СПЧ

Совет при Президенте Российской Федерации
по развитию гражданского общества и
правам человека

Цифровая трансформация и защита прав граждан в цифровом пространстве 2.0

Доклад Совета
при Президенте Российской Федерации
по развитию гражданского общества
и правам человека

Москва, 2025

Содержание

Введение. И свобода и безопасность: императивы общественного договора

В **2021** году Совет при Президенте Российской Федерации по развитию гражданского общества и правам человека (далее – Совет) опубликовал доклад, посвящённый проблематике соблюдения и защиты прав и свобод человека и гражданина в условиях стремительной, часто форсированной, цифровизации всех сторон жизни личности, общества и государства[1]. Доклад вызвал большой резонанс среди специалистов и впоследствии послужил концептуальной основой для разработки в **2022-2023** годах проекта Концепции обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве РФ и плана действий («дорожной карты») по её реализации[2].

Проект Концепции и «дорожной карты» получил поддержку ряда федеральных органов публичной власти, однако так и не стал нормативным документом стратегического планирования. В связи с этим в **2023-2024** годах представители Совета сосредоточились на работе над концепцией и структурой Цифрового (Информационного) кодекса РФ в составе Межведомственной рабочей группы Минцифры России. Однако и этот проект пока остаётся весьма далёк от своей практической реализации.

Вместе с тем, отдельные инициативы Совета были реализованы в **2024** году в виде поправок к уголовному и административному законодательству, устанавливающих «оборотные штрафы» за нарушения в области оборота персональных данных. Кроме того, по замечаниям Совета был доработан федеральный закон, устанавливающий механизмы противодействия мошенническим киберпреступлениям, и принятый в **2025** году[3].

Совет исходит из доктрины «общественного договора», согласно которой правовое государство призвано обеспечивать для человека и гражданина одновременно и безопасность, и возможность полноценной реализации своих прав и свобод. В том числе – в информационной (цифровой) среде. Этот пункт

---

[1] Текст первой версии доклада доступен по адресу: https://president-sovet.ru/presscenter/news/spch_podgotovil_doklad_o_polozhenii_del_s_pravami_i_svobodami_cheloveka_i_grazhdanina_v_tsifrovom_pr

[2] Проект был подготовлен в соответствии с подп. «г» п. 3 перечня поручений Президента РФ от 28 января 2021 г. № Пр-133 – см.: http://kremlin.ru/acts/assignments/orders/64952

[3] Федеральный закон от 1 апреля 2025 г. № 41-ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации».

«общественного договора» зафиксирован в Конституции РФ и, применительно к реалиям информатизации (цифровизации), специально усилен отдельной конституционной поправкой **2020** года. Речь идет о пункте «м» статьи **71**, закрепляющем в федеральном ведении *«обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных»*[4].

Внедрение современных цифровых технологий формирует новую среду и новые правовые реалии для человека, общества и государства, а также значительно видоизменяет уже существующие. Технологии «больших данных», искусственного интеллекта (далее – ИИ), беспилотный транспорт, цифровая медицина, виртуальные среды общения создают обширные возможности для развития нового экономического уклада, международного сотрудничества и конкуренции. Однако усугубившиеся в ходе пандемии **2020-2021** годов процессы атомизации общества и дистанцирования людей способствовали резкому ускорению «погружения» человека в цифровую среду. Это создает новые возможности для государства и бизнеса, но и несёт с собой новые, очень серьёзные угрозы и риски, как для прав и интересов человека и гражданина, так и для государственного суверенитета, остающегося необходимым условием реализации прав и свобод человека.

При должном использовании современные цифровые технологии могут быть полезным и стратегически важным явлением. Они позволяют вывести управление государством, экономикой и развитием территорий на новый технологический уровень. Цифровая среда обладает серьезным потенциалом для вовлечения уязвимых групп населения в создание добавленной стоимости, в целом для накопления человеческого потенциала. Однако сейчас в России новые цифровые технологии внедряют безоглядно, без должных обоснований, в спешке, часто принудительно, методом «ковровой цифровизации». Цифровизация публичного управления и городской среды уже приобрела характер типичной бюрократической кампании, напоминающей «перестройку и ускорение» **1980**-х годов, с лозунгами, шумовыми категориями, а также формальной «отчётностью с мест».

Целый спектр актуальных проблем реализации прав и свобод граждан обусловлен тем, что внедрение «цифры» в коммерческом секторе экономики

[4] Отметим порядок упоминания объектов правовой охраны, где на первом месте указана личность (что соответствует генеральному принципу ст. 2 Конституции РФ о высшей ценности человека, его прав и свобод) и только затем – общество и государство.

отличается низкой социальной ответственностью бизнеса, серыми внеправовыми схемами сбора и перепродажи данных, усиливающейся дискриминацией пользователей. Основной недостаток такой «лавинной» государственной и частной цифровизации состоит в том, что она ведётся без внимания к праву и защите ключевых конституционных прав и свобод граждан, без прогнозирования возможных социальных рисков и без сценарного моделирования последствий цифровизации для будущего людей.

Отметим, что цифровое, а также научно-технологическое развитие является необходимым условием обеспечения суверенитета страны, конкурентоспособности нашей экономики. Однако всё это не может и не должно достигаться путём умаления достоинства граждан, возможностей реализации ими всей полноты основных прав, свобод и законных интересов.

Сегодня граждане, общество в целом, бизнес и власть должны осознать, что, наряду с наземной территорией, воздушным и водным пространством, средой нашей жизни и деятельности является информационное (цифровое) пространство. При этом отсутствует кодифицированный акт, который, – по аналогии с Правилами дорожного движения, земельным, воздушным и морским кодексами, – регулировал бы отношения и деятельность в цифровом пространстве. Расплывчатость его виртуальных границ и неопределенность применяемой юрисдикции (в совокупности именуемые трансграничностью) не должны приводить к ошибочному выводу о невозможности правового регулирования складывающихся в нем отношений.

Мы исходим из того, что цифровое пространство России является частью её суверенного пространства, в котором наша страна имеет возможность самостоятельно определять законы, правила, правоприменение, национальную стратегию и безопасность. Под цифровым (информационным) пространством мы понимаем всё пространство, где происходит «доставка» информации: социальные сети, где коммуницируют наши граждане, государственные услуги, интернет-сервисы (поисковики, интернет-коммерцию, рекламные системы), а также всё «электронное» пространство – цифровые устройства, программные средства и операционные системы.

В целях обеспечения реализации и защиты прав и свобод человека и гражданина в цифровом пространстве РФ предлагается определять его, как совокупность цифровых технологий, цифровых ресурсов, цифровой инфраструктуры, субъектов, обеспечивающих их создание, функционирование, развитие и использование, цифровых процессов, средств цифрового

взаимодействия, а также системы регулирования возникающих при этом общественных отношений. Понятия «цифровое пространство», «цифровая среда» и «цифровая сфера» мы предлагаем считать синонимами в рамках данного Доклада.

Основу Доклада составляют материалы, которые были подготовлены и использованы в ходе работы над проектом Концепции защиты прав и свобод человека и гражданина в цифровом пространстве РФ и «дорожной карты» по её реализации, проекта концепции Информационного (Цифрового) кодекса РФ, экспертных заключений Совета на различные законодательные инициативы последних лет.

Доклад состоит из двух частей. В первой части описан широкий спектр новых рисков для прав граждан, общества и государственного суверенитета России, порождаемых «галопирующей» и хаотичной цифровизацией, реализуемой вне правового поля. Вторая часть отвечает на вопрос «что делать?», содержит концептуальные подходы к осмыслению проблематики цифровизации, а также законодательные, организационные и иные решения по «стерилизации» и предупреждению указанных рисков.

Часть 1. «Цифровизация» сегодня: вызовы и угрозы правам человека и конституционному строю Российской Федерации

Цифровая трансформация государственного и муниципального управления, экономики и социальной сферы является одной из национальных целей развития нашей страны на период до **2030** года и на перспективу до **2036** года[5]. Цифровая трансформация, согласно принятому подходу, должна содействовать:

– прорывному развитию страны,

– повышению уровня жизни граждан, созданию комфортных условий для их проживания,

– раскрытию таланта каждого человека.

Однако совершенно очевидно, что **цифровая трансформация будет способствовать развитию государства, общества и каждого отдельного человека только при соблюдении прав и свобод человека и гражданина**. По крайней мере, такова «конституционная философия» нашего общества и государства.

1.1. Идеология цифровизации – вызов ценностям достоинства, свободы и прав человека

1.1.1. «Цифровые» и «аналоговые» права: что мы защищаем?

В современной дискуссии можно выделить два аспекта, касающихся соблюдения «традиционных» («аналоговых») прав и свобод человека. С одной стороны, в процессах цифровизации эти права нарушаются и ограничиваются, причем сами формы дезорганизации принимают неочевидный и спорный характер. С другой стороны, происходит «перенос» некоторых прав в цифровое пространство, где возникают производные «цифровые права»[6] – особые цифровые «проекции» прав. При этом «цифровые права» также страдают от хаотичной, мозаичной, навязываемой цифровизации.

Наша принципиальная позиция состоит в том, что личность гражданина, его суверенитет, достоинство и неприкосновенность частной жизни

[5] Указ Президента РФ от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года».

[6] Здесь мы не имеем в виду отраслевое определение в ст. 141.1 Гражданского кодекса РФ, где под «цифровыми правами» понимается имущественное право в отношении активов в цифровой форме.

обеспечивают и оберегают указанные в Конституции, а также в ратифицированных международных правовых актах, положения об основных правах и свободах человека и гражданина. В цифровом пространстве эти основные права и свободы имеют соответствующие «преломления»: право на защиту цифровой идентичности, право на доступ или отказ от доступа к цифровым технологиям, право на защиту ментальной неприкосновенности личности и защиту от манипуляции, право на защиту биометрических и других персональных данных, право на забвение и так далее.

В своей совокупности «цифровые» права формируют «**цифровой суверенитет» личности**, в основе которого лежит понимание, что человек не равен «цифровому вектору», то есть набору цифровых коэффициентов, вычисленных цифровыми платформами и помещённых в тот или иной реестр. Вышеперечисленные права и свободы, суверенитет личности, включая их цифровые аспекты, сейчас находятся в зоне прямых рисков, связанных с неконтролируемым и сверхбыстрым развитием цифровой среды.

Здесь важно сделать принципиальное замечание. Совершенно естественно, что регулирование цифровой среды должно сохранять и защищать права граждан на информированность, выражение своего мнения и т.д. Однако защита прав и свобод человека и гражданина – это не обеспечение максимальной индивидуальной свободы людей и экономических агентов в абсолютно свободной от регулирования среде[7]. Бенефициарами такого понимания подхода к деятельности по защите основных прав и свобод выступает очень незначительное число граждан и экономических агентов, а большая часть граждан (как, впрочем, и экономических агентов) остается за пределами правового регулирования и защиты.

Мы рассматриваем «цифровые» проблемы и меры по их решению, исходя из приоритета прав, свобод и законных интересов каждого человека и гражданина в регулировании отношений в цифровой среде. Условием соблюдения приоритета выступает достижение и поддержание баланса интересов личности, общества и государства, обеспечение государственной и общественной безопасности, нравственности и социального порядка.

[7] Мы не разделяем известную (но ни на чём не основанную) идеологическую установку «Интернет – это зона абсолютной свободы», поскольку в разумном и справедливом обществе не может быть «зон», свободных от морали, регулирования и правопорядка. Если какие-то государства готовы принимать и продвигать у себя такую модель неконтролируемого развития цифровой среды, это их ответственность и выбор.

Соответственно, признанию и защите в цифровом пространстве РФ подлежит **весь объем конституционных прав и свобод человека и гражданина**. Разработка и принятие нормативных правовых актов, подзаконных актов, документов стратегического планирования и иных документов в рамках цифровой трансформации, внедрение новых цифровых технологий не должны отменять или умалять права и свободы человека и гражданина, закрепленные законодательством РФ.

1.1.2. Идеология ускоренной цифровизации отрицает ценностные основы конституционного строя

Анализ российских и зарубежных практик цифровизации, связанных с ними вызовов правам и свободам человека составляют основное содержание первой части доклада. Однако прежде всего необходимо обозначить серьёзную проблему, о которой сегодня в публичном поле говорится незаслуженно мало.

Это проблема противоречия «идеологии цифровизации», «дискурса цифровизации» и ценностных, идейных основ нашего конституционного строя. Более того, дискурс тотальной цифровизации по своим ценностным установкам, пониманию человека, его природы и предназначения находится в непримиримом противоречии с ценностными основами российской культуры. Таким образом, идеология массовой, «ковровой» цифровизации, в ускоренном темпе, в том её виде, в каком она продвигается энтузиастами и проповедниками «цифры», представляет собой не только попытку легитимации происходящего в этой сфере, но и самостоятельную угрозу гражданскому и конституционному сознанию нашего общества.

Необходимо отметить, что сегодняшняя цифровизация и сопутствующая ей идеология являются ядром и движущей силой глобального научно-технологического и общественно-политического процесса – т.н. «НБИКС-революции», активно продвигаемой «евангелистами» нового мирового порядка»[8]. Проблематика цифровизации продолжает оставаться в фокусе общественного внимания, однако без должного понимания, что она тесно смыкается со всем спектром «больших вызовов» современности (нанотехнологии, биотехнологии, генетические эксперименты, когнитивные

[8] НБИКС – гипотетическое ядро 6-го технологического уклада (включающее нано-, био-, инфо-, когнтивные и социогуманитарные технологии), синергия которых якобы обеспечит всеобщее глобальное процветание и счастье.

технологии, трансформация социальных технологий и т.д.), а также связанными с ними этическими и правовыми вопросами.

Глобальный характер и мощь цифровизации (НБИКС-революции), часто кажущаяся, но впечатляющая эффективность ее «достижений» в отдельных областях общественной жизни создают предпосылки для утверждения в общественном сознании **комплекса утопических представлений**:

– о возможности тотальной исчислимости, количественной редукции феноменов частной и общественной жизни человека;

– о возможности полной предсказуемости и фактической безальтернативности трендов общественного развития;

– о возможности тотального контроля условий и параметров человеческого и общественного бытия.

Принятие указанных представлений (которые в сумме можно обозначить как **радикальный технологический детерминизм**) в качестве руководящих принципов программирования общественного развития означает радикальную же **дегуманизацию** проектного мышления и проектной деятельности (например: отказ от поиска соответствия целей общественного развития структуре человеческой личности (экзистенции), вынесение человека, его классических и традиционных смысловых и жизненных установок за контур принятия решений о целях общественного развития и его методах).

«Образ будущего», соответствующий глобальной идеологии цифровизации, проникающей извне в наше общество и сознание элиты в формате пропаганды, футурологии, программ Давосского форума и Всемирного банка, отдельных «международных стандартов» и пр., можно изложить следующим набором формул:

1) человек, свобода и права человека – это исторически преходящие ценности, «социальные конструкты». Их возникновение обусловлено социально-экономическим и технологическим развитием, которое на определённом этапе истории может потребовать отказа от этих ценностей (уже требует). Новые (в частности, цифровые) форматы жизни человеческих сообществ могут потребовать существенного переосмысления классических представлений о достоинстве личности, правах и свободах человека и гражданина, вплоть до полного отказа от них;

2) дальнейшее развитие человечества неизбежно предполагает глубокую трансформацию исторически сложившихся человеческих сообществ (народов, государств, цивилизаций) под воздействием технологических

факторов, а также – возможно – их селекцию и ранжирование, в зависимости, например, от способности реагировать на глобальные вызовы и угрозы, включаться в соответствующие глобальные кампании и планы действий; в том числе устаревшим и более ненужным становится понятие суверенитета государств, наций, личности;

3) дальнейшее социально-историческое развитие связано с радикальным усилением зависимости человека от новых технологий, а успешность развития обеспечивается максимально полным включением человеческих существ в логику и алгоритмику техносоциальных систем, максимальным отказом от рисков, связанных с человеческой свободой и стремлением к автономии;

4) будущее человечества и человеческих сообществ – это не открытый к изменениям результат взаимодействия, сотрудничества и (возможно) борьбы автономных личностей и социальных сил, а предмет социальной инженерии со стороны технократической элиты, формирующей будущее по «заранее известным» планам и лекалам, с помощью технологий анализа данных и ИИ.

С сожалением отметим, что в медийном и «развлекательном» сегменте российского информационного пространства мы все чаще и чаще сталкиваемся с форсируемыми, навязываемыми сюжетами о мире «управляемого будущего» – без собственно человека (во всяком случае, в его классическом понимании). При этом главный вопрос – **как идеология цифровизации соотносится с нашими ценностями и нашим конституционным правосознанием?** – цифровизаторами даже не поставлен и не рассматривается как важный.

1.1.3. Носители идеологии цифровизации. Возникновение «цифровой власти» и приход нового «цифрового класса»

Идеология цифровизации – отнюдь не плод отвлечённого от реальности алармизма и луддизма. Эта идеология – реальность, ею «заражены» широкие слои мировой технологической и финансовой элиты, создатели массовой культуры, международные организации, часть российской элиты, государственных и муниципальных служащих. Уже сегодня, при нынешнем развитии цифровых технологий, эта идеология позволяет «обосновывать» и «оправдывать» практики нового, формирующегося «цифрового класса», претендующего на статус будущего общественного гегемона. В наши дни возможность «узнать всё» о гражданине, а затем использовать данные о нём для рекламы, продаж, пропаганды, манипуляции и управления создаёт новый, особый вид власти над гражданами. А также – головокружительное ощущение

всевластия и всемогущества, или иначе «административный восторг» (Ф.М. Достоевский).

Цифровая власть – особая, новая, она не создаётся обычными механизмами делегирования власти и полномочий, такими как выборы, или назначение, а возникает по факту получения доступа к данным и является фактически отдельной, «параллельной» ветвью социальной власти. Эту новую власть получают чиновники и их ИТ-специалисты (в том числе, в органах региональной и муниципальной власти), а также менеджмент и ИТ-специалисты крупных частных ИТ-корпораций (к которым относятся цифровые платформы, производители смартфонов и операционных систем, интернет-провайдеры и мобильные операторы, операторы уличных камер, кредитные и страховые организации, прочие операторы персональных данных).

Параллельная «цифровая» власть в России и в мире остаётся слабо регламентированной. В нашей стране она не укладывается и в рамки плохо работающего на практике законодательства о персональных данных[9]. Эта власть сейчас проявляет себя как ей угодно, существуя в «серой зоне» или правовом вакууме. Нужно заметить, что большинство менеджеров и специалистов, получающих эту новую власть по факту своего служебного положения или доступу к цифровым инструментам, не являются сотрудниками правоохранительных органов с соответствующим регламентом доступа к информации о частной жизни граждан, не дают присяги и не носят погоны. Они, как правило – гражданские лица, не несущие серьёзной ответственности (в лучшем случае, свобода их действий ограничена Федеральным законом от 29.07.2004 г. № 98-ФЗ "О коммерческой тайне" и общими правилами о дисциплине труда), что создаёт риски утечки, продажи, разглашения данных и манипуляции ими в личных и корпоративных целях.

В массе своей представители «цифрового класса» получают в среднем среднерыночные зарплаты и уязвимы к подкупу, причём их число и возможности доступа к данным быстро растут. У представителей «цифрового класса» сохраняется разрыв между возможностями применения цифровых

[9] Прежде всего, речь идёт о Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и связанных с ним положений отдельных законодательных актов. Вопрос о путях совершенствования указанных актов выходит за рамки данного доклада, но актуальность его несомненна.

технологий и крайне низкой ответственностью за их ненадлежащее или скомпрометированное использование.

Нужно заметить, что «гражданские версии» алгоритмов ИИ, доступные сейчас в виде свободного программного обеспечения не только крупным корпорациям, но и физическим лицам, имеют точность и другие характеристики качества почти такие же, как дорогие промышленные решения, используемые цифровыми гигантами и государством. Фактически это означает, что программные средства, имеющие двойное назначение и большой потенциал нарушения прав и свобод граждан (технологии распознавания лиц и речи, вычисления персональных данных, шантажа и слежки, фабрикации «глубоких фейков[10]» и др.), сейчас доступны кому угодно – как если бы огнестрельное оружие можно было бы купить в любом магазине.

С момента возникновения первых государств и до сегодняшнего дня, во взаимоотношениях «власть-народ», разделительные линии между привилегированным классом и остальным населением традиционно проходили по двум основным признакам: социальному положению и уровню материального достатка. При всех известных изъянах такой градации правила взаимодействия внутри социума являлись понятными и принимаемыми большинством членов общества. С внедрением тотальной цифровизации реальная власть в контексте воздействия на общественно-политические и экономические процессы сосредотачивается в руках разработчиков, владельцев и операторов цифровых технологий и платформ. Такие лица могут не иметь явно высокого социального статуса или больших финансовых ресурсов, однако их влияние на коммуникации и взаимодействие внутри общества (и, таким образом, на все его слои, включая привилегированный класс) будет возрастать пропорционально внедрению цифровых технологий, заменяющих классические социальные связи, методы коммуникации и способы предоставления услуг. Этот разрыв – ненадолго, мы уже наблюдаем радикальное увеличение достатка и изменение социального положения у представителей нового привилегированного класса.

В классической теории «общественного договора» считается, что привилегированный класс стал таковым с некоего дозволения, санкции

[10] Deep-fake – подделка изображения, видео, речи или документа с помощью нейронных сетей, позволяющая изготавливать неотличимые от реальности фальшивки. Например, они позволяют изготовить видеоролик с известным политиком, где он говорит то, чего никогда не говорил, или подделать запись телефонного разговора.

большей части общества, в силу объективной необходимости эффективно распределять и контролировать использование имеющихся ресурсов и не допускать при этом диспропорции и перекосов при осуществлении людьми взятых на себя социальных ролей. Таким образом, самые предприимчивые, сильные или умные в результате применения своих неординарных способностей оказываются на верхних этажах социальной «пирамиды» и это, с точки зрения народа и государства, в целом справедливо. Однако в цифровую эпоху дистанция для транзита в привилегированный класс нового типа сокращается ровно до одного шага – доступа к «начинке» массовых цифровых платформ и сервисов. Имея возможность вносить коррективы в работу сложных алгоритмических цифровых систем, даже рядовой оператор будет в состоянии, например, улучшить свой «цифровой профиль» или положение в цифровом рейтинге, скомпрометировать работу всей системы или вывести себя за рамки воздействия цифровизации. Оператор технологии, не говоря уже о её владельце и разработчике, до некоторой степени получит функции «цифрового бога», формируя правила «игры» для одних граждан и видоизменяя или отменяя их вовсе для других. Это в свою очередь создаёт основу для развития представлений об исключительности, превосходстве над «обычными» гражданами, неприменимости к представителям нового класса правовых и этических норм, «придуманных для простых смертных».

В случае реализации сценария «прихода нового цифрового класса» государственный аппарат превратится в статиста, не способного к содержательной деятельности по защите своих граждан. На чиновников всех уровней разработчиками, владельцами и операторами цифровых технологий будут накладываться те же правила и те же ограничения, что и на подавляющее большинство граждан. Ограниченный «цифрой» чиновник, пусть и с некоторыми формальными полномочиями, вряд ли сможет обеспечить больше цифровой свободы другим, чем есть у него самого.

Новый «цифровой класс» состоит в первую очередь из ИТ-специалистов, создающих системы слежения, хранения персональных и больших данных, систем ИИ для управления массами людей, транспортом, государственными и медицинскими услугами и т.п., «цифровых клерков», имеющих доступ к цифровым данным и системам, а также их непосредственного руководства. Доступ к цифровым средствам производства и управлению, централизованным базам больших персональных данных даёт широчайшие возможности для управления, манипуляции, несравнимые с теми возможностями, что раньше

давали личные данные граждан, диверсифицированные в бумажном или электронном виде по различным государственным институтам и базам данных.

Фактическое наличие у «цифрового класса» скрытых («теневых») полномочий, возможностей и рычагов воздействия на граждан и общество – при почти полном отсутствии ответственности – создаёт большие риски для прав и свобод граждан России, а также для устойчивости «традиционной» государственной власти. Таким образом, **«идеология цифровизации» – это «работающая» идеология,** имеющая активно растущий «класс-носитель», «пророков», учителей, сторонников, «авангардные отряды» и т.д. **Вопрос: на каком этапе государство и общество осознают эту угрозу?**

1.2. «Цифровые» причины и факторы возникновения рисков для прав и свобод граждан, безопасности общества и государства

1.2.1. Факторы скорости изменений и растущей сложности цифровой среды

Цифровая среда в России и в мире продолжает развивается хаотично, несогласованными усилиями, разрозненными программами и проектами органов публичной власти и крупных корпораций. Никаких единых «правил дорожного движения» в этой среде не создано. Усугубляет ситуацию низкая цифровая грамотность и осведомлённость о цифровой гигиене граждан и обществ в целом, низкая социальная и этическая ответственность крупного и среднего бизнеса при внедрении цифровых технологий.

Бизнес цифровых платформ и сервисов исповедует правовой и этический нигилизм, считая свою деятельность по сбору данных граждан и предоставлению цифровых услуг не только внеправовой, но и вне-моральной[11]. Многие хозяйствующие субъекты в лучшем случае готовы принимать на себя символические этические обязательства без реального общественного или государственного контроля за их соблюдением. Бизнес-модель крупных цифровых платформ зачастую основывается на стремлении объявить себя «нейтральным посредником», самоустранившись от какой-либо ответственности за предоставляемые услуги и сервисы и действуя по принципу «бери или уходи». Новые цифровые технологии и сервисы используются бизнесом в первую очередь с целью получения конкурентных преимуществ и извлечения сверхприбыли, но никак не в интересах защиты прав, свобод и законных интересов граждан.

Усилению рисков и угроз способствуют **особые факторы риска цифровой среды, зачастую не осознаваемые операторами и «евангелистами» цифровизации**.

К этим факторам относятся:

– высокая скорость изменений, выражающаяся в сверхбыстром, экспоненциальном развитии цифровой среды;

[11] Деятельность цифровых платформ (поисковиков, рекламных систем, мобильных операторов и т.п.) в области пользовательских данных напоминает массовый «бизнес» по обналичиванию денег в 1990-х и 2000-х годах, когда такая деятельность не только практически не преследовалась по закону, но и не считалась аморальным или вредным занятием, потому что «все так делали».

– высокая, постоянно растущая сложность цифровой среды.

Сохраняется стремительно углубляющийся **разрыв между скоростью процессов цифровизации и скоростью осознания их обществом**. Наше общество и органы публичной власти не до конца оценивают реальность и глубину развивающихся угроз, зачастую не видят негативные стороны происходящих процессов цифровой трансформации и не принимают в расчёт усиливающуюся конкуренцию между государствами и глобальными ИТ-корпорациями, развивающуюся под привлекательными лозунгами «удобства и пользы» цифровых технологий. В результате процессы цифровизации государства и общества идут со значительным опережением развития законодательства, призванного защищать права и свободы личности в цифровой среде и обеспечивать информационный (цифровой) суверенитет российского государства.

Стремление к тотальной цифровизации имеет в своей основе **иллюзию полного контроля над цифровой средой**, которой подвержены многие убеждённые «цифровизаторы» (в том числе, среди государственных и муниципальных служащих). В реальности современная цифровая среда настолько сложна, что никто не может контролировать и обезопасить её полностью. Непредсказуемость динамики и направлений развития цифровой среды является ее объективной характеристикой.

К числу факторов, увеличивающих непредсказуемость цифровой среды, относятся:

– ненадёжность программного обеспечения. Не существует программного обеспечения без ошибок и «дыр» в безопасности. Ускоряющийся темп внедрения и сокращение сроков тестирования пропорционально снижает надёжность программного обеспечения цифровых платформ[12];

– разнообразие используемых одновременно технологий. Постоянно растущее разнообразие используемых платформ, приложений, устройств, протоколов создаёт так называемый «комбинаторный взрыв» в цифровой среде, не позволяющий предсказать все возможные комбинации условий, при которых могут возникать сбои и катаклизмы, «дыры» и утечки;

[12] Отметим здесь продолжающиеся многочасовые сбои глобальных цифровых платформ, затрагивающие сотни миллионов пользователей по всему миру. Если от сбоев не застрахованы глобальные лидеры цифрового мира, имеющие десятки тысяч программистов и миллиарды пользователей – то кто тогда застрахован?

– падение компетенций у масс ИТ-специалистов вследствие широкого использования общедоступных алгоритмов искусственного интеллекта и иных готовых решений (т.н. *low code* или *no code* программирование) для решения базовых задач по программированию без их критической оценки и без фактической работы с программным кодом;

– большое количество самостоятельных игроков. Цифровые платформы и приложения к ним разрабатывают десятки тысяч компаний и миллионы разработчиков. Значительная часть из них недостаточно профессиональна, а часть имеет криминальные намерения;

– скрытая деятельность криминальных операторов и зарубежных спецслужб. В цифровом пространстве оперирует множество мошенников, манипуляторов и представителей спецслужб. Они находят «дыры» в программном обеспечении устройств и платформ, взламывают протоколы доступа, производят троянское программное обеспечение для захвата устройств и платформ[13] – в целях кражи данных, денег и слежки. Количество сбоев в используемых программно-аппаратных комплексах, программных и аппаратных «закладок», дыр и «задних дверей» для проникновения криминала и враждебных государственных операторов всё время растёт, а соответственно – каждый год растёт и количество утечек персональных и чувствительных государственных и коммерческих данных.

Это означает, что **цифровая среда постоянно создаёт новые риски для безопасности граждан и общества в силу своей сложности**: **никто не может быть уверенным в своей способности контролировать эту среду или обеспечить безопасность в ней**. При этом у органов публичной власти сохраняется **иллюзия контроля**. В результате граждане, государство и общество всё больше полагаются на цифровую среду в организации своей повседневной жизни.

1.2.2. Большие данные, искусственный интеллект, технологии идентификации как факторы риска

В последнее десятилетие в сфере сбора, обработки и применения данных о людях, территориях, организациях, произошла настоящая технологическая революция. В области цифровой идентификации людей по их биометрическим данным – по лицу, голосу, походке, фигуре и т. п. – за счёт развития технологий

[13] Утечка «Седьмой сейф» от WikiLeaks показывает, что только в одном Центральном Разведывательном Управлении США над взломом устройств и цифровых платформ по всему миру работают многие тысячи специалистов.

ИИ впервые в истории достигнута технологическая точность распознавания, превышающая возможности человека. Это же относится к идентификации материальных объектов, зданий, транспорта, номеров автомашин, животных, надписей, брендов, географических объектов и т.д.

В области сбора и обработки «больших данных», являющихся «топливом» для ИИ, получены технологические прорывы, позволяющие вести небывалую в истории массовую слежку за гражданами: выявлять и прослеживать места проживания, маршруты, склонности, взгляды, собирать биометрические данные, личные особенности и привычки граждан. На этой основе формируется т.н. «цифровой след» гражданина – **в бесконтактном и безакцептном режиме**, на базе анализа данных с камер, смартфонов, автомобилей, аккаунтов в социальных сетях, банковских счетов и т.п.

Динамично развивающимся направлением разведки по открытым источникам (*OSInt, Open-Source Intelligence*) стала **геопространственная разведка** (*GeoInt, Geospacial Intelligence*), позволяющая без осуществления взломов устройств и иных неправомерных действий идентифицировать места, где были сделаны пользовательские фотографии. Тактики GeoInt включают анализ многочисленных открытых профилей в социальных сетях, инструменты поиска по похожим фотографиям, использование панорамных и 3D-карт и иные технологии. Благодаря этому даже в отсутствие геометки или общеизвестных достопримечательностей сегодня можно установить место, где была сделана практически любая опубликованная фотография.

Различные экономические и криминальные субъекты получили технологическую возможность использовать эти беспрецедентные по объёму и глубине данные о гражданах для рекламы, манипуляции и противоправных действий. Эта возможность реализуется игроками цифрового мира с полным пренебрежением к интересам и правам «исследуемого» индивидуума, который воспринимается ими, как «цифровой конструкт», «вектор коэффициентов» вместо личности. Это **новый набор серьёзных рисков** для личных и общественных прав и свобод, не встречавшийся ранее. Государство и общество должны осознать эти риски, а также создать средства для их купирования.

1.2.3. «Серая зона» оборота данных

В цифровом пространстве продолжается массовый, тотальный сбор персональных данных граждан, в том числе биометрических (несмотря на принятый в **2022** году федеральный закон[14], содержащий множество ограничений на этот счёт). Сбор персональных данных осуществляют частные цифровые платформы (социальные сети, поисковики, рекламные системы, мобильные операторы, провайдеры доступа в Интернет, интернет-СМИ, мессенджеры) и публично-правовые образования. Часто такой сбор данных производится **в бесконтактном режиме**, без согласия и даже без ведома человека (особенно это касается городского видеонаблюдения, съёма данных с устройств мобильной связи, журналов доступа в Интернет, истории посещения сайтов и поисковиков).

Можно сказать, что данные собирают все, кто может до них дотянуться, несмотря на требования законодательства о персональных данных[15]:

- данные собираются цифровыми платформами не для решения конкретной задачи, а «вообще»;
- данные сливаются в единые, гигантские базы с максимально полными «профилями» граждан;
- данные не удаляются после выполнения конкретной задачи, а хранятся «вечно»;
- данные собираются для «профилирования» граждан, которое представляет собой систематический и целенаправленный процесс сбора, фиксации и классификации данных, относящихся к отдельным лицам (или социальным группам). Автоматизированное алгоритмическое профилирование в эпоху «больших данных» позволяет формировать детальные и точные профили на каждого гражданина на основе интеллектуального анализа данных, собранных из различных источников.

Классификация граждан посредством алгоритмов ИИ основана на выделении групп людей с общими характеристиками. Эти характеристики предоставляют цифровым сервисам сами граждане, также они могут быть

[14] Федеральный закон от 29 декабря 2022 г. № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации».

[15] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

собраны и вычислены посредством бесконтактного или даже скрытого наблюдения за гражданами. Решения, основанные на данных, могут касаться целых групп лиц, но могут влиять и на отдельных индивидуумов. Одним из примеров этого является ценовая дискриминация отдельных пользователей, основанная на их возрасте, привычках или уровне доходов.

В других случаях прогнозы, основанные на обобщениях профилей, влияют на всю группу и выделяют её из остального общества. Примером может служить «общий кредитный рейтинг района», принятый кредитными компаниями, который побуждает компании предоставлять кредитные продукты людям, живущим в данном районе, таким образом, который не имеет никакого отношения к их индивидуальным условиям, но основан на совокупном балле района.

Основной объем оборота больших пользовательских данных (биометрия, геоданные, данные о транспорте, производстве, движении отдельных граждан и масс людей, финансовых транзакциях граждан и юридических лиц, частных покупках, коммуникациях и др.), собираемых хозяйствующими субъектами и публично-правовыми образованиями продолжает оставаться **в «серой правовой зоне»**. Гигантские массивы данных о гражданах собираются и вычисляются без их согласия (и даже осведомлённости о факте сбора), а затем многократно копируются, передаются, перепродаются, используются для рекламы, слежки, манипуляции, «скоринга» (в основном в скрытом режиме, но иногда и совершенно открыто).

Данными своих клиентов практически открыто торгуют мобильные операторы, предоставляя желающим данные о местоположении, покупках, сообщениях своих абонентов широкому кругу корпоративных клиентов. Между тем, абоненты сотовых операторов платят им за связь, но не делегировали им полномочия дополнительно зарабатывать на своих персональных данных и вмешиваться в личную жизнь. Другой яркий пример – заблокированный в **2025** году телеграм-бот «по пробиву» персональных данных «Глаз Бога», который за годы своего существования собрал сотни тысяч подписчиков и зарабатывал десятки млн. руб. в месяц[16]. Более того, данный инструмент был популярен и у рядовых сотрудников правоохранительных органов, позволяя им получать важную информацию о фигурантах дел без бюрократической волокиты.

[16] Данный информационный ресурс, к сожалению, не является единственным в своём роде.

1.2.4. Растущая угроза: не сбор, а вычисление персональных данных

Существующее законодательное регулирование устанавливает ограничения на сбор и получение персональных данных о гражданах. Однако параллельно прямым нарушениям данного запрета продолжает развиваться новый способ получения персональных данных – их **вычисление** и вычленение по косвенным признакам в «больших данных» с последующим их сведением в «цифровой профиль» гражданина (пользователя).

Так, по поисковым запросам, данным о покупках, общению в социальных сетях, коротким сообщениям (СМС) крупные цифровые платформы, мобильные операторы и другие игроки цифровой сферы могут скомпоновать личный профиль пользователя, включающий его предполагаемые возраст, пол, различные физиологические и психические черты (заболевания), наличие беременности, сексуальные, религиозные и политические предпочтения, семейные обстоятельства, сведения об уровне дохода, а также другие чувствительные личные данные. Далее платформа, провайдер, оператор могут с помощью разнообразных средств идентификации **атрибутировать вычисленные данные**, то есть привязать их к конкретному гражданину, его ФИО, адресу, домашней сети wi-fi, атрибутам смартфона, месту работы и т.п., что даёт широчайшие возможности для цифровой слежки, дискриминации, шантажа и манипуляции. При этом законодательный запрет на сбор персональных данных не будет нарушен явным образом, так как данные о гражданине «вычислены» оператором самостоятельно, без их непосредственного сбора или получения от третьей стороны[17].

Это означает, что регулирование только **сбора** данных не сможет остановить процессы вычисления персональных данных для манипуляции и цифровой дискриминации. Необходимо детальное регулирование способов использования «чувствительных» типов личной информации, например, запрет на использование данных о болезнях (в т.ч., о психических заболеваниях), состоянии беременности, личных и родственных связях, запрет на любой анализ поведения и использование личных данных несовершеннолетних и т.д.

[17] Есть мнение, что этот вид получения данных охватывается понятием обработки персональных данных в 152-ФЗ, но нам это представляется натяжкой; в любом случае на практике 152-ФЗ здесь не применяется.

1.2.5. Новые формы глобальной преступности: цифровое мошенничество и криминал

Цифровая среда значительно расширяет возможности для совершения противоправных деяний: вместо того, чтобы искать индивидуальные, «физические» подходы к гражданам в реальной жизни (на улицах, в транспорте и в организациях), что требует больших издержек, злоумышленник получает в цифровой среде широкий и постоянный доступ к потенциальным жертвам в масштабе всей страны. Государство пока не успевает защитить граждан от этого вала цифрового криминала – ни в области правового регулирования, ни в области правоприменения.

Мы можем это видеть на примере «цунами» мошеннических звонков последних лет, достигшего в **2025** году беспрецедентной цифры в **20** млн. мошеннических звонков ежедневно. Были проданы или украдены из баз данных банков и мобильных операторов личные данные десятков миллионов граждан (ФИО, номера телефонов, номера кредитных договоров и т.п.), украдены сотни миллиардов рублей клиентов банков. Оценка ежегодного фактического ущерба от мошеннических действий, совершаемых дистанционно, колеблется в диапазоне от **200** до **500** млрд. руб. ежегодно, т.е. около **1** млрд. руб. в день.

Цифровая среда не снижает, а **повышает риски совершения преступлений** по следующим причинам:

– лёгкость совершения преступлений. Для кражи данных, шантажа и пр. достаточно нескольких кликов мышкой, не требуется и высокой квалификации (достаточно владения смартфоном или компьютером на уровне базового пользователя и наличия доступа к данным);

– лёгкость сокрытия следов преступлений. Цифровые преступления практически невидимы, у большинства населения и даже у правоохранителей нет эффективного способа для обнаружения преступников. Более того, преступник с достаточным уровнем квалификации и доступа к данным может после совершения преступления уничтожить следы доступа к данным, ведь это просто текстовые файлы журналов работы серверов и приложений;

– отсутствие корпоративного (профессионального) осуждения. Лишь самые вопиющие нарушения закона и морали (такие, как распространение детской порнографии) получают выраженную негативную оценку интернет-сообщества и профессиональных кругов (блогеров, SMM-щиков, рекламораспространителей, журналистов и др.). В остальном действия по

манипуляции пользователями, распространению фейков, травле и пр. далеко не всегда вызывают эффект «потери лица» (репутации) и правовые последствия. Моральные нормы в цифровом пространстве продолжают стремительно демонтироваться. Это приводит к ощущению «несерьёзности» происходящего и вседозволенности у пользователей, формирует оправдания в духе «все так делают». Становится «можно всё»;

– **отсутствие неотвратимости.** Несмотря на принятые в **2024** году поправки, ужесточающие ответственность хозяйствующих субъектов за утечки и продажу данных[18], в правоприменительной практике по-прежнему отсутствуют примеры наказания физических лиц, организующих кражу персональных данных. Напротив, общественный резонанс вызывают случаи, когда утечка базы данных в миллионы пользовательских строк обходилась компании в несколько десятков тысяч рублей административного штрафа. Вследствие этого кибермошенники и коррумпированные инсайдеры продолжают оставаться уверенными в своей безнаказанности[19];

– **сбор, хранение и использование персональных данных в «серой правовой зоне» приводит к тому, что эти данные фактически стали товаром.** В России по-прежнему можно купить все данные на конкретного гражданина за несколько тысяч рублей. Специально проводимые эксперименты показывают, что за несколько часов можно купить набор фото и видео о своей поездке в другой город, полученный с камер системы «Безопасный город» – посмотреть на себя в аэропорту и на улицах посещённого города. Система «коврового» видеонаблюдения за всеми гражданами, созданная якобы для безопасности – уже страдает уязвимостями, вызванными не «закладками» и «троянами», а человеческим фактором и коррупционной ёмкостью таких сервисов.

Судя по тому, что до сих пор, в ситуации «девятого вала» телефонного мошенничества, в открытых источниках нет сведений об уголовных делах в отношении цифровых коррупционеров, торгующих данными, этот вид преступной деятельности сейчас остаётся безнаказанным. **1** апреля **2025** г. был принят федеральный закон № 41-ФЗ, направленный на борьбу с телефонным

[18] Федеральный закон от 30 ноября 2024 г. № 420-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях».

[19] На криминальных форумах «теневого Интернета» (Даркнета) продолжают размещаются заказы на поиски инсайдеров в банках, примерно такого содержания: «нужны все записи клиентов такого-то банка в городе N, у которых на счету не менее X тыс. руб». И продавцы этих данных быстро находятся.

мошенничеством, однако для того, чтобы он полноценно «заработал», потребуется время и десятки подзаконных нормативных актов[20].

1.2.6. Проблема «невидимок» в ИИ

Системы ИИ, массово и систематически внедряемые в государственное управление, управление городской средой, транспорт и т.п., в подавляющем большинстве представляют собой «чёрный ящик», в котором невозможно увидеть причины принятия решений и провести надёжный аудит алгоритма. Обнаружить наличие случайных или чаще умышленных «закладок» в такой системе, основанной на предварительном автоматическом обучении нейронных сетей на массивах образцов («датасетах») – значительно сложнее, чем при поставке традиционных ИТ-систем, основанных на прозрачных алгоритмах и правилах. Это позволяет разработчику или поставщику при поставке предобученной системы ИИ закладывать в неё «невидимок» – объекты, которые не распознаются системой и обходят её правила[21].

Например, уже сейчас поставщики систем распознавания лиц для домовых (подъездных) камер предлагают сделать отдельного жильца «невидимым» для городской системы распознавания лиц[22]. Есть также криминальная услуга по превращению номера автомобиля в «невидимку» для дорожных камер ГИБДД, в результате чего на этот номер перестают приходить штрафы за нарушение ПДД. Заметим, что услуга на рынке есть, а о случаях пресечения такой деятельности и наказания виновных по-прежнему ничего не слышно.

При этом культура заказа, проверки на безопасность, регламентной передачи заказчику инфраструктуры, архитектуры и алгоритмов нейронной сети и самой системы ИИ сейчас в России слабо развита, как и процедуры внешнего аудита систем ИИ. Легко представить себе последствия внедрения подобных «невидимок» в системы распознавания, используемые при проходе на режимные объекты, поиске преступников и т.п.

---

[20] Самостоятельную группу рисков, связанных с данным законом, образуют риски, связанные с дополнительным сбором персональных данных граждан (в том числе, биометрических) и их хранением в отдельной государственной информационной системе.

[21] В системах распознавания, построенных на нейросетях, достаточно встроить промежуточный нейронный «слой», портящий распознавание «невидимок» из «белого списка». Чтобы обнаружить наличие такого «лишнего» слоя, ИТ-специалистам заказчика или внешнему аудитору ИИ-системы нужно иметь очень высокую квалификацию.

[22] Внешний наблюдатель не сможет сказать наверняка, куда вносятся закладки в описанном случае – в обучающие данные для нейросети или в алгоритм обработки распознанных идентификаторов гражданина или автомобиля, но в данном случае это не важно.

1.2.7. Коррупционная ёмкость цифровой среды

Вопреки заверениям идеологов тотальной цифровизации, цифровая среда не снижает возможности коррупции, а расширяет их, поскольку:

1) **позволяет эффективно скрывать следы коррупционной активности** (стирать журналы доступа и т.п.), в том числе, путём проведения расчётов за коррупционные услуги анонимно и трансгранично (например, при помощи криптовалют);

2) **«ретуширует» факт причинения вреда людям**, поскольку у мошенников и коррупционеров, оперирующих в цифровой среде, возникает принципиальный, «встроенный» конфликт восприятия пользователя цифровых систем не как личности с её интересами и правами, а как «цифрового конструкта», вектора из вычисленных маркетинговых и поведенческих коэффициентов, который не имеет права на справедливость и человеческое отношение;

3) **снимает ответственность,** поскольку внедрение систем ИИ, которые в формате «чёрного ящика» якобы беспристрастно решают судьбу людей (зачастую в очень важных для них ситуациях: получения кредита, участия в образовательной олимпиаде, трудоустройстве и пр.), позволяет коррупционеру иметь совершенное прикрытие для продажи услуг по «подкрутке» любых цифровых оценок и рейтингов («ведь это ИИ решил!»).

На современном этапе решения, «принятые ИИ», становятся выше судебных актов, поскольку последние имеют устоявшиеся и прозрачные механизмы оспаривания, а решения ИИ преподносятся, как финальная точка в любом арбитраже. По сути, ИИ используется для **легитимизации произвольных решений**, в том числе незаконных или дискриминирующих граждан. Можно предположить, что с углублением цифровизации, введением частичных или полных социальных рейтингов ассортимент коррупционных услуг значительно расширится.

1.2.8. Ненадёжность носителей данных

Цифровизаторы в органах публичной власти энергично ведут нашу страну к ситуации, когда в большинстве областей взаимодействия граждан и бизнеса с государством (публичные услуги, ЗАГСы, земельный кадастр, образование, медицина, налоговые отношения и т.п.) **оригиналом документа будет признаваться его электронная версия**, а печатная версия – только копией. Это направление движения «в цифру», перехода на «цифровой документооборот», которое обосновывается удобством и повышением контроля, в реальности

создаёт многочисленные риски, среди которых основным выступает компрометация и потеря данных и документов.

Цифровые документы, вопреки представлениям энтузиастов цифровизации, гораздо более подвержены утечке, краже, искажению, потере, компрометации – по следующим причинам:

1) **«Сверхпроводимость» цифровых копий.** Лёгкость тиражирования и передачи цифровых копий на порядок выше, чем у бумажных документов, что позволяет их легко копировать при краже, а также делает целевой аудиторией мошенников не одну организацию, а сразу всю страну, и создаёт принципиально новые типы массового мошенничества, наподобие веерной рассылки в тысячи адресов фишинговых писем в электронной почте или веерных звонков «от службы безопасности банка». Это уже реализующиеся, актуальные угрозы. Продолжают поступать сообщения о мошенничествах с недвижимостью при помощи подделки данных цифровых кадастров и реестров (с помощью коррумпированных ИТ-специалистов). Скрыть врачебную ошибку в электронной карте стало гораздо проще: чтобы подстраховаться на случай возникновения претензий у пациента или его родственников, нужно просто post factum изменить данные врачебного приёма или назначений. Этот риск усугубляется малой осведомлённостью об информационных технологиях у обычных граждан, а также отсутствием института аудита и независимой экспертизы информационных систем, в т.ч. систем хранения и передачи данных.

2) **Низкая надёжность хранения цифровых документов и материалов.** Мало кто из современных «цифровизаторов» отдаёт себе отчёт, какова средняя продолжительность жизни форматов и носителей данных. Мы по-прежнему способны читать тексты и изображения, возрастом в тысячи лет (на бумаге, керамике, камне, металле, пергаменте, дереве и бересте), но уже практически неспособны прочесть цифровые данные конца 1980-х и начала 1990-х годов. Это объясняется следующими обстоятельствами:

а) **носители информации живут не более 15–20 лет:** в большинстве организаций (или на дому) невозможно прочесть данные с дискеты 7’’ (конец **1980**-х), с дискеты 5'' (начало **1990**-х), с дискет 3,5'' (начало **2000**-х); затруднительно найти устройство для чтения когда-то популярных CD или DVD

дисков (начало **2000**-х)[23]. Магнитные жёсткие диски, CD/DVD-диски выходят из строя еще раньше вследствие воздействия внешней среды (ультрафиолетового излучения и магнитных полей, перепадов температур и влажности, царапин, ударов и др.).

б) **средний срок жизни операционных систем и офисных приложений также не превышает 20 лет:** смена более полутора десятков версий операционных систем и офисных приложений для ПК за последние годы сделала «нечитаемыми» огромные массивы старых документов, программ и изображений. Практически нигде не хранятся персональные компьютеры с операционными системами MS DOS, Windows 3.1, Windows 1998 на тот случай, если появится необходимость прочесть «документ из 1990-х». Та же проблема наблюдается и с языками программирования, на которых создаются ИТ-системы, через 20–25 лет их станет невозможно поддерживать и развивать;

в) **уязвимость ИТ-инфраструктуры:** опыт хранения критически важных данных в базах данных, в Интернете, в «облаках» за последние годы показывает, что сбои баз данных, банкротства компаний, закрытие проектов[24], пожары в дата-центрах и др. не позволяют надеяться на сохранность конкретных экземпляров важных данных свыше все тех же **15-20** лет. Более того, в случае чрезвычайных ситуаций природного, техногенного или социального характера в первую очередь исчезнут не бумажные документы, а именно электронные данные – причём мгновенно.

Это означает, что при переходе на электронное хранение всех важных документов и материалов в качестве основного метода хранения государству, бизнесу и обществу придётся обеспечивать мощный, очень дорогой **процесс постоянного резервирования** («бэкапирования») и переноса данных в новые форматы. Этот процесс будет заведомо давать огромные искажения и потери в результате не только неизбежной халатности персонала и программно-аппаратных сбоев, но и в результате того, что в силу нехватки ресурсов далеко не всё будет переноситься в новые форматы, часть данных будет признаваться неважными и оставляться в старом формате или просто удаляться.

[23] Этот список можно продолжить цифровыми аудио- и видеокассетами, которые сегодня не на чем смотреть и слушать, популярным форматом представления графики и звука Flash (использовался при создании интернет-сайтов), картриджами для игровых приставок и др.

[24] Показательный пример – уничтожение миллионов сайтов при закрытии «народного» сервиса хостинга сайтов Geocities. Сервис был запущен в 1994 году, в 2009 году купившая его компания Yahoo закрыла сервис и удалила все сайты пользователей.

Таким образом, оцифровка всех данных не повышает надёжность хранения, а кардинально снижает её в среднесрочном периоде, создаёт риски забвения и потери данных.

При этом оцифровка значительно повышает доступность и «сверхпроводимость» документов и данных для ненадлежащих лиц – мошенников, манипуляторов. Особенно это критично в отношении важных для граждан документов об идентичности, рождении и смерти, собственности, семейном положении, заболеваниях, образовании и т.п., определяющих их жизнь в правовом пространстве.

Мы считаем, что принципиально важно предписать органам публичной власти, учреждениям и предприятиям **сохранять во всех случаях «гибридный» электронно-бумажный документооборот, особенно в тех случаях, когда он содержит персональные данные граждан, признавая бумажную, «твёрдую» копию оригиналом документа.** Граждане, в свою очередь, должны сохранить право на «бумажное» взаимодействие с органами публичной власти по собственному выбору.

1.3. Социально-политические угрозы, связанные с форсированной цифровизацией

1.3.1. Принудительное вовлечение граждан в цифровую среду

В публичном пространстве, в выступлениях публичных должностных лиц, а также в стратегиях по развитию цифровой экономики и ИИ невозможно найти хоть сколько-нибудь убедительных объяснений, зачем нужна сверхбыстрая и тотальная цифровизация всех сфер частной, общественной и государственной жизни. Именно стихийность цифровизации является первым очевидным риском. Вместо последовательной политики, учитывающей потребности и возможности разных групп и слоев населения, учета институциональных особенностей и «болезни» нашего общества, лоббисты предлагают довериться стихии процессов, не отдавая себе отчет о возможностях контроля этих и связанных с ними процессами. Важно отметить, что 35 лет назад наше общество уже доверилось стихии рынка, обещаниям быстрого оздоровления экономики и застойного общества, радикального повышения эффективности производства и осознанного вовлечения граждан в общественные процессы. Стоит ли повторять допущенные ошибки, тем более что население с опаской относится к любым подобным «стихийным обещаниям»? Ведь в конечном счете за всеми призывами и обещаниями нет главного – лица, готового принять на себе персональную ответственность за возможные негативные последствия.

Обычно аргументы «евангелистов» цифровизации и их экспертов сводятся к банальностям маркетингового и журналистского толка: «это инновационно», «нельзя стоять на пути прогресса», «весь мир уже идёт туда», «нам нельзя опоздать», «всё равно все там будем», а кроме того, «это же очень удобно», «вот смотрите, что можно сделать на вашем замечательном смартфоне!»[25].

Заметим, что **ни в одном документе стратегического планирования нашей страны нет такого национального приоритета или цели, как «удобство».** Любое «удобство» необходимо рассматривать в контесте его потенциальной устойчивости при различных сценариях развития социально-экономической, внутри- и внешнеполитической ситуации, а также интереса разных групп и слоев населения. Не исключено, что цифровое нововведение

[25] Мы могли бы привести длинный список цитат из высказываний конкретных должностных лиц и руководителей корпораций за последние годы о невероятных благах цифровизации, но не будем здесь этого делать – все мы и так слышим и читаем эти смелые прогнозы и эмоциональные призывы ежедневно.

будет восприниматься как существенное улучшение среди представителей одной группы и как ухудшение для другой (молодежь и пожилые люди, предприниматели и потребители). Поэтому при рассмотрении вопросов цифровизации принципиально важно исходить не из абстракции «удобство», а выявленных в ходе социологических обследований потребностей и возможностей конкретных групп населения.

Представляется, что сегодня важно не отказываться от цифровизации, а сделать ее разумной и контролируемой. В частности, необходимы исследования: диагностические, позволяющие предложить действительно концептуальное решение в части поэтапного развития цифровой среды, учитывающее социальный механизм этого процесса, а также территориальные и воспроизводственные факторы его действия; и мониторинговые – для контроля самого процесса цифровизации. Без подобной информационной обеспеченности мы не вправе говорить о безопасности цифровизации.

Ещё один аргумент, которым цифровизаторы обосновывают тотальный сбор данных о гражданах и всеобщую слежку (камеры на улицах, единые реестры и профили граждан и т. п.) – это безопасность. Это также лукавый аргумент, ложная дилемма, не имеющая прямого отношения к настоящей безопасности.

К сожалению, большое количество программ и стратегий цифровизации и внедрения ИИ (включая ГОСТы и другие отраслевые стандарты) в нашей стране являются некритично переведёнными методичками западных организаций (от Международной организации по стандартизации и Всемирного банка до аналитических центров Министерства обороны США). Аргументами для такого некритичного заимствования обычно служат рассуждения о «лучших мировых практиках». В реальности, как легко понять, таких практик ни у кого в мире нет, нет соответствующего опыта и, соответственно, данных, полученных в ходе изучения последствий обвальной цифровизации.

В итоге чиновники закладывают в национальные программы и стратегии планирование **100 %** принудительной цифровизации в области государственных услуг, образования, медицины. **При этом игнорируется право граждан на сохранение традиционных способов взаимодействия с государством, а также медицинские, экономические и технологические ограничения** (возможности доступа у разных социальных групп, стоимость устройств, качество связи, уровень цифровой грамотности, желание и

возможность переходить на «цифру»). В ходе такой «ковровой» цифровизации, которая уже ведётся, никто не спрашивает мнения граждан – хотят ли они быть втянутыми в это цифровое пространство.

Принудительное вовлечение в цифровую среду создаёт для граждан также и чисто материальные, бытовые трудности: необходимость приобретать не всегда нужные в семье электронные устройства для взаимодействия с государством, системой образования, здравоохранения и т.п.[26], необходимость освоения цифровых технологий коммуникации (что может быть трудно для пожилых людей, инвалидов и других уязвимых категорий граждан), отсутствие надёжной связи в отдалённых регионах России и т.п.

Здесь, как и во многих случаях, происходит нарушение естественного права гражданина не использовать цифровые технологии. Гражданин имеет право на отказ взаимодействовать с государством и обществом в электронной форме – без необходимости объяснять кому-либо причины такого решения. Во второй части Доклада мы предлагаем закрепить это право на «отказ от цифры» законодательно.

1.3.2. Информационные посредники, «уберизация экономики», снятие социальной ответственности с бизнеса и государства

Наступление цифровизации и усиление влияния цифровых платформ («экосистем») сопровождается принципиальным изменением сущности труда, трудовых и экономических отношений в обществе. Это явление называется «шеринговой экономикой»[27], а также «уберизацией», по названию американской компании Uber, пионера данной бизнес-модели. Кратко её суть можно изложить следующим образом: цифровая платформа предлагает некую услугу как информационный посредник, сводя вместе заказчиков и поставщиков услуги, причём и те, и другие – «свободные экономические агенты», а платформа просто получает комиссию за «сводничество». Таковы сейчас службы такси, совместного использования автомобилей, велосипедов и самокатов, аренды квартир, интернет-агрегаторы товаров, образовательных услуг, новостей и т.п.

[26] Многодетные семьи с несколькими учащимися детьми вынуждены покупать несколько компьютеров или планшетов, а также обеспечивать быстрый Интернет для одновременных занятий в дистанционном режиме.

[27] От англ. «share» – делить, разделять. Имеется в виду разделение ресурсов, услуг, устройств между пользователями.

Данная модель опасна тем, что, приобретая огромную власть над рынком и его «свободными» экономическими агентами, цифровая платформа – информационный посредник – для повышения прибыли **снимает с себя все социальные обязательства.** Например, назначая таксистам рейтинги, беря с них существенную комиссию, постоянно ужесточая условия работы, повышая комиссию и требования к условиям труда, платформа-посредник не отвечает за них, как за работников, не имеет ответственности по трудовому законодательству, то есть не оплачивает им отпуска и листы нетрудоспособности, не имеет обязательств по декретным отпускам и иным выплатам[28].

Пользующийся платформой работник является самостоятельным агентом (например, самозанятым или индивидуальным предпринимателем). При этом в реальности он – фактически наёмный работник, получающий относительно невысокую зарплату, не имея никакой социальной защищённости, предусмотренной Трудовым кодексом РФ, так как формально у него нет нанимателя. Он работает с ненормированным рабочим днём, без отпусков, отгулов, сверхурочных, бюллетеней, двух оплаченных месяцев при увольнении и прочих социальных гарантий работника. Если работник такой системы заболел, не вышел на линию – он мгновенно лишается заработка.

Перед обществом и государством информационный посредник, как вообще принято при продвижении идеологии цифровизации, обосновывает своё существование стандартными аргументами **инновационности** и **удобства**. Действительно, такси стало приезжать быстро, значит, с точки зрения цифровизаторов это – полезная для общества бизнес-модель, не требующая особого регулирования. Между тем, в этой модели сформировалась серьёзная **социальная угроза** трудовым правам граждан и стабильности общества[29].

Более того, за последнее десятилетие в России несколько раз делались попытки ввести «уберизованную» медицину, в которой цифровая платформа за комиссию сводила бы между собой врачей и больных, также ни за что не отвечая по существу. Эти попытки будут продолжаться, потому что уберизация

[28] Известны отдельные примеры из судебной практики зарубежных стран, когда суды признавали отношения между работником и цифровой платформой трудовыми, однако они пока не носят системного характера. На эту проблему неоднократно обращала внимание Международная организация труда (МОТ).

[29] Например, в сфере такси работают миллионы граждан, для которых это стало профессией и единственным источником заработка.

рынков даёт огромные прибыли инфопосредникам. Такие же попытки «уберизации», замены учителей на информационных посредников и «уберизованных» репетиторов наблюдаются и в сфере образования.

Лексика цифровизаторов характерна и показательна: в своих программных заявлениях они открыто говорят и пишут о «*нераспакованных отраслях*» образования и медицины, имея в виду будущие огромные прибыли и для тех, кто «распакует» (то есть, по сути, приватизирует эти отрасли первым). Фактически же уберизация нивелирует, отменяет последние сто лет прогресса в деле совершенствования социальных отношений и защиты прав трудящихся как при социализме, так и при капитализме, возвращает нас во времена дикого капитализма **XVIII-XIX** веков.

Развитие уберизации и информационных посредников в формате дикого капитализма производит социальную напряжённость. Под наше общество закладывается «социальная бомба» в виде поражённых в правах миллионов граждан, управляемых программными средствами ИИ и дискриминируемых всемогущими информационными посредниками ради прибылей[30]. Эта «бомба» может сработать в недалёком будущем, если не начать регулировать и контролировать деятельность информационных посредников. В этой связи Совет возлагает большие надежды на проект федерального закона «О платформенной экономике», разработка которого активно ведется в настоящее время. Он должен состоять не из «индульгенций» для информационных посредников, а из ясно определенных правил поведения, неисполнение которых повлечет за собой реальную ответственность.

Другим аспектом цифровизации является проблема доступности услуг, сервисов и в целом создаваемого цифрового пространства для людей с разными ограничениями восприятия (слухового, зрительного, интеллектуального), речи или моторики рук. Таких людей в нашей стране со статусом «инвалид» и без него – десятки миллионов. Однако ни в одной концепции или программном заявлении сторонников цифровизации не упоминается проблема обеспечения доступности.

[30] Моделью такой социальной напряжённости в форме противостояния работников и инфопосредников может служить затяжной конфликт водителей и сервиса Яндекс.Такси, с пикетами и демонстрациями у офиса, петициями и забастовками, а также акции европейских водителей против компании Uber в европейских столицах, в некоторых случаях собиравшие сотни тысяч протестующих, с элементами беспорядков, уличного насилия, поджогами автомобилей и т.п.

Наконец, есть не менее значимая проблема «атрофии аналогового навыка». Очевидно, что цифровой мир не застрахован от энергетических и технических коллапсов. Длительное «проживание» в мире цифры приводит к забыванию аналогового порядка вещей, навыков и проч. Поэтому лица, осуществляющие критически важные функции, должны поддерживать умение выполнять конкретные действия в аналоговой форме. Последнее требует системы регулярных мероприятий на подобии тех, что обеспечивают технику безопасности и навыки действий на случай чрезвычайных ситуаций.

1.3.3. Цифровая дискриминация граждан на основе собираемых и вычисляемых данных

В общественной практике применения ИТ-систем произошел «цифровой поворот»: **интеллектуальные системы перешли от поддержки решений, принятых людьми, к принятию решений за них**. Этот сдвиг вызывает серьёзные опасения относительно влияния решений, принимаемых алгоритмами, на отдельных граждан, социальные и демографические группы и общество в целом.

Сбор и классификация личных данных цифровыми платформами и их алгоритмами обработки больших данных позволяют классифицировать и «сортировать» людей, присваивать им характеристики и рейтинги, а затем управлять ими и дискриминировать их различными способами, в зависимости от вычисленной категории, класса, рейтинга (например, платёжеспособности). Легко увидеть, что здесь возникают широчайшие возможности для социальной дискриминации граждан на основе закрытых, частных алгоритмов принятия «автоматических» решений – в области кредитования, лечения, трудоустройства, образования и т. п., нарушающих принцип равенства граждан. Так уже работают кредитные алгоритмы в крупных банках, назначение цен на авиабилеты, поездки на такси и т.п.

Для пояснения мысли о дискриминации на основе персональных данных приведём простой мысленный эксперимент с дискриминацией в области трудоустройства. Предположим, некая девушка в течение трёх дней отправляла в поисковые системы запросы о товарах для беременных. Эти данные были собраны системой обработки «больших данных» поисковика, ее профиль в поисковике получил соответствующую пометку (категорию). Далее к профилю получили доступ бизнес-партнёры поисковика, среди которых – кадровые агентства. У них, в свою очередь, тысячи корпоративных клиентов – кадровых отделов компаний, органов публичной власти и др. Кадровик одного

из клиентов, изучая резюме этой девушки, которая ищет работу, увидел пометку «возможно, беременна», и перешёл к резюме других соискателей. В этот момент поисковик, кадровый сервис и кадровик компании совершили по отношению к девушке уголовное преступление, предусмотренное ст. **145** Уголовного кодекса РФ (отказ в трудоустройстве по основанию беременности). При этом никто из названных субъектов не только не считает себя невиновным, но даже и не осознает факта совершения преступления: «*А что такого, это же просто обработка данных и профилирование»*.

Даже если упомянутые субъекты будут отрицать, что отказ в трудоустройстве произошел именно по описанный выше причине, ни у общества ни у государства нет возможности проверить, так ли это на самом деле. Нет ни процедуры, ни институтов независимой инструментальной экспертизы потоков персональных данных и защиты прав их носителей.

Другой пример – **ценовая дискриминация.** Известно, что сидящие рядом пассажиры самолёта иногда могут заплатить за идентичные посадочные места цены, отличающиеся в разы. Цена билета зависит от множества факторов: сезона, времени покупки, наличия мест, «налёта миль» и т.п. В эпоху интернет-торговли билетами цена также может зависеть от цифрового профиля клиента, и прежде всего от оценки его платёжеспособности системой бронирования: богатым (с точки зрения алгоритма) клиентам выставляют более высокие цены.

Тот же принцип ценовой дискриминации действует при назначении стоимости поездки в такси в некоторых агрегаторах (например, клиент, вызывающий такси с дорогого смартфона или от входа бизнес-центр класса «премиум», скорее всего, получит более высокую цену[31]), при заказе в интернет-магазинах (стоимость товара и его доставки может значительно отличаться в зависимости от коммерческого профиля клиента и истории его покупок и т.п.

Заметим, что власти Китая уже увидели эту опасность дискриминации на основе «коммерческих» профилей и осознали необходимость регулирования. Еще в **2021** году антимонопольный комитет Госсовета Китая опубликовал руководство, в котором указал, что использование больших данных в ценообразовании представляет собой злоупотребление доминирующим положением компании на рынке. В том же году в Шэньчжэне разработали и

[31] Многочисленные эмпирические опыты подтверждают этот тезис, хотя агрегаторы такси его опровергают.

начали публично обсуждать «Положение по использованию цифровых данных в Шэньчжэньской специальной экономической зоне». В нём предлагается запретить анализ цифровых данных участников интернет-торговли, а также дифференцированный режим ценообразования для клиентов при одинаковых условиях торговли под угрозой крупных штрафов. Нам стоит присмотреться к этому опыту.

1.3.4. Попытки введения социальных рейтингов

Социальный рейтинг – это попытка автоматически приписать каждому гражданину число (набор чисел, вектор, социальный индикатор) его «добропорядочности»: этичности, благонадёжности и законопослушности. На сегодняшний день, насколько можно судить по открытым источникам, в Китае активно применяется социальный рейтинг: каждому гражданину начисляется сколько-то начальных баллов, а затем они зарабатываются или списываются в зависимости от оценки поведения гражданина по различным критериям этичности и законопослушности. Оценивается поведение масс граждан автоматически: с помощью цифровых технологий слежки и анализа. По сути, речь идёт об автоматическом управлении массами людей.

В последние годы в российских медиа появляются «прощупывающие» публикации о перспективах социального рейтинга в России. Проводится мысль, что социальный рейтинг при надлежащей реализации – это в целом «хорошая вещь», помогающая вознаграждать «хороших» граждан и наказывать «плохих».

Отметим, что различные виды автоматических цифровых рейтингов уже работают в нашей стране. Это, прежде всего, кредитный рейтинг банков (на основе кредитных историй) и страховых компаний, рейтинги пассажиров и таксистов, продавцов и покупателей. Симптоматичны попытки введения рейтингов учеников и студентов – вплоть до установки камер в классах с распознаванием эмоций и оценкой уровня трудолюбия и старательности школьника[32].

Цифровой рейтинг пользователя давно уже существует внутри массовых рекламных систем компаний Google Ads, Meta (Facebook), Яндекс, Mail.ru и более мелких рекламных игроков, где пользователю присваивается множество параметров, в том числе один из главных – параметр платёжеспособности, что приводит к скрытой ценовой дискриминации, когда пользователям с разным

[32] Такой эксперимент был начат в 2020 году в нескольких средних школах г. Перми без согласия родителей и завершен досрочно после общественного резонанса.

рекламным рейтингом одни и те же товары и услуги предлагаются по ценам, иногда отличающимся в несколько раз.

Мы считаем, что любой массовый социальный рейтинг обязательно станет жертвой социальных же факторов:

– **положительной обратной связи**, когда программа цифрового рейтингования будет загонять неудачливого гражданина на «социальное дно» без возможности выбраться обратно;

– **криминализации**, включая коррупцию и компрометацию, когда чиновники и программисты, управляющие программами цифрового рейтингования, смогут тайно торговать рейтингами.

Ещё одним следствием введения социального рейтинга будет лишение граждан их прав не по суду, а по воле программ на базе ИИ, которую невозможно будет оспорить ни в суде, ни где-либо ещё. Уже сейчас отказ гражданину в кредите частным банком происходит мгновенно, без объяснений, притом с занесением этого факта в системы кредитной истории. Оспорить это решение и исправить записи систем кредитных историй, как правило, нет никакой возможности.

Фактически перед нами неявное намерение создать параллельную систему прав граждан, получаемых ими не в рамках реализации Конституции РФ и федерального законодательства, а из рук и по воле «цифрового класса», а также ввести **параллельную систему власти**, в которой контроль над населением приобретается не через легитимные механизмы, а по факту и без спроса. Мы часто слышим: нашей стране нужен образ будущего. Вряд ли ожиданиям граждан соответствует образ будущего, которое можно назвать новым («цифровым») крепостным правом: со всеобщей слежкой, цифровым отчуждением, подчинением безличным алгоритмам ИИ под управлением цифровых чиновников.

1.4. Угрозы цифровому суверенитету Российской Федерации

Цифровой суверенитет – одна из важных составляющих «общего» национального суверенитета любого постиндустриального государства. Он включает в себя следующие возможности:

- самостоятельно и независимо определять основные направления внутренней и внешней политики в цифровой сфере;
- самостоятельно реализовывать такую политику;
- распоряжаться собственными информационными ресурсами, формировать национальную критическую информационную инфраструктуру;
- гарантировать информационную безопасность личности, общества и государства.

В основе цифрового суверенитета лежат регулятивные механизмы (национальные технические стандарты и правовой режим), использование защищённых от внешнего воздействия аппаратных и программных средств связи собственного производства, способов распространения информации, а также государственно-частное партнёрство, необходимое для контроля над сбором, обработкой, хранением и использованием больших массивов данных национальных пользователей. Кроме того, цифровой суверенитет не может быть полным без эффективных механизмов «очистки» внутренней виртуальной среды от нежелательной или вредоносной информации, а также без инструментов противодействия «вшитым» в импортируемый информационный продукт (новостные сервисы, киноиндустрия, соцсети, индустрия развлечений и т.д.) внешним и враждебным социально-политическим, историческим, религиозным, нравственно-культурным и другим идеологическим установкам.

Рассмотрим наиболее актуальные угрозы цифровому суверенитету России.

1.4.1. Захват рынков данных и слежки ИТ-корпорациями

Основными игроками на рынке больших пользовательских данных и их использования сейчас являются не государства, а частные цифровые операторы данных: поисковые системы, браузеры, социальные сети, мессенджеры, видео– и фотохостинги, рекламные системы, мобильные операторы, магазины приложений и интернет-СМИ. Именно они накапливают самые большие объёмы пользовательских данных, имеют огромные аудитории, а также владеют самыми мощными технологиями анализа и использования данных.

Государственные органы не только не успевают в том же темпе развивать свои средства сбора и анализа данных, но и не имеют сравнимой аудитории,

вследствие чего зачастую являются **просителями и получателями этих данных от частных цифровых платформ**. При этом, чем шире линейка цифровых сервисов у платформы («экосистемы») – тем выше её возможности сведения и совместного анализа разнородных данных о пользователях. Сведение воедино данных о поисковых запросах, электронных письмах, посещениях сайтов, покупках, медиапотреблении, общении в социальных сетях позволяет создать максимально полный профиль пользователя и затем манипулировать его товарным спросом, медиапотреблением, картиной дня, кругом общения и политическими взглядами, использовать в целях пропаганды, мошенничества, шантажа и криминальной деятельности.

«Экосистемы» стремятся к монополизации рынка данных. Такими широкими линейками сервисов обладают или стремятся обладать всего несколько крупнейших игроков на нашем цифровом рынке (Apple, Google, Mail Group, Meta[33], Ozon, Telegram, WB, Сбер, Яндекс, 4 федеральных мобильных оператора). Там, где какому-то крупному игроку не хватает элемента линейки сервисов и данных, он вступает в альянсы или производит поглощения. В результате «экосистемы» накапливают не только огромные объёмы ценных данных, но и получают мощнейший экономический, идеологический и геополитический рычаг воздействия на население России и любой другой страны мира.

Актуальной проблемой остаётся незаконная с точки зрения российского законодательства передача американскими телекоммуникационными гигантами и интернет-компаниями правительству США персональных данных россиян. Их дата-центры (серверы хранения персональных данных пользователей) располагаются в основном, на территории США и подпадают под действие американского «антитеррористического законодательства»[34], в соответствии с которым компании обязаны предоставлять прямой доступ спецслужбам США к любой информации, включая доступ к аккаунтам,

[33] Решением Тверского районного суда города Москвы от 21 марта 2022 г. по делу № 02-2473/2022 деятельность американской транснациональной компании *Meta Platforms Inc.* по реализации продуктов социальных сетей *Facebook* и *Instagram* признана экстремистской и запрещена на территории России. Далее по тексту указанная компания и социальные сети будут упоминаться без такой оговорки.

[34] В частности, «Акт о свободе» от 2015 года, заменивший «Патриотический акт», принятый после терактов 11 сентября 2001 года и предоставляющий спецслужбам почти неограниченные права по подслушиванию и ведению электронной слежки.
См. сайт Конгресса США: https://congress.gov/bill/114th-congress/house-bill/2048

банковским картам, переписке, всем личным данным пользователей, что нарушает требования законодательства большинства стран мира.

При этом американские компании в своей операционной деятельности активно применяют доктрину экстерриториального действия законодательства США: каждый пользователь вне зависимости от гражданства или страны нахождения, принимая соглашение о конфиденциальности «разных американских компаний» в рамках использования платных, условно платных и бесплатных цифровых сервисов, автоматически разрешает собирать и анализировать свои персональные данные, данные о своем устройстве, о мобильной сети и интернет-провайдере, о своих взглядах, убеждениях и предпочтениях, а также прочую информацию, ставшей доступной при взаимодействии пользователя с этими цифровыми сервисами.

1.4.2. Фактическая автономия глобальных цифровых платформ

Крупнейшие глобальные цифровые платформы и экосистемы, оперирующие в нашей стране, уже сейчас имеют бюджеты и «сетевое население» больше, чем у большинства стран-членов ООН. Эти платформы, будучи по своей природе транснациональными, имеют корпоративные интересы, политику продвижения на внешних рынках, которая по большей части определяется решениями их менеджмента и юрисдикцией страны происхождения компании, а не законами тех стран, где ведется деятельность. Огромные доходы и технологическая мощь позволяют им чувствовать себя уверенно даже в спорах с органами государственной власти многих стран мира.

По сути, это новый тип «цифровых государств» со своим цифровым суверенитетом, накладывающимся поверх суверенитетов государств реального мира. Это тревожная тенденция, поскольку такие «цифровые государства» не подчиняются международному праву и не имеют каких-либо ограничений, кроме своих внутрикорпоративных целей, задач и интересов, а также требований и правил правительства страны своей национальной юрисдикции (т.е. в подавляющем большинстве случаев – американской).

Некоторые государства сейчас вырабатывают способы «приземления» цифровых гигантов в свои юрисдикции, в частности, такой закон о «приземлении» (о создании юридических лиц в локальной юрисдикции) в **2021**

году был принят и в нашей стране[35]. Однако это довольно слабый и притом чисто *экономический* механизм (особенно для стран, относящихся в лучшем случае к третьему разряду локальных рынков у цифровых гигантов), который не сможет существенно повлиять на идеологическую и информационно-пропагандистскую работу цифровых агентов на территории третьих стран, а также на сбор ими данных.

Существующая во многих стран практика штрафования крупных компаний-нарушителей за отказ удалять противоправный контент, или напротив, за непрозрачную внутрикорпоративную цензуру, пока показывает невысокую эффективность, если меры финансового воздействия не подкрепляется технологическими способами замедления работы или блокировки платформ.

1.4.3. Цифровая колонизация России

Основные риски ускоренной цифровизации, описанные выше, усугубляются для нашей страны тем, что большинство «экосистем» – не отечественные, а зарубежные. Их повсеместное использование, в том числе представителями государственного сектора для рабочих нужд, создает прямую угрозу цифровой «колонизации» России в интересах других стран, в том числе, недружественных.

Американские цифровые платформы сохраняют долю в русскоязычном Интернете более, чем в **50 %** пользовательских аккаунтов социальных сетей, около **50 %** поисковых запросов, более **90 %** аккаунтов в мессенджерах, более **95 %** просмотров видеороликов, более **50 %** показов рекламы. Нужно понимать, что разработчик (тот, кто создаёт технологию или платформу) всегда остаётся её истинным владельцем, вне зависимости от того, в каком виде разработчик продаёт технологию или предоставляет для использования. Все информационные посредники самостоятельно определяют, какую ленту новостей и сообщений показывать владельцу аккаунта, что разрешать ему писать и когда его заблокировать, то есть являются фактическими владельцами и аккаунта, и контента, который на нём производится пользователем.

История предвыборной борьбы **2019–2020** годов в США, в том числе блокирование аккаунтов действующего президента и его сторонников цифровыми платформами и сервисами хостинга в январе **2020** года, наглядно

[35] Федеральный закон от 1 июля 2021 г. № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации».

продемонстрировала силу настоящих владельцев медиапространства. По существу, в руках американских глобальных ИТ-корпораций, управляемых Демократической партией США, сейчас находится «контрольный пакет Рунета».

Цифровая сфера России в целом в ещё большей степени является цифровой колонией Запада: подавляющее количество операционных систем и офисных приложений на частных устройствах россиян и в организациях разработаны в США; управление предприятиями использует по преимуществу западные системы; управление российским дискретным и непрерывным производством (металлургия, химические производства, нефтедобыча, газопроводы, прочее), некоторой другой критической инфраструктурой – ведётся почти исключительно с помощью западных систем.

Ускорение цифровизации парадоксальным образом приводит не к снижению колониальной цифровой зависимости, а к её усилению, потому что под лозунгом цифровой трансформации в России происходит всё большее заимствование и внедрение **готовых западных технологий и платформ**.

В этой связи стоит отметить, что **90–95%** всех систем ИИ, создаваемых сейчас в России и представляемых как отечественные разработки, основаны на общедоступных открытых решениях (так называемых *нейронных фреймворках*) Google и Facebook, а не на отечественных программных решениях[36].

Следует пояснить, что из себя представляет «открытое ПО», часто преподносимое как простое и удобное решение проблемы импортозамещения. На самом деле оно уже **15–20** лет финансируется и разрабатывается не «свободным и бескорыстным сообществом программистов», а крупнейшими американскими ИТ-корпорациями, такими как Google, Microsoft, IBM и Oracle, которые сохраняют неявный, но полный контроль за «открытым ПО». Это не случайный процесс: американские ИТ-корпорации целенаправленно захватывают цифровые рынки и медийные пространства суверенных стран, при мощной поддержке своего государства, с целью усиления влияния и контроля над чужими цифровыми пространствами.

Это серьёзный риск для цифрового суверенитета России.

[36] Для собственных нужд эти компании используют другие (более передовые и мощные) закрытые решения.

1.5. Отсутствие системного регулирования цифровой среды и защиты в ней прав и свобод человека и гражданина

В условиях быстрого развития цифровой среды в нашей стране до сих пор отсутствует её комплексное правовое регулирование (хотя уже **5** лет действует поправка к ст. **71** Конституции РФ, закрепляющая вопросы защиты данных граждан в федеральном ведении). Налицо очевидное отставание и несовершенство законодательства, регулирующего цифровую среду, в том числе в области защиты прав и свобод человека и гражданина.

Это отставание выражается в отсутствии комплекса правовых норм, обеспечивающих добровольность использования гражданами цифровых технологий при взаимодействии с государством и бизнесом, устанавливающими ограничения для повальной цифровизации публичного управления и некоторых важных сфер жизнедеятельности общества.

Ниже будут приведены положения документов стратегического планирования, действующих в период **2019-2024** годов, однако по имеющейся информации, многие их концептуальные положения сохраняются и в проектах аналогичных документов, рассчитанных на **2025-2030** годы.

1.5.1. Государственное управление личными данными граждан

В **2019-2024** годах в рамках реализации программы «Цифровая экономика» в нашей стране была сформирована Национальная система управления данными (далее – НСУД)[37]. Одним из принципов НСУД является оценка персональных данных граждан, внесённых в государственные информационные системы, как «государственных» данных, что даёт больше полномочий органам публичной власти по их сбору, обработке и передаче третьим лицам, что, в свою очередь, негативным образом скажется на защите прав граждан в сфере обработки персональных данных. Кроме того, в числе задач НСУД закреплено **предоставление доступа к государственным данным «широкому кругу потребителей на безвозмездной и на возмездной основе»**.

Таким образом, НСУД фактически направлена на формирование «цифровых профилей» граждан, предполагает замену понятия «персональные данные» на «государственные», что позволяет осуществлять их обработку и

[37] См. распоряжение Правительства РФ от 3 июня 2019 г. № 1189-р «Об утверждении Концепции создания и функционирования национальной системы управления данными и плана мероприятий ("дорожной карты") по созданию национальной системы управления данными на 2019–2021 годы».

коммерциализацию, включая продажу доступа к ним третьим лицам без согласия субъектов персональных данных. Представители Правительства РФ в публичных выступлениях неоднократно заявляли о готовности «делиться такими данными с бизнесом»[38]. Реализация такого подхода лишает граждан возможности полноценного управления своими персональными данными, противоречит принципам обработки персональных данных, закреплённым в законодательстве, создаёт угрозу манипулирования и иных злоупотреблений со стороны третьих лиц.

1.5.2. Социальные рейтинги и «индивидуальные траектории» как вектор государственной политики

Социальный рейтинг – это система индивидуальной социальной оценки граждан по различным личным параметрам, значения которых формируются с помощью инструментов массового наблюдения и технологии анализа больших данных, а впоследствии определяют возможности граждан для реализации отдельных конституционных прав и свобод. Отдельные положения документов стратегического планирования и высказывания публичных должностных лиц свидетельствуют о намерении ввести такие цифровые рейтинги, именуемые в документах «профилями», «траекториями» и другими эвфемизмами.

Так, паспорт национального проекта «Национальная программа «Цифровая экономика РФ»[39] предусматривает формирование «открытого формата **профилей компетенций граждан, траекторий их развития** и процедуры их создания» (п. 1.3. Федерального проекта «Кадры для цифровой экономики»); создание «цифрового сервиса, обеспечивающего формирование **персонального профиля компетенций, персональной траектории развития и непрерывного образования граждан**» (п. 1.24 федерального проекта «Кадры для цифровой экономики»); создание «платформы идентификации, включая **биометрическую идентификацию, облачную квалифицированную электронную подпись, цифровые профили гражданина** и юридического лица, а также единое пространство доверия электронной подписи на базе единой системы идентификации и аутентификации» (п. 1.10 федерального проекта «Цифровое государственное управление»). В **2019** году предпринимались попытки ввести в понятийный аппарат информационного законодательства

[38] https://ria.ru/20210604/chernyshenko-1735579125.html

[39] Утверждён президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 N 7

понятие цифрового профиля гражданина, не предполагающее получение его согласия, однако они не увенчались успехом[40].

«Траектории развития» понимаются в приведённых документах, как автоматическое отслеживание «жизненного пути» гражданина с выработкой рекомендаций по корректировке образовательного и профессионального пути человека в зависимости от особенностей его цифрового профиля и данных о ходе реализации гражданином рекомендованной личной «траектории». По сути, речь идёт о попытке управлять судьбой человека «сверху», со стороны отдельных органов публичной власти, или вообще их автономных ИИ-систем.

Среди документов, в которых прямо сказано о необходимости формирования «цифрового профиля» и «индивидуальной траектории», следует отметить приказ Минцифры России от 18 ноября 2020 г. № 600, устанавливающий в качестве целевых показателей **2030** года национальной цели развития "Цифровая трансформация" долю учащихся, по которым осуществляется ведение цифрового профиля в **100 %**[41]. При этом доля учащихся, которым должны быть предложены рекомендации по повышению качества обучения и формированию индивидуальных траекторий с использованием данных цифрового портфолио учащегося должна к **2030** году составить **80 %**[42].

Строящаяся система «цифровых профилей граждан» фактически будет представлять собой реализацию идей социального рейтинга. Данные выводы подтверждаются методическими документами, реализуемыми на практике, рекомендующими среди прочего внедрение цифровых профилей граждан. В **2019** году Центр подготовки руководителей цифровой трансформации РАНХиГС выпустил доклад «Государство как платформа: люди и технологии», в котором предусмотрено создание «цифровых двойников» (профилей) людей (а именно того, «что юридически валидно представляет» субъекта)[43]. В тексте доклада отмечается: «Развитие интернета вещей, удалённой биометрической

---

[40] https://sozd.duma.gov.ru/bill/747513-7

[41] П. 4.1 Приложения № 1 к Методике расчета целевого показателя "Достижение "цифровой зрелости" ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления", утв. приказом Минцифры России от 18 ноября 2020 г. № 600 «Об утверждении методик расчёта целевых показателей национальной цели развития РФ "Цифровая трансформация"».

[42] П. 4.2. Приложения № 1 к Приказу № 600.

[43] https://gspm.ranepa.ru/uploads/files/2019/01/17-01-2019_0.pdf. С. 8.

идентификации, систем массового видеонаблюдения и 5G *позволяет повысить детализацию знаний о конкретном человеке, в результате чего для государства «цифровой человек» становится более прогнозируемым в своём поведении,* данные «государственного хранения» позволят *персонализировать и прогнозировать целый ряд жизненных траекторий: от медобслуживания и образования* ***до гражданской добропорядочности и предпочтений при реализации избирательной функции***»[44]. В качестве удобства применения ИИ в госуправлении в указанном докладе отмечается возможность формирования *«социального рейтинга»*[45].

Введение социального рейтинга в любых видах ведёт к дискриминации граждан. Фактически социальное рейтингование – это отказ от конституционного принципа равенства прав и обязанностей граждан, установленного ч. **2** ст. **6** и ст. **19** Конституции РФ. Любое ограничение конституционных прав граждан в результате получения низких оценок в рейтинге является прямым нарушением Конституции РФ.

«Сжатие» прав при применении «профилей», «рейтингов» и «рекомендаций» может дойти до такой степени, что гражданин, формально не совершивший правонарушение, будет приравнен в объёме прав к осуждённому лицу, причём без законного (судебного) установления вины. Иными словами, социальный рейтинг ставит под угрозу презумпцию невиновности граждан, гарантированную ст. **49** Конституции РФ.

1.5.3. Переход на исключительно электронную форму общения с органами государственной и муниципальной власти

В федеральном проекте «Цифровое государственное управление» было прямо закреплено «*исключение участия человека из процесса принятия решения при предоставлении приоритетных государственных услуг»* (п. **1.2.**). В «Общенациональном плане действий, обеспечивающих восстановление занятости и доходов населения, рост экономики и долгосрочные структурные изменения в экономике»[46] предусмотрен «переход на исключительно электронный формат поступающих и обрабатываемых обращений граждан».

[44] Там же. С. 46.
[45] Там же. С. 27.
[46] Одобрен Правительством РФ 23 сентября 2020 г., протокол № 36, раздел VII.

Исходя из приведённых норм, в краткосрочной перспективе предполагается полный отказ от традиционной формы взаимодействия государства с гражданами. В частности, в **2020** году были кардинальным образом изменены нормы Федерального закона от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»[47] (далее – Закон о госуслугах). Так, прежняя редакция п. **6** ст. **4** Закона о госуслугах предусматривала следующий принцип предоставления услуг: «возможность получения государственных и муниципальных услуг в электронной форме, если это не запрещено законом, а также в иных формах, предусмотренных законодательством РФ, **по выбору заявителя**». В п. **3** ст. **5** Закона о госуслугах говорилось, что заявители имеют право на получение госуслуг «в электронной форме, если это не запрещено законом, а также в иных формах, предусмотренных законодательством РФ, **по выбору заявителя**».

Поправки **2020** года дополнили указанные нормы оговоркой: «за исключением случая, если на основании федерального закона предоставление государственной или муниципальной услуги осуществляется **исключительно в электронной форме»**. Таким образом, общее правило о возможности использования любой формы получения услуг по усмотрению гражданина, было заменено правом государства императивно устанавливать электронный формат взаимодействия. Кроме того, поправки допускают прекращение личного приёма граждан в органах, предоставляющих услуги, в случае передачи соответствующих функций МФЦ (ч. **1.8** ст. **7** Закона о госуслугах). Следует отметить, что МФЦ не являются органами публичной власти.

Такое регулирование противоречит ст. **33** Конституции РФ, согласно которой граждане имеют право обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления. По смыслу формулировки «лично» речь идёт о личном предъявлении гражданином должностному лицу своего обращения – в устной форме (на личном приёме), либо путём передачи письменного экземпляра обращения.

1.5.4. Принудительное вовлечение граждан в ЕСИА

Предоставление государственных и муниципальных услуг в электронной форме осуществляется в отношении заявителей, прошедших процедуру

[47] Федеральный закон от 30 декабря 2020 г. № 509-ФЗ «О внесении изменений в отдельные законодательные акты РФ».

регистрации в Единой системе идентификации и аутентификации (далее - ЕСИА), данное требование безальтернативно. Верховный Суд РФ в **2012** году рассматривал административное дело об оспаривании Постановления Правительства РФ, определяющего порядок использования ЕСИА для предоставления услуг в электронной форме[48]. Заявители указывали на нарушение данным постановлением права на достоинство личности, на свободу вероисповедания и действия в соответствии со своими религиозными убеждениями, право идентифицировать себя по фамилии, имени, отчеству, дате, месту рождения, отношению к гражданству, а не по идентификационному номеру, присваиваемому в ЕСИА.

Суд отказал в удовлетворении исковых требований, однако важно обратить внимание на аргументацию суда: «Использование в регистрах ЕСИА идентификаторов не нарушает свободу совести и вероисповедания граждан, поскольку в системе используются идентификаторы, установленные федеральными законами, **и только с согласия заявителей**. …Постановление применяется лишь к гражданам, обратившимся за получением государственных или муниципальных услуг в электронном виде, **и только с их согласия**». Суд также прямо указал, что граждане вправе обращаться за получением государственных и муниципальных услуг не только в электронной форме, но и в иных формах, предусмотренных законодательством, по своему выбору, а органы публичной власти, в свою очередь, обязаны обеспечить им такую возможность [49].

С поправками **2020** года граждане оказались лишены права выбора формы госуслуг и, соответственно, возможности отказаться от регистрации в ЕСИА, если они нуждаются в получении госуслуги, оказываемой исключительно в электронной форме. Таким образом, вопрос о несоответствии Конституции РФ порядка использования ЕСИА вновь оказался актуальным.

Отметим, что Стратегия развития информационного общества в РФ на 2017–2030 годы, утверждённая Указом Президента РФ от 9 мая 2017 г. № 203, предусматривает «развитие технологий электронного взаимодействия

[48] Постановление Правительства РФ от 28 ноября 2011 г. N 977 "О федеральной государственной информационной системе "Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме".

[49] Решение Верховного Суда РФ от 29 мая 2012 г. № АКПИ12-645.

граждан, организаций, органов государственной власти и местного самоуправления **наряду с сохранением возможности взаимодействия граждан с указанными организациями и органами без применения информационных технологий**»[50];

1.5.5. Переход на «цифровые оригиналы» документов

1 января **2022** г. вступила в силу новая редакция ч. **2** ст. **7.4** Закона о госуслугах, согласно которой «результат предоставления государственной или муниципальной услуги не оформляется в форме документа на бумажном носителе, если иное не установлено нормативными правовыми актами, регулирующими порядок предоставления такой услуги». То есть, по общему правилу, результаты взаимодействия гражданина и государства оформляются исключительно в электронном виде.

В связи с этим у граждан неизбежно возникнут сложности с доказыванием тех или иных юридических фактов своей жизни. Мы убеждены, что такое регулирование – не только нарушение прав граждан, но и провокатор киберпреступности. А в случае сбоя информационных систем или злонамеренных действий лиц, получивших к ним доступ, граждане могут быть полностью лишены возможности восстановить свои нарушенные права.

Отметим также, что согласно поправкам **2019** года к трудовому законодательству[51], формирование сведений о трудовой деятельности лиц, впервые поступающих на работу после **31** декабря **2020** года, осуществляется в соответствии со ст. **66.1** Трудового кодекса РФ, а **трудовые книжки на указанных лиц не оформляются**». Таким образом, для работников, впервые приступающих к работе с **2021** года, не предусмотрено альтернативы электронному формату учёта сведений о трудовой деятельности (в виде трудовой книжки в бумажной версии). Этот механизм может вызвать проблемы через **35-45** лет, когда такие работники будут массово выходить на пенсию и столкнутся с необходимостью подтверждения трудового стажа.

[50] Подп. «д» п. 40 Стратегии развития информационного общества в РФ на 2017–2030 годы, утверждённой Указом Президента РФ от 9 мая 2017 г. № 203.

[51] Федеральный закон от 16 декабря 2019 г. № 439-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации в части формирования сведений о трудовой деятельности в электронном виде».

1.5.6. Отслеживание событий частной жизни граждан Госуслугами

Согласно п. **1** ч. **1** ст. **7.3** Закона о госуслугах, при наступлении событий, являющихся основанием для предоставления услуг, орган, предоставляющий услугу, вправе «проводить мероприятия, направленные на подготовку результатов» предоставления госуслуг, «после чего уведомлять заявителя о возможности подать запрос о предоставлении соответствующей услуги для немедленного получения результата предоставления такой услуги». Данная норма направлена на переход к проактивному (беззаявительному) предоставлению услуг (прежде всего, это актуально для мер социальной поддержки). Однако эта норма предполагает и отслеживание событий частной жизни граждан без их согласия, поскольку иным образом принципиально невозможно проводить «мероприятия» по подготовке предоставления услуг.

1.5.7. Цифровизация здравоохранения

В нашей стране создана Единая государственная информационная система в сфере здравоохранения (далее - ЕГИСЗ), которая включает несколько регистров, среди которых «федеральная интегрированная электронная медицинская карта» – подсистема, нацеленная на сбор данных о здоровье граждан[52]. Внесение данных в такую медицинскую карту происходит в течение одного рабочего дня со дня установления лечащим врачом медицинской организации диагноза соответствующего заболевания или со дня получения им актуализированных данных о пациенте при наличии **добровольного согласия** гражданина на передачу данных.

Статья **94** федерального закона от 21 ноября 2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ» предусматривает, что в системе персонифицированного учета осуществляется обработка следующих персональных данных о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования: 1) фамилия, имя, отчество (последнее – при наличии); 2) пол; 3) дата рождения; 4) место рождения; 5) гражданство; 6) данные документа, удостоверяющего личность; 7) место жительства; 8) место регистрации; 9) дата регистрации; 10) страховой номер индивидуального лицевого счета (при наличии); 11) номер полиса

[52] П. 22 Приложения № 1 к Положению о единой государственной информационной системе в сфере здравоохранения, утверждено Постановлением Правительства РФ от 5 мая 2018 г. № 555 «О единой государственной информационной системе в сфере здравоохранения».

обязательного медицинского страхования застрахованного лица (при наличии); 12) анамнез; 13) диагноз; 14) сведения об организации, осуществляющей медицинскую деятельность; 15) вид оказанной медицинской помощи; 16) условия оказания медицинской помощи; 17) сроки оказания медицинской помощи; 18) объем оказанной медицинской помощи, включая сведения об оказанных медицинских услугах; 19) результат обращения за медицинской помощью; 20) серия и номер выданного листка нетрудоспособности (при наличии); 21) сведения о проведённых медицинских экспертизах, медицинских осмотрах и медицинских освидетельствованиях и их результаты; 22) применённые стандарты медицинской помощи; 23) сведения о медицинском работнике или медицинских работниках, оказавших медицинскую помощь, проводивших медицинские экспертизы, медицинские осмотры и медицинские освидетельствования».

Указанные данные вносятся в ЕГИСЗ с учётом требований об их обезличивании[53], однако сам факт возможности доступа к ним (для оказания медицинской помощи) свидетельствует о наличии рисков взлома системы, утечки, продажи, утраты, кражи, деанонимизации, других видов злоупотребления столь чувствительными данными. Создание централизованной системы с детальными данными о здоровье всех граждан страны несёт серьёзные риски с точки зрения национальной безопасности.

Кроме того, упомянутый приказ Минцифры России устанавливает в качестве целевого показателя **2030** года наличие **у 100% граждан** к **сформированных интегрированных электронных медицинских карт**, доступных на платформе Единого портала госуслуг. Таким образом, подзаконным актом Минцифры России **игнорируется принцип добровольности передачи данных** граждан в электронную медицинскую карту.

1.5.8. Цифровизация образования

Продолжается коренная реформа образовательной сферы, направленная на её цифровизацию. Среди проблем, с которыми сталкиваются граждане в образовательной сфере в связи с цифровизацией, следует отметить:

[53] Приказ Минздрава России от 14 июня 2018 г. № 341н «Об утверждении Порядка обезличивания сведений о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования».

1) **«добровольно-принудительный» сбор данных** об участниках образовательных отношений, включая сбор биометрических персональных данных в образовательных учреждениях;

2) **принуждение к подписанию согласий** на обработку персональных данных, к получению государственных и муниципальных услуг в электронной форме (включая подачу заявлений о зачислении в образовательные организации);

3) **принуждение к электронному обучению**, включая регистрацию на цифровых образовательных платформах, внедрение цифровых сертификатов на дополнительное образование и сбор персональных данных, как условие доступа к дополнительному образованию.

В **2020** году в рамках реализации национального проекта «Образование»[54] стартовал эксперимент по внедрению цифровой образовательной среды (далее – ЦОС)[55] с заранее запланированным результатом в виде внедрения ЦОС на постоянной основе на всей территории РФ. Во всех школах была внедрена цифровая платформа «Сферум» на базе социальной сети «ВКонтакте», которая является частной компанией[56]. При этом в Положении о ЦОС никак не была гарантирована возможность обучения в традиционной форме. На примерах некоторых регионов известно, что родителей ставили перед фактом превращения класса в «цифровой» с раздачей их детям планшетов для обучения. Таким образом происходит подмена обучения по закону (как реализации государственной функции) обучением по договору с непредсказуемым результатом.

Планы по цифровизации образования определены также в распоряжении Минпросвещения России от 18 мая 2020 г. № Р-44 «Об утверждении методических рекомендаций для внедрения в основные общеобразовательные программы современных цифровых технологий». В этих рекомендациях обозначены, в частности, технологии виртуальной и дополненной реальности, использование социальных сетей в обучении,

[54] Паспорт утверждён президиумом Совета при Президенте РФ по стратегическому развитию и нацпроектам, протокол от 24 декабря 2018 г. № 16.

[55] Постановление Правительства РФ от 7 декабря 2020 г. № 2040 «О проведении эксперимента по внедрению цифровой образовательной среды» (вместе с «Положением о проведении на территории отдельных субъектов Российской Федерации эксперимента по внедрению цифровой образовательной среды»).

[56] Кроме того, в описании системы Сферум есть упоминание об использовании её на смартфонах, что вообще является опасным для здоровья детей.

реализация персонализированных учебных планов, **«геймификация» обучения** через «включение цифровых игровых форм», **производство «цифровых двойников» действий учащегося, симуляции поведения учителя**. Ключевая роль учителя в образовании при таком подходе переходит к ИИ. Бумажные учебники вытесняются цифровыми со ссылкой на дороговизну первых, проблемы перевыпуска при наличии ошибок и т.п.

Представляется, что это сомнительные аргументы, которые игнорируют ключевые причины недопустимости такого рода решений (б*о*льшая эффективность для обучения бумажных учебников и их безвредность для здоровья, в частности, для зрения – в отличие от электронных носителей). Существуют многочисленные, в том числе, западные, научно-практические исследования, доказывающие вред, причиняемый внедрением электронных средств обучения в школы, как в отношении здоровья детей, так и эффективности обучения[57]. Применение цифровых технологий формирует у детей вредные зависимости, негативно влияет на их когнитивные способности, поскольку они полноценно развиваются лишь при постижении реального мира. «Использование Интернета способствует ухудшению памяти, … снижению способности к самостоятельному поиску информации, а в долгосрочной перспективе нередко приводит **к болезненной зависимости от Интернета**»[58]. Исследования всё чаще показывают, что молодые люди с экранной зависимостью демонстрируют «микроструктурные и объёмные различия или аномалии как серого, так и белого вещества по сравнению со здоровыми контрольными группами»; при этом различия в структуре и функциях мозга наблюдаются во многих из тех же самых областей, в которых они проявляются при наркотической зависимости[59].

Другой важный аспект цифровизации образования – сокращение времени на живое общение и проблемы социализации. «Социальные сети ни в коей мере не способствуют ни расширению, ни углублению контактов. Единственный их результат – социальная изоляция и поверхностные контакты…». Ухудшение социализации влечёт нарушение общественных связей, качества коммуникации. Расстройства, связанные с экранной зависимостью, провоцируют сидячий образ жизни у детей, снижая аэробную

[57] Например: *Шпитцер М.* Антимозг. Цифровые технологии и мозг. – Москва, 2014.
[58] Там же. С. 69, 144-145.
[59] Sigman A: Screen Dependency Disorders: a new challenge for child neurology. P. 4.

нагрузку, которая «играет важную роль в неврологическом здоровье детей, особенно в структуре и функциях мозга»[60].

Качественное образование предполагает непосредственное живое взаимодействие учеников и учителя, включая проверку заданий, зрительный и эмоциональный контакт, живую обратную связь, социализацию и воспитание в непосредственном человеческом общении, что исключено при трансляции информации через экран, выполнении заданий и их автоматизированной проверке на электронном устройстве.

Несмотря на отмеченные обстоятельства, включение цифровых технологий и ИИ в образование декларируется в качестве одной из основных тенденций развития системы образования уже на период до **2040** года (соответствующий проект концепции готовится Правительством РФ). В качестве одной из ключевых задач декларируется «приведение уровня цифровизации сферы образования в соответствие с уровнем цифровизации повседневной жизни, использование больших данных для управления в сфере образования». **Эти идеологические установки нуждаются в корректировке, в противном случае дальнейшая цифровизация образования создаст риски поражения граждан в их правах на образование, на неприкосновенность частной жизни и на охрану здоровья.**

1.5.9. Цифровизация сферы социального обслуживания

В **2015** году в законодательство о государственной социальной помощи были внесены поправки[61], предусматривающие запуск с **2018** года Единой государственной информационной системы в области социального обеспечения (далее – ЕГИССО), призванной аккумулировать информацию о семьях граждан, в том числе для анализа вопроса о наличии нуждаемости в социальном обеспечении.

Одной из целью создания ЕГИССО является автоматизация процессов назначения и предоставления мер социальной защиты (поддержки), социальных услуг, иных социальных гарантий и выплат путем использования инфраструктуры, обеспечивающей информационно-технологическое

[60] Там же. С. 5.

[61] Федеральный закон от 29 декабря 2015 г. № 388-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части учёта и совершенствования предоставления мер социальной поддержки, исходя из обязанности соблюдения принципа адресности и применения критериев нуждаемости».

взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме.

В перечень собираемых в ЕГИССО сведений включены: СНИЛС, ФИО, пол, дата и место рождения, телефон, гражданство, данные документа, удостоверяющего личность, реквизиты записи акта о рождении, адрес места жительства (пребывания), сведения о выплатах и иных вознаграждениях, полученных лицом в связи с осуществлением трудовой деятельности, сведения о периодах трудовой деятельности и (или) иной деятельности, сведения о сумме пенсии, сведения о периоде назначения и предоставления меры социальной защиты (поддержки), номера СНИЛС всех членов семьи или домохозяйства, учитываемых при назначении мер социальной защиты (поддержки), предоставляемых семье или домохозяйству, размер занимаемой площади жилого помещения для мер социальной защиты (поддержки) по оплате жилищно-коммунальных услуг и др.[62] При этом одним из принципов ЕГИССО является «открытость для интеграции с …государственными **и иными информационными ресурсами**, …на основе единых форматов информационного взаимодействия» (подп. «ж» п. **9** Положения о ЕГИССО).

Согласно п. **27** Положения о ЕГИССО «согласие гражданина на обработку его персональных данных подтверждается заявлением, поданным гражданином в орган, предоставляющий меры социальной защиты (поддержки)». На практике эта норма трактуется чиновниками так, что **само заявление о получении мер поддержки и является согласием** на обработку персональных данных гражданина в ЕГИССО. Несмотря на положительный опыт проактивного (беззаявительного) начисления выплат Социальным фондом России в условиях пандемии Covid-19, принципиально важно учесть отмеченные выше риски для прав и свобод граждан, не допуская также коммерциализации сформированных в системе ЕГИССО социальных профилей. Здесь стоит отметить риски навязывания дополнительных банковских услуг лицам, обратившимся за начислением пенсии, а также «рекламной атаки» на

[62] Постановление Правительства РФ от 14 февраля 2017 г. № 181 «О Единой государственной информационной системе социального обеспечения» (вместе с «Положением о Единой государственной информационной системе социального обеспечения», «Порядком предоставления информации в Единую государственную информационную систему социального обеспечения»).

семью, получившую право на семейный (материнский) капитал со стороны девелоперов, предлагающих приобрести новое жилье.

1.5.10. Региональный разнобой регулирования и «законодательные песочницы»

Наряду с федеральными процессами цифровизации, в настоящее время продолжают реализовываться множество несогласованных процессов цифровизации регионального и городского уровней. Например, деятельность мэрии Москвы (как и руководства некоторых других городов и регионов) в сфере цифровизации и сбора данных граждан является совершенно самостоятельной. Зачастую такая самостоятельность в деле внедрения цифровых технологий легализуется в формате «особых экспериментальных режимов», так называемых «законодательных песочниц».

Этот порядок вызывает серьёзные опасения с точки зрения защиты прав граждан, потому что Конституция РФ устанавливает **равенство прав всех граждан** России перед законом, вне зависимости от места их проживания, а кроме того, поправки **2020** года в ст. **71** Конституции РФ устанавливают именно **федеральную ответственность** за оборот данных граждан и защиту их прав в цифровом пространстве.

Граждане, «попавшие» помимо своего желания, в такую «законодательную песочницу» или «экспериментальный правовой режим» по факту своего проживания в том или ином регионе, оказываются по факту поражёнными в правах по сравнению с остальными соотечественниками[63]. Кроме того, такая разнонаправленная региональная активность в области цифровизации и внедрения ИИ означает, что в нашей стране нет единого плана «цифровой трансформации» и учёта её рисков, в том числе правовых.

1.5.11. Саморегулирование цифровой отрасли: объективные пределы эффективности

Со стороны цифровой отрасли часто звучат публичные заверения в том, что социально ответственная отрасль сможет создать для себя этический кодекс, а также правила саморегулирования, которые в том числе защитят и

[63] В рамках федеральной «песочницы» (259-ФЗ) и московской «песочницы» (129-ФЗ) должны обрабатываться т. н. «обезличенные данные» (что вызывает определённые сомнения, в том числе про необратимость такого «обезличивания»), вместе с тем в стране инициируются региональные и федеральные проекты по обработке персональных данных, в том числе биометрия учеников в школах.

права граждан. Признавая необходимость развития механизмов этического, ценностно-ориентированного саморегулирования в цифровой сфере, обозначим объективные причины, по которым саморегулирование, само по себе, без соответствующей трансформации законодательства и государственной политики, имеет сегодня ограниченную перспективу.

1. **Фактическое отсутствие социальной ответственности и превалирование частного интереса.** В настоящее время цифровой бизнес не демонстрирует социальной ответственности. Процессы сбора и использования персональных данных повсеместно идут с нарушением требований Конституции РФ, законодательства о персональных данных, информации и связи. Возникает закономерный вопрос: каким образом и отчего, долгие годы системно нарушая требования законодательства, бизнес внезапно создаст и станет исполнять собственные ограничительные по содержанию кодексы?

2. **Разочаровывающий опыт «саморегулирования».** Все попытки создать законы о больших данных, больших пользовательских данных, общедоступных данных в рамках правового направления национального проекта «Цифровая экономика» со стороны Ассоциации больших данных[64] и представителей крупных цифровых платформ и «экосистем» сводились к попытке приватизации и монополизации пользовательских данных крупным бизнесом, то есть закрепления в законе имеющихся фактически нарушений конституционных прав граждан и монополизации отрасли.

3. **Доминирование иностранных платформ в цифровом пространстве России.** Саморегулирование отечественной цифровой отрасли распространяется лишь на небольшое число цифровых платформ, работающих в иностранных юрисдикциях. Законодательство «о приземлении» иностранных платформ может изменить их правовое положение, но не их коммерческие интересы и лоббистские возможности.

4. **Национальная безопасность не может «саморегулироваться».** Персональные данные, права граждан на защиту идентичности, частной жизни, доступа к информации – это вопросы национальной безопасности. Такие вопросы не могут решаться исключительно «саморегулированием».

[64] АБД создана в 2018 г., включает исключительно крупный цифровой бизнес: «Яндекс», Mail.Ru, «Сбербанк», «Газпромбанк», «Тинькофф Банк», «МегаФон», «Ростелеком», oneFactor, QIWI, «Билайн», «МТС», Банк ВТБ, «Магнит», несколько правительственных фондов и структур.

В **2021** году крупными игроками отрасли ИИ был разработан и подписан «Кодекс этики ИИ»[65]. Документ подписали Яндекс, Сбер, другие цифровые платформы, и разработчики ИИ, всего более **850** компаний. Некоторые авторы данного доклада участвовали в корректировке положений кодекса, это хороший пример достижения общественного согласия с принятием согласованных норм большим цифровым бизнесом. Тем не менее, Кодекс этики ИИ является добровольным для подписантов, никак не трактует вопросы соблюдения законности в ходе развития и применения ИИ, не содержит механизмов проверки исполнения норм Кодекса и принуждения участников соглашения к исполнению декларированных норм. В отношении прав граждан и их персональных данных Кодекс этики ИИ формулирует благие пожелания для отрасли, а отнюдь не обязательные нормы. Это привело к тому, что Кодекс этики ИИ практически не исполняется большинством его подписантов.

С нашей точки зрения, регулированием цифровой сферы, а также защитой прав граждан в ней, в первую очередь, должно заниматься государство, а все виды саморегулирования («Этический кодекс операторов больших данных», «Кодекс этики ИИ» и тому подобные) могут быть только дополнением к государственному регулированию, «надстройкой» над ним.

Общий вывод части I:

Беспорядочная, хаотичная и бесконтрольная цифровизация создаёт серьезные риски массовых нарушений прав и свобод личности, ущемления информационного (цифрового) суверенитета нашей страны со стороны хозяйствующих субъектов (в том числе, трансграничных корпораций), управляющих данными процессами. Среди особо уязвимых с точки зрения прав человека сфер следует выделить сферы образования, здравоохранения и социальной поддержки населения. Необходимо выработать и закрепить на законодательном уровне российскую модель цифровизации, фиксирующую и купирующую эти риски.

[65] https://rg.ru/2021/10/26/v-rossii-podpisan-kodeks-etiki-iskusstvennogo-intellekta.html Текст Кодекса: https://d-russia.ru/wp-content/uploads/2021/10/kodeks_etiki_ii.pdf

Часть 2. Цифровизация и правовое государство: российская модель. Пути и решения

Если исходить из нашей конституционной философии и традиционных российских духовно-нравственных ценностей, отечественная модель цифровой трансформации должна обеспечивать разумный баланс между стремительным развитием информационных технологий, цифровой трансформацией экономики и государственного управления и сохранением всех конституционных прав и свобод, соответствующих представлениям граждан и общества о безопасности, равенстве и справедливости.

Это довольно очевидное положение требует формирования принципов реализации и защиты прав и свобод человека и гражданина в цифровом пространстве РФ, и выработки на их основе системы мер, призванных обезопасить личность, общество и государство от тех угроз и рисков, которые были рассмотрены нами в первой главе Доклада.

2.1. Принципы реализации и защиты прав и свобод граждан России в цифровой среде

Для понимания того, что необходимо сделать для снижения рисков цифровизации, необходимо обозначить цель: куда мы идём, **каков образ цифрового будущего России?** На наш взгляд, этот образ будущего должен соответствовать нравственным ориентирам, закреплённым в Конституции РФ и Основах государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей[66].

2.1.1. Принципы российской конституционной философии

В основе конституционной философии российского государства лежит представление о человеке как высшей ценности: **человек, его права и свободы являются высшей ценностью.** Признание, соблюдение и защита прав и свобод человека и гражданина — обязанность государства. В свою очередь, ценность и достоинство человеческой личности связано с уникальным положением человека в бытии, наличием у него сознания, разума, воли, способности к творчеству, стремлению к благу и красоте.

Говорить об этом сегодня – крайне актуально. В том числе в контексте рассмотренной «идеологии цифровизации», осуществляющей тотальный

[66] утв. Указом Президента РФ от 9 ноября 2022 г. № 809.

пересмотр традиционных представлений о человеке как субъекте развития, обладающем разумом, волей, свободой и ответственностью (то есть способностью определять цели, выбирать и реализовывать сценарии и стратегии развития). Если мы встаём на позиции радикального технологического детерминизма и ценностного релятивизма, характерные для «идеологии цифровизации», поднимать вопрос об «образе будущего» (страны, мира, человечества) не приходится. Кто мы (граждане, гражданские объединения, народы и т.д.) в таком случае? Согласно этой идеологии, мы просто заложники технологических «трендов», «тенденций», «логик», цифровые векторы и «профили», которыми можно манипулировать в автоматическом режиме, определяя их «траектории» движения.

При этом в случае отказа рассматривать проблематику развития через призму субъектности человека и человеческих объединений, не приходится говорить и о «вызовах». Вызов – категория из арсенала социальной мысли, всерьёз относящейся к человеку как к актору социально-исторического процесса, который «принимает» вызов и даёт на него человеческий же «ответ». В смысловом горизонте «идеологии цифровизации» нет места и «общественному договору», нет в конечном счёте места этике, праву, культурным идеалам. Возможность и необходимость общественного договора определяется субъектностью и свободой человека как стороны договора.

Наша конституционная философия, культурное и интеллектуальное наследие дают нам правовые, моральные и интеллектуальные основания говорить о возможности и осуществимости «цифровой альтернативы» в интересах личности, общества и государства, о возможности сохранения и развития конституционной модели правового государства в условиях глобальных технологических трансформаций.

В самом широком виде дальнейшее развитие человечества должно отвечать следующим характеристикам:

1) оно должно остаться свободным развитием свободных человеческих существ и их сообществ;

2) оно должно сохранить в качестве своей цели реализацию прав и свобод личности, как самобытного, автономного, саморегулируемого существа, наделённого разумом и волей;

3) проблематика будущего мироустройства должна остаться открытой, поливариантной; мы не должны пытаться описать будущее суммой жёстких формул, исключая из сценариев развития лишь такие, которые несовместимы с

признанием необходимости уважения достоинства и свободы человека, ценности каждой человеческой личности и жизни.

Реализация вектора альтернативного «цифрового» развития предполагает в качестве своего условия принятие к руководству следующих императивов:

1) принципы достоинства личности, уважения прав и свобод человека и гражданина должны неукоснительно соблюдаться при внедрении и использовании технологий во всех сферах жизнедеятельности человека, общества и государства;

2) технологии являются продуктом разумной человеческой деятельности, проекцией свойств человеческой природы, и их ценность ни при каких обстоятельствах не может быть выше ценности человека или равной ей;

3) информация о человеке, обществе и мире никогда не является исчерпывающей при любых её объёмах, поэтому следует избегать рассматривать результаты её обработки системами ИИ, иными технологическими системами в качестве безальтернативных, не подлежащих критической оценке и пересмотру;

4) функционирование новейших технологических и информационных платформ подлежит общественному этическому контролю, решения систем ИИ, иных систем обработки информации, несовместимые с принципами достоинства личности, уважения прав и свобод человека и гражданина, – ничтожны, а их практическая реализация должна преследоваться по закону;

5) использование технологических систем во всех сферах жизнедеятельности человека, общества и государства должно сообразовываться с традиционными российскими духовно-нравственными ценностями, разделяемыми большинством граждан;

6) при использовании новейших технологий должны быть исключены риски нарушения фундаментальных прав и свобод человека и гражданина, в том числе, политических, социальных и экономических прав;

7) внедрение новых технологических решений не должно создавать угроз и рисков для исторически-сложившихся социальных общностей: семейно-родственных, национальных, культурных, территориальных;

8) использование технологий не должно создавать угрозу свободе предпринимательской, трудовой, иной законной хозяйственной деятельности.

9) использование технологий в сфере распространения массовой информации должно способствовать максимальной реализации прав граждан на информацию, культурных и образовательных прав; использование

цифровых технологий, систем ИИ для преднамеренной дезинформации граждан должно преследоваться по закону;

10) передача любых властных полномочий технологическим системам, в том числе ИИ, иным цифровым технологиям не допускается; наделение систем ИИ, а также иных технических систем правосубъектностью недопустимо.

Таким образом, альтернатива «цифрового» развития предполагает отказ от жёсткого технологического детерминизма. Мы исходим из презумпции неизменности базовых принципов прав, морали и природы человека, из постулата, что **никакие «технологические революции» и «новые технологические уклады» не меняют ни природы человека, ни моральных ценностей, ни сути общественных отношений, ни основных прав человека**.

Цифровое пространство не порождает каких-то особых видов прав граждан, как не порождают их другие особые пространства, где оперируют государство, общество и граждане: воздушное, морское, дорожное, земельное, космическое и т.п. Это значит, что здесь мы не вводим каких-то новых «цифровых прав человека», а обсуждаем принципы и меры защиты обычных, традиционных прав и свобод граждан в их реализации в цифровом пространстве. Поэтому в настоящем докладе не ставится вопрос о закреплении «права на доступ в Интернет» или «на доступ к цифровым технологиям», которое появляются в некоторых странах мира – мы считаем, что эти правомочия охватываются конституционным правом гражданина на получение и распространение информации.

Пережитый нами в **2020-2021** годы опыт пандемии коронавирусной инфекции свидетельствует, что гарантировать безопасность гражданам может только эффективное государство, а безопасность вкупе с правами и свободами человека и гражданина может гарантировать только эффективное правовое государство. Поэтому исходя из принципов достоинства личности, уважения прав и свобод человека и гражданина, мы должны найти современную модель правового государства, которая обеспечит их реализацию одновременно в новых технологических условиях и в контексте актуальных вызовов и угроз.

2.1.2. Конституционные принципы и принципы обеспечения национальной безопасности и стратегического развития страны

Итак, конституционный порядок и, прежде всего, его основополагающие принципы: достоинства личности, уважения прав и свобод человека и гражданина; принадлежности суверенитета народу России; правового

государства, – должны рассматриваться в качестве руководящих ценностей, не подверженных влиянию технологических факторов.

Реализация конституционных принципов обеспечения прав и свобод человека и гражданина в национальном цифровом пространстве предполагает:

1) формирование условий для реализации и защиты конституционных прав и свобод человека и гражданина в цифровом пространстве РФ;

2) учёт необходимости обеспечения безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных;

3) создание условий, обеспечивающих достойную жизнь и свободное развитие человека и общества в условиях цифровой трансформации государственного управления, общественной жизни и экономики;

4) целенаправленное использование потенциала цифровых технологий для укрепления единства многонационального народа России, гражданского мира, согласия и солидарности в российском обществе.

Указанная деятельность должна осуществляться на основе принципов:

1) приоритета конституционно-правовых представлений о человеке, его правах и свободах как высшей ценности по отношению к иным представлениям о человеке, его правах и свободах;

2) признания, соблюдения и защиты достоинства личности, прав и свобод человека и гражданина в цифровом пространстве как конституционной обязанности государства, институтов гражданского общества и граждан России;

3) защиты суверенитета России в национальном цифровом пространстве как условия реализации прав и свобод человека и гражданина, в целях сбережения народа России, развития человеческого потенциала, повышения качества жизни и благосостояния граждан;

4) осуществления власти многонациональным народом России – носителем суверенитета и единственным источником власти – непосредственно, а также через органы публичной власти;

5) непосредственного действия прав и свобод человека и гражданина, определяющих смысл, содержание и применение законов, деятельность органов публичной власти;

6) единства правового пространства нашей страны;

7) приоритета федерального законодательства в правовом регулировании цифрового пространства РФ;

8) признания и защиты в цифровом пространстве РФ всей полноты правовых, культурных, этических и иных норм, принятых российским обществом и государством;

9) системного подхода к правовому регулированию вопросов защиты прав и свобод человека и гражданина в цифровом пространстве нашей страны;

10) формирования цифрового пространства России в качестве среды, благоприятной для становления и развития личности в соответствии с традиционными духовно-нравственным ценностями российского общества;

11) заботы о безопасности, нравственном, культурном, образовательном, гражданском и патриотическом развитии детей и молодёжи в цифровом пространстве РФ;

12) неотвратимости наказания за противоправные деяния в цифровом пространстве РФ;

13) запрета на принудительное вовлечение граждан в цифровую среду, в т.ч., под угрозой ограничений реализации их прав, свобод и законных интересов;

14) признания права человека на сохранение традиционных, нецифровых способов взаимодействия с государством и обществом;

15) опережающего регулирования развития цифрового пространства в России и социальных отношений, возникающих в цифровом пространстве, с учётом прогнозных оценок будущих рисков, угроз национальной безопасности и возможных негативных последствий цифровизации.

Наряду с конституционно-правовыми нормами, особое значение для обеспечения прав и свобод человека и гражданина в цифровом пространстве имеют подходы, положенные в основу комплекса документов в области национальной безопасности и стратегического планирования. Согласно Стратегии национальной безопасности РФ[67], достижение цели обеспечения информационной безопасности осуществляется путем реализации государственной политики, направленной на решение, в частности, следующих задач: снижение до минимально возможного уровня количества утечек информации ограниченного доступа и персональных данных, а также уменьшение количества нарушений требований законодательства по защите такой информации и персональных данных; обеспечение защиты

[67] Утверждена Указом Президента РФ от 2 июля 2021 г. № 400.

конституционных прав и свобод человека и гражданина при обработке персональных данных, в т.ч. с использованием информационных технологий[68].

В соответствии с п. **3** Стратегии развития информационного общества в РФ на **2017–2030** годы[69] ее основными принципами являются:

а) обеспечение прав граждан на доступ к информации;

б) обеспечение свободы выбора средств получения знаний при работе с информацией;

в) сохранение традиционных и привычных для граждан (отличных от цифровых) форм получения товаров и услуг;

г) приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий;

д) обеспечение законности и разумной достаточности при сборе, накоплении и распространении информации о гражданах и организациях;

е) обеспечение государственной защиты интересов российских граждан в информационной сфере.

Среди задач, указанных в Стратегии развития информационного общества в РФ, следует отметить «развитие технологий электронного взаимодействия граждан, организаций, государственных органов, органов местного самоуправления наряду с сохранением возможности взаимодействия граждан с указанными организациями и органами без применения информационных технологий» (подп. «д» п. **40**).

Таким образом, одним из главных условий, которое позволит обеспечить социальную стабильность и доверие граждан государству, является соответствие федерального законодательства и подзаконных актов, атакже практики их применения положениям Конституции РФ и приведённых документов стратегического планирования.

2.1.3. Полнота действия прав и свобод человека и гражданина в цифровом пространстве Российской Федерации

Мы убеждены: **защите и реализации в цифровом пространстве РФ подлежит весь объём конституционных прав и свобод человека и гражданина.** Разработка нормативных правовых актов, документов стратегического планирования и иных документов в рамках цифровой

[68] Подпункты 6, 8 пункта 57 Стратегии национальной безопасности РФ.
[69] Утверждена Указом Президента РФ от 9 мая 2017 г. № 203.

трансформации, внедрение новых цифровых технологий **не должны отменять или умалять права и свободы** человека и гражданина, установленные российским законодательством. Защита прав и свобод человека и гражданина в цифровом пространстве РФ должна быть целевым и ценностным ориентиром развития экономики данных и общества знаний.

К числу **специфических (но вытекающих из конституционных) прав и свобод** человека и гражданина, подлежащих защите в цифровом пространстве РФ, относятся:

– право на защиту цифровой идентичности;

– право на обеспечение цифрового суверенитета человека;

– право на защиту от информационно-психологической манипуляции;

– право на защиту от цифровой дискриминации;

– право на защиту биометрических и иных персональных данных;

– право на отзыв данных и забвение в цифровом пространстве;

– право на защиту от противоправных деяний в цифровом пространстве;

– право на оспаривание решений и действий цифровых систем;

– право на использование традиционных форм взаимодействия граждан, бизнеса и государства;

– право на защиту от негативных социальных последствий цифровизации.

Особое значение имеет защита прав и свобод несовершеннолетних граждан в цифровом пространстве РФ, в том числе:

– от противоправного контента в цифровом пространстве;

– от сетевого манипулирования;

– от цифровой дискриминации;

– от передачи образовательной и воспитательных функций учителя системам ИИ;

– от цифровой зависимости;

– от причинения вреда их здоровью при использовании цифровых технологий.

В свою очередь, право родителей, воспитателей, преподавателей ограничивать присутствие несовершеннолетних в цифровом пространстве является важным условием обеспечения защиты их прав.

2.1.4. Обеспечение суверенитета РФ над национальным цифровым пространством

Поскольку многие страны мира, а также международные организации, включая ЮНЕСКО и Совет Европы, в настоящий момент озабочены

регулированием цифровой среды, нам нужно ответить на естественно возникающие важные вопросы о соотношении российского и международного регулирования:

- нужно ли России применять внутри страны мировой опыт регулирования цифрового пространства?
- нужно ли стремиться участвовать в создании международных соглашений и законов о регулировании цифрового пространства и синхронизировать законодательство РФ с ними?

Заметим, что основные игроки цифровой сферы – США, Китай и ЕС – сейчас энергично занимаются разработкой и введением национального регулирования в этой сфере. Более мелкие игроки – Турция, арабские страны, страны Юго-Восточной Азии – также вырабатывают собственные подходы, часто с интересными и оригинальными законодательными решениями (наподобие «приземления» цифровых экосистем и «цифрового налога»). Нужно внимательно изучать мировой опыт в этой области, однако необходимо понимать, что все упомянутые крупные игроки придерживаются **разных цивилизационных ценностей**, и движутся в области регулирования цифровой сферы в соответствии с ними. Скажем, Китай движется в сторону усиления контроля над своими гражданами, в том числе планирует вводить тотальные социальные рейтинги, создавая цифровую «антиутопию» в реальности.

В США продолжается политика обеспечения максимального экономического и законодательного благоприятствования собственным глобальным цифровым суперкорпорациям (правда, с возрастающим идеологическим контролем за ними со стороны правительства и спецслужб). В ЕС, напротив, регулирование цифрового пространства движется в сторону всё больших ограничений деятельности цифровых платформ в области оборота пользовательских данных и публикации контента, с существенным смещением в сторону экономических механизмов контроля и принуждения.

Эти различия объясняются, в первую очередь, различными представлениями о благом и должном социальном порядке, то есть разными цивилизационными установками и целями. Кроме того, сильное влияние оказывает реальное положение стран в цифровом мире: США – абсолютный лидер цифровой сферы, носитель полноценного цифрового суверенитета; ЕС – технологически зависимое пространство без собственных цифровых платформ; Китай – практически независимая страна в области как собственных цифровых платформ и медийного пространства, так и аппаратного обеспечения.

Россия в этом смысле находится в особом положении: мы не являемся полностью зависимыми от США в технологическом смысле и уже взяли курс на импортозамещение; в ценностной сфере мы не готовы превратить страну в «цифровой концлагерь» или отдать власть «цифровым экосистемам». **Это означает, что России придётся искать баланс, свой собственный «цифровой путь».** Впрочем, это не мешает изучать мировой опыт законотворчества и заимствовать наиболее подходящие идеи и механизмы регулирования.

Следует также обратить внимание на распространённую точку зрения, согласно которой нам нужно прежде всего добиваться заключения международных соглашений в области регулирования цифрового пространства, введения общемировых правил информационной безопасности, а уже затем приводить национальное законодательство в соответствие с ними. Мы считаем эту позицию неверной по следующим причинам:

1) **перспективы создания всеобщего международного «цифрового» законодательства крайне туманны,** страны - лидеры в развитии цифровых «экосистем» и технологий ИИ (США и Китай) не захотят добровольно накладывать на себя серьёзные ограничения и обязательства, не соответствующие их видению дальнейшего развития;

2) **предыдущие попытки международного регулирования цифровой среды провалились,** двадцатилетний опыт попыток создать международное законодательство в сфере информационной безопасности или передать управление маршрутизацией Интернета в руки международного сообщества не завершился принятием международных правовых актов в этой сфере;

3) **подходы к регулированию цифровой среды у США, Китая и ЕС разнятся**, эти противоречия вряд ли получится сгладить при проектировании международных норм;

4) **перспективы международного правоприменения в цифровом пространстве ещё более туманны,** есть большие сомнения в том, что страны-лидеры согласятся на международное расследование компьютерных инцидентов, имеющих цифровой след на их территории, а тем более – выдачу киберпреступников, действующих с этой территории[70]. Конституция РФ также

[70] Последнюю четверть века 60-80% всех кибератак, взломов, вирусов, спама в мире исходят с территории США. Согласно утечкам Викиликс, в США этим только официально занимаются тысячи офицеров Киберкомандования Минобороны США и разведсообщества.

запрещает экстрадицию российских граждан по любым зарубежным уголовным делам, запросам и основаниям;

5) **глобальные цифровые платформы можно «приземлять» только локально,** перспективы создания всемирного законодательства, регулирующего их деятельность близки к нулю. Национальные представления о приемлемом и неприемлемом контенте, требованиях к поведению цифровых платформ кардинально отличаются в разных странах, что легко прослеживается по политике и основаниям блокировок пользовательских аккаунтов;

6) **средства принуждения цифровых платформ к исполнению требований национального законодательства также локальны**, по сути, сводятся к штрафам и блокировкам. Подобных международных средств и механизмов не существует, и сейчас даже не просматриваются пути к их созданию;

7) **при разработке и последующей ратификации международных соглашений в «цифровой» сфере, нам может быть навязана чужая этическая и юридическая модель.** Практика показывает (например, в случаях с ВТО или Киотским протоколом), что международное сообщество может под давлением «лидеров свободного мира» закладывать в международные правовые акты односторонние представления о законности и справедливости.

Безусловно, стоит проявлять добрую волю к сотрудничеству в области создания международных правил и норм для цифрового пространства и участвовать во всех разумных международных инициативах, однако рассчитывать на полезные результаты в ближайшее время и откладывать формирование собственной нормативной базы нельзя. Национальное законодательство нужно исправлять и дорабатывать параллельно участию в международных инициативах и даже с опережением. При этом присоединение к международным соглашениям в этой сфере должны осуществляться не в ущерб национальным интересам нашей страны.

2.1.5. Принципы работы с данными

В целях защиты прав и свобод человека и гражданина, обеспечения суверенитета России, необходимо сформулировать и законодательно закрепить новые принципы использования персональных данных. Несмотря на различные подходы к регулированию, правам граждан и общей системе ценностей, мы вполне можем заимствовать некоторые идеи и методы у других стран с последующей их адаптацией под российские реалии и стратегические национальные приоритеты. В частности, стоит разработать российский аналог

разумных принципов работы с данными, закреплённых в европейском Общем регламенте о правилах работы с данными (GDPR)[71]. Среди таких принципов можно выделить:

1) **законность, справедливость и прозрачность –** персональные данные должны обрабатываться законно, справедливо и прозрачно, а любую информацию о целях, методах и объёмах обработки персональных данных следует излагать максимально открыто, доступно и просто;

2) **ограничение цели** – данные должны собираться и использоваться исключительно в тех целях, которые заявлены компанией или организацией (онлайн-сервисом);

3) **минимизация данных** – нельзя собирать личные данные в большем объёме, чем это необходимо для заявленных целей их обработки;

4) **точность и достоверность** – личные данные, которые являются неточными или ложными, должны быть удалены или исправлены (в том числе по требованию пользователя);

5) **ограничение хранения** – личные данные должны храниться в форме, которая позволяет идентифицировать субъекты данных на срок не более, чем это необходимо для целей обработки;

6) **целостность и конфиденциальность** – при обработке данных пользователей компании и органы публичной власти обязаны обеспечить их защиту от несанкционированной или незаконной обработки, уничтожения и повреждения.

Многие из названных принципов в том или ином виде закреплены в Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных», но вместе с тем, нуждаются в дальнейшем уточнении и детализации. Представляется, что обсуждение оптимальных механизмов реализации названных принципов может стать основой для консолидации ответственных представителей «цифровой» сферы, политиков, экспертов, институтов гражданского общества, а также одной из стартовых стратегий ценностной «перезагрузки» процессов цифровизации.

[71] Регламент Европейского Парламента и Совета Европы от 27 апреля 2016 г. № 2016/679 «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46/ЕС» (Общие правила защиты данных) // URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

2.1.6. Использование потенциала цифровых технологий для культурного развития личности и общества

К сожалению, новые технологии распространения информации прочно ассоциируются с вытеснением высокой культуры, культурного наследия из центра общественного внимания, с доминированием массового «низового» спроса, примитивизацией образования, навязыванием масскультуры. Дальнейшее глобальное развитие этих трендов ведёт к неприемлемым состояниям государства и общества, таким как тотальный контроль над обществом со стороны цифровых корпораций, рекламных систем, торговых площадок, эксплуатирующий «низовые» стороны человека и общества; стратегическая неуправляемость и отсутствие развития в условиях отсутствия ценностных мотиваций, свободы и саморегуляции человека. Обозначенные состояния несовместимы с конституционными идеалами правового государства, демократии, прав и свобод человека и гражданина, уважения к достоинству личности, её культурному и природному наследию и развитию.

Во многом именно **культурные трансформации, связанные с цифровизацией, являются решающими** с точки зрения формирования и реализации образа будущего страны. Выбор «цифрового пути» России сегодня выглядит так: либо разложившееся, деградировавшее в культурном отношении общество станет социальной почвой для нового «цифрового тоталитаризма» и нового «цифрового крепостного права», либо государством и обществом будут предприняты усилия и меры к тому, чтобы наши конституционные идеалы, правовое государство сохранили и развили свою социальную базу, существовали и развивались в стратегической перспективе.

Мы считаем, что сегодня необходимо принять в качестве руководящего принципа «**принцип высокой планки»** (или презумпцию высокого достоинства человека) как основу для взаимодействия государства, бизнеса и общества, ключевой вектор государственной культурной политики и государственной системы образования, а также принцип функционирования медиапространства. Иными словами, в основу этики публичного диалога, этики организации информационного пространства должен быть положен важнейший императив российской культуры – **иметь человека в центре политики и права, даже вопреки человеческому несовершенству**.

Подчеркнём – речь идёт не о цензуре контента цифрового пространства, а об уважении достоинства личности, признании права человека жить и развиваться в публичном информационном пространстве, где поддерживаются

соответствующие стандарты и уровни. Нам нужна не цензура, а всеобщая культура уважения к человеческому достоинству. В практической плоскости это означает, что перед российским гражданским обществом, политиками, интеллектуалами и представителями бизнеса стоит задача по выработке такой модели организации информационного пространства, которая будет соответствовать нашим конституционным ценностям, модели правового государства, принципу уважения к человеческому достоинству и станет полноценной средой жизни гражданина как субъекта культуры.

Каким критериям должна отвечать эта модель?

1. Человек в правовом государстве – не только статистическая единица, «потребительский вектор». Он – наследник и субъект высокой культуры, к нему обращены требования Конституции РФ, в том числе – требование хранить культурное наследие. Эта модель должна решать одну из важнейших проблем нашего общества – проблему отчуждения значительной части сограждан (особенно младших поколений) от собственного культурного наследия, как фактора формирования личности и трендов общественного развития.

2. **Модель развития цифрового пространства России должна соответствовать закреплённым в Конституции РФ правам и свободам человека и гражданина**, что исключает идеологическую цензуру, но означает необходимость соответствия цифровой среды традиционным духовно-нравственным ценностям российского общества.

3. Наше государство должно развиваться как социальное, публичное пространство не должно быть тотально коммерциализировано, а граждане должны иметь равный доступ к культурному наследию.

Только эффективное государство в современном мире может создать развитую информационную («цифровую») инфраструктуру. Однако сделать ее инструментом культурного и интеллектуального развития граждан – одновременно признак и обязанность эффективного правового государства.

2.2. Пути и решения в области защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации

Достижение целей обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве РФ осуществляется посредством решения комплекса задач на следующих направлениях:

1) **совершенствование и развитие законодательства** в сфере обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве РФ;

2) **институциональное развитие** цифрового пространства РФ, а также развитие **саморегулирования** в данной сфере;

3) формирование устойчивой и достаточной для безопасного развития **цифровой грамотности граждан** РФ;

4) **правозащитная и общественная деятельность, гражданские инициативы** в области развития цифрового пространства;

5) **научные исследования** процессов формирования и развития цифрового пространства.

Раскроем далее содержание указанных направлений.

2.2.1. Совершенствование и развитие законодательства

Согласно пункту «м» ст. **71** Конституции РФ в федеральном ведении находится обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных. Согласно ч. **1** ст. **76** Конституции РФ, по предметам ведения РФ принимаются федеральные конституционные законы и федеральные законы, имеющие прямое действие на всей территории России. Реализация указанных положений в области регулирования цифровой среды требует серьёзной и системной законотворческой деятельности.

На данный момент, с учётом обозначенных вызовов и угроз реализации прав и свобод человека и гражданина в цифровом пространстве РФ, наиболее актуальными представляются следующие меры по совершенствованию и развитию российского законодательства:

1. Дальнейшее развитие законодательства в области защиты суверенитета нашей страны в цифровом пространстве, в том числе, по развитию правовых механизмов регулирования деятельности зарубежных и транснациональных компаний в соответствии с требованиями российского законодательства.

2. Разработка Цифрового (Информационного) кодекса, систематизирующего правовое регулирование отношений в цифровом пространстве РФ, устанавливающего принципы и механизмы защиты прав и свобод человека и гражданина в цифровом пространстве РФ, а также механизмы обеспечения информационной безопасности нашей страны – сначала в виде поправок к существующим нормативным правовым актам и выработки рамочных законов, а затем в формате самостоятельного кодифицированного акта.

3. Дальнейшее совершенствование законодательных гарантий доступа граждан к культурным ценностям, образованию, просвещению в цифровом пространстве.

4. Дальнейшее законодательное обеспечение развития инфраструктуры электронной демократии, в частности, установление запрета на использование иностранных «цифровых посредников» в виде социальных сетей, мессенджеров и иных небезопасных каналов связи при взаимодействии граждан с органами публичной власти.

5. Сохранение бумажного документооборота в критически значимых сферах защиты интересов государства, гражданского общества, коммерческих и некоммерческих организаций, общественных объединений и граждан.

6. Обеспечение реализации всех прав и свобод граждан, не использующих возможности цифрового пространства, вне зависимости от причин (свободное волеизъявление, состояние здоровья, инвалидность, психологические и возрастные особенности, уровень образования, уровень дохода и т.д.).

7. Введение моратория на формирование и использование интегральных баз данных о гражданах, создаваемых путём объединения баз персональных данных, обработка которых осуществляется в целях, несовместимых с целями, заявленными при создании отдельных баз данных.

8. Введение запрета на создание систем социального рейтингования, способных иметь негативные последствия для реализации прав и свобод человека и гражданина, а также установление ответственности за создание, внедрение таких систем и причинённый ими ущерб.

9. Совершенствование правовых механизмов, регулирующих сбор персональных данных граждан, в том числе, уточнение условий и порядка дачи информированного добровольного согласия граждан на сбор данных.

10. Дальнейшая дифференциация ответственности за несанкционированный сбор и противоправное использование персональных

данных, несанкционированное распространение, кражу, организацию утечек, несанкционированную продажу и покупку таких данных.

11. Создание правовых основ института аудита и независимой экспертизы цифровых технологий, цифровых платформ и сервисов, систем хранения и передачи персональных данных.

12. Установление запрета на многократное использование ранее собранных и не обновляемых персональных данных, в том числе системами, которые не осуществляли первичный сбор этих данных.

13. Установление запрета на использование систем идентификации («вычисления») персональных данных по косвенным признакам, обнаруженным в больших данных о пользователях.

14. Совершенствование правовых механизмов защиты граждан от цифровой дискриминации на основе собираемых и вычисляемых данных (в том числе, посредством создания «социальных рейтингов»).

15. Законодательное закрепление обязанностей хранения персональных данных в электронном виде в государственных информационных системах по месту возникновения таких данных (в локальных базах данных).

16. Совершенствование правовых механизмов профилактики экстремизма, противодействия экстремистским, коррупционным, криминальным, иным деструктивным действиям в цифровом пространстве, нацеленным на разрушение основ общественного и государственного устройства.

17. Совершенствование правовых механизмов реализации в цифровом пространстве свободы договоров, свободы предпринимательской деятельности, защиты венчурного, малого и среднего бизнеса, а также самозанятых граждан.

18. Ужесточение ответственности за противоправное изготовление, использование и оборот цифровых документов.

19. Совершенствование трудового законодательства, в том числе в части установления социальных обязательств для хозяйствующих субъектов, в настоящее время не несущих таких обязательств (цифровые посредники и др.).

20. Повышение эффективности правовых механизмов противодействия манипулированию в цифровом пространстве общественным мнением, сознанием и поведением граждан.

21. Совершенствование законодательства об особых экспериментальных режимах («законодательных песочницах)» в целях недопущения создания

предпосылок к нарушению прав и свобод человека и гражданина на региональном и местном уровнях.

22. Системное развитие правовых механизмов защиты и реализации специфических прав, возникающих в ходе развития цифрового пространства (права на защиту цифровой идентичности, на обеспечение цифрового суверенитета личности, на защиту от информационно-психологической манипуляции, на отзыв данных, на забвение в цифровом пространстве, на защиту от противоправных деяний в цифровом пространстве, на защиту от негативных социальных последствий цифровизации и иные права).

23. Приоритетное развитие законодательства в области защиты прав несовершеннолетних в цифровом пространстве, а также гарантий прав родителей, воспитателей, преподавателей регламентировать или ограничивать присутствие несовершеннолетних в цифровом пространстве.

24. Развитие законодательства о государственно-частном партнёрстве в решении задач развития цифрового пространства и обеспечения защиты в цифровом пространстве прав и свобод человека и гражданина, интересов государства и общества.

25. Развитие законодательства в области установления (использования) режима тайны и категории защищаемых данных.

26. Законодательное закрепление категорий особо уязвимых в цифровом отношении граждан и обеспечение для них соответствующего правового режима.

27. Законодательное закрепление порядка раскрытия информации цифровыми сервисами, а также порядка сбора и хранения данных.

28. Установление упрощённого режима оспаривания гражданами данных о себе в частных и государственных базах данных.

29. Установление запрета на ограничение информационного суверенитета человека.

30. Установление запрета цифровой слежки, цифровых «двойников», «профилей», «траекторий» и «рейтингов».

31. Установление квалификационных требований к специалистам по обработке данных и мер ответственности за их нарушения.

32. Разработка единых стандартов пользовательских соглашений и политики цифровых сервисов для всех цифровых сервисов, как отечественных, так и зарубежных, на территории России.

33. Установление запрета на присвоение единого номера-идентификатора человеку в общенациональном цифровом пространстве.

34. Минимизация состава обрабатываемых персональных данных, необходимых для решения возлагаемых на государственные, муниципальные и частные информационные системы задач.

35. Установление запрета обработки персональных данных в рамках единой инфраструктуры.

2.2.2. Развитие институциональной структуры цифрового пространства Российской Федерации. Саморегулирование

Обеспечение защиты прав и свобод человека и гражданина должно включать в себя решение комплекса задач по развитию институциональной структуры цифрового пространства РФ, а также саморегулирования в данной сфере. К числу этих задач следует отнести:

1. Дальнейшее развитие публичной инфраструктуры электронной демократии в цифровом пространстве РФ. Здесь необходимо преодолеть дисбаланс, при котором существующая система государственных и муниципальных сервисов (в том числе, контрольного характера) не уравновешена системой электронных сервисов и возможностей для гражданского действия, выражения гражданской позиции. Мы считаем неприемлемым положение, при котором граждане используют для выражения собственных позиций, в том числе для коллективного гражданского действия, социальные сети и иные частные (часто зарубежные) ресурсы, не имея при этом эффективных и легитимных государственных сервисов, гарантирующих обратную связь от органов публичной власти.

2. Дальнейшее развитие публичной инфраструктуры образования, культуры и просвещения в цифровом пространстве РФ.

3. Дальнейшее развитие системы рекомендательных актов и этических кодексов использования цифровых технологий как основы для саморегулирования субъектов цифрового пространства, работающих с данными пользователей на территории РФ с последующей перспективой их трансформации в законодательные акты.

4. Проведение информационных кампаний в целях развития социальной ответственности бизнеса при внедрении новых цифровых технологий.

5. Создание института «правозащитного аудита» и независимой экспертизы цифровых технологий и систем хранения и передачи данных, а также повышение вовлеченности институтов гражданского общества в разработку документов стратегического планирования в области цифровых технологий.

2.2.3. Рост и поддержание высокого уровня цифровой гигиены и компетентности граждан

Среди мер по обеспечению роста цифровой грамотности граждан можно предложить следующие:

1. Проведение массовых просветительских кампаний по повышению осведомлённости граждан об их правах и свободах в условиях цифровой трансформации, а также о возможностях их реализации.

2. Проведение массовых просветительских кампаний по повышению и осведомлённости граждан о цифровой гигиене и правилах безопасности в цифровом пространстве.

3. Создание системы просветительских организаций и проектов, поддерживающих приемлемый уровень цифровой грамотности и осведомлённости о цифровой гигиене, в том числе, для граждан с ограниченными возможностями, пожилых и несовершеннолетних граждан.

4. Включение в образовательные программы, реализуемые в государственных и муниципальных учреждениях образования, знаний и навыков, необходимых для реализации прав и свобод новых поколений граждан, развития у них установок на неприятие и противодействие экстремистским, криминальным, иным деструктивным действиям в цифровом пространстве, нацеленным на разрушение основ общественного и государственного устройства, этических основ российского общества и культуры.

2.2.4. Правозащитная и общественная деятельность, гражданские инициативы

Важнейшим условием формирования и реализации российской модели цифровизации выступает осознанное участие граждан, правозащитников и гражданских объединений в решении вопросов защиты прав и свобод граждан в цифровом пространстве. Основные направления деятельности здесь таковы:

1. Проведение правозащитной и гражданской экспертизы программ цифровизации и цифрового развития. Проекты цифровизации, затрагивающие широкие круги населения и/или уязвимые категории граждан, такие как цифровизация образования, создание реестров персональных данных и пр., создающие риски, угрожающие правам и свободам граждан, должны проходить экспертизу со стороны общественных правозащитных организаций, Общественной палаты РФ, Совета при Президенте РФ по развитию гражданского общества и правам человека, родительских ассоциаций и т.д.

2. Содействие гражданам и организациям в реализации их прав и свобод в цифровом пространстве. Развитие на массовом уровне гражданских и общественных инициатив в области формирования и развития цифрового пространства, защиты прав и свобод человека и гражданина, активное выражение гражданского мнения и гражданской позиции по различным аспектам цифровой трансформации, формирования цифрового пространства.

3. Повышенная защита несовершеннолетних и уязвимых групп граждан при реализации их прав и свобод в условиях цифровой трансформации.

4. Формирование квалифицированного общественного мнения и развитие диалога государства, общества и бизнеса по вопросам совершенствования механизмов обеспечения реализации прав и свобод человека и гражданина в цифровом пространстве РФ.

5. Использование различных форм изучения общественного мнения (опросы, общественные слушания, голосования) по ключевым вопросам цифровизации, затрагивающим основные права и свободы граждан, таким как: цифровизация образования и медицины, создание единых реестров граждан, цифровая трансформация рынка труда и городской среды, правила работы цифровых СМИ и медийных платформ.

2.2.5. Научные исследования проблем цифровизации

Цифровизация – комплексный вызов обществу и государству, имеющий сложную природу и разноплановые эффекты в различных сферах бытия личности, общества и государства. Соответственно, его изучение должно носить междисциплинарный характер, включать не только подходы естественных и технических наук, но и методологии социально-гуманитарного знания. К наиболее актуальным направлениям научных исследований, которые будут востребованы обществом и государством, на наш взгляд, относятся:

1. Изучение общественного мнения по вопросам цифровой трансформации, формирования цифрового пространства.

2. Прогнозирование развития цифрового пространства и цифровых технологий.

3. Прогнозирование возможных социальных, экономических и политических последствий цифровизации, потенциальных нарушений прав и свобод граждан, влияния на здоровье нации, уровень безработицы и социальной напряжённости.

4. Выявление гуманитарных и культурных последствий цифровизации.

5. Изучение опыта и модели регулирования реализации прав и свобод граждан в ведущих странах мира.

6. Создание сценариев развития цифрового пространства для России.

Заключение

Безусловно, полезная и перспективная для общества и государства цифровизация отраслей экономики нашей страны, государственного управления может и должна быть проведена без создания и умножения рисков, обозначенных в настоящем Докладе, без ущемления прав и свобод граждан России и без снижения выгод от цифровизации.

Здесь уместно провести аналогию с появлением автомобилей в начале XX века. Первые десятилетия существования автомобилей и их эксплуатации на дорогах общего пользования этот вид транспорта практически не регулировался, рос, произвольно и бесконтрольно, порождал всё большее количество рисков и трагических инцидентов. Массовое распространение личного автотранспорта выявило необходимость создания Правил дорожного движения (ПДД), которые и в итоге были введены в большинстве стран к **1920–1930** годам, хотя первые светофоры и дорожные знаки появились в конце **XIX** века. Появление ПДД никак не ограничило развитие автомобильной отрасли, а напротив, купировало нараставшие риски и позволило энергично развивать отрасль, которая сейчас является неотъемлемой частью экономики и жизни в целом.

Мы сейчас находимся в аналогичной ситуации: цифровая отрасль растёт неупорядоченно, в серых правовых зонах, создаёт большие, не до конца определённые риски, поэтому нам нужны «правила движения» в цифровом пространстве. На фоне распространения всё более изощрённой слежки и социального отчуждения при помощи цифровых технологий в большинстве стран мира (в чём бесспорными лидерами являются Китай и США) **Россия, как демократическое правовое государство, может предложить миру привлекательную модель цифровой трансформации экономики и механизма государственного управления:**

– защищая в цифровом пространстве РФ весь объем прав и свобод человека и гражданина;

– защищая традиционные духовно-нравственные ценности общества;

– решая задачи минимизации угроз, рисков ущемления прав и свобод человека и гражданина, возникающих при цифровизация экономики, социальной сферы, государственного и муниципального управления.

Для этого нужно ввести «Правила дорожного движения в цифровом пространстве», учитывающие в том числе мировые усилия в этом направлении, но при этом опирающиеся на свои, оригинальные и независимые представления граждан и общества о безопасности, справедливости и равенстве, а также приложить максимальные усилия по предупреждению и сглаживанию негативных социальных эффектов цифровизации.

При этом нельзя «выплеснуть с водой и ребёнка», то есть путём чрезмерных запретов и ограничений затормозить развитие отечественной ИТ-отрасли, разработку отечественных технологий обработки больших данных и искусственного интеллекта.

Все это говорит о необходимости гармонизации требований соблюдения прав и свобод человека и гражданина, требований научно-технологического и социально-экономического развития России, задач развития безопасного информационного пространства, защиты российского общества от деструктивного информационно-психологического воздействия, культурного развития граждан и роста человеческого потенциала нашей страны, обеспечения безопасности личности, общества и государства.

Такой взвешенный «срединный путь» позволит нам получить все положительные эффекты цифровизации, не превратив своих граждан в бесправные «винтики» в общем машинном конвейере «новой экономики».

Авторский коллектив

- **Ашманов Игорь Станиславович**, канд. техн. наук, президент аналитической компании «Крибрум», член Совета при Президенте РФ по развитию гражданского общества и правам человека
- **Волобуев Сергей Григорьевич**, философ, автор гражданской инициативы «Хартия Рунета», координатор проекта «Гражданский экзамен», эксперт Центра социально-консервативной политики
- **Дейнеко Алексей Геннадьевич**, канд. юрид. наук, профессор департамента права цифровых технологий и биоправа НИУ «Высшая школа экономики», Государственный советник РФ 2 класса
- **Кабанов Кирилл Викторович**, председатель Национального антикоррупционного комитета, член Совета при Президенте РФ по развитию гражданского общества и правам человека
- **Касперская Наталья Ивановна**, специалист по информационной безопасности, президент группы компаний InfoWatch
- **Куринов Сергей Александрович**, канд. полит. наук, Действительный государственный советник РФ 3 класса
- **Наумов Виктор Борисович**, д-р юрид. наук, главный научный сотрудник Сектора информационного права и международной информационной безопасности Института государства и права РАН, руководитель практики в области интеллектуальной собственности, ИТ и телекоммуникаций, партнёр санкт-петербургского офиса Nextons
- **Новиков Игорь Алексеевич,** эксперт Программы развития ООН, директор АНО «Пространство равных возможностей», член Совета при Президенте РФ по развитию гражданского общества и правам человека
- **Сидоренко Элина Леонидовна,** д-р юрид. наук, профессор МГИМО(у) МИД России, генеральный директор АНО «Платформа для работы с обращениями предпринимателей», член Совета при Президенте РФ по развитию гражданского общества и правам человека
- **Фадеев Валерий Александрович**, советник Президента РФ, председатель Совета при Президенте РФ по развитию гражданского общества и правам человека, научный руководитель Института наследия и современного общества РГГУ