, директивам и технологическим компаниям. Её предмет — попытка понять, как в начале XXI века строится цифровая мощь.

Мы увидим, почему Европейский союз стремится стать не только рынком цифровых услуг, но и центром нормотворчества. Разберёмся, как возникли идеи «цифрового десятилетия», «европейских пространств данных», «доверенного искусственного интеллекта» и «суверенного облака». Проследим путь от промышленного робота на немецком заводе до цифрового кошелька гражданина ЕС; от суперкомпьютера до беспилотной системы; от правил для глобальных платформ до вопроса о том, кто владеет данными и вычислительными мощностями.

Но эта книга будет говорить и о трудностях. В цифровой политике Европы много громких целей, однако не все они становятся реальностью с одинаковой скоростью. Европейский союз умеет создавать сложные правовые конструкции, но порой медленнее конкурентов превращает идеи в масштабные коммерческие продукты. Он защищает персональные данные, но зависит от иностранных облачных платформ. Он строит политику в области искусственного интеллекта, но сталкивается с нехваткой специалистов, вычислительных ресурсов и компаний, способных быстро расти на мировом рынке.

И здесь возникает один из главных вопросов нашего исследования: может ли объединение государств стать цифровым центром силы, если его главная технологическая роль заключается в установлении правил для чужих платформ?

Ответ не может быть простым. Европейский союз уже доказал, что правила имеют силу. Но цифровая эпоха требует не только норм, но и машин; не только запретов, но и лабораторий; не только контроля, но и способности создавать новое.

Мир, построенный из кода

Представим себе современный порт. Когда-то его мощь определялась количеством причалов, глубиной фарватера, размерами складов и числом грузовых кранов. Сегодня к этому добавляется невидимый слой: системы навигации, цифровые модели грузопотоков, базы данных, спутниковая связь, автоматизированные таможенные процедуры, датчики состояния контейнеров, программные комплексы управления логистикой.

Если этот невидимый слой перестанет работать, порт может остаться физически целым — с кранами, дорогами, железнодорожными путями и кораблями, — но его способность действо-

вать резко снижается. Контейнеры не получают назначения, диспетчеры теряют достоверную картину, документы не проходят проверку, а цепочка поставок начинает давать сбои.

Так устроена почти вся современная экономика. Цифровые технологии больше не являются отдельной отраслью, подобной текстильной промышленности или судостроению. Они стали средой, в которой работают остальные отрасли.

Сельское хозяйство использует спутниковую навигацию, датчики влажности почвы и системы точного земледелия. Энергетика управляет сложными сетями, в которых постоянно меняются производство и потребление. Транспорт опирается на цифровые платформы планирования маршрутов. Банковская система существует как сеть защищённых коммуникаций и программных решений. Оборона всё сильнее зависит от связи, разведывательной информации, автоматизированного управления, беспилотных комплексов и обработки больших массивов данных.

В такой ситуации слово «цифровой» перестаёт означать только «компьютерный». Оно означает **связанный, управляемый данными, зависящий от алгоритмов**.

Данные часто называют новой нефтью. Это сравнение удобно, но неточно. Нефть сгорает в двигателе. Данные, напротив, могут использоваться многократно. Один и тот же набор сведений о движении транспорта способен помочь городскому планированию, логистике, страхованию, экологическому мониторингу и работе экстренных служб. Но, подобно нефти, данные сами по себе не создают богатства. Нужны средства добычи, переработки, транспортировки и применения. В цифровом мире такими средствами становятся датчики, сети связи, вычислительные центры, программный код, алгоритмы и специалисты.

Важнейшая особенность цифровой экономики состоит в том, что она стремится к концентрации. Чем больше пользователей у платформы, тем больше данных она получает. Чем больше данных, тем лучше она может настраивать свои сервисы. Чем удобнее сервис, тем больше приходит новых пользователей. Возникает замкнутый круг роста.

Именно поэтому крупнейшие цифровые платформы получили такую власть. Они не просто продают товары или показывают рекламу. Они определяют, какие приложения видит пользователь, какие новости попадают в его ленту, как малый бизнес находит покупателей, на каких условиях разработчик получает доступ к аудитории, где хранятся данные организации и какие цифровые инструменты становятся стандартом.

Для государства такая концентрация создаёт сложную дилемму. С одной стороны, крупные платформы удобны, технологически развиты и часто предлагают быстрые решения. С другой — зависимость от них может означать утрату контроля над критическими данными, экономическими потоками и информационной средой.

Европа особенно остро почувствовала эту проблему. На её территории находятся ведущие мировые автопроизводители, машиностроительные концерны, фармацевтические компании, банки и научные центры. Но в списке крупнейших глобальных цифровых платформ долгое время преобладали компании из США и Китая. Европейский рынок был велик, европейский потребитель был платежеспособен, европейская наука была сильна — однако значительная часть цифровой прибыли, данных и инфраструктурных преимуществ концентрировалась за пределами ЕС.

Отсюда и выросла новая европейская повестка: недостаточно быть пользователем цифровой эпохи, необходимо стать одним из её архитекторов.

Три силы цифрового мира

В начале третьего десятилетия XXI века на цифровой карте мира особенно ясно выделились три крупных центра.

Первый — Соединённые Штаты. Их сила строится на сочетании университетов, венчурного капитала, частного предпринимательства, военных исследований и глобальных корпораций. Американская модель умеет быстро превращать научную идею в стартап, стартап —

в платформу, а платформу — в глобальную инфраструктуру. Облачные сервисы, поисковые системы, социальные сети, операционные системы, проектирование полупроводников и значительная часть рынка искусственного интеллекта развиваются здесь в тесном взаимодействии бизнеса, науки и государства.

Второй центр — Китай. Его цифровая модель основана на масштабе внутреннего рынка, мощной промышленной базе, активной государственной политике, инвестициях в телекоммуникации, электронику и искусственный интеллект. Китай создал собственные технологические платформы, развернул широкие сети связи, развивает производство оборудования и стремится закрепиться в международной стандартизации.

Третий центр — Европейский союз. Его путь иной. Европа не располагает равным США числом глобальных цифровых гигантов и не обладает китайской степенью централизованной координации. Зато она располагает другим ресурсом: правом, рынком и способностью устанавливать стандарты.

Если крупная компания хочет работать с сотнями миллионов европейских пользователей, она должна учитывать европейские правила. Так европейское регулирование начинает влиять и на компании, находящиеся далеко за пределами ЕС. Это явление иногда называют «брюссельским эффектом»: нормы, принятые в Брюсселе, становятся ориентиром для глобального бизнеса, потому что разделять продукты и сервисы на «европейские» и «неевропейские» часто дорого и неудобно.

Но право — это не волшебная палочка. Невозможно запретить технологическое отставание одним нормативным актом. Если у страны или объединения нет собственных вычислительных мощностей, инженеров, оборудования, инвестиций и производственных цепочек, то даже самые совершенные правила будут регулировать преимущественно деятельность внешних игроков.

Именно эта двойственность определяет европейский цифровой проект. Европа хочет одновременно защищать граждан, ограничивать монопольную власть платформ, развивать инновации, укреплять промышленность, обеспечивать кибербезопасность и сохранять открытость экономики. Каждая из этих целей разумна. Но вместе они образуют сложную систему противоречий.

Быстрая инновация требует свободы эксперимента. Защита прав требует ограничений и контроля. Промышленная автономия требует поддержки национальных и европейских производителей. Открытый рынок требует конкуренции и недискриминации. Кибербезопасность требует проверки поставщиков и ограничения рисков. Международная торговля требует сотрудничества.

Цифровая политика ЕС — это постоянная попытка удержать равновесие между этими силами.

Российский ракурс

Для российского читателя европейский опыт интересен прежде всего как опыт большого, технологически развитого пространства, вынужденного действовать в условиях зависимости от внешних центров силы.

Россия располагает значительной научной и инженерной школой, сильными компетенциями в математике, программировании, криптографии, ядерных и космических технологиях, системах связи, ряде направлений искусственного интеллекта и кибербезопасности. Одновременно она сталкивается с задачей укрепления собственной производственной и программной базы в условиях ограниченного доступа к части внешних технологий, компонентов, финансовых инструментов и кооперационных цепочек.

Европейский опыт здесь важен в нескольких отношениях.

Он показывает, что цифровая независимость требует долгосрочного планирования. Нельзя построить современную отрасль микроэлектроники за один бюджетный цикл. Нельзя

подготовить поколение инженеров за несколько месяцев. Нельзя добиться доверия к национальным цифровым сервисам, если они неудобны, непрозрачны или не обеспечивают надёжной защиты данных.

Он показывает и другое: национальная или наднациональная стратегия должна быть связана с реальными производственными задачами. Цифровизация ради отчётности быстро превращается в формальность. Другое дело — внедрение технологий в энергетику, транспорт, промышленность, сельское хозяйство, здравоохранение, городское хозяйство, образование и безопасность. Там цифровые решения проверяются не красивой презентацией, а надёжностью, экономическим эффектом и способностью работать в сложных условиях.

Наконец, европейская история напоминает о необходимости различать **технологический суверенитет** и **технологическую автаркию**. Автаркия стремится производить всё внутри собственных границ. Суверенитет означает иное: владеть критическими компетенциями, иметь резервные решения, защищать ключевую инфраструктуру, развивать национальную науку и сохранять свободу политического выбора.

Для России, как и для любой крупной страны, наиболее продуктивна именно такая логика. Цель состоит не в отказе от международного технологического взаимодействия, а в снижении уязвимости там, где зависимость может превратиться в инструмент давления или угрозу безопасности.

Вопрос, с которого начинается путь

Перед Европейским союзом встала задача, которую можно сформулировать очень просто:

может ли общество сохранить политическую самостоятельность, если его цифровая инфраструктура, программные платформы, вычислительные мощности и ключевые технологии принадлежат внешним центрам силы?

Ответ на этот вопрос Европа ищет через законы, инвестиционные программы, промышленную политику, научные проекты, защиту рынка, развитие связи и обучение граждан. Иногда эти попытки дают заметные результаты. Иногда они обнаруживают, что между политической декларацией и технологической реальностью лежит долгий путь.

Этот путь и станет предметом нашего дальнейшего рассказа.

В следующей главе мы обратимся к истокам европейской цифровой стратегии: к тому моменту, когда ЕС понял, что цифровой рынок нельзя строить как набор разрозненных национальных правил, а технологическое будущее требует общей политической воли.

Часть I. Стратегия и институты

Глава 1. От Единого цифрового рынка к «Цифровому десятилетию»

История цифровой трансформации Европейского союза началась не с искусственного интеллекта и не с моды на «цифровой суверенитет». Её истоки лежат в более раннем, на первый взгляд скромном замысле: сделать так, чтобы европейское цифровое пространство перестало быть мозаикой из разрозненных национальных правил, платформенных барьеров и несовместимых режимов регулирования. Именно из этой логики выросла стратегия Единого цифрового рынка — Digital Single Market, или DSM.

За внешне технической формулировкой скрывалась большая политико-экономическая идея. Если в XX веке европейская интеграция строилась вокруг угля, стали, общего рынка и единой валюты, то в XXI веке в центр постепенно переместились данные, сети, облака, цифровые платформы и электронные услуги. ЕС стремился не просто «подключить» экономику к интернету, а превратить цифровую среду в новую форму внутреннего рынка, где товаром становятся не только вещи, но и сервисы, вычислительные ресурсы, программные решения и массивы данных.

Для России в этом процессе важно увидеть не только европейскую специфику, но и более общий урок. Любое крупное политико-экономическое пространство, претендующее на стратегическую самостоятельность, рано или поздно сталкивается с одним и тем же вопросом: можно ли сохранить суверенитет, если ключевые каналы связи, программные стандарты, данные и платформы развиваются вне собственного контура управления? Европейский союз искал ответ именно на этот вопрос, хотя формулировал его языком рынка, прав потребителей, конкуренции и инноваций.

От фрагментации к общему пространству

До середины 2010-х годов цифровая реальность Европы оставалась противоречивой. С одной стороны, ЕС уже имел огромный внутренний рынок, развитую промышленность, сильные университеты и высокий уровень проникновения связи. С другой стороны, цифровая экономика продолжала дробиться по национальным границам. Электронная коммерция, защита данных, телекоммуникационные правила, электронная идентификация, авторское право и налогообложение платформ развивались неравномерно. Для бизнеса это означало дополнительные издержки, а для граждан — неравный доступ к услугам и разную степень цифровой защищённости в зависимости от страны.

Стратегия Digital Single Market была задумана как способ преодолеть эту раздробленность. Её цель состояла в том, чтобы убрать барьеры для трансграничных цифровых услуг, усилить доверие к онлайн-среде, развить цифровую инфраструктуру и заложить основу для новой волны инноваций. По существу, речь шла о переносе классической логики европейской интеграции — свободного движения товаров, услуг, капитала и людей — в цифровую сферу.

Здесь возникла важная особенность европейского подхода. В отличие от США, где цифровая экономика во многом росла снизу вверх под воздействием венчурного капитала и платформенного бизнеса, ЕС делал ставку на нормативное и институциональное выравнивание пространства. Европа пыталась сначала создать общие правила, а затем уже ускорять рынок. Такой подход имел очевидные плюсы: он создавал предсказуемую среду, защищал права пользователей и ограничивал фрагментацию. Но у него был и минус: скорость согласования общеевропейских решений часто уступала темпам технологических изменений. Именно из этого противоречия в дальнейшем вырастет вся драматургия европейской цифровой политики.

Логика стратегии Digital Single Market

Стратегия DSM строилась вокруг нескольких взаимосвязанных направлений. Во-первых, требовалось облегчить трансграничную электронную торговлю и сделать так, чтобы гражданин одной страны ЕС мог пользоваться цифровыми услугами в другой не как иностранным исключением, а как обычным участником общего рынка. Во-вторых, необходимо было создать более справедливые и единообразные условия для бизнеса, работающего в онлайн. В-третьих, Европа стремилась развивать инфраструктуру, цифровые сети и технологические экосистемы, без которых цифровой рынок превращается в юридическую схему без материальной опоры.

Но довольно быстро выяснилось, что цифровой рынок — это не только торговля и услуги. Как только государства и корпорации стали опираться на большие массивы данных, облачные вычисления, промышленные платформы и алгоритмическое управление, цифровая повестка вышла за рамки экономики. Она стала затрагивать общественную безопасность, устойчивость цепочек поставок, контроль над критической инфраструктурой и способность государства сохранять управление в условиях кризиса. Именно поэтому позднее европейская цифровая политика начала использовать более жёсткие понятия: устойчивость, автономия, безопасность, доверенный ИИ, стратегические технологии.

Иначе говоря, Digital Single Market был начальной стадией более широкого процесса. Он создавал пространство, в котором цифровизация переставала быть набором национальных экспериментов и превращалась в предмет общей политической воли. Для научно-популярного понимания это особенно важно: сначала Европа строила цифровой рынок, а затем обнаружила, что строит цифровую власть.

Что дала стратегия DSM

Оценивать результаты Digital Single Market нужно не как завершённый проект с окончательной датой сдачи, а как переходную ступень. Главное достижение DSM заключалось в том, что цифровая повестка была институционально закреплена в центре европейской интеграции. Она перестала быть периферийным направлением телекоммуникационной политики и стала одним из основных измерений развития Союза.

Именно на этой основе ЕС смог перейти к более сложной архитектуре регулирования и стратегического планирования. В дальнейшем DESI — индекс цифровой экономики и общества — был встроен в более широкую систему наблюдения за прогрессом в рамках «Цифрового десятилетия», а сама цифровая политика получила официальную форму через специальную программу до 2030 года.

Однако у стратегии DSM были и ограничения. Она не решила автоматически проблему технологического лидерства Европы. Создание общего пространства ещё не означало появления европейских глобальных платформ, передовых облачных гигантов, мощной микроэлектронной базы или масштабируемых экосистем искусственного интеллекта. ЕС оказался относительно успешным в сфере правил, координации и защиты рынка, но гораздо менее однозначным — в выращивании сопоставимых с США и Китаем цифровых чемпионов. Это обстоятельство имеет принципиальное значение и для российских дискуссий: единая нормативная среда необходима, но сама по себе она не заменяет промышленной, научной и инвестиционной базы.

Переход к «Цифровому десятилетию»

К началу 2020-х годов стало ясно, что цифровая трансформация уже не может описываться исключительно через рынок. Слишком многое изменилось. Пандемия показала зависимость государств от цифровых сервисов, удалённой работы, сетевой связности и устойчивых платформ. Обострилась мировая технологическая конкуренция. Возросло значение облаков, полупроводников, искусственного интеллекта и кибербезопасности. Одновременно в самой Европе усилилось ощущение, что будущее цифровой сферы нельзя отдавать только логике крупных внешних платформ.

Так возникла программа «Цифровое десятилетие — 2030» — уже не просто набор инициатив, а полноценная рамка стратегического управления цифровой трансформацией Союза. Решение о создании программы «Цифровое десятилетие — 2030» закрепило общий подход ЕС к движению до 2030 года и определило систему целей, индикаторов и мониторинга.

Здесь заметен важный сдвиг. Если стратегия DSM была во многом проектом снятия барьеров, то «Цифровое десятилетие» стало проектом целенаправленного развития. ЕС больше не ограничивался расчисткой пространства для рынка. Он начал формулировать, каким должен быть сам цифровой порядок: сколько людей должны обладать базовыми навыками, какой уровень инфраструктуры считать достаточным, как измерять цифровизацию бизнеса и насколько глубоко должны преобразоваться государственные услуги.

Для России этот переход особенно показателен. Он демонстрирует, что современная цифровая политика эффективна лишь тогда, когда соединяет три уровня: нормативный, институциональный и измерительный. Иными словами, мало провозгласить приоритеты — их нужно перевести в систему целевых показателей, механизмов наблюдения и бюджетных решений.

Четыре измерения политики

Программа «Цифровое десятилетие» строится вокруг четырёх так называемых «cardinal points» — опорных направлений цифровой трансформации. Это цифровые навыки, цифровая инфраструктура, цифровизация бизнеса и цифровизация государственных услуг. Именно через эти четыре измерения ЕС пытается охватить ключевые стороны современной цифровой среды.

Первое измерение — навыки. Европейская логика здесь проста: никакая инфраструктура не даёт результата, если граждане и специалисты не умеют ею пользоваться. Поэтому в центр ставится задача формирования населения, грамотного в части цифровых технологий, и расширения корпуса высококвалифицированных цифровых профессионалов. Ещё в ранних обсуждениях «цифрового компаса» Европарламент и Еврокомиссия ориентировались на цель: к 2030 году не менее 80% взрослых должны обладать базовыми цифровыми навыками. Для Европы это вопрос не только образования, но и конкурентоспособности, занятости, социальной связности и демократической устойчивости.

Второе измерение — инфраструктура. Здесь речь идёт не просто о том, чтобы «провести интернет». Цифровая инфраструктура включает высокоскоростные сети, защищённую и устойчивую связность, облачные и периферийные вычисления, центры обработки данных, высокопроизводительные вычисления и технологическую основу для развития ИИ и промышленной цифровизации. Программа подчёркивает необходимость именно безопасной и устойчивой инфраструктуры, а не только её формального наличия.

Третье измерение — цифровизация бизнеса. Для ЕС это особенно болезненная тема. Европа сильна в промышленности, машиностроении, энергетике, логистике и ряде сложных производств, однако цифровое преобразование компаний идёт неравномерно. Крупные корпорации имеют больше ресурсов для внедрения облаков, аналитики данных, ИИ и автоматизации, тогда как малый и средний бизнес нередко отстаёт. Поэтому цифровизация бизнеса становится не только вопросом инноваций, но и вопросом сохранения общеевропейской промышленной конкурентоспособности.

Четвёртое измерение — цифровые государственные услуги. Оно охватывает электронное взаимодействие граждан и государства, развитие цифровой идентичности, доступ к ключевым публичным сервисам и способность административной системы работать как единое, интероперабельное пространство. В европейской модели этот компонент имеет особое политическое значение: через него ЕС стремится продемонстрировать, что цифровая трансформация служит не только рынку, но и гражданину.

Если смотреть шире, то эти четыре измерения образуют своеобразный каркас цифрового государства и цифровой экономики. Навыки дают человеческую основу, инфраструктура —

материальную, бизнес — хозяйственную, государственные услуги — институциональную. В сумме они создают то, что можно назвать минимальной архитектурой цифровой субъектности.

Индикаторы и механизмы мониторинга

Европейская бюрократия часто становится объектом иронии, однако именно в вопросах мониторинга она проявляет одну из своих сильнейших сторон. Программа «Цифровое десятилетие» не ограничивается декларациями. Она создаёт рамку, в которой движение к целям должно регулярно измеряться и сопоставляться как на общеевропейском, так и на национальном уровне.

В этой системе ключевую роль играют KPI — показатели эффективности, установленные в актах Комиссии. Они опираются на более раннюю практику DESI, но уже встроены в новую стратегическую логику. DESI, по сути, не исчез, а был трансформирован и интегрирован в ежегодный отчёт о состоянии «Цифрового десятилетия». Это важный момент: Европа не отбросила накопленные инструменты измерения, а включила их в более широкую модель управления.

Механизм мониторинга включает несколько элементов. Во-первых, используются сами KPI, измеряющие продвижение к целевым параметрам. Во-вторых, формируются общеевропейские траектории — теоретические линии движения каждого показателя к уровню 2030 года. Эти траектории позволяют оценивать не только текущее состояние, но и достаточность темпа прогресса. Иначе говоря, вопрос ставится не так: «Стало ли лучше?», а так: «Улучшается ли достаточно быстро, чтобы успеть к 2030 году?».

В-третьих, ежегодно публикуется Digital Decade report — доклад о состоянии цифрового десятилетия. В нём Комиссия сопоставляет фактические значения показателей с целевыми траекториями, анализирует ситуацию по странам и при необходимости формулирует рекомендации. В результате создаётся механизм, сочетающий статистику, сравнительный анализ и политическое давление. Формально это мониторинг, но фактически — инструмент дисциплинирования и координации.

Для российского читателя эта схема интересна как пример государственного управления в цифровую эпоху. Она показывает, что сложные преобразования требуют не разовых кампаний, а постоянной обратной связи между целями, измерением и корректировкой курса. В противном случае стратегия быстро превращается в набор лозунгов.

Национальные дорожные карты и проблема согласования приоритетов

После запуска первой отчётной рамки государства-члены ЕС должны были подготовить собственные национальные дорожные карты, увязанные с общеевропейскими целями. Так был создан механизм двойного уровня: единые цели формулируются на наднациональном уровне, а конкретные инструменты, реформы и инвестиции закрепляются на уровне государств.

На бумаге это выглядит логично. Но именно здесь обнаруживается одно из главных противоречий европейской цифровой политики. Экономики, административные традиции, бюджетные возможности и технологические позиции стран ЕС заметно различаются. Одни государства ближе к лидерам по навыкам, цифровым услугам и инфраструктуре, другие вынуждены догонять. Одни делают ставку на промышленную цифровизацию, другие — на государственные сервисы, третьи — на телекоммуникации, стартапы или исследовательские экосистемы. В результате общая стратегия неизбежно сталкивается с национальной селективностью.

К 2025 году, по оценке Еврокомиссии, государства-члены включили в свои обновлённые национальные стратегические дорожные карты 1 910 мер на общую сумму 288,6 млрд евро, что эквивалентно примерно 1,14% ВВП ЕС. Это внушительная цифра, свидетельствующая о серьёзности намерений. Но сама Комиссия подчёркивала, что даже такой объём не снимает проблемы недостаточности ресурсов и требует дальнейшей мобилизации как публичных, так и частных инвестиций.

Именно здесь проявляется структурная особенность европейского проекта. ЕС умеет задавать общую рамку и стимулировать национальные планы, но не располагает в цифровой сфере единым централизованным бюджетом, сопоставимым с масштабом вызова. Поэтому реализация стратегии зависит от сочетания национальной политической воли, европейских фондов, частных инвестиций и способности стран-членов действительно координировать действия, а не просто отчитываться о них.

С точки зрения российских интересов это наблюдение особенно ценно. Оно показывает, что даже крупное интеграционное объединение с сильными институтами не может автоматически превратить стратегию в единый технологический рынок. Между общеевропейской целью и конкретным национальным результатом лежат различия в ресурсах, управленческой культуре, кадровой базе и промышленной структуре.

Финансирование: от стратегии к ресурсам

Любая цифровая программа рано или поздно упирается в вопрос денег. Можно сколько угодно подробно описывать навыки, инфраструктуру, бизнес и государственные сервисы, но без финансовых каналов стратегия остаётся интеллектуальной конструкцией. Именно поэтому важнейшей частью «Цифрового десятилетия» стал набор европейских инструментов финансирования.

Первое и наиболее мощное направление — Recovery and Resilience Facility, или RRF, связанный с логикой постпандемического восстановления и более широкой рамкой NextGenerationEU. Комиссия исходила из того, что планы восстановления должны включать заметную цифровую компоненту, причём предлагался минимальный уровень цифровых расходов в 20% для соответствующих национальных планов. На практике именно RRF стал крупнейшим вкладом в поддержку целей Digital Decade среди основных общеевропейских инструментов.

Второй важный канал — Digital Europe Programme. Комиссия прямо определяет его как центральную программу ЕС по финансированию цифровой повестки в многолетнем финансовом плане 2021–2027 годов. В отличие от более общих исследовательских инструментов, эта программа ориентирована на прикладные направления цифрового развития: вычислительные мощности, искусственный интеллект, кибербезопасность, цифровые навыки и внедрение технологий.

Третье направление — Horizon Europe. Это уже не просто цифровая программа, а более широкий рамочный механизм поддержки исследований и инноваций, в котором предусмотрен значительный блок «Цифровые технологии, промышленность и космос». Около 35% усилий Horizon Europe, по данным Комиссии, поддерживают цифровой переход. Для ЕС Horizon Europe важен тем, что соединяет науку, технологическое развитие и промышленную модернизацию.

Четвёртый инструмент — Connecting Europe Facility, особенно его цифровая компонента CEF Digital. Она предназначена для поддержки трансъевропейской цифровой связности и инфраструктур, прежде всего в области широкополосных и 5G-сетей, а также иных высокопроизводительных и безопасных коммуникационных решений. Если RRF работает как широкая восстановительная рамка, то CEF Digital скорее напоминает инфраструктурный нерв европейской цифровой интеграции.

Пятое направление — InvestEU. Его особенность в том, что он должен не просто распределять бюджетные средства, но и привлекать частный капитал в проекты, соответствующие долгосрочным приоритетам ЕС. Комиссия подчёркивает, что по крайней мере 10% программы ориентировано на цифровые цели. Это особенно важно, потому что Европа всё яснее осознаёт: публичных денег недостаточно, если они не запускают более широкий инвестиционный мультипликатор.

Наряду с этими программами Комиссия и исследовательские структуры ЕС анализируют совокупный вклад основных инструментов в достижение целей «Цифрового десятилетия». По расчётам JRC, основные инструменты дают более 165 млрд евро поддержки целям Digital Decade, причём свыше 70% этой суммы связано с RRF. Уже из этого видно, что европейская цифровая стратегия в значительной степени опирается на логику восстановительных и стимулирующих инвестиций, а не только на долгосрочное отраслевое программирование.

Что всё это означает

Переход от Digital Single Market к «Цифровому десятилетию» показывает, как менялось само понимание цифровой политики в Европе. Сначала цифровизация мыслилась как устранение барьеров внутри рынка. Затем — как формирование общеевропейской инфраструктуры правил и прав пользователей. Наконец, к началу 2020-х годов она превратилась в проект стратегического управления: с целями, индикаторами, траекториями, дорожными картами, ежегодными отчётами и системой финансирования.

Но вместе с ростом управленческой сложности возросло и число противоречий. Чем более амбициозной становилась программа, тем отчётливее проявлялись различия между странами, нехватка частных инвестиций, зависимость от внешних технологий и разрыв между нормативной силой ЕС и его реальной технологической базой. Именно поэтому к 2025 году Еврокомиссия, признавая масштаб уже запланированных мер на 288,6 млрд евро, одновременно настаивала на необходимости дополнительной публичной и частной мобилизации ресурсов.

Для российской аудитории из этого вытекает важный вывод. Цифровая трансформация — это не техническое приложение к экономике и не набор модных сервисов. Это новая форма организации власти, производства и общественной жизни. Европейский союз сумел создать одну из самых сложных и институционально продуманных систем цифрового управления в мире. Но именно эта история показывает: суверенитет в цифровую эпоху определяется не только наличием стратегии, но и способностью наполнить её инфраструктурой, кадрами, промышленностью и капиталом.

В следующей главе внимание будет сосредоточено на институтах цифрового управления ЕС — на том, кто именно в европейской системе принимает решения, как распределяются компетенции, и почему административная архитектура цифровой Европы одновременно является источником её силы и её уязвимости.

Глава 2. Институты цифрового управления ЕС

Цифровая трансформация Европейского союза не управляется единым «цифровым министерством». Она складывается из работы многочисленных институтов, генеральных директоратов, агентств, фондов, экспертных структур и национальных администраций. Такая система отражает саму природу ЕС: это не централизованное государство, а объединение государств, которые передали часть полномочий наднациональному уровню, но сохранили значительную самостоятельность.

В цифровой сфере эта особенность заметна особенно ярко. Один орган отвечает за телекоммуникации и цифровые платформы, другой — за промышленную конкурентоспособность, третий — за космическую инфраструктуру и оборонную промышленность, четвёртый — за кибербезопасность, пятый — за инновации. В результате возникает сложная институциональная карта, где успех зависит не только от качества отдельных решений, но и от способности разных структур действовать согласованно.

Для Европейского союза такое многообразие — источник силы, поскольку оно позволяет учитывать экономические, правовые, технологические и общественные последствия цифровизации. Но оно же становится источником слабости: согласование решений занимает время,

ответственность оказывается распределённой, а бизнес и национальные органы получают всё более сложную систему требований.

Европейская комиссия: центр стратегического управления

В институциональной системе ЕС Европейская комиссия играет роль, близкую к роли правительства, хотя полностью с национальным правительством её сравнивать нельзя. Она обладает правом законодательной инициативы по большинству направлений европейской политики, следит за исполнением общеевропейских норм, управляет значительной частью программ финансирования и представляет общий интерес Союза.

В цифровой сфере Комиссия формирует стратегические документы, готовит проекты регламентов и директив, координирует национальные программы, распределяет гранты и контролирует выполнение решений. Именно через Комиссию проходили важнейшие инициативы последнего десятилетия: стратегия единого цифрового рынка, программа «Цифровое десятилетие», регулирование цифровых платформ, политика данных, нормы об искусственном интеллекте, кибербезопасности и полупроводниках.

Однако Европейская комиссия не представляет собой монолит. Внутри неё существуют генеральные директораты — крупные административные подразделения, отвечающие за отдельные сферы. В цифровой политике особое значение имеют DG CONNECT, DG GROW и DG DEFIS. Их названия могут показаться сухими аббревиатурами, но за ними стоят три различных взгляда на цифровое будущее Европы.

DG CONNECT — Генеральный директорат по коммуникационным сетям, контенту и технологиям — отвечает прежде всего за цифровую стратегию в узком смысле слова. В его поле зрения находятся телекоммуникации, цифровая инфраструктура, платформы, данные, искусственный интеллект, медиа, цифровые навыки и общая политика цифрового развития. Если сравнить цифровую трансформацию с большим городом, DG CONNECT занимается его нервной системой: сетями связи, информационными потоками, цифровыми сервисами и правилами их функционирования.

Именно этот директорат стал одним из главных архитекторов европейского цифрового регулирования. Через него проходят вопросы реализации Digital Services Act, Digital Markets Act, Data Act, политики в области искусственного интеллекта и программы «Цифровое десятилетие». При этом его задача состоит не только в разработке норм. Он должен думать о совместимости национальных систем, о цифровом разрыве между регионами, о внедрении технологий в экономику и о том, как сделать европейский рынок привлекательным для инноваций.

DG GROW — Генеральный директорат по внутреннему рынку, промышленности, предпринимательству и малым, и средним предприятиям — смотрит на цифровизацию через призму производства и конкурентоспособности. Для него цифровые технологии важны не сами по себе, а как инструмент модернизации промышленности, развития единого рынка, поддержки стартапов, укрепления цепочек поставок и повышения эффективности малых и средних компаний.

Такой подход особенно заметен в европейской политике «Индустрии 4.0». Роботизация, цифровые двойники, промышленный интернет вещей, аддитивное производство, автоматизация складов и внедрение искусственного интеллекта на предприятиях — всё это находится на пересечении цифровой и промышленной повестки. DG GROW стремится сделать так, чтобы цифровой переход не усилил зависимость европейской промышленности от внешних поставщиков программного обеспечения, микросхем и облачных сервисов, а, напротив, укрепил её позиции.

DG DEFIS — Генеральный директорат по оборонной промышленности и космосу — представляет третье измерение цифровой политики: безопасность и стратегическую автономию. В XXI веке космические системы, спутниковая навигация, дистанционное зондирование

Земли, защищённая связь, средства наблюдения, беспилотные комплексы и системы обработки данных становятся неотделимыми от обороны и гражданской инфраструктуры.

Под его влиянием цифровизация приобретает двойное назначение. Одна и та же технология может использоваться для гражданской логистики и военного управления, для мониторинга климата и разведки, для связи в удалённых районах и обеспечения устойчивости критической инфраструктуры. В такой логике цифровая независимость уже не сводится к защите рынка или персональных данных. Она становится частью оборонно-промышленной политики.

Разделение компетенций: сила специализации и риск распыления

На первый взгляд распределение задач между разными директоратами выглядит рационально. DG CONNECT понимает цифровые сети и платформы. DG GROW ориентируется на промышленность и рынок. DG DEFIS связывает технологии с безопасностью, космосом и оборонной промышленностью. Но цифровая эпоха плохо укладывается в административные границы.

Искусственный интеллект, например, одновременно является объектом правового регулирования, инструментом для промышленности, средством киберзащиты, компонентом беспилотных систем и элементом военной разведки. Облака нужны и для частного бизнеса, и для государственных сервисов, и для обработки космических данных. Полупроводники важны для потребительской электроники, автомобилей, телекоммуникаций, энергетики и вооружений.

Поэтому в ЕС постоянно возникает задача межведомственной координации. Решение, подготовленное одним директоратом, почти неизбежно затрагивает компетенции другого. Если координация недостаточна, появляются дублирование программ, противоречивые требования, задержки в принятии решений и борьба за бюджетные ресурсы.

Вместе с тем европейская модель имеет важное преимущество: она не позволяет свести цифровую трансформацию к одной узкой логике. Технологии рассматриваются одновременно как фактор экономического роста, объект правовой защиты, элемент социальной политики, инструмент геополитики и часть системы безопасности. Для России этот опыт полезен именно в таком аспекте: цифровая повестка требует постоянного взаимодействия между органами, отвечающими за связь, промышленность, науку, образование, безопасность, финансовое развитие и государственное управление.

ENISA: кибербезопасность как общеевропейская функция

Особое место в цифровой архитектуре ЕС занимает Европейское агентство по кибербезопасности — ENISA. Оно было создано ещё в начале 2000-х годов, когда киберугрозы воспринимались прежде всего как техническая проблема защиты компьютерных сетей. Но с развитием цифровой экономики его роль резко возросла.

Сегодня кибербезопасность касается не только компьютеров в офисе. Она определяет устойчивость энергетики, транспорта, здравоохранения, банковской системы, связи, водоснабжения, промышленных предприятий и государственных реестров. Кибератака на критическую инфраструктуру способна вызвать не только утечку данных, но и реальные физические последствия: остановку производства, перебои в поставках, сбои в больницах, нарушение работы городской среды.

ENISA выполняет несколько функций. Агентство готовит экспертные рекомендации, участвует в разработке общих стандартов, помогает государствам-членам обмениваться информацией, содействует проведению учений и поддерживает развитие европейской системы сертификации в области кибербезопасности. Его деятельность особенно важна там, где национальные границы не совпадают с границами цифровых сетей.

Киберпространство не знает таможенных пунктов. Уязвимость в одной стране может затронуть сеть поставщиков и потребителей в другой. Поэтому ЕС стремится строить киберустойчивость как коллективную функцию. Эта идея близка и российскому пониманию

защиты критической информационной инфраструктуры: безопасность цифровой системы определяется не прочностью одного узла, а надёжностью всей цепи.

Однако наднациональная координация не отменяет национальной ответственности. ENISA может разрабатывать рекомендации и содействовать обмену опытом, но конкретные системы связи, энергетические объекты, государственные базы данных и предприятия находятся в юрисдикции государств-членов. Именно здесь возникает известная проблема: общеевропейские требования должны быть достаточно едиными, чтобы обеспечивать безопасность общего пространства, но достаточно гибкими, чтобы учитывать различия национальных систем.

Европейское агентство обороны: цифровизация военной сферы

Европейское агентство обороны занимает особое место между гражданской цифровой политикой и оборонным измерением технологий. Его задача состоит в содействии сотрудничеству государств-членов в сфере оборонных возможностей, исследований, совместных закупок, стандартизации и развития военных технологий.

Цифровая трансформация радикально меняет оборонную сферу. В прошлом военная мощь ассоциировалась прежде всего с численностью армии, количеством танков, самолётов и кораблей. Сегодня к этим параметрам добавляются скорость обработки информации, защищённость каналов связи, качество разведывательных данных, устойчивость спутниковой навигации, способность применять беспилотные системы и использовать алгоритмы для поддержки решений.

В этой среде Европейское агентство обороны выступает не как единый военный штаб, а как механизм кооперации. Оно должно помогать государствам ЕС искать области, где совместное развитие технологий выгоднее, чем разрозненные национальные программы. Это особенно важно для дорогостоящих цифровых решений: систем управления, защищённой связи, разведывательных платформ, киберзащиты, автономных комплексов и обработки больших данных.

Однако оборонная интеграция Европы сталкивается с фундаментальным ограничением. Вопросы национальной безопасности остаются одной из наиболее чувствительных сфер государственного суверенитета. Страны ЕС по-разному оценивают угрозы, имеют разные бюджеты, традиции военного строительства и отношения с внешними союзниками. Поэтому кооперация развивается медленнее, чем этого требовала бы технологическая логика.

Для России эта особенность европейской системы имеет двойное значение. С одной стороны, она показывает, насколько трудно создать единое оборонно-технологическое пространство даже при наличии общего рынка и развитых институтов. С другой стороны, она подчёркивает возрастающую роль технологий двойного назначения — тех, которые одновременно важны для гражданской экономики и военной сферы. Современные средства связи, микроэлектроника, навигация, ИИ, робототехника и беспилотные системы уже нельзя строго разделить на «гражданские» и «военные».

Европейский совет по инновациям: поиск технологических чемпионов

Если ENISA отвечает за устойчивость цифровой среды, а Европейское агентство обороны — за её оборонные аспекты, то Европейский совет по инновациям, European Innovation Council, призван решать другую задачу: превращать научные идеи в масштабируемые технологические проекты.

Европа давно сильна в фундаментальной науке. На её территории расположены старейшие университеты мира, крупные исследовательские центры и высокотехнологичные промышленные компании. Но между лабораторным открытием и мировым рынком существует опасный промежуток. Идея может быть блестящей, прототип — успешным, но компания всё равно не сможет вырасти: ей не хватит капитала, доступа к рынку, управленческого опыта, производственных мощностей или терпения инвесторов.

Именно этот этап часто называют «долиной смерти» инноваций. Проект уже перестал быть чисто академическим исследованием, но ещё не стал полноценным бизнесом. В США его могут подхватить венчурные фонды, крупные технологические корпорации или оборонные программы. В Европе такая цепочка исторически работала менее устойчиво.

Европейский совет по инновациям пытается заполнить этот разрыв. Он ориентирован на поддержку прорывных технологий и компаний, работающих в сферах глубоких технологий: искусственного интеллекта, робототехники, квантовых решений, биотехнологий, новых материалов, космических систем, энергетики и микроэлектроники. Его задача — не просто выдать грант на исследование, а помочь перспективной разработке пройти путь от идеи к рынку.

В европейской стратегии это имеет особое значение. Без собственных компаний, способных создавать глобально значимые продукты, ЕС рискует остаться главным арбитром чужого технологического соревнования. Он сможет устанавливать правила для платформ, но не будет владеть самими платформами. Поэтому Европейский совет по инновациям — это попытка сделать европейскую цифровую политику не только нормативной, но и предпринимательской.

AI Office: попытка управлять искусственным интеллектом

Создание Европейского AI Office стало одним из наиболее заметных институциональных шагов ЕС в области искусственного интеллекта. Оно связано с принятием AI Act — европейского законодательства, впервые попытавшегося выстроить комплексное регулирование ИИ по принципу оценки рисков.

Европейская логика состоит в том, что не все системы искусственного интеллекта одинаково опасны. Алгоритм, который помогает сортировать фотографии, и алгоритм, влияющий на решение о трудоустройстве, предоставлении кредита, медицинском диагнозе или работе критической инфраструктуры, не могут регулироваться одинаково. Чем выше потенциальный риск для прав, безопасности и жизненных перспектив человека, тем строже должны быть требования к разработчикам и операторам системы.

Но принятие закона — лишь начало. Чтобы нормы работали, нужен орган, способный разъяснять правила, координировать их применение, поддерживать стандартизацию, взаимодействовать с национальными надзорными органами и отслеживать развитие наиболее мощных моделей ИИ. Именно такую роль должен выполнять AI Office.

Его появление отражает важную тенденцию. Искусственный интеллект перестал быть только предметом научных исследований, продуктом корпораций или темой общественной дискуссии. Он становится объектом постоянного наднационального управления. Европейский союз пытается создать административную структуру, которая будет сопровождать ИИ так же, как финансовые регуляторы сопровождают банковский сектор или авиационные органы — безопасность полётов.

Однако здесь возникает принципиальный вопрос. Может ли регулирование поспевать за технологией? ИИ развивается стремительно: появляются новые модели, методы обучения, способы применения, коммерческие продукты и риски. Бюрократическая система по своей природе действует медленнее. Ей нужны процедуры, консультации, согласования, юридические определения и единообразные трактовки.

Поэтому AI Office оказался в сложной позиции. От него ждут одновременно строгого контроля, правовой определённости, защиты граждан, поддержки инноваций и быстрого реагирования на новые технологии. Эти ожидания не всегда совместимы. Слишком мягкое регулирование может создать риски; слишком жёсткое — затруднить развитие европейских компаний и стимулировать перенос инновационной активности в другие юрисдикции.

Для России этот сюжет важен как пример необходимости баланса. Государственное регулирование ИИ должно обеспечивать безопасность, защиту прав и ответственность разработчиков. Но оно не должно превращаться в систему, в которой исследователь, стартап или про-

мышленная компания тратят больше сил на прохождение административных процедур, чем на создание самой технологии.

Европейские цифровые инновационные хабы

Европейские центры цифровых инноваций (European Digital Innovation Hubs, EDIH) стали одним из наиболее практических инструментов европейской цифровой политики. Если Европейская комиссия создаёт стратегию, а специализированные агентства формируют правила и экспертные стандарты, то цифровые инновационные хабы должны помогать технологиям дойти до реального пользователя.

Это особенно важно для малых и средних предприятий, региональных органов власти, муниципалитетов, больниц, образовательных учреждений и организаций, не обладающих собственными крупными ИТ-подразделениями. Большая корпорация может нанять консультантов, купить программное обеспечение, создать собственный центр компетенций и экспериментировать с ИИ. Малое предприятие часто не может позволить себе ни дорогое оборудование, ни длительный период ошибок.

Хаб работает как посредник между технологией и практикой. Он может предоставить доступ к экспертизе, тестированию решений, обучению сотрудников, консультациям по финансированию, вопросам кибербезопасности и внедрению ИИ. В идеале предприятие или государственная организация получает возможность сначала проверить технологию в относительно безопасной среде, оценить её эффект и лишь затем инвестировать в масштабное внедрение.

Для ЕС EDIH важны не только как сервисные центры. Они являются попыткой сократить цифровой разрыв между столицами и регионами, между крупными компаниями и малыми предприятиями, между технологическими лидерами и теми, кто только начинает цифровую трансформацию. В этом смысле хабы напоминают сеть «передаточных станций», через которые общеевропейская стратегия достигает конкретного завода, фермы, муниципалитета или медицинского учреждения.

Российский опыт технопарков, инжиниринговых центров, центров трансфера технологий, научно-образовательных центров и региональных цифровых инициатив позволяет увидеть близкую проблему. Технология становится фактором развития только тогда, когда она встроена в повседневную хозяйственную практику. Создать передовую разработку недостаточно; необходимо обеспечить её внедрение, обслуживание, кадровое сопровождение и экономическую целесообразность.

Лабиринт институтов

Сложность европейской цифровой архитектуры имеет исторические причины. ЕС объединяет государства с разным уровнем развития, разной промышленной структурой и разной политической культурой. Он должен одновременно учитывать интересы крупных технологических держав внутри Союза, потребности небольших стран, права граждан, интересы бизнеса, требования обороны и принципы конкуренции.

Поэтому европейская система неизбежно производит большое количество институтов, программ, директив, регламентов, рабочих групп, фондов и координационных механизмов. Каждый из них появился по понятной причине. Один защищает данные, другой развивает связь, третий поддерживает стартапы, четвёртый занимается кибербезопасностью, пятый — промышленностью, шестой — обороной и космосом.

Но в совокупности эта система может превратиться в лабиринт.

Для крупной корпорации, располагающей юридическими департаментами и ресурсами, сложное регулирование часто становится управляемой задачей. Для малого предприятия, научного коллектива или регионального органа власти оно может оказаться непреодолимым барьером. Нужно понимать, какие правила применяются, к какому органу обращаться, какие

документы готовить, как соотносить нормы о данных, ИИ, кибербезопасности, конкуренции и защите потребителей.

Парадокс состоит в том, что стремление ЕС обеспечить надёжность и защиту способно создавать новую форму неравенства. Технологически сильные игроки лучше справляются с регулированием, чем слабые. А значит, избыточная сложность может косвенно укреплять позиции именно тех крупных компаний, чью власть Европа стремится ограничить.

Это не означает, что регулирование следует отменить. Напротив, цифровая экономика нуждается в правилах. Но правила должны быть соразмерны рискам, понятны исполнителям и согласованы между собой. Там, где каждая новая проблема встречается новым регламентом, а каждый регламент — новой процедурой, возникает опасность регуляторной перегруженности.

Европейский урок

Институты цифрового управления ЕС показывают, что в XXI веке технология больше не может быть оставлена исключительно инженерам или рынку. Она влияет на суверенитет, экономику, безопасность, культуру, социальную справедливость и права человека. Поэтому цифровое управление неизбежно становится межведомственным и многоуровневым.

Европейская модель сильна тем, что стремится охватить всю картину: связь, данные, промышленность, инновации, безопасность, оборону, образование и государственные услуги. Она понимает, что цифровой переход — это не один сектор, а новая среда существования общества.

Но её слабость — в тяжеловесности. Большое число институтов и правил может обеспечить защиту от ошибок, но иногда снижает скорость действий. В мире, где технологические решения меняются быстрее, чем согласуются нормативные акты, это становится серьёзным вызовом.

Для Российской Федерации европейский опыт полезен прежде всего как предостережение и как источник практических наблюдений. Цифровой суверенитет требует сильных институтов, ясного распределения ответственности, защиты критической инфраструктуры и способности поддерживать инновации. Но он требует также простоты управленческих контуров, понятных правил для разработчиков и предприятий, реальной координации между гражданскими, промышленными и оборонными структурами.

Будущее цифровой политики определяется не количеством созданных органов и не числом принятых документов. Оно определяется тем, способны ли институты превращать стратегические замыслы в работающие технологии, конкурентоспособные продукты, защищённую инфраструктуру и рост качества жизни.

Часть II. Право и регулирование

Глава 3. ЕС как «регуляторная сверхдержава»

Когда в XX веке говорили о силе государства или союза государств, обычно вспоминали армию, промышленность, торговый флот, валюту, природные ресурсы. В XXI веке к этому списку добавилась ещё одна форма мощи — способность устанавливать правила для цифрового мира. Европейский союз именно здесь сумел добиться одного из самых заметных результатов. Он не создал столько глобальных цифровых гигантов, сколько США, и не выстроил столь централизованную технологическую мобилизацию, как Китай. Но он научился делать нечто иное: превращать право в инструмент глобального влияния.

В этом и заключается феномен, который часто называют «регуляторной сверхдержавой». ЕС воздействует на мировую цифровую экономику не столько через собственные платформы, сколько через нормы, без соблюдения которых крупнейшим компаниям становится трудно работать на европейском рынке. Это не отменяет технологической зависимости Европы, но создаёт другую форму власти — власть над условиями доступа к одному из крупнейших и наиболее платёжеспособных рынков мира.

Для России здесь скрывается важный аналитический урок. В современном мире регулирование перестало быть лишь внутренним правовым делом. Оно стало способом формировать международную среду, перераспределять издержки между государствами и компаниями, влиять на стандарты разработки технологий и даже определять, какие модели бизнеса окажутся жизнеспособными, а какие — будут вытеснены как несоответствующие новым правилам.

«Брюссельский эффект»

Чтобы понять особенность европейской силы, полезно представить себе огромный вокзал, через который проходят почти все поезда континента. Тот, кто управляет правилами движения на таком узле, влияет не только на пассажиров на перроне, но и на всю систему расписаний, составов, сигналов и маршрутов. Европейский союз занял в цифровом мире похожее положение.

Если крупная технологическая компания хочет обслуживать сотни миллионов пользователей в ЕС, она вынуждена соблюдать европейские правила. Для глобального бизнеса часто оказывается невыгодно создавать одну архитектуру сервиса для Европы, а другую — для остального мира. Гораздо проще распространить европейский стандарт шире, чем требовал исходный закон. Так внутреннее право ЕС начинает жить за пределами самого ЕС. Именно этот механизм принято называть «брюссельским эффектом».

В цифровой экономике он проявился особенно ярко. Европейские нормы в области защиты персональных данных, платформенной ответственности, конкуренции и регулирования цифровых посредников стали ориентиром не только для компаний, работающих на европейском рынке, но и для законодателей в других странах. Иногда этот эффект проявляется прямо, когда другие государства заимствуют элементы европейского регулирования. Иногда — косвенно, когда транснациональная корпорация перестраивает свои внутренние процедуры под европейские требования и тем самым фактически распространяет их на глобальный бизнес-процесс.

С точки зрения ЕС это большое достижение. Союз, не располагающий абсолютным технологическим лидерством, сумел навязать миру свои подходы к персональным данным, ответственности платформ и честности цифровых рынков. Но существует и другая сторона. Критики утверждают, что экспорт европейских правил может увеличивать издержки, затруднять

инновации и особенно тяжело ложиться на развивающиеся экономики и небольшие компании, не участвовавшие в выработке этих норм.

Здесь возникает важное противоречие: там, где Европа видит защиту прав, справедливость и упорядочение цифровой среды, другие могут видеть нормативное давление и перераспределение преимуществ в пользу уже сильных участников рынка. Это противоречие необходимо иметь в виду и российскому читателю, поскольку вопрос о трансграничном действии цифровых норм касается не только ЕС, но и любой крупной юрисдикции, стремящейся отстаивать собственную модель цифрового развития.

GDPR: данные как предмет политической власти

Наиболее известным выражением европейской регуляторной силы стал GDPR — Общий регламент по защите данных. В популярном восприятии он часто сводится к надоедливым всплывающим окнам про cookies. Но в действительности GDPR гораздо глубже. Это попытка заново определить отношение между человеком, государством и цифровой экономикой в эпоху, когда данные становятся одним из главных ресурсов.

Старая индустриальная экономика строилась вокруг сырья, энергии, транспорта и фабрик. Цифровая экономика опирается на информацию о поведении, предпочтениях, перемещениях, социальных связях, финансовых действиях, медицинских состояниях и профессиональной активности людей. Каждое действие в сети оставляет след, а совокупность таких следов превращается в ценнейший материал для рекламы, аналитики, кредитного скоринга, автоматизированного управления и работы алгоритмов искусственного интеллекта.

GDPR закрепил подход, при котором персональные данные рассматриваются не как бесхозное сырьё для платформ, а как объект правовой защиты, связанный с достоинством, автономией и свободой личности. В этом заключается фундамент европейской модели управления данными. Регламент стремится обеспечить, чтобы обработка персональных данных происходила на определённых основаниях, была прозрачной, ограниченной по целям и поддавалась контролю со стороны самого человека.

Для цифрового капитализма это означало важный перелом. Платформы и сервисы больше не могли исходить из молчаливого предположения, что любой собранный массив данных допустим к использованию, если он приносит прибыль или улучшает таргетинг. GDPR заставил компании выстраивать процедуры согласия, информирования, хранения, передачи и удаления данных, а также готовиться к серьёзным санкциям в случае нарушений.

Но ещё важнее символический эффект. Европа сформулировала мысль, имеющую мировое значение: цифровая модернизация не должна автоматически вести к тотальной коммерциализации личности. Человек не обязан становиться просто источником данных для извлечения прибыли. Для многих обществ, включая Россию, этот принцип имеет самостоятельную ценность, даже если конкретные формы его правового воплощения могут различаться.

Вместе с тем GDPR не решил всех проблем. Большие компании лучше справляются с режимами соответствия, чем малый бизнес. Пользователь нередко формально соглашается на обработку данных, не читая длинных текстов и не понимая архитектуру цифрового сервиса. А сама защита данных не устраняет автоматически рыночную власть крупнейших платформ. Поэтому вскоре стало ясно: одного GDPR недостаточно. Требовались новые инструменты, способные работать уже не только с данными как объектом прав личности, но и с платформами как центрами экономической и общественной силы.

DSA: платформенная ответственность и системные риски

Если GDPR стал регламентом о данных, то Digital Services Act, DSA, стал регламентом о цифровой среде как пространстве общественного риска. Его логика строится на вопросе: что происходит, когда онлайн-платформы перестают быть просто техническими посредниками и начинают активно влиять на распространение контента, поведение пользователей, информационные потоки, общественные дискуссии и даже политическую стабильность?

DSA вводит набор правил для посреднических сервисов, а для очень крупных онлайн-платформ и очень крупных поисковых систем предусматривает особые обязанности, связанные с оценкой и снижением системных рисков. Речь идёт уже не только о незаконном контенте в узком смысле, но и о более широких негативных последствиях — для основных прав, общественного здоровья, безопасности, избирательных процессов и гражданского дискурса.

Здесь проявляется характерная особенность европейского подхода. Европа стремится регулировать не отдельные сообщения и не только факт публикации, а саму архитектуру платформенного воздействия. Важен вопрос не просто «что опубликовано?», а «какие механизмы дизайна, рекомендации, ранжирования, рекламной модели и алгоритмического усиления создают системный риск?»

Такой подход можно сравнить с правилами безопасности для большого моста. Проблема не только в том, кто именно проходит по мосту, но и в том, как рассчитана конструкция, как распределяется нагрузка, где расположены опоры и что произойдёт при сильном ветре. DSA пытается перенести эту инженерную логику в цифровую среду: платформы должны учитывать риски, создаваемые самой структурой их деятельности.

В этом есть большое достоинство. Современные платформы влияют на общество не только через отдельные нарушения, но и через накопительный эффект. Дезинформация, усиление радикального контента, непрозрачная реклама, манипулятивный интерфейс, дискриминационные алгоритмы и массовое распространение вредоносных материалов могут быть результатом не одной ошибки, а логики всей системы.

Но у DSA есть и слабые места. Критики указывают, что акцент на очень крупных платформах может оставлять часть рисков вне поля полноценного контроля, а зависимость системы от обязательных аудитов и оценок способна порождать новые формы административного захвата или формализации контроля. Иначе говоря, платформа может научиться не столько уменьшать общественные риски, сколько правильно оформлять документы об их снижении.

Для российского анализа это важное наблюдение. Регулирование цифровых платформ должно учитывать не только правовую сторону, но и техническую, организационную и поведенческую. Иначе контроль над платформами превращается в спор юристов, тогда как реальная сила по-прежнему остаётся у тех, кто управляет алгоритмами, данными и интерфейсами взаимодействия с пользователем.

DMA: борьба с «привратниками»

Если DSA отвечает на вопрос о вреде и общественной ответственности платформ, то Digital Markets Act, DMA, отвечает на другой вопрос: что делать с платформами, которые стали воротами в цифровую экономику? Именно здесь появляется знаменитое понятие gatekeepers — «привратники».

Под ним понимаются крупнейшие цифровые платформы, которые контролируют ключевые сервисы — поисковые системы, магазины приложений, мессенджеры, социальные сети, рекламные платформы и другие базовые элементы цифровой среды. Европейская логика здесь проста: если бизнесу или пользователю для выхода на рынок необходимо пройти через несколько частных ворот, то владелец этих ворот получает чрезмерную рыночную и инфраструктурную власть.

DMA устанавливает объективные критерии для определения таких «привратников». Среди них — масштаб оборота или рыночной капитализации, наличие не менее 45 миллионов ежемесячных конечных пользователей и 10 тысяч бизнес-пользователей в ЕС, а также контроль над основными платформенными сервисами в как минимум трёх государствах-членах. Иначе говоря, речь идёт не просто о большой компании, а о такой, которая стала системным посредником между бизнесом и потребителем.

После признания платформы «привратником» на неё распространяются специальные обязанности и запреты. Такие компании не должны неправомерно продвигать собственные

сервисы за счёт конкурентов, мешать использованию альтернативных платёжных систем, навязывать несправедливые условия бизнес-пользователям или препятствовать удалению предустановленного программного обеспечения. Они обязаны обеспечивать большую свободу выбора, предоставлять определённые данные бизнес-пользователям, уведомлять Комиссию о сделках и в ряде случаев обеспечивать интероперабельность, например в сфере обмена сообщениями.

Смысл DMA состоит в том, чтобы перейти от классической антимонопольной логики, когда злоупотребление властью нужно долго доказывать постфактум, к более раннему, упреждающему регулированию. Это своего рода экз-анти-контроль, рассчитанный на то, чтобы предотвратить закрепление несправедливых практик ещё до того, как рынок окончательно закроется для конкурентов.

Для Европы это чрезвычайно важный шаг. ЕС признаёт, что в цифровой экономике классическое конкурентное право часто не поспевает за скоростью платформенной концентрации. Пока идёт расследование, компания уже усиливает сетевой эффект, поглощает перспективных конкурентов и закрепляет зависимость пользователей и бизнеса. DMA пытается вмешаться раньше.

Но и здесь регуляторная сила имеет пределы. Даже если запретить отдельные формы само-преференции или обязать платформу к большей открытости, это ещё не означает автоматического появления сильных европейских конкурентов. Закон может расширить пространство возможностей, но не способен сам по себе создать крупную инновационную компанию. Для этого нужны капитал, кадры, технологическая база, предпринимательская среда и доступ к глобальным рынкам.

Регулирование как замена силы — и как её дополнение

Европейское цифровое право часто воспринимают как попытку компенсировать недостаток собственных технологических гигантов. В этом есть доля истины. ЕС действительно использует регулирование там, где не располагает равной США платформенной мощью. Но было бы ошибкой считать это лишь «заменой» технологического лидерства.

Право в цифровую эпоху стало самостоятельным производительным фактором. Оно влияет на дизайн продуктов, политику модерации, рекламные модели, архитектуру обмена данными, условия конкуренции и стратегию инвестиций. Когда компания меняет интерфейс согласия на обработку данных, перестраивает систему ранжирования или открывает доступ к части своих сервисов, это не только юридическое событие. Это изменение самой цифровой реальности.

Таким образом, регуляторное лидерство ЕС — это не вторичная, а вполне материальная форма власти. Европа воздействует не только на правовой текст, но и на код, на бизнес-модель, на поведение компаний и пользователей. Она заставляет мировые платформы принимать во внимание ценности и интересы, сформулированные в европейском политическом пространстве.

Однако эта сила действует эффективнее в оборонительном, чем в наступательном режиме. Она хорошо подходит для ограничения злоупотреблений, защиты пользователей, выравнивания условий и повышения прозрачности. Но она слабее работает как инструмент создания новых технологических лидеров. Европейское право способно ограничить монопольную власть, но не гарантирует, что освободившееся пространство займут именно европейские фирмы, а не другие внешние игроки.

Достоинства регуляторного лидерства

У европейского подхода есть несколько несомненных преимуществ.

Во-первых, он возвращает в цифровую политику идею общественного интереса. Платформы и сервисы больше не рассматриваются как нейтральные инструменты, развитие которых можно оставить исключительно рынку. ЕС показывает, что цифровая среда нуждается в

правилах, если общество хочет сохранить права личности, справедливую конкуренцию и хотя бы минимальную прозрачность алгоритмической власти.

Во-вторых, европейское регулирование стремится связать технологию с ответственностью. Это особенно важно в мире, где цифровые корпорации склонны представлять свои продукты как естественный результат инноваций, а не как управляемые конструкции с определёнными рисками и последствиями. DSA и DMA по-разному, но последовательно говорят одно и то же: крупная платформа не может ссылаться на собственный размер как на оправдание безответственности.

В-третьих, ЕС создаёт предсказуемую правовую среду. Для бизнеса это может быть одновременно и нагрузкой, и преимуществом. Сложные правила увеличивают издержки, но прозрачные и единообразные нормы иногда лучше, чем хаотическое сосуществование разрозненных национальных режимов. Именно поэтому европейский рынок продолжает оставаться притягательным, несмотря на жёсткость регулирования.

В-четвёртых, европейская модель показывает, что защита гражданских прав и регулирование цифровых корпораций могут быть соединены в единой политике. Для России этот аспект особенно интересен в контексте обсуждения цифрового суверенитета. Суверенитет — это не только защита государства от внешнего давления, но и способность выстраивать такую цифровую среду, где экономическая эффективность не уничтожает правовую субъектность человека.

Ограничения и пределы

Но у регуляторного лидерства есть свои границы.

Главная из них заключается в том, что право не производит технологии автоматически. Можно обязать платформу не злоупотреблять своей властью, но невозможно регламентировать создать новый поисковик, облачный сервис, процессор или модель ИИ мирового класса. Европа сильна в задаче «как ограничить», но слабее — в задаче «как быстро вырастить». Именно отсюда возникает разрыв между нормативной амбициозностью ЕС и его более скромными результатами в сфере глобальных цифровых чемпионов.

Вторая проблема — стоимость соответствия. Крупные корпорации обычно имеют ресурсы для адаптации к новым требованиям. Для малых и средних компаний, стартапов и организаций из менее развитых юрисдикций та же система может оказаться чрезмерно тяжёлой. Критики «брюссельского эффекта» прямо указывают, что экспорт европейских норм может повышать барьеры для инноваций и усиливать преимущества уже крупных западных игроков.

Третья проблема — скорость. Цифровая среда меняется быстрее, чем право. Пока разрабатывается регламент, проходят консультации, согласования, принятие и ввод в действие, рынок уже может сменить технологическую логику. Поэтому европейское регулирование постоянно рискует реагировать на вчерашнюю проблему, тогда как новые вызовы возникают в другом месте — например, в генеративном ИИ, облачной инфраструктуре или архитектуре вычислительных ресурсов.

Наконец, существует и политический предел. Чем больше ЕС распространяет своё регулирование вовне, тем сильнее будет встречное сопротивление. Для одних государств европейские стандарты выглядят как образец правовой современности; для других — как нормативная экспансия, не учитывающая их экономические условия и стратегические интересы.

Европейский парадокс

В итоге возникает парадокс, который можно считать центральным для всей цифровой стратегии ЕС. Европа добилась огромного влияния именно там, где не обладала абсолютным технологическим превосходством. Она превратила рынок и право в источник глобальной силы. GDPR, DSA и DMA стали не просто актами внутреннего регулирования, а элементами мировой борьбы за то, как должна выглядеть цифровая среда.

Но этот успех одновременно высвечивает ограниченность чисто регуляторного пути. Если правила становятся главной формой цифрового влияния, то ЕС рискует остаться архитектором чужого технологического мира. Он сможет определять, на каких условиях действуют крупные платформы, но не обязательно будет сам владеть платформами, вычислительными центрами, ключевыми программными экосистемами и критическими компонентами.

Для России из этого следует важный вывод. Регуляторная сила имеет значение, особенно когда речь идёт о защите данных, обеспечении конкуренции, сдерживании платформенной власти и поддержании цифрового суверенитета. Но она должна быть связана с промышленной, научной и инфраструктурной политикой. Без собственной технологической базы любое регулирование в конечном счёте начинает обслуживать рынок, архитектура которого создана другими.

Именно поэтому следующая логика европейского развития неизбежно выходит за пределы чистого права — к данным, искусственному интеллекту, облакам, полупроводникам и критической инфраструктуре. Там становится ясно, что регулировать цифровой мир недостаточно: необходимо ещё и обладать средствами его материального построения.

Глава 4. Управление данными и искусственным интеллектом

В цифровую эпоху государство всё чаще напоминает не только администратора территории, но и распорядителя потоков данных. Оно должно решать, кто получает доступ к информации, на каких условиях она может использоваться, кому принадлежат результаты её обработки, как защищаются права человека и где проходит граница между инновацией и злоупотреблением. Именно здесь Европейский союз сделал следующий шаг после GDPR, DSA и DMA: он попытался выстроить целостную архитектуру управления данными и искусственным интеллектом.

Это был неизбежный шаг. Если защита персональных данных — лишь одна часть цифровой реальности, то огромные массивы промышленной, медицинской, транспортной, энергетической и иной информации вообще не укладываются в старую схему «платформа — пользователь — реклама». Они создаются машинами, датчиками, станками, логистическими цепями, электросетями, автомобилями, больницами, спутниками и системами управления. Эти данные могут повышать производительность, улучшать здравоохранение, экономить энергию, усиливать безопасность и ускорять научные исследования. Но они могут также усиливать рыночную зависимость, создавать новые формы контроля и перераспределять власть в пользу тех, кто владеет вычислительными ресурсами и алгоритмами.

Поэтому европейская стратегия в области данных и искусственного интеллекта строится вокруг двух больших задач. Первая — сделать доступ к данным более справедливым, предсказуемым и полезным для экономики и общества. Вторая — не допустить, чтобы внедрение ИИ разрушило права человека, подорвало доверие к институтам и передало слишком много власти непрозрачным системам.

Для России в этом узле проблем есть особая ценность. Европейский опыт показывает, что спор о данных и ИИ — это не второстепенная тема цифровой политики. Это её сердцевина. Здесь решается вопрос о том, кто будет управлять инфраструктурой знания, на основе которой работают промышленность, медицина, транспорт, государство, рынок и безопасность.

Европейская стратегия данных

Европейская стратегия данных выросла из осознания простой, но важной истины: данные создаются во множестве мест, но их экономическая и социальная ценность раскрывается лишь тогда, когда существуют понятные правила доступа, обмена и использования. Если информация заперта внутри корпораций, ведомств или отдельных платформ, экономика теряет часть

возможностей. Если же она свободно циркулирует без правил, возникает риск злоупотреблений, утечек, нарушения прав и усиления зависимости от сильнейших игроков.

Поэтому Европа попыталась построить промежуточную модель. Она не равна ни полной коммерческой приватизации данных, ни их бесконтрольной открытости. Её логика состоит в том, чтобы создать доверенную среду обмена, где доступ к данным может расширяться, но при сохранении правовых гарантий, механизмов посредничества и защиты законных интересов участников.

Одним из первых элементов этой архитектуры стал Data Governance Act. Его смысл можно понять через образ общеевропейского «водопровода данных». Важен не только сам источник, но и трубы, насосные станции, фильтры, распределительные узлы и правила подключения. Регламент о управлении данными должен был заложить механизмы, позволяющие делиться данными между секторами и странами ЕС при более высоком уровне доверия и предсказуемости.

Следующим шагом стал Data Act — гораздо более жёсткий и прикладной инструмент. Он регулирует справедливый доступ к данным и их использование, прежде всего в контексте connected products и связанных цифровых услуг. Если упростить, речь идёт о вопросе: кому принадлежат и кто может использовать данные, создаваемые «умными» машинами, устройствами, системами и сервисами? В цифровой экономике это вопрос огромной важности. Производитель оборудования, владелец устройства, сервисный оператор, облачный провайдер и пользователь часто претендуют на разные права в отношении одного и того же массива информации.

Data Act вступил в силу 11 января 2024 года, а применяться начал с 12 сентября 2025 года. Комиссия прямо описывает его как крупный шаг к формированию более справедливой и инновационной европейской экономики данных. Тем самым ЕС попытался ограничить ситуацию, при которой данные, создаваемые устройствами и машинами, фактически монополизированы ограниченным кругом поставщиков услуг или производителей.

Для российской аудитории это особенно интересно в контексте промышленности, транспорта, энергетики и городской инфраструктуры. В мире «умных» станков, автомобилей, сетей и датчиков вопрос о данных — это не вопрос удобства интерфейса. Это вопрос экономической ренты, зависимости от поставщика, возможности сервисного обслуживания, импортозамещения и даже контроля над критической инфраструктурой.

Пространства данных: новая география цифровой экономики

Одной из самых характерных идей европейской политики стали European Data Spaces — общеевропейские пространства данных. Их замысел состоит не в создании единой гигантской базы, куда будут стекаться все данные Европы. Скорее это сеть отраслевых и межотраслевых сред, где данные могут использоваться по согласованным правилам, быть совместимыми по форматам и доступными для уполномоченных участников.

Иначе говоря, Европа пытается построить не цифровой склад, а цифровую логистику. Важно не только накопить данные, но и обеспечить их перемещение, совместимость, доверие и практическую полезность. В такой модели данные становятся чем-то вроде инфраструктурного ресурса — подобно железным дорогам, энергосетям или системе внутренних водных путей.

Значение этой идеи трудно переоценить. Современная экономика всё меньше зависит от изолированных информационных массивов и всё больше — от способности соединять их. Данные о промышленном оборудовании важны для сервисного обслуживания и планирования производства. Медицинские данные важны для диагностики, персонализированного лечения и исследований. Энергетические данные необходимы для управления распределённой генерацией и балансировки сетей. Транспортные — для логистики, безопасности и оптимизации потоков. А совмещение разных массивов часто рождает новые эффекты, которых невозможно добиться внутри одной организации.

Но вместе с выгодами возникают и риски. Чем шире объединяются данные, тем выше требования к безопасности, анонимизации, правовым основаниям доступа и защите чувствительной информации. Поэтому европейские пространства данных строятся как компромисс между открытостью и контролем.

Промышленные пространства данных

Промышленная сфера — один из центральных объектов европейской стратегии данных. Для ЕС это естественно: промышленность остаётся важнейшей основой его экономической силы. Машиностроение, автомобилестроение, химия, энергетическое оборудование, высокоточное производство и сложные производственные цепочки создают огромные массивы данных, которые могут быть использованы для повышения эффективности и снижения затрат.

Представим себе современный завод. Каждый станок передаёт информацию о нагрузке, температуре, вибрациях, простоях и качестве выпускаемой продукции. Линия сборки генерирует поток сигналов о темпе работы. Складские системы фиксируют перемещение компонентов. Программные модели оценивают износ оборудования. Если все эти данные остаются у отдельных поставщиков или разрозненных подразделений, предприятие теряет возможность увидеть полную картину.

Промышленное пространство данных должно помочь преодолеть эту разобщённость. Оно открывает возможности для предиктивного обслуживания, цифровых двойников, гибкого производства, энергетической оптимизации, управления цепочками поставок и более точного контроля качества. Для ЕС это ещё и способ уменьшить зависимость от замкнутых экосистем внешних платформ и производителей оборудования.

Для России здесь скрыт практический урок. В условиях, когда технологическая независимость становится вопросом национальной устойчивости, доступ к данным промышленных систем означает не только рост эффективности, но и контроль над жизненно важными производственными процессами. Страна, не управляющая собственными промышленными данными, рискует зависеть не только от оборудования, но и от логики его цифрового обслуживания.

Медицинские и биомедицинские данные

Здравоохранение — ещё одна область, где европейская политика данных приобрела стратегический характер. Медицинские данные включают электронные карты пациентов, результаты анализов, изображения, сведения о терапии, генетическую информацию, данные носимых устройств и многое другое. Их правильное использование способно улучшить диагностику, ускорить исследования, повысить качество лечения и дать врачам новые инструменты для принятия решений.

Но именно здесь особенно остро сталкиваются инновация и защита прав. Медицинские данные относятся к числу наиболее чувствительных. Их утечка или неправомерное использование могут нанести человеку серьёзный вред: от дискриминации до вмешательства в частную жизнь. Поэтому европейская стратегия стремится соединить возможность научного и клинического использования данных с очень жёсткими требованиями к правовым основаниям доступа, защите конфиденциальности и контролю над вторичным использованием.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.