СПЧ

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

Цифровая трансформация и защита прав граждан в цифровом пространстве

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

Москва, 2021

Содержание:

Введение. И свобода, и безопасность: императивы общественного договора

Настоящий Доклад посвящён проблематике соблюдения и защиты прав и свобод человека и гражданина в условиях стремительной, часто форсированной, цифровизации всех сторон жизни личности, общества и государства.

Мы говорим здесь о важнейшем пункте «общественного договора», согласно которому правовое государство призвано обеспечивать для человека и гражданина одновременно и безопасность, и возможность полноценной реализации прав и свобод. В том числе – в информационной (цифровой) среде.

Этот пункт «общественного договора» зафиксирован в Конституции Российской Федерации и, применительно к реалиям информатизации (цифровизации), специально усилен отдельной конституционной поправкой 2020 года. Речь идет о пункте «м» статьи 71, закрепляющем в ведении Российской Федерации *«обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных»*[1].

Внедрение современных цифровых технологий формирует новые реалии для человека, общества и государства, а также значительно видоизменяет уже существующие. Технологии больших данных, искусственного интеллекта, беспилотный транспорт, цифровая медицина, виртуальные среды общения создают обширные возможности для развития нового экономического уклада,

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

международного сотрудничества и конкуренции. Однако усугубившиеся в ходе пандемии процессы атомизации общества и дистанцирования людей способствовали резкому ускорению «погружения» человека в цифровую среду. Это сопровождается развитием новых возможностей 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.

Безусловно, современные цифровые технологии – полезная и стратегически важная вещь. Они позволяют вывести управление государством, экономикой и развитием территорий на совершенно новый технологический уровень. Однако сейчас в России новые цифровые технологии внедряют безоглядно, без должных обоснований, в спешке, часто принудительно, методом «ковровой бомбёжки». Цифровизация госуправления и городской среды уже приобрела характер типичной бюрократической кампании, напоминающей приснопамятные «перестройку и ускорение» середины 1980-х годов, с лозунгами, шумовыми категориями, а также формальной «отчётностью с мест».

Целый спектр актуальных, если не сказать – жгучих, проблем для реализации прав граждан обусловлен тем, что внедрение так называемой «цифры» в коммерческом секторе экономики 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 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, возможности реализации ими всей полноты конституционно-гарантированных прав и свобод.

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 мы сегодня не имеем кодекса, 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 в применяемой юрисдикции (в совокупности именуемые трансграничностью киберпространства) не должны приводить к ошибочному выводу о невозможности правового регулирования отношений в цифровом пространстве.

Решительным шагом к созданию российского «Цифрового кодекса» авторы доклада считают Поручение Президента Российской Федерации В.В. Путина Совету при Президенте Российской Федерации по развитию гражданского общества и правам человека и Правительству Российской Федерации разработать до 1 августа 2021 г. проект Концепции защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации[2].

Данное Поручение было дано по итогам ежегодной встречи Президента с Советом, состоявшейся 10 декабря 2020 г. В ходе данной встречи члены Совета, подводя своего рода итоги «пандемийного» года, обозначили комплекс правовых, в том числе конституционно-правовых коллизий, выявившихся в самом масштабном со времени принятия действующей Конституции в 1993 году наступлении на права и свободы человека в нашей стране.

[2] Ссылка: http://kremlin.ru/acts/assignments/orders/64952

На момент публикации настоящего доклада Поручение главы государства исполнено. Проект Концепции защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации разработан Советом во взаимодействии с экспертным и научным сообществом и представлен в Правительство и Администрацию Президента Российской Федерации.

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 Российской Федерации. Формат упомянутого проекта Концепции не подразумевает погружение в детали, а также сведение воедино всех экспертных наработок, тезисов и предложений. Вместе с тем большинство документов стратегического уровня, подобные Концепции защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации, как правило, нуждаются в комментариях и экспертных материалах, раскрывающих суть изложенного и служащих в качестве ориентира в рамках реализации такого рода документов (в том числе в законотворческой деятельности). В связи с этим мы приняли решение подготовить настоящий Доклад, как смысловую и терминологическую основу для Концепции.

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 является одной из национальных целей развития Российской Федерации на период до 2030 года.

Цифровая трансформация, согласно принятому и утверждённому 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 о проблемах соблюдения прав человека в условиях цифровизации можно выделить два аспекта. С одной стороны, ставшие уже «традиционными» («аналоговыми») права граждан нарушаются и ограничиваются в процессах цифровизации. С другой стороны, происходит «перенос» этих прав в цифровое пространство, где возникают производные «цифровые права»[3] – особые цифровые «проекции» общих прав граждан. При этом «цифровые права» также страдают от хаотичной, мозаичной, навязываемой цифровизации.

Наша принципиальная позиция состоит в том, что личность гражданина России, его суверенитет, достоинство и неприкосновенность частной жизни обеспечивают и оберегают указанные в Конституции Российской Федерации, а также в ратифицированных Российской Федерацией международно-правовых актах, положения об основных правах и свободах человека и гражданина. В цифровом пространстве эти основные права и свободы имеют соответствующие цифровые «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

[3] Здесь мы не имеем в виду отраслевое определение в ст. 141.1 Гражданского кодекса РФ, где под «цифровыми правами» понимаются исключительно права собственности на активы в цифровой форме.

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 и бесспорно, 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[4]. Бенефициарами такого понимания подхода к деятельности по защите основных прав и свобод выступает очень незначительное число граждан и экономических агентов, а бóльшая 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 понимания, что в Российской Федерации приоритетом в регулировании отношений и прав в цифровой среде являются, в первую очередь, права и законные интересы каждого гражданина. Условием их реализации выступают баланс интересов личности, общества и государства, обеспечение государственной и общественной безопасности, поддержание общественной нравственности и социального порядка.

Соответственно, защите и реализации в цифровом пространстве Российской Федерации подлежит **весь объем конституционных прав и свобод человека и гражданина**. Разработка и принятие нормативных

[4] Мы не разделяем известную, но ни на чём не основанную, идеологическую установку, что «Интернет – это зона абсолютной свободы», поскольку в разумном и справедливом правовом 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.

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 действующим законодательством Российской Федерации.

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 крайне 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.

Здесь надо оговориться, что сегодняшняя цифровизация и сопутствующая ей «идеология» являются ядром и движущей силой глобального научно-технологического и общественно-политического процесса - так называемой

«НБИКС-революции»[5], активно продвигаемой «евангелистами» нового мирового порядка».

Проблематика цифровизации находится сегодня на острие общественного внимания, однако без должного понимания, что она тесно смыкается со всем спектром «больших вызовов» современности (нанотехнологии, биотехнологии, генетические эксперименты, когнитивные технологии, трансформация социальных технологий и т.д.), а также связанными с ними этическими и правовыми вопросами.

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

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

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:

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

– дальнейшее развитие человечества якобы 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;

– 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;

– 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 искусственного интеллекта.

С сожалением следует отметить, что в массовом, 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 самый 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 параллельной «цифровой власти» и приход нового «цифрового класса»

Описанная выше «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.

Уже 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, как писал Ф. М. Достоевский, – «административный восторг».

Эта цифровая власть – особая, новая, она не создаётся обычными механизмами делегирования власти и полномочий, такими как выборы, назначения «сверху» или законодательство, а возникает «по месту», по самому факту получения доступа к данным, и является «параллельной» веткой власти.

Эту новую, фактическую власть получают чиновники и их ИТ-специалисты (в региональной и муниципальной власти, на транспорте, в налоговом ведомстве и т.п.), а также менеджмент и ИТ-специалисты крупных частных ИТ-корпораций (к которым относятся все цифровые интернет-платформы, производители смартфонов и операционных систем, интернет-провайдеры, мобильные операторы, операторы уличных камер, банки, прочие операторы персональных данных).

Параллельная «цифровая» власть в России и в мире пока фактически никак не регламентирована. В нашей стране она не укладывается в рамки и без того плохо работающего на практике и почти неисполняемого федерального закона № 152-ФЗ «О персональных данных». 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» служебного положения, доступу к цифровым инструментам, не являются сотрудниками спецслужб или силовых ведомств с ограничением доступа к информации, не дают присяги и не носят погоны.

Они, как правило, обычные штатские лица, не несущие серьёзной ответственности (в лучшем случае, они ограничены корпоративным договором

о неразглашении), что создаёт большие риски утечки, продажи, разглашения данных и манипуляции ими в личных и корпоративных целях.

В массе своей представители нового цифрового класса получают в среднем невысокие зарплаты, уязвимы к подкупу, причём их число и возможности доступа к данным быстро растут в ходе цифровизации. У представителей нового цифрового сословия (или *класса*) сейчас имеет место принципиальный разрыв между полученными по факту возможностями применения цифровых технологий и крайне низкой ответственностью за их ненадлежащее или скомпрометированное использование.

> Нужно заметить также, что «гражданские версии» алгоритмов искусственного интеллекта (ИИ), широкодоступные сейчас в виде «свободного программного обеспечения» (СПО) не только крупным корпорациям, но и одиночкам, и малому бизнесу, 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 граждан и использования для мошенничества (распознавание лиц, речи, вычисление персональных данных, шантаж, слежка, фабрикация «глубоких фейков[6]»), сейчас доступны кому угодно – как если бы огнестрельное нарезное автоматическое оружие можно было купить в любом продуктовом магазине.

По сути, во многих странах мира, в том числе и в нашей стране, возникает новый, «цифровой класс», выделяющийся по факту доступа к цифровым средствам производства и управления.

С момента возникновения первых государств и до сегодняшнего дня, в привычной для всего мирового сообщества схеме взаимоотношений «власть-

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

народ», разделительные линии между привилегированным классом и основной массой жителей традиционно проходили по двум основным признакам: социальному положению в иерархической пирамиде общества и по уровню материального достатка.

При всех известных изъянах такой градации правила взаимодействия внутри социума являются также понятными и принимаемыми абсолютным большинством членов общества.

С внедрением тотальной цифровизации факторы «статуса», «денег», «знаний», «умений» (за исключением цифровых) перестают быть решающими. Отныне 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.

Отметим: в классической теории «общественного договора» считается, что привилегированный класс стал таковым с некоего дозволения, санкции 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, является в целом справедливым. 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 массовой технологии будет в состоянии, например, улучшить свой «цифровой профиль» или положение в цифровом рейтинге, скомпрометировать работу всей системы или вывести себя за рамки воздействия цифровизации.

По сути, мы здесь видим не одобренную большинством передачу «кому-то достойному» статуса и власти, а так называемый «заговор специалистов», захват власти «по факту». Оператор технологии, не говоря уже о её владельце и разработчике, до некоторой степени получит функции «цифрового бога», формируя определённые 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, неподсудности представителей нового класса правовым и этическим нормам, «придуманных для простых смертных».

В случае полной реализации сценария «прихода нового цифрового класса» государственный аппарат превращается в статиста, не способного к какой-либо содержательной деятельности по защите своих же граждан. На чиновников всех уровней разработчиками, владельцами и даже 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 искусственного интеллекта для управления массами людей, транспортом, государственными и медицинскими услугами и т.п., «цифровых клерков», имеющих доступ к цифровым данным и системам, а также из их непосредственного начальства.

Доступ к цифровым средствам производства и управлению, централизованным базам персональных и больших данных даёт этому новому классу широчайшие возможности для управления, манипуляции, несравнимые с теми возможностями, что раньше давали личные данные граждан, тонким слоем «размазанные» в бумажном или электронном виде по различным государственным институтам и базам данных.

Фактическое наличие у нового цифрового класса «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[7].

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. Специфические «цифровые» причины и факторы возникновения рисков для прав граждан, безопасности общества и государства

1.2.1. Факторы скорости изменений и растущей сложности цифровой среды

В настоящее время цифровая среда как в России, так и во всем мире развивается хаотично, несогласованными усилиями, разрозненными программами и проектами органов власти и крупных цифровых корпораций. Никаких единых «правил дорожного движения» в этой среде не создано.

[7] Заметим, что государственные и муниципальные служащие, включая ответственных за цифровизацию, являются также уязвимыми для этих рисков, в силу преимущественно слабого владения технологиями и зависимости от своих ИТ-специалистов.

Усугубляет эту ситуацию низкая цифровая грамотность и осведомлённость о цифровой гигиене не только граждан, но и общества в целом, а также крайне низкая социальная и этическая ответственность крупного и среднего бизнеса при внедрении новых цифровых технологий.

Бизнес цифровых платформ и сервисов исповедует в настоящее время практически абсолютный правовой и этический нигилизм, считая область своей деятельности по сбору данных граждан и предоставлению цифровых услуг не только внеправовой, но и вне-моральной[8]. Новые цифровые технологии и сервисы сейчас используются бизнесом в первую очередь с целью получения конкурентных преимуществ и извлечения прибыли, но без должной защиты прав и интересов граждан.

Усилению рисков и угроз также способствуют **особые факторы риска цифровой среды, зачастую вообще не осознаваемые операторами и «евангелистами» цифровизации**. К этим факторам относятся:

– **фактор скорости изменений**, выражающийся в сверхбыстром, экспоненциальном развитии цифровой среды;

– **фактор высокой, постоянно возрастающей сложности цифровой среды**.

Сегодня существует стремительно углубляющийся **разрыв между скоростью процессов цифровизации и скоростью осознания их обществом**. Наше общество, законодатели, исполнительная власть, в том числе и ответственные за цифровизацию чиновники, не до конца оценивают реальность и глубину развивающихся угроз, зачастую не осознают возможные негативные стороны происходящих глобальных процессов цифровой трансформации и не

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

принимают в расчёт усиливающуюся конкуренцию между государствами и глобальными ИТ-корпорациями, развивающуюся под привлекательными лозунгами удобства и пользы цифровых технологий. При этом существенный разрыв между воспринимаемой и реальной глубиной изменений общественных отношений, частной и общественной жизни, госуправления, имеет объективный характер. В результате процессы цифровизации государства и общества идут со значительным опережением развития законодательства, призванного защищать права граждан в цифровой среде и цифровой суверенитет нашей страны.

Стремление к тотальной цифровизации имеет своей основой **иллюзию полного контроля над цифровой средой**, которой подвержены многие убеждённые «цифровизаторы» (прежде всего – 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 обстоятельств, 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[9];

[9] Только в последние 3 месяца осени 2021 года происходили многочисленные многочасовые сбои глобальных цифровых платформ Meta (Facebook), Google, YouTube, Instagram, задевшие сотни миллионов пользователей; но если от сбоев не застрахованы глобальные лидеры цифрового мира, имеющие десятки тысяч программистов и миллиарды пользователей – то кто тогда застрахован? Любые заверения в «абсолютной надёжности» цифровых систем – либо наивность, либо откровенная ложь и манипуляция.

– большое количество и 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;

– большое количество самостоятельных игроков. Цифровые платформы и приложения к ним сейчас 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[10] – 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.

Сказанное означает, что **цифровая среда постоянно создаёт всё новые риски для безопасности граждан и общества просто в силу своей сложности**; **никто не может быть уверенным в своей способности контролировать эту среду или обеспечить безопасность в ней**.

[10] Утечка «Седьмой сейф» от WikiLeaks показывает, что только в одной спецслужбе США, Центральном Разведывательном Управлении, над взломом всех существующих в мире устройств и цифровых платформ работают многие тысячи специалистов: https://ru.wikipedia.org/wiki/Vault_7

При этом у «официальных операторов» этой среды (органов публичной власти) есть **иллюзия контроля**. В результате и граждане, и 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 последние 10–12 лет 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 искусственного интеллекта (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 цифровых 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 (образцы голоса, внешности, походки, отпечатков пальцев, радужной оболочки глаза и т. п.), личные особенности, взгляды и привычки граждан. На этой основе формируется так называемый «цифровой след» каждого гражданина – **в бесконтактном и безакцептном режиме**, на базе анализа данных с камер, смартфонов, автомобилей, аккаунтов в социальных сетях, счетов в банках и т. п.

Различные экономические и криминальные агенты получили технологическую возможность использовать эти беспрецедентные по объёму и глубине данные о гражданах для рекламы, манипуляции и цифровой

дискриминации. И эта возможность активно реализуется практически всеми игроками цифрового мира – с полным пренебрежением к интересам и правам «исследуемого» индивидуума, который воспринимается ими как «цифровой конструкт», «вектор коэффициентов» вместо личности.

Отметим: это **совершенно новый набор очень серьёзных рисков** для личных и общественных прав и свобод, не встречавшийся ранее в истории. Государство и общество должны осознать эти риски, а также создать средства для их купирования.

1.2.3. «Серая зона» оборота данных

В настоящее время в цифровом пространстве во всём мире и в России происходит массовый, тотальный сбор персональных данных граждан, в том числе биометрических. Сбор персональных данных осуществляют как частные цифровые платформы (социальные сети, поисковики, рекламные системы, мобильные операторы, провайдеры доступа в Интернет, интернет-СМИ, мессенджеры), так и государственные структуры.

Часто сбор данных делается **в бесконтактном режиме**, незаметно, без согласия и даже без ведома человека (особенно это касается городского видеонаблюдения, съёма данных с устройств мобильной связи, журналов доступа в Интернет, посещения сайтов и поисковиков).

Можно сказать, что данные собирают все, кто может до них дотянуться, несмотря на требования Федерального закона № 152-ФЗ «О персональных данных»:

- данные собираются цифровыми платформами и государственными структурами не под решение 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 так называемого «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 искусственного интеллекта основана на выделении групп людей с общими характеристиками. Эти характеристики предоставляют цифровым сервисам сами граждане, а также они могут быть собраны и вычислены посредством бесконтактного или даже скрытого наблюдения за гражданами[11]. Решения, основанные на данных, могут касаться целых групп лиц, но могут влиять и на отдельных индивидуумов в этих группах. Одним из примеров этого является ценовая дискриминация отдельных пользователей, основанная на возрасте, привычках или уровне достатка.

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[12].

В настоящее время основной объем оборота цифровых пользовательских данных и других больших данных (биометрия, геоданные, данные о

[11] Mantelero A. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection //Computer Law & Security Review. Vol. 32. Iss. 2. P. 238-255

[12] См.: Dixon P., Gellman R., ‘The Scoring of America: How Secret Consumer Scores Threat Your Privacy and Your Future’ (2014), 21, 44.

транспорте, производстве, движении отдельных граждан и масс людей, финансовых транзакциях граждан и юридических лиц, частных покупках, коммуникациях), собираемых как частными, так и государственными цифровыми игроками, происходит по существу **в серой правовой зоне**.

Гигантские массивы данных о гражданах (в том числе персональных и часто совершенно интимных) собираются и вычисляются цифровыми платформами, провайдерами интернет-доступа и интернет-сервисами без согласия (и даже осведомлённости о факте сбора) и затем многократно копируются, передаются, перепродаются из рук в руки, используются для рекламы, слежки, манипуляции, «скоринга», в основном в скрытом режиме, но часто и совершенно открыто.

- Данными своих клиентов сейчас практически открыто торгуют все мобильные операторы России, продавая и передавая данные о местоположении, покупках, коротких сообщениях своих абонентов широкому кругу корпоративных клиентов (рекламным сетям, маркетинговым агентствам, региональным администрациям). Между тем, абоненты сотового оператора платят ему за связь, но не делегировали ему право дополнительно зарабатывать на своих персональных данных и вмешиваться в личную жизнь.
- В 2020-2021 годах самый популярный телеграм-бот «по пробиву» персональных данных «Глаз Бога»[13] (всего за год существования – 800 000 подписчиков) зарабатывал десятки миллионов рублей в месяц, причём без каких-то проблем с правоохранительными органами, не считая блокировок Роскомнадзора (возможно, это объясняется тем, что рядовые и средние сотрудники МВД и ФСБ являются одними из самых активных пользователей этого сервиса, который удобен

[13] Статья в Википедии про сервис «Глаз Бога»: https://ru.wikipedia.org/wiki/Глаз_Бога

правоохранителям тем, что не требует длительных бюрократических ведомственных согласований для получения данных по фигурантам расследований).

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

Существующие законы и правила (в первую очередь Конституция и 152-ФЗ) касаются в основном ограничений на сбор и получение персональных данных о гражданах. Однако параллельно незаконному и неурегулированному законом сбору данных о гражданах сейчас возникает и быстро распространяется новый способ получения персональных данных – **вычисление** и вычленение по косвенным признакам в больших данных с последующим их сведением в «профиль пользователя» или «цифровой профиль гражданина».

Например, по поисковым запросам, данным о покупках, общению в социальных сетях, коротким сообщениям СМС крупные цифровые платформы, мобильные операторы и другие игроки цифровой сферы уже сейчас могут достаточно уверенно скомпоновать о пользователе/пользовательнице личный профиль, включающий возраст, пол, наличие беременности, различных физиологических и психических заболеваний, сексуальные, религиозные и политические предпочтения, семейные обстоятельства, связи интимного рода, 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, к месту работы и т. п., что даёт широчайшие возможности для цифровой слежки с заделом на дискриминацию, шантаж и манипуляции.

При этом законы о сборе данных не будут нарушены или будут нарушены весьма косвенным, неявным образом, так как данные о гражданине

«вычислены» оператором самостоятельно, без непосредственного сбора или получения от другой стороны[14].

Это означает, что регулирование только **сбора** данных не сможет остановить получение и применение персональных данных для манипуляции и цифровой дискриминации. Необходимо регулирование способов использования «чувствительных» типов персональных данных, например, запрет на использование любых данных о болезнях, психических отклонениях, беременности, личных семейных и родственных обстоятельствах, запрет на любой анализ поведения и использование личных данных несовершеннолетних и т. д.[15]

1.2.5. Новые формы глобальной преступности: цифровое мошенничество, криминал

Цифровая среда значительно расширяет возможности криминала: вместо того, чтобы искать индивидуальные, «физические» подходы к гражданам в реальной жизни (на улицах, в транспорте и в организациях), что довольно сильно ограничено во времени и пространстве, злоумышленник получает в цифровой среде широкий и постоянный доступ к потенциальным жертвам в масштабе всей страны (или, точнее, в масштабе всех социальных сетей, мессенджеров и смартфонов и всех собираемых персональных данных на территории страны – что почти то же самое).

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

[15] Обработка особых категорий персональных данных регулируется статьёй 10 152-ФЗ (без упоминания уязвимых категорий граждан), однако там неявно подразумеваются данные, полученные в результате сбора тем или иным способом. При этом установлено требование немедленного удаления и прекращения обработки при устранении причины такой обработки – что, очевидно, в принципе не выполняется сейчас в описанном случае никаким оператором данных.

Государство пока не успевает защитить граждан от этого вала цифрового криминала – ни в области правового регулирования, ни в области правоприменения.

> Мы можем это видеть непосредственно на примере «цунами» мошеннических звонков в 2018–2021 годах, когда практически каждому владельцу телефона в России неоднократно позвонили мошенники в попытке узнать данные банковского счёта и украсть деньги. 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.), совершены буквально миллиарды мошеннических звонков, украдены десятки миллиардов рублей частных вкладчиков банков. При этом государство не только не защитило граждан от этой цифровой «Фукусимы», но и постфактум не нашло виновных в продаже и утечках миллионов персональных записей граждан.

Цифровая среда не снижает, а **повышает** риски возникновения преступлений и коррупции по следующим причинам:

– лёгкость совершения преступлений. Для кражи данных, «пробива», шантажа, «разводки» часто достаточно нескольких кликов мышкой. Кроме того, не требуется и высокой квалификации – достаточно владения смартфоном на уровне пользователя и наличия доступа к данным, например, предусмотренного служебными обязанностями в частной цифровой платформе или органах публичной власти;

– лёгкость сокрытия следов преступлений. Цифровые правонарушения – невидимы, у большинства населения и даже у правоохранителей нет квалификации для обнаружения признаков и следов правонарушения. Более того, для мошенника/инсайдера с достаточным уровнем прав доступа к цифровым системам достаточно легко после совершения кражи данных уничтожить следы доступа к данным – ведь это просто текстовые файлы журналов работы серверов и приложений;

– отсутствие общественного осуждения и моральных запретов. Сейчас практически нет поступков, которые можно совершить в цифровом

пространстве (оперируя данными пользователей, манипулируя сознанием, размещая рекламу, вбрасывая фейки, устраивая травлю), которые категорически осуждались бы обществом, законом и профессиональными кругами (за исключением, пожалуй, педофилии и детской порнографии), вызывали бы эффекты «потери лица/репутации», «вон из профессии», «надо звонить в полицию» и им подобные. Более того, моральные барьеры в цифровом пространстве не воздвигаются с его развитием, а продолжают стремительно демонтироваться. К этому добавляется ощущение «несерьёзности» происходящего у большинства деятелей цифровой среды, оправдания в духе «а что такого», «все так делают». Становится «можно всё». В частности, потому, что нет наказаний и ответственности, нет работающего механизма по выявлению правонарушений и наказанию виновных;

– **отсутствие ответственности.** В современной России практически неизвестны случаи наказаний за организацию утечки и продажу данных. Кибермошенник и коррумпированный инсайдер сейчас фактически уверены в своей безнаказанности. По крайней мере, в публичном поле практически нет примеров наказания телефонных мошенников и системных администраторов, продающих базы данных мошенникам. «Цифровой клерк» рискует в крайнем случае увольнением – после того, как он заработает сотни своих окладов при торговле данными с криминалом[16];

– **сбор, хранение и использование персональных данных в серой правовой зоне и ненадлежащими операторами приводит к тому, что эти данные стали товаром.** Уже сейчас в России можно купить все данные на нужного гражданина за несколько тысяч рублей. Для этого существует множество сервисов «пробива».

[16] На криминальных форумах «теневого Интернета» (Даркнета) сейчас постоянно размещаются заказы на поиски инсайдеров в банках, примерно такого содержания: нужны все записи клиентов такого-то банка в Ростове, у которых на счету не менее 200 тыс. руб. И продавцы этих данных быстро находятся.

Более того, специально проводимые эксперименты показывают, что за несколько часов можно найти теневого поставщика и купить не очень дорого набор фото и видео о своей поездке в другой город – полученный с камер системы «Безопасный город» – и посмотреть на себя в аэропорту и на улицах посещённого города. Система «коврового» видеонаблюдения за всеми гражданами, созданная якобы для безопасности – уже «дырявая, как решето», потому что дыры в цифровых системах создают не закладки и «трояны», а человеческий фактор и коррупционная ёмкость таких сервисов.

Пример. Мы уже писали выше, что нашу страну захлестнула волна мошеннических звонков от «контакт-центров» организованной преступности (часто прямо из тюрем или исправительных колоний ФСИН, а также с территории Украины), которые под видом «службы безопасности Сбербанка» и других банков, от «следователей» и т.п., вымогают деньги у доверчивых граждан, в первую очередь самых незащищённых категорий: пожилых, несовершеннолетних, бедных, одиноких, малообразованных.

Например, в одной из новейших «схем» заёмщику банка, просрочившему обслуживание кредита, может позвонить «следователь прокуратуры» и, угрожая «уголовным делом», будет настаивать на погашении части кредита переводом на «левый» счёт, «чтобы не возбуждать дело».

Все страты общества: граждане, чиновники и бизнес, – выражают горячее негодование. МВД, ФСИН, банки, Правительство обещают принять меры против преступников. Но по какой-то причине никто не задаётся вопросом: откуда у мошенников в такой массе данные граждан (ФИО, телефонные номера, сведения о кредитной ситуации и т.п.)? Совершенно очевидно, что это – результат именно **цифровой коррупции**: данные продаются преступникам сотрудниками мобильных операторов и банков.

Судя по тому, что до сих пор, при массовом вале случаев телефонного мошенничества, в открытых источниках практически нет сведений о судебных делах против цифровых коррупционеров, торгующих данными, этот вид преступлений сейчас никто не расследует или не доводит до стадии обвинения. Продавцы персональных данных из частных и государственных «контор» чувствуют свою безнаказанность.

1.2.6. Проблема «невидимок» в ИИ

Системы искусственного интеллекта, массово и систематически внедряемые в государственное управление, управление городской средой, транспорт и т.п., в подавляющем большинстве представляют собой так называемый «чёрный ящик», в котором невозможно увидеть причины принятия решений и провести надёжный аудит алгоритма.

Обнаружить наличие «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 алгоритмах и правилах.

Это позволяет разработчику или поставщику при поставке предобученной системы закладывать в неё так называемых «невидимок» – объекты, которые не распознаются системой и обходят её правила[17].

Например, уже сейчас поставщики систем распознавания лица для домовых (подъездных) камер предлагают по знакомству (и вероятно, также за деньги) сделать жильца «невидимым» для системы распознавания мэрии. То же самое уже происходит с системами распознавания лиц для городских камер в метро и на улицах[18].

Есть также криминальная услуга по превращению номера автомобиля в «невидимку» для дорожных камер ГИБДД, в результате чего на этот номер не приходят штрафы за нарушение ПДД. Заметим, что услуга есть – а о случаях пресечения такой деятельности и наказания виновных – ничего не слышно.

---

[17] 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.

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

При этом культура заказа, проверки на безопасность, регламентной передачи заказчику всей инфраструктуры, архитектуры и алгоритмов нейронной сети и самой системы искусственного интеллекта – сейчас в России не развита, как и процедуры внешнего аудита систем искусственного интеллекта.

Легко представить себе опасность внедрения подобных «невидимок» в системы распознавания, используемые при проходе на режимные объекты, поиске преступников и т. п.

Это приводит нас к очевидному выводу о **повышенной коррупционной ёмкости цифровой среды**.

1.2.7. Коррупционная ёмкость цифровой среды

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

а) **позволяет эффективно скрывать следы коррупционной активности** (стирать журналы доступа и тому подобное), а расчёты за коррупционные услуги также в большинстве случаев производятся анонимно и часто кросс-гранично (например, в биткоинах или других анонимных платёжных системах);

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

в) **снимает ответственность.** Внедрение систем ИИ, которые в формате «чёрного ящика» якобы беспристрастно «решают» судьбу людей, зачастую в

очень важных ситуациях – кредит, конкурс, олимпиада, приём на работу – также позволяет коррупционеру (цифровому клерку, разработчику, системному администратору) иметь совершенно неуязвимое прикрытие для продажи услуг «подкрутки» любых цифровых оценок и рейтингов. Ведь это «ИИ решил»!

Уже сейчас имеет место абсолютизация любых решений, принятых ИИ, и невозможность их пересмотра. Если давно существующая в обществе юридическая система имеет встроенные механизмы оспаривания решений/оценок и их пересмотра (апелляций, кассаций и т. п.), вплоть до международного уровня, то «решение ИИ» сейчас – это финальная точка в любом арбитраже.

По сути, ИИ сейчас может использоваться и уже используется для **легитимизации любых произвольных решений**, в том числе незаконных или дискриминирующих граждан.

Можно предположить, что с углублением цифровизации, с введением разнообразных частичных или полных социальных рейтингов, кредитных рейтингов, образовательных рейтингов, «траекторий учащегося» и т. п. 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, бизнеса, общества и государства (Госуслуги, ЗАГСы, земельный кадастр, образование, медицина, налоговые отношения, малый и средний бизнес и т. п.) о**ригиналом 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 порядки выше, чем у бумажных документов, что позволяет их легко копировать при краже, а также делает целевой аудиторией мошенников не одну организацию или один подъезд, 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 вашего банка».

Это уже реализующиеся, актуальные угрозы. Уже сейчас в публичное поле поступают сообщения о массовых мошенничествах с собственностью (например, недвижимостью) при помощи подделки цифровых кадастров и реестров (с помощью коррумпированных ИТ-специалистов). Скрыть врачебную ошибку сейчас также гораздо проще в электронной карте – нужна просто пара кликов «мышкой» в случае возникновения претензий пациента или его родственников (что может сделать не сам врач, а его соучастник-сисадмин).

Кража идентичности также стала не сложнее, а проще с повсеместным внедрением «цифры».

Этот риск усугубляется малой осведомлённостью об информационных технологиях и низким уровнем «цифровых навыков» у обычных граждан, а также практическим отсутствием института аудита и независимой экспертизы информационных систем и технологий, 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 данных и носителей данных. Мы по-прежнему способны читать тексты и изображения, имеющие давность в тысячи лет (на бумаге, керамике, камне, металле, пергаменте, дереве, даже на бересте),

но уже практически неспособны прочесть цифровые данные конца 1980-х и начала 1990-х годов. Это объясняется следующими обстоятельствами:

а) цифровые форматы живут не более 15–20 лет. Сейчас в большинстве организаций (или на дому) практически невозможно прочесть когда-то сохранённые данные с семидюймовой дискеты (конец 1980-х), с пятидюймовой дискеты (начало 1990-х), с дискет 3,5 дюйма (середина 1990-х и начало 2000-х); более того, уже довольно затруднительно найти устройство для чтения когда-то популярных дисков CD или DVD (конец 1990-х – начало 2000-х). Форматы цифровых кассет для видео и аудио из начала 2000-х годов – также устарели, такие кассеты практически не на чём просмотреть. Популярный в 1990-х-2010-х годах формат представления графики и звука Flash уже фактически «умер», многие сделанные на Flash проекты и контент «умерли» вместе с форматом. Та же проблема наблюдается и с картриджами игр для устаревших игровых приставок.

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 30 лет сделала практически «нечитаемыми» огромные массивы старых документов, программ и изображений. Практически нигде не хранятся старые версии персональных компьютеров с устаревшими версиями MS DOS, Windows 3.1, Windows XP на тот невероятный случай, когда появится необходимость прочесть «документ из 90-х». Та же проблема наблюдается и с языками программирования, на которых создаются ИТ-системы: старые ИТ-системы через 20–25 лет становится станет невозможно поддерживать и развивать. Итак, средний срок жизни каждого цифрового формата хранения и обработки данных, после истечения которого им практически невозможно массово пользоваться, в реальности не превышает 15–20 лет. Можно предположить, что в

ближайшие десятилетия этот процесс устаревания форматов, программ и оборудования продолжится и даже ускорится.

в) срок жизни физических носителей также укладывается в указанные 15–20 лет. Большинство носителей данных, наподобие магнитных жёстких дисков, CD-дисков, магнитных лент остаются работоспособными не долее 15–20 лет, а зачастую выходят из строя (осыпаются, размагничиваются, теряют данные) гораздо раньше из-за воздействия внешней среды (ультрафиолетового излучения, влажности, магнитных полей, перепадов температур, ударов и падений).

г) уязвимость ИТ-инфраструктуры. Опыт хранения критически важных данных в базах данных, в Интернете, в «облаках» в последние 30 лет – показывает, что сбои баз данных, банкротства компаний, закрытие проектов (показательный пример – уничтожение миллионов сайтов при закрытии «народного» сервиса хостинга сайтов Geocities[19]), пожары в дата-центрах, также 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 (массовых беспорядков, пожара, катастроф, войны, бомбёжек, ядерного удара) в первую очередь исчезнут не бумажные документы, а именно электронные данные – причём мгновенно.

Даже простое отключение электричества по той или иной причине на большой территории на сколько-нибудь серьёзный срок (от нескольких дней) сделает невозможным использование данных и документов в электронной форме на этой территории. Бумажные же документы будут по-прежнему доступны и функциональны.

[19] Сервис был запущен в 1994 году, в 2009 году купившая его компания Yahoo закрыла сервис и удалила все сайты пользователей. Ссылка: https://ru.wikipedia.org/wiki/GeoCities

Все это означает, что при переходе на электронное хранение всех важных документов и материалов как основной метод 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 обычной нехватки ресурсов (рабочих рук, времени и денег) далеко не всё будет переноситься в новые форматы, часть данных будет признаваться неважными и «забываться», оставляться в старом формате или просто выбрасываться.

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, как мы отметили выше, 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 государственным и частным организациям **сохранять во всех случаях «гибридный» электронно-бумажный документооборот, особенно в части содержащих персональные данные документов граждан, признавая бумажную, «твёрдую» копию оригиналом документа.**

1.3. Социально-политические угрозы, связанные с форсированной цифровизацией

1.3.1. Принудительное вовлечение граждан в цифровую среду

В публичном пространстве, в выступлениях высоких чиновников, а также в стратегиях по развитию цифровой экономики и искусственного интеллекта невозможно найти хоть сколько-нибудь убедительных объяснений того, зачем нужна такая сверхбыстрая и тотальная цифровизация всех сфер частной, общественной и государственной жизни.

Обычно аргументы «евангелистов» цифровизации и их экспертов, создающих программы и стратегии цифровизации, 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!»[20].

Заметим, что **ни в каких основных документах стратегического планирования Российской Федерации нет такого национального приоритета как «удобство».**

Ещё один аргумент, которым цифровизаторы государственного управления и городской среды 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, своеобразная ложная дилемма, не имеющая прямого отношения к настоящей безопасности, что мы покажем ниже.

[20] Мы могли бы привести длинный список цитат из высказываний конкретных государственных чиновников и руководителей госкорпораций за 2019–2021 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.

К сожалению, большое количество программ и стратегий цифровизации и внедрения искусственного интеллекта (включая ГОСТы и другие отраслевые стандарты, принимаемые в последнее время) в нашей стране являются просто 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 госуслуг, образования, медицины. **При этом игнорируется право граждан на сохранение традиционных способов взаимодействия с государством, а также медицинские, экономические и технологические ограничения** (возможность доступа в сеть 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.

Из новостей (апрель 2021 года):

«Первые две поликлиники Москвы полностью перешли на электронные медкарты: пилотный проект стартовал в двух детских поликлиниках столицы. Власти уже оцифровали более 1 млн детских медкарт и к осени планируют расширять практику полного перехода на электронные медкарты и на другие детские поликлиники».

Из этой новости[21] о миллионе оцифрованных карт на самом деле следует, что оцифровали не карты в двух поликлиниках, а практически все карты детей в Москве. Никакого согласия родителей на перевод данных их детей в электронную форму, очевидно, никто не спрашивал.

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 и медицины и т. п.[22], необходимость освоения цифровых технологий коммуникации (что может быть трудно и нежелательно для пожилых людей, а также 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

[21] https://www.rbc.ru/technology_and_media/29/04/2021/6089a3d89a79470a83e54e24

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

«шеринговой экономикой»[23], 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, самокатов, аренды квартир, интернет-агрегаторы товаров, образовательных услуг, новостей и т. п.

Данная модель опасна для прав граждан 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, всё время ужесточая условия работы, повышая комиссию и требования к условиям труда, платформа-посредник не отвечает за них, как за работников, не имеет ответственности по Трудовому Кодексу Российской Федерации, то есть не оплачивает им отпуска и больничные листы, не имеет обязательств по декретным отпускам и иным выплатам[24].

Пользующийся платформой работник формально – является самостоятельным агентом (например, самозанятый или индивидуальный предприниматель). При этом в реальности он, фактически, наёмный работник, получающий относительно невысокую зарплату, не имея никакой социальной защищённости, предусмотренной Трудовым Кодексом, так как формально у

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

[24] 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).

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 очень быстро, значит, с точки зрения цифровизаторов это – безусловно полезная для общества бизнес-модель, не требующая особого регулирования.

Между тем, в этой модели создаётся довольно серьёзная **социальная угроза** трудовым правам граждан и стабильности общества (напомним, что, например, таксистами в агрегаторах такси в России работают миллионы людей, для которых это стало профессией, но они не являются наёмными работниками и не защищены Трудовым Кодексом).

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 рынков даёт огромные прибыли инфопосредникам.

Такие же попытки «уберизации», замены учителей на информационных посредников и «уберизованных» репетиторов делаются в отношении сферы образования.

Лексика цифровизаторов довольно 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 создаёт, производит социальную напряжённость. Под наше общество закладывается «социальная бомба» в виде поражённых в правах миллионов граждан, управляемых программными средствами искусственного интеллекта и дискриминируемых всемогущими информационными посредниками ради прибылей[25]. Эта «бомба» может сработать в недалёком будущем, если не начать как можно быстрее и решительнее регулировать и контролировать деятельность информационных посредников.

1.3.3. Цифровая дискриминация граждан на основе собираемых и вычисляемых данных

В настоящее время в общественной практике применения ИТ-систем наблюдается «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

[25] 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.

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.

Например, таким образом 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 давала в поисковые машины запросы о товарах для беременных. Эти данные были собраны системой обработки больших данных использованного поисковика, ее профиль в поисковике получил соответствующую пометку (категорию). Далее к профилю получили доступ бизнес-партнёры поисковика– в том числе онлайновые кадровые агентства. У них, в свою очередь, есть тысячи корпоративных клиентов – кадровых отделов компаний, госорганов и других организаций. Кадровик одного из клиентов, изучая резюме девушки, которая сейчас ищет работу, увидел пометку, что она, возможно, беременна, и просто закрыл её страничку и перешёл к резюме других соискателей.

Нужно отметить, что в этот момент вся цепочка передачи данных – поисковик, кадровый сервис, кадровик компании – фактически совершила по отношению к девушке уголовное преступление по ст. 145 УК РФ (отказ в трудоустройстве по основанию беременности). При этом, очевидно, что никто из ИТ-деятелей в цепочке не только не считает себя ни в чём невиноватым, но даже и не понимает, что именно было ими совершено. «*А что тут такого? – просто обработка данных и профилирование пользователей*».

Таким образом, все операторы и пользователи цифровых данных в этой цепочке помогли совершить уголовное преступление против своего лояльного, честного пользователя, доверяющего им. Однако в итоге – никто не виноват, поскольку «все так делают». Заметим, что даже если упомянутые акторы - поисковик, кадровый сервис и сотрудник кадрового отдела компании-нанимателя - будут отрицать, что описанная выше предполагаемая обработка и передача данных о пользователе происходит в реальности, основная проблема описанного условного примера состоит в том, что сейчас у общества и даже у государственных регуляторов **нет никакого способа узнать, так ли это на самом деле.**

У нас сейчас нет ни процедуры, ни институтов независимой инструментальной экспертизы потоков персональных данных и защиты прав их носителей.

Другой яркий пример - ценовая дискриминация. Известно, что сидящие рядом пассажиры самолёта иногда могут заплатить за идентичные посадочные места цены, отличающиеся в несколько раз. Цена билета переменная и зависит от множества факторов: сезона, срока выкупа билета, наличия мест, «налёта миль» и т. п.

Однако в эпоху интернет-торговли билетами цена также может зависеть от цифрового профиля клиента, и прежде всего от оценки платёжеспособности системой бронирования: богатым (с точки зрения системы профилирования) клиентам выставляют более высокие цены.

Тот же принцип ценовой дискриминации сейчас 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), при заказе в интернет-магазинах (цена на покупку и доставку одного и того же товара может

значительно отличаться в зависимости от коммерческого профиля клиента и истории его покупок и т.п.[26]

Заметим, что, например, власти Китая уже увидели эту опасность дискриминации на основе «коммерческих» профилей и необходимость регулирования. В феврале 2021 года антимонопольный комитет Госсовета Китая опубликовал руководство, в котором указал, что использование больших данных в ценообразовании представляет собой злоупотребление доминирующим положением компании на рынке.

В Шэньчжэне в начале 2021 года разработали и 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 анализу социальных проявлений цифровизации у нашего азиатского соседа.

1.3.4. Попытки введения социальных рейтингов

Социальный рейтинг – это попытка автоматически приписать каждому гражданину число или набор чисел, вектор, социальный индикатор его «добропорядочности»: этичности, благонадёжности и законопослушности. На сегодняшний день, насколько можно судить по открытым источникам, в Китае активно применяется соцрейтинг по китайскому образцу: 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. Естественно, оценивать поведение масс граждан и назначать им баллы предполагается автоматически: с помощью

[26] См., например, публикацию «Ozon заподозрили в более высоких ценах для постоянных клиентов», ссылка: https://habr.com/ru/news/t/567602/

цифровых технологий слежки и анализа. По сути, речь идёт об автоматическом управлении массами людей.

Последние годы в российских медиа (СМИ, соцсетях, Telegram-каналах и т. п.) время от времени появляются «прощупывающие» статьи и посты 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 давно работают или вводятся в мире, в том числе в нашей стране. Это, прежде всего, кредитный рейтинг банков (на основе кредитных историй), это рейтинги пассажиров и таксистов, это попытки вводить различные рейтинги учеников и студентов – вплоть до установки камер в классах с распознаванием эмоций и оценкой трудолюбия и старательности школьника (такой эксперимент уже начинали в 2020 году в нескольких средних школах Перми без предварительного согласия родителей, с очевидным нарушением прав несовершеннолетних).

Цифровой рейтинг пользователя давно уже существует внутри массовых рекламных систем компаний Google, 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 рекламным рейтингом одни и те же товары и услуги предлагаются по ценам, иногда отличающимся в несколько раз.

Часть этих рейтингов – пока ещё частные: рейтинги покупателей, заёмщиков или рейтинги таксистов. Впрочем, негативные эффекты непрозрачности и несправедливости видны даже на таком низовом уровне.

Вместе с тем, попытки тотальной цифровизации российского образования и введения «персональных траекторий» (то есть фактически – управления

судьбой учащегося) – показывают нам уже полностью государственные инициативы по введению социальных рейтингов.

Заметим, если какая-то институция вводит параллельную систему власти и раздельного существования (цифрового апартеида) на основе цифрового рейтинга, гражданам и обществу не очень важно, частная она или государственная.

Граждане России пока не вполне осознают всех рисков подобных нововведений. Накануне проведения в Пресс-центре «РИА Новости» 15 апреля 2021 г. круглого стола под эгидой Совета о рисках и угрозах введения социальных рейтингов участники дискуссии ознакомились с апрельским отчётом ВЦИОМ об отношении граждан России к идее социального рейтинга. Общие выводы опроса были примерно такие: 55% опрошенных против идеи соцрейтинга, ещё 35% – колеблются в разной степени, однако допускают, что могут быть и положительные стороны, 10% вообще не знают, что это такое, и не имеют своего мнения.

Скорее всего, даже среди этих 55%, выступивших против социального рейтинга, многие впервые услышали о социальном рейтинге из самого опроса.

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

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

– **криминализации**, включая: коррупцию и компрометацию, когда чиновники и программисты, управляющие правилами и программами цифрового рейтингования, будут иметь высокие рейтинги, а также смогут тайно торговать рейтингами.

Ещё одним следствием введения социального рейтинга будет лишение граждан их прав не по суду, а по воле программ на базе искусственного

интеллекта, 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 и законов, 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 любой страны постиндустриальной эпохи. Это право и исключительная прерогатива государства:

- самостоятельно и независимо определять и внутренние, и геополитические национальные интересы в цифровой сфере;
- проводить самостоятельную внутреннюю и внешнюю информационную политику;
- распоряжаться собственными информационными ресурсами, формировать национальную инфраструктуру информационного пространства;

- гарантировать электронную и информационную безопасность личности, общества и государства.

В основе цифрового суверенитета лежат соответствующие регулятивные механизмы (национальные технические стандарты и уникальный правовой режим), использование защищённых от внешнего воздействия аппаратных и программных средств связи собственного производства и способов доставки/распространения информации до конечного потребителя, 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 игр и 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 (платформы, «экосистемы», ИТ-сервисы): 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 этих данных.

Государственные органы не только не успевают в том же темпе развивать свои средства сбора и анализа, но и не имеют сравнимой аудитории, так что зачастую являются **просителями и получателями этих данных от частных цифровых платформ**.

При этом, чем шире линейка цифровых сервисов у платформы – или «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 соцсетях позволяет создать максимально полный профиль пользователя и затем манипулировать его товарным спросом, медиапотреблением, картиной дня, а также кругом общения и политическими взглядами, использовать в целях пропаганды, мошенничества, шантажа и другой криминальной деятельности.

«Экосистемы» стремятся к монополизации рынка данных. Такими широкими линейками сервисов обладают или стремятся обладать всего несколько крупнейших игроков на нашем цифровом рынке: Google, Meta (Facebook), Яндекс, Mail.ru, Сбербанк, четвёрка федеральных мобильных операторов. А там, где какого-то элемента линейки сервисов и данных с него какому-то крупному игроку не хватает, он вступает в альянсы или производит поглощения.

В результате эти «экосистемы» накапливают не только огромные объёмы очень ценных данных, но и получают мощнейший экономический, идеологический и геополитический рычаг воздействия на население России и практически любой другой страны мира.

Актуальной проблемой остаётся незаконная передача американскими телекоммуникационными гигантами и интернет-компаниями (прежде всего Microsoft, Yahoo, Google, Facebook, Apple, Skype, Zoom и YouTube) правительству США персональных данных россиян. Их дата-центры (серверы хранения персональных данных пользователей) располагаются в большинстве

своём на территории США и подпадают под действие американского «антитеррористического законодательства»[27], в соответствии с которым американские компании обязаны предоставлять прямой доступ спецслужбам США к любой информации, включая доступ к аккаунтам, банковским картам, переписке, всем личным данным пользователей, что напрямую нарушает законодательства большинства стран мира, в том числе российское.

При этом американские компании в своей операционной деятельности активно применяют доктрину экстерриториального действия законодательства США: каждый пользователь вне зависимости от страны проживания/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/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, – Google, Meta (Facebook), Twitter, Instagram, TikTok – 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

[27] В частности, «Акт о свободе» от 2015 года, заменивший «Патриотический акт», принятый после теракта в США 11 сентября 2001 года и предоставляющий спецслужбам почти неограниченные права по подслушиванию и ведению электронной слежки.

Ссылка: сайт Конгресса США: https://www.congress.gov/bill/114th-congress/house-bill/2048

страны происхождения компании, а не законами тех стран, где ведется операционная деятельность. Огромные доходы и технологическая мощь позволяют им чувствовать себя уверенно даже в спорах с государственным аппаратом большинства стран мира.

По сути, это новый тип «цифровых государств» со своим особым цифровым суверенитетом, накладывающимся поверх суверенитетов традиционных государств реального мира. Это довольно тревожная тенденция, поскольку такие цифровые государства практически никак не подчиняются международному праву и не имеют, по сути, каких-либо ограничений, кроме своих внутрикорпоративных целей, задач и интересов, а также требований и правил правительства страны происхождения, то есть в подавляющем большинстве случаев - правительства США.

Некоторые национальные государства сейчас вырабатывают способы «приземления» цифровых гигантов в свои юрисдикции, в частности, такой закон о «приземлении» (то есть о создании юридических лиц в локальной юрисдикции) в 2021 году принят и в Российской Федерации[28].

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 иностранных агентов на территории третьих стран.

Существующая во многих стран практика штрафования крупнейших компаний-нарушителей (прежде всего, Google, Twitter, Meta (Facebook) за отказ удалять противоправный контент и непрозрачную внутрикорпоративную цензуру, пока показывает довольно слабую эффективность, если меры

[28] Федеральный закон от 01 июля 2021 г. № 236-ФЗ "О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации"

финансового воздействия не подкрепляется технологическими способами замедления работы платформ или их блокировкой.

1.4.3. Цифровая колонизация России

Основные риски ускоренной цифровизации цифровыми платформами и «экосистемами», описанные выше, усугубляются для нашей страны тем, что большинство этих «экосистем» – не отечественные, а зарубежные, преимущественно американские. Их повсеместное использование, в том числе представителями госсектора для рабочих нужд, создает прямую угрозу цифровой «колонизации» России в интересах США.

Американские цифровые платформы имеют сейчас в русскоязычном Интернете (Рунете) больше 50% пользовательских аккаунтов соцсетей, 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 и/или платформу – всегда остаётся её истинным владельцем, вне зависимости от того, в каком виде разработчик продаёт технологию или предоставляет для использования.

Все так называемые «информационные посредники», то есть поисковики, социальные сети, фото– и видеохостинги 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 в 2019–2020 годах в США, в том числе блокирование действующего президента и его сторонников цифровыми платформами и сервисами хостинга в январе 2020 года, наглядно продемонстрировала настоящих владельцев этого 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 этой колониальной цифровой зависимости, а к её усилению, потому что под флагом ускорения цифровой трансформации в России происходит всё большее заимствование и внедрение в госорганах, отраслях народного хозяйства и частном бизнесе **готовых западных технологий и платформ**.

В этой связи стоит отметить, что 90–95% всех «систем искусственного интеллекта», 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[29].

Следует пояснить, что вообще из себя представляет так называемое «открытое ПО», часто преподносимое как простое и удобное решение проблемы импортозамещения для России. На самом деле оно уже 15–20 лет в основном финансируется и разрабатывается не «свободным и бескорыстным

[29] Для собственных нужд эти компании между тем используют другие, более передовые и мощные, закрытые решения.

сообществом программистов», как принято считать, 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 захватывают цифровые рынки и медийные пространства суверенных стран вполне целенаправленно, при мощной поддержке своего государства, с целью усиления влияния и контроля над чужими цифровыми пространствами.

Это, безусловно – серьёзный риск для суверенитета России, поскольку все крупные американские цифровые платформы и ИТ-корпорации тесно связаны с правительством США (прямо называющим нас врагом в своих национальных стратегиях).

1.5. Отсутствие системного регулирования цифровой среды и защиты прав граждан в России

В условиях быстрого развития цифровой среды в нашей стране до сих пор отсутствует адресное законодательство (хотя уже имеется поправка в 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 граждан в новой цифровой среде.

Сегодня к наиболее острым проблемам следует отнести, в частности, отсутствие комплекса норм, обеспечивающих добровольность использования гражданами цифровых технологий при взаимодействии с государством, а также масштабный сбор персональных данных в централизованные базы данных федерального уровня.

В последние годы распространёнными становятся также факты принуждения к электронной форме государственных и муниципальных услуг, к подписанию согласия на обработку персональных данных в случаях, когда

таковое не требуется для реализации государственных или муниципальных функций.

Серьёзные возражения в обществе вызывают нормы правовых актов, связанных с безальтернативной цифровизацией в сфере государственного управления в целом и конкретных областях жизнедеятельности, в частности.

В данном разделе ниже приведён обзор деструктивных тенденций правоприменительной практики в Российской Федерации, ограничивающей информационный суверенитет человека и угрожающей неприкосновенности частной жизни.

1.5.1. Государственное управление личными данными граждан

В целях реализации программы «Цифровая экономика» предусмотрено формирование Национальной системы управления данными (далее – НСУД).

03 июня2019 г. распоряжением Правительства РФ № 1189-р утверждена Концепция создания и функционирования национальной системы управления данными и план мероприятий ("дорожная карта") по созданию национальной системы управления данными на 2019–2021 годы.

Концепция вводит понятие «государственные данные», которые составляет «информация, содержащаяся в информационных ресурсах органов и организаций государственного сектора, а также в информационных ресурсах, созданных в целях реализации полномочий органов и организаций государственного сектора».

Такой подход приведёт к оценке персональных данных граждан, внесённых в информационные системы государственных структур, 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.

Среди задач НСУД согласно Концепции:

- «…установление требований к созданию и (или) управлению **сервисами предоставления государственных данных в целях предоставления к ним доступа широкого круга потребителей на безвозмездной и на возмездной основе»**;
- «определение и реализация способов финансовой поддержки деятельности, направленной на создание и функционирование Системы, включая **коммерциализацию сервисов предоставления государственных данных**».

К принципам создания и обеспечения НСУД отнесён также следующий: «доступность работы с государственными данными **для широкого круга пользователей** за счет формирования единой "экосистемы", обеспечивающей **взаимовыгодное** сотрудничество с органами и организациями государственного сектора и **с иными заинтересованными органами и организациями**, за счет внедрения механизмов по развитию сервисов в области обработки, аналитики данных, постоянного обучения пользователей государственных данных, развития культуры хранения и использования государственных данных, а также обеспечивающей возможность участия представителей органов и организаций государственного сектора **и иных заинтересованных органов и организаций** в проверке согласованности и качества государственных данных, очистке и обогащении государственных данных, доступных посредством Системы».

Как представляется, НСУД фактически направлена на формирование «цифровых профилей» граждан, предполагает замену понятия «персональные данные» на «государственные», допускает их обработку и коммерциализацию, включая продажу доступа к данным третьим лицам, умалчивая о согласии субъектов персональных данных (что связано с лукавой квалификацией этих данных в качестве «государственных»).

Заместитель Председателя Правительства Российской Федерации Д.Н. Чернышенко на конференции ПМЭФ-2021 в начале июня 2021 года отмечал: «*Правительство РФ не намерено монополизировать доступ к информационным данным**, готово делиться ими с бизнесом**…У правительства нет никакого намерения конкурировать с бизнесом*»[30]. Как отмечалось выше, государственные данные будут включать в себя персональные данные граждан. Правительство, согласно приведённому заявлению, готово ими «делиться с бизнесом».

Как указывает судья Конституционного суда РФ, д.ю.н., профессор Н.С. Бондарь «*информация, защита которой обеспечивается в рамках конституционного права на неприкосновенность частной жизни, охватывает все персональные данные*»[31]. Реализация подхода, предлагаемого в Концепции НСУД и озвученного в планах Правительства РФ, может лишить граждан полноценного права управления своими персональными данными и создать угрозу манипулирования и иных злоупотреблений со стороны третьих лиц, включая коммерческие структуры.

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

Социальный рейтинг – это система социальной оценки отдельных граждан по различным личным параметрам, значения которых получаются с помощью инструментов массового наблюдения, использующих технологию анализа больших данных; такая система автоматических оценок предполагает наделение граждан теми или иными правами или поражение в правах в зависимости уровня в рейтинге.

---

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

[31] Бондарь Н.С. Информационно-цифровое пространство в конституционном измерении: из практики конституционного суда Российской Федерации // СПС «Консультант Плюс».

О рисках и угрозах социального рейтинга уже было сказано выше. Вместе с тем, в настоящее время нашими законодателями и органами исполнительной власти, судя по принимаемым правовым актам и высказываниям отдельных чиновников, ведётся подготовка к введению различных общеобязательных цифровых рейтингов граждан России, называемых в документах «профилями», «траекториями» и тому подобными эвфемизмами.

В России принят *"Паспорт национального проекта "Национальная программа "Цифровая экономика Российской Федерации"*[32]).

Указанная программа 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»).

Понятия «профиль гражданина» и «траектория развития» в программе «Цифровая экономика» не раскрыты. Для реализации этого был подготовлен, в частности, проект федерального закона №747513–7 «О внесении изменений в

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

отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)»[33].

Согласно положениям данного законопроекта, «цифровой профиль является совокупностью сведений о гражданах и юридических лицах, содержащихся в информационных системах государственных органов, органов местного самоуправления и организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, а также в единой системе идентификации и аутентификации».

Характерно, что **законопроект не предусматривает получение согласия граждан на заполнение цифрового профиля сведениями о гражданине**.

Против системы цифровых профилей граждан выступила в 2019 г. Федеральная служба безопасности[34]. В ФСБ России справедливо подчеркнули, что предлагаемая система «цифрового профиля гражданина» несёт в себе угрозу повышения рисков утечек информации о россиянах и не содержит никаких заявленных конкретных целей, для достижения которых нужна обработка персональных данных граждан в предлагаемом объёме.

«Траектории развития» понимаются в рассматриваемых нормативно-правовых актах 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 госорганов – или вообще их автономных ИИ-систем.

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

[34] https://gov.cnews.ru/news/top/2019-11-13_fsb_obrushilas_s_kritikoj

Среди документов, в которых также прямо сказано о формировании «цифрового профиля» и «индивидуальной траектории», следует отметить Приказ Минцифры России от 18.11.2020 г. № 600 «Об утверждении методик расчёта целевых показателей национальной цели развития РФ "Цифровая трансформация"» (далее – Приказ № 600).

Согласно нормам Приказа №600 «доля учащихся, по которым осуществляется ведение цифрового профиля на платформе ЦОС» к 2030 году должна составить 100%[35]. При этом «доля учащихся, которым предложены рекомендации по повышению качества обучения и формированию *индивидуальных траекторий с использованием данных цифрового портфолио учащегося*» должна к 2030 году составить 80%[36].

Внедрение цифровых рейтингов и траекторий развития граждан будет означать попытку активного внешнего (притом автоматического или полуавтоматического) влияния на судьбы людей, что создаёт риски злоупотреблений и поражения граждан в правах (в частности, за уклонение от следования рекомендациям «траекторий»).

Строящаяся сейчас 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

[35] 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 № 600. Далее – Приложение № 1 к Приказу № 600.

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

двойников» (профилей) людей (а именно того, «что юридически валидно представляет» субъекта)[37].

В тексте доклада отмечается: «Развитие интернета вещей, удалённой биометрической 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»**[38].

Заметим, что тут прямо говорится, что нужно автоматически управлять **добропорядочностью и избирательной функцией**!

В качестве удобства применения искусственного интеллекта в госуправлении в указанном докладе РАНХиГС отмечается возможность формирования *«социального рейтинга»*[39].

Введение социального рейтинга в любых видах ведёт к дискриминации граждан в зависимости от уровня их рейтингов. Фактически социальное рейтингование – это отказ от конституционного принципа равенства прав и обязанностей граждан (установленного ч. 2 ст. 6 и ст. 19 Конституции РФ).

Следует уточнить, что конкретное право, которого человек будет лишён в результате получения низких оценок в рейтинге, всегда будет нарушать определённую норму Конституции, например право на труд, право на образование, на отдых, на свободу передвижения, свободу слова, право частной собственности и т. д.

---

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

[38] Там же. С. 46.

[39] Там же. С. 27.

«Сжатие» прав при применении «профилей», «рейтингов» и «рекомендаций» может дойти до такой степени, что гражданин, формально будучи свободным и невиновным в каких-либо правонарушениях, будет практически приравнен в объёме прав к осуждённому лицу, причём без законного (судебного) установления вины. Иными словами, социальный рейтинг ставит под угрозу презумпцию невиновности граждан (ст. 49 Конституции РФ).

1.5.3. Переход на исключительно электронную форму общения с государством и муниципальной властью

В рамках программы «Цифровая экономика РФ» предусмотрен Федеральный проект «Цифровое государственное управление», в котором 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»[40] предусмотрен «переход на исключительно электронный формат поступающих и обрабатываемых обращений граждан».

Исходя из приведённых норм, предполагается полный отказ от традиционной формы взаимодействия государства с гражданами. И, похоже, этот план уже реализуется. В частности, принят *Федеральный закон РФ от 30.12.2020 г. № 509-ФЗ «О внесении изменений в отдельные законодательные акты РФ»* (далее – ФЗ № 509), который кардинальным образом меняет ключевые нормы Федерального закона РФ от 27.07.2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (далее – ФЗ № 210).

[40] Одобрен Правительством РФ 23.09.2020, протокол № 36, раздел VII.

Ранее п. 6 ст. 4 ФЗ № 210 предусматривал следующий принцип предоставления государственных и муниципальных 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 ФЗ № 210 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**».

П. 2 ч. 1 статьи 6 ФЗ № 210-ФЗ гласил, что органы, предоставляющие госуслуги, обязаны обеспечивать возможность получения заявителем государственных и муниципальных услуг «в электронной форме, если это не запрещено законом, **а также в иных формах, предусмотренных законодательством РФ, по выбору заявителя**».

Теперь же ФЗ № 509 дополняет указанные нормы оговоркой – «за исключением случая, если на основании федерального закона предоставление государственной или муниципальной услуги осуществляется **исключительно в электронной форме»**. Таким образом, если ранее по ФЗ № 210 действовало общее правило о возможности использования любой формы государственных и муниципальных услуг **по усмотрению гражданина**, и государство было обязано удовлетворить этот выбор, то после поправок, внесённых ФЗ № 509, государство может ввести запрет на традиционное «офлайновое» взаимодействие с чиновниками по любым государственным и муниципальным услугам.

Кроме того, ФЗ № 509 допускает прекращение личного приёма граждан в органах, предоставляющих госуслуги, в случае передачи соответствующих функций МФЦ (ч. 1.8 ст. 7 ФЗ № 210). При этом следует учесть, что **МФЦ не является государственным органом**!

Подчеркнём: такое регулирование прямо противоречит ст. 33 Конституции РФ, согласно которой «граждане РФ имеют право обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления».

«Обращение гражданина» – это «направленные в государственный орган, орган местного самоуправления или должностному лицу в письменной форме или в форме электронного документа предложение, заявление или жалоба, а также устное обращение гражданина в государственный орган, орган местного самоуправления» (п. 1 ст. 4 Федерального закона РФ от 02.05.2006 г. ФЗ-59 «О порядке рассмотрения обращений граждан РФ»).

Что касается личного обращения, упомянутого в ст. 33 Конституции РФ, то речь идёт о: **«фактическом личном предъявлении гражданином должностному лицу органа власти своего обращения. Здесь возможны два варианта: личное устное озвучивание обращения должностному лицу или подача письменного экземпляра обращения»**[41].

1.5.4. Принудительное вовлечение граждан в ЕСИА

Предоставление государственных и муниципальных услуг в электронной форме по ФЗ-509 осуществляется в отношении заявителей, прошедших процедуру регистрации в Единой системе идентификации и аутентификации (далее - ЕСИА), поэтому получение госуслуг в ближайшем будущем будет **безальтернативно** требовать регистрации в ЕСИА по любым услугам, переведённым в исключительно электронный вид.

Следует отметить, что Верховный Суд Российской Федерации уже рассматривал дело об оспаривании Постановления Правительства РФ от 28 ноября 2011 г. № 977 “О федеральной государственной информационной системе «ЕСИА в инфраструктуре, обеспечивающей информационно-

[41] Савоськин А.В. Размышления о проблемах реализации конституционного права граждан обращаться лично // Конституционное и муниципальное право. 2018. N 10. С. 33 – 37.

технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»”).

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 требований, но здесь 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**.

Не нарушает Постановление ВС РФ право заявителей идентифицировать себя в любых отношениях по фамилии, имени, отчеству, дате, месту рождения и месту жительства, отношению к гражданству, а не по идентификационному номеру, поскольку граждане вправе обратиться за получением государственных и муниципальных услуг не только в электронной форме, но и в иных формах, предусмотренных законодательством РФ, по их выбору, а органы, предоставляющие государственные услуги, обязаны обеспечить такую возможность (п. 3 ст. 5, п. 2 ч. 1 ст. 6 ФЗ от 27 июля 2010 г. № 210-ФЗ)»[42]

Указанное решение было оставлено в силе Апелляционной коллегией Верховного Суда Российской Федерации, которая отметила, что лица, не желающие получать госуслуги «в электронном виде, вправе получать их в иных формах, предусмотренных законодательством РФ **(в том числе посредством**

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

личного обращения в орган, предоставляющий услугу, с предоставлением документов на бумажном носителе)[43].

С поправками, предусмотренными ФЗ № 509, 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.

Итак, вышеприведённые планы и нормы ФЗ № 509:

- нарушают ст. 33 Конституции РФ, согласно которой «граждане РФ имеют право обращаться **лично, а также направлять индивидуальные и коллективные обращения** в государственные органы и органы местного самоуправления»;
- противоречат Стратегии развития информационного общества в РФ на 2017–2030 годы, утверждённой Указом Президента РФ от 9 мая 2017 г. № 203, которой предусмотрено «развитие технологий электронного взаимодействия граждан, организаций, госорганов, органов местного самоуправления **наряду с сохранением возможности взаимодействия граждан с указанными организациями и органами без применения информационных технологий**»[44];
- нарушают ч. 1 ст. 23 Конституции РФ, согласно которой «каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну» и ст. 24 Конституции РФ, согласно которой «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются».

[43] Определение Верховного Суда РФ от 20 сентября 2012 г. № АПЛ12-503.

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

1.5.5. Переход на «цифровые оригиналы»

С 1 января 2022 г. вступает в силу новая редакция ч. 2 ст. 7.4 ФЗ № 210, 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, все результаты взаимодействия гражданина и государства будут оформляться 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.

1.5.6. Отслеживание событий частной жизни граждан Госуслугами

Согласно п. 1 ч. 1 ст. 7.3. ФЗ № 210 «при наступлении событий, являющихся основанием» для предоставления государственных и муниципальных услуг, орган, предоставляющий государственную услугу или муниципальную услугу (далее – госуслуги), 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, очевидно, предполагает отслеживание событий частной жизни граждан без их согласия, поскольку иным образом принципиально невозможно проводить «мероприятия» по **подготовке** предоставления госуслуг при «наступлении тех или иных событий» в жизни гражданина.

1.5.7. Переход на исключительно электронную форму учёта сведений о трудовой деятельности

Согласно программе «Цифровая экономика РФ» (п. 1.16 федерального проекта «Нормативное регулирование цифровой среды») принят федеральный закон, предусматривающий учёт данных о трудовой деятельности работников в электронном виде. Причём, согласно Федеральному закону 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» (ч. 8 ст. 2) «формирование сведений о трудовой деятельности лиц, **впервые поступающих на работу** после 31 декабря 2020 года, осуществляется в соответствии со статьей 66.1 Трудового кодекса Российской Федерации, а **трудовые книжки на указанных лиц не оформляются**».

Таким образом, для работников, впервые приступающих к работе в 2021 году, в принципе не предусмотрено альтернативы электронному формату учёта сведений о трудовой деятельности (в виде трудовой книжки в бумажной версии).

1.5.8. Цифровизация здравоохранения

В России создаётся Единая государственная информационная система в сфере здравоохранения (далее - ЕГИСЗ). Статья 91.1 Федерального закона РФ от 21 ноября 2011 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (далее – ФЗ № 323), которая регулирует создание данной системы, введена в действие с 1 января 2018 года.

ЕГИСЗ включает несколько регистров, среди которых «федеральная интегрированная электронная медицинская карта» – а именно, подсистема, нацеленная на сбор данных о здоровье граждан[45].

[45] 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».

Согласно ст. 94 ФЗ № 323 «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), принятый в соответствии с законодательством Российской Федерации об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования; 11) номер полиса 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».

Постановление Правительства РФ от 05 мая 2018 г. № 555 «О единой государственной информационной системе в сфере здравоохранения» предусматривает, что внесение данных в Федеральную интегрированную электронную 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»[46].

Указанные данные вносятся в ЕГИСЗ с учётом требований, предусмотренных Приказом 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». Между тем, вне зависимости от способов защиты данных, факт возможности доступа к ним (для оказания медпомощи) 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 нацбезопасности.

Заметим, что в данном Положении пока ещё упоминается **необходимость добровольного согласия** гражданина на передачу данных.

> «Представление в единую систему сведений, содержащих информацию, относящуюся прямо или косвенно к определённому или определяемому физическому лицу, осуществляется с согласия такого лица и с учетом требований законодательства Российской Федерации в области персональных данных» (п. 44 Положения о единой государственной информационной системе в сфере здравоохранения).

Между тем, Приказ Минцифры № 600 предусматривает наличие **у 100% граждан** к 2030 г. **сформированных интегрированных электронных медицинских карт**, доступных на платформе Единого портала госуслуг (п. 3.2. Приложения № 1 к Приказу). Таким образом, Приказом № 600 планируется сплошной сбор данных в электронные медицинские карты и **игнорируется**

[46] Там же.

добровольность для граждан решения вопроса о внесении персональных данных в электронную медкарту.

Кроме того, практика регионов уже сейчас показывает, что чиновники дают указания о формировании электронных медкарт без учёта мнения граждан[47].

1.5.9. Цифровизация образования

В настоящее время в нашей стране разворачивается коренная реформа образовательной сферы, направленная на её цифровизацию. Среди проблем, с которыми сталкиваются граждане в образовательной сфере в связи с цифровизацией, следует отметить:

- **«добровольно-принудительный» сбор данных** об участниках образовательных отношений, включая сбор биометрических персональных данных в образовательных учреждениях;
- **принуждение к подписанию согласий** на обработку персональных данных, к получению государственных (муниципальных) услуг в электронной форме (включая подачу заявлений о зачислении в образовательные организации);
- **принуждение к электронному обучению**, включая регистрацию на цифровых образовательных платформах, внедрение цифровых сертификатов на дополнительное образование и сбор персональных

[47] «Во всех детских поликлиниках города будут внедрены электронные медкарты. Об этом заявил губернатор Александр Беглов… «В этом году мы переведём детей на систему электронных медицинских карт, а потом начнём работать со взрослыми поликлиниками», - сказал глава города. По его словам, электронная медицинская карта будет включать информацию обо всех посещениях врача вне зависимости от того, какие медицинские учреждения оказывают услуги – частные, государственные и даже приём врача в школе. *Глава города поручил поликлиникам уже сейчас вносить полную информацию о маленьких пациентах, включая номера школ и детских садов, а также прикреплённых к учебным заведениям медицинских учреждений:* «Вы стоите у истоков электронной системы. Формировать все данные должна поликлиника, а не школа. Сразу с первых дней жизни ребёнка» // https://www.gov.spb.ru/press/governor/184760/

данных в системе «Навигатор» как условие доступа к дополнительному образованию в «пилотных» регионах.

Планы по дальнейшей цифровизации школ предусмотрены, в частности, Национальным проектом «Образование»[48].

Согласно Нацпроекту к концу 2024 года «во всех субъектах РФ внедрена целевая модель цифровой образовательной среды» (далее – ЦОС); появятся «цифровые двойники»; **«к 2024 году обучающимся 5–11 классов предоставлены возможности освоения основных общеобразовательных программ по индивидуальному учебному плану»**.

В развитие Нацпроекта принято Постановление Правительства РФ от 07 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»; далее – Положение). Согласно п. 4 Положения: *«***Целями эксперимента являются … обеспечение возможности дальнейшего внедрения и использования цифровой образовательной среды на постоянной основе на всей территории Российской Федерации…***»*.

Как мы видим, несмотря на декларирование режима эксперимента, акт Правительства предусматривает внедрение ЦОС «на постоянной основе на всей территории» страны. То есть никаких других выводов из «эксперимента» - не планируется, они заранее известны.

Положением запланировано создание «информационно-коммуникационной образовательной платформы» как **«совокупности используемых в рамках эксперимента информационных ресурсов,**

[48] Паспорт утверждён президиумом Совета при Президенте РФ по стратегическому развитию и нацпроектам, протокол от 24 декабря .12.2018 г. № 16; далее – Нацпроект

информационных систем и технологий, функционирующих на базе российских социальных сетей, с наибольшим количеством пользователей».

В частности, в настоящее время в школах внедряется цифровая платформа «Сферум» на базе соцсети ВКонтакте[49]. При этом Положение о ЦОС никак не гарантирует полный объём обучения в традиционной форме и не описывает механизмы реализации прав граждан, не желающих, чтобы их дети участвовали в эксперименте.

На примере некоторых регионов известно, что родителей детей ставили перед фактом превращения их класса в «цифровой» с раздачей учащимся планшетов для обучения. Из практики регионов ясно просматривается недобровольный принцип внедрения ЦОС по стране.

Следует отметить, что регистрация на цифровых платформах для обучения представляет собой – согласно пользовательским соглашениям платформ – акцепт-оферты, то есть, заключение договора с вынужденным согласием на обработку персональных данных обучающихся и с возможностью любого одностороннего изменения договора со стороны операторов платформ, о чём родителей школы даже не ставят в известность. Такие механизмы приводят к незаконной подмене обучения по закону (как реализации государственной функции) обучением по договору с непредсказуемым результатом.

Планы принудительного тотального перевода на ЦОС всех учащихся подтверждает тот самый Приказ № 600. Согласно его нормам:

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

- «доля учащихся, по которым осуществляется ведение цифрового профиля на платформе ЦОС» к 2030 году **должна составить 100%**[50];
- «доля учащихся, которым предложены рекомендации по повышению качества обучения и формированию индивидуальных траекторий с использованием данных цифрового портфолио учащегося» к 2030 году составит 80%[51];
- «доля заданий в электронной форме для учащихся, проверяемых с использованием технологий автоматизированной проверки» к 2030 году должна составить 70%[52].

Это показывает, что по существующим планам:

- 100% учащихся должны будут передавать свои персональные данные в базу ЦОС с целью формирования цифрового профиля (чем игнорируется конституционное право граждан на отказ от подобных действий);
- как минимум 80% учащихся должны будут следовать траектории (действиям), рекомендуемой цифровыми платформами (с закономерным лишением их возможности получения полноценного разностороннего образования и исключением единого образовательного пространства в масштабах страны);

[50] 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".

[51] П. 4.1 Приложения № 1. При этом по госпрограмме Московской области “«Цифровое Подмосковье» на 2018-2024 годы”, утв. Постановлением Правительства Московской обл. от 17 октября 2017 г. № 854/38, «доля обучающихся по программам общего образования, дополнительного образования для детей и среднего профессионального образования, для которых формируется цифровой образовательный профиль и индивидуальный план обучения с использованием федеральной информационно-сервисной платформы цифровой образовательной среды, в общем числе обучающихся по указанным программам» должна составлять к 2024 году 90 процентов.

[52] П. 4.5 Приложения № 1.

- как минимум 70% обучения должно будет стать электронным (игнорируются угрозы нанесения вреда здоровью, возможного снижения эффективности обучения).

Планы по цифровизации образования следуют также из Распоряжения Минпросвещения России от 18 мая 2020 г. № Р-44 «Об утверждении методических рекомендаций для внедрения в основные общеобразовательные программы современных цифровых технологий» (далее – Распоряжение № Р-44). В этих рекомендациях обозначены, в частности:

- технологии виртуальной и дополненной реальности;
- использование соцсетей в обучении;
- «реализация персонализованных планов учения и индивидуальных учебных планов обучающихся в зависимости от возраста и типологически ясных особенностей и возможностей»,
- «геймификация учения через включение цифровых игровых форм»;
- обеспечение с помощью искусственного интеллекта логистики персонализированного учебного расписания, **производства «цифровых двойников» действий учащегося, симуляции поведения учителя**.

Ключевая роль учителя в образовании при таком подходе переходит к искусственному интеллекту. Бумажные учебники вытесняются со ссылкой на их дороговизну, проблемы перевыпуска при наличии ошибок[53] 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).

[53] См. Паспорт стратегии «Цифровая трансформация образования» // https://docs.edu.gov.ru/document/267a55edc9394c4fd7db31026f68f2dd/download/4030/

Существуют многочисленные научно-практические исследования, доказывающие вред, причиняемый внедрением электронных средств обучения (ЭСО) в школы, как в отношении здоровья детей, так и эффективности обучения[54]. Применение ЭСО и Интернета формирует у детей вредные зависимости, негативно влияет на 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**»[55].

Обширные 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[56].

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…»[57].

Ухудшение социализации влечёт нарушение общественных связей, качества коммуникации. Расстройства, связанные с экранной зависимостью, провоцируют сидячий образ жизни у детей, снижая аэробную нагрузку, которая «играет важную роль в неврологическом здоровье детей, особенно в структуре и функциях мозга»[58].

---

[54] Наприме: Шпитцер М. Антимозг. Цифровые технологии и мозг. Москва, 2014. С. 22, 23.

[55] Там же. С. 69, 144-145.

[56] Sigman A: Screen Dependency Disorders: a new challenge for child neurology. P. 4.

[57] Шпитцер М. Антимозг. Цифровые технологии и мозг. С. 23, 24.

[58] Sigman A: Screen Dependency Disorders: a new challenge for child neurology. P. 5.

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.

Анализ нормативной базы, планов и практики показывает, что в настоящее время фактически заново – но в неявной, скрытой форме – происходит формирование системы – аналога системы «Контингент обучающихся», которая предлагалась в 2016 году[59] и предусматривала массовый сбор данных об учащемся и его родителях. В 2016 г. закон был отклонён Президентом РФ.

Проведение масштабной цифровизации образования создаёт высочайшие риски поражения граждан в праве на образование, в праве на неприкосновенность частной жизни, способно привести к причинению серьёзного вреда здоровью, к дискриминации граждан, создаёт угрозу суверенитету страны, формирует почву для роста киберпреступности.

1.5.10. Сфера социального обслуживания

В 2015 г. был принят Федеральный закон № 388-ФЗ «О внесении изменений в отдельные законодательные акты РФ в части учёта и совершенствования предоставления мер социальной поддержки, исходя из обязанности соблюдения принципа адресности и применения критериев нуждаемости».

[59] Законопроект № 1048557-6 «О внесении изменений в статьи 15 и 16 Федерального закона «Об общих принципах организации местного самоуправления в Российской Федерации» и Федеральный закон «Об образовании в Российской Федерации» (о создании государственной системы «Единая федеральная межведомственная система учета контингента обучающихся по основным и дополнительным образовательным программам»).

Ссылка: https://rg.ru/2016/12/30/putin-otklonil-zakon-o-sozdanii-sistem-kontingent-obuchaiushchihsia.html

Этим законом дополнен Федеральный закон РФ от 17 июля 1999 г. № 178-ФЗ «О государственной социальной помощи» (далее – ФЗ № 178) в части создания единой государственной информационной системы в области социального обеспечения (далее – ЕГИССО) с 1 января 2018 г.

ЕГИССО призвана аккумулировать масштабную информацию о семьях граждан, в том числе для анализа вопроса о наличии нуждаемости в социальном обеспечении.

Согласно актуальной редакции п. 1 ст. 6.9. ФЗ № 178 ЕГИССО является «федеральной государственной информационной системой, создаваемой в целях обеспечения граждан, органов государственной власти, органов местного самоуправления, а также организаций, предоставляющих меры социальной защиты (поддержки), социальные услуги в рамках социального обслуживания и государственной социальной помощи, иные социальные гарантии и выплаты, информацией о мерах социальной защиты (поддержки), социальных услугах в рамках социального обслуживания и государственной социальной помощи, об иных социальных гарантиях и выплатах, предоставляемых гражданам в Российской Федерации за счет средств федерального бюджета, бюджетов субъектов Российской Федерации и местных бюджетов, а также **в целях автоматизации процессов назначения и предоставления указанных мер социальной защиты (поддержки), социальных услуг, иных социальных гарантий и выплат путем использования инфраструктуры, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг и исполнения государственных и муниципальных функций в электронной форме**».

Состав ЕГИССО прописан в Постановлении Правительства РФ от 14 февраля 2017 года № 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»). Примечательно, что Закон № 388-ФЗ даёт лишь примерный перечень собираемой информации (ст. 6.9), оставляя детали регулирования перечня Правительству.

В перечень собираемых по Положению о ЕГИССО сведений включены: СНИЛС, ФИО, пол, дата рождения, 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), страховые номера индивидуальных лицевых счетов (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.

При этом, как указано в Положении о ЕГИССО, ФИО, пол, дата рождения и место рождения включаются в ЕГИССО **исключительно для «первичной выверки сведений о гражданине»**. В п. 13 Положения о ЕГИССО прямо сказано, что персонификация сведений о гражданине осуществляется в ЕГИССО на основании СНИЛС. Также отмечается, что принципом системы 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 (без заявления гражданина) начисления Пенсионным фондом России социальных выплат 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. В частности, велики риски навязывания дополнительных банковских услуг лицам, обратившимся за начислением пенсии, а также «рекламной атаки» на семью, получившую право на семейный (материнский) капитал со стороны девелеперов, предлагающих приобрести новое жилье.

1.5.11. Региональный разнобой регулирования и «законодательные песочницы»

В настоящее время в Российской Федерации, кроме процессов цифровизации, инициируемых с федерального уровня, идёт 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 в городе или регионе легализуется в формате «особых экспериментальных режимов», так называемых «законодательных песочниц».

Этот порядок вызывает серьёзные опасения с точки зрения защиты прав граждан, потому что:

- поправки 2020 года в Конституцию РФ в ст. 71 устанавливают именно **федеральную ответственность** за оборот данных граждан и защиту их прав в цифровом пространстве,

- Конституция РФ устанавливает **равенство прав всех граждан** России перед законом.

Граждане, «попавшие» помимо своего желания, просто в силу проживания в «инновационном регионе», в такую «законодательную песочницу» или «экспериментальный правовой режим», разрешающий, например, произвольные манипуляции с их персональными данными для «нужд развития рынка ИТ и цифровизации», оказываются по факту поражёнными в правах по сравнению с остальными соотечественниками[60].

Кроме того, 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.

1.5.12. Саморегулирование цифровой отрасли: объективные пределы эффективности

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

[60] 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.

бизнес не демонстрирует социальной ответственности. Процессы сбора и использования персональных данных повсеместно идут с нарушением Конституции, законодательства о персональных данных, информации и связи.

Возникает закономерный вопрос: каким образом и отчего, долгие годы системно нарушая федеральные законы, бизнес внезапно создаст и станет исполнять собственные, ограничивающие развитие бизнеса и получение прибыли 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[61] 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 РФ.** Саморегулирование цифровой отрасли. даже если оно «пойдёт», будет осуществляться под сильнейшим влиянием западных цифровых платформ, работающих в чужой юрисдикции. Законодательство «о приземлении» иностранных платформ может изменить правовое положение иностранных платформ, но не их коммерческие интересы и лоббистские возможности.
4. **Национальная безопасность не может «саморегулироваться» частным бизнесом.** Персональные данные, права граждан на защиту идентичности, частной жизни, доступа к информации – это вопросы

[61] 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.

национальной безопасности. Такие вопросы не могут решаться исключительно «саморегулированием».

26 октября 2021 года был согласован и подписан крупными игроками отрасли Искусственного интеллекта «Кодекс этики ИИ»[62]. Кодекс подписали Яндекс, Сбербанк и другие цифровые платформы, а также многие российские разработчики ИИ.

Авторы данного доклада участвовали в корректировке этого кодекса, как и многие другие участники отрасли и представители госсектора в области цифровизации и информационного пространства, включая Министерство обороны РФ, Администрацию Президента РФ и Аналитический Центр Правительства РФ.

Это хороший пример достижения широкого общественного согласия с принятием согласованных норм в том числе большим цифровым бизнесом.

Тем не менее, Кодекс этики ИИ является добровольным для его подписантов, 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.

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.

---

[62] 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

Общий вывод части I:

Беспорядочная, хаотичная и бесконтрольная цифровизация создаёт огромные риски для прав граждан и суверенитета страны. Необходимо вырабатывать и закреплять в законодательстве российскую модель цифровизации, защищающую права граждан и национальный суверенитет, обеспечивать её общественную поддержку и институциональную базу.

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

Если исходить из нашей конституционной философии, из высших ценностей российской культуры, 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 трезвого рассмотрения и оценки существующих и прогнозируемых рисков, угроз и вызовов реализации прав и свобод человека и гражданина в цифровом пространстве, а также выработки системы мер, призванных обезопасить личность, общество и государство.

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

Для понимания того, что нужно делать для снижения рисков цифровизации, необходимо обозначить цель: куда мы идём, **каков образ цифрового будущего России?**

Очевидно, что этот «образ будущего» должен соответствовать нашей Конституции и нашей культуре.

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 (ст. 2 Конституции Российской Федерации).

В свою очередь, ценность и достоинство каждой человеческой личности связано с уникальным положением человека в бытии, наличием у него сознания собственной личности, 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 пересмотр традиционных и классических 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, характерных 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? Мы просто бессильные заложники технологических «трендов», «тенденций», «логик», цифровые векторы, «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 «общественному договору», нет в конечном счёте места и этике, праву, культурным идеалам. Возможность и необходимость общественного договора

определяется именно субъектностью и свободой человека как стороны и участника общественного договора.

Наша конституционная философия, культурное и интеллектуальное наследие дают нам право, моральные силы 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 наш путь в «цифровое завтра» должен описываться следующими формулами:

– дальнейшее развитие человечества должно остаться свободным развитием свободных человеческих существ и их исторически сложившихся сообществ;

– дальнейшее социально-историческое развитие должно сохранить в качестве своей цели реализацию прав и свобод человека, как самобытного, автономного, саморегулируемого существа, наделённого разумом и волей;

– проблематика будущего мироустройства должна остаться принципиально открытой, поливариантной; мы не должны пытаться описать будущее суммой жёстких формул, исключая из числа рабочих сценариев и альтернатив 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:

– принципы достоинства, свободы и прав человека должны неукоснительно соблюдаться при внедрении и использовании технологий во всех сферах жизнедеятельности человека, общества и государства;

–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;

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

– функционирование новейших технологических и информационных платформ подлежит общественному этическому контролю; решения систем искусственного интеллекта, иных систем обработки информации, не совместимые с принципами достоинства, свободы и прав человека, – ничтожны, а их практическая реализация должна преследоваться по закону;

– использование технологических систем во всех сферах жизнедеятельности человека, общества и государства должно сообразовываться с ценностными и культурными стандартами, разделяемыми большинством граждан;

– при использовании новейших технологий должны быть исключены риски нарушения фундаментальных прав и свобод человека и гражданина, политических, социальных и экономических прав;

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

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

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

технологий, систем искусственного интеллекта для преднамеренной дезинформации граждан должно преследоваться по закону;

– передача любых властных полномочий технологическим системам, в том числе искусственному интеллекту, иным цифровым технологиям не допускается; наделение систем искусственного интеллекта, а также иных технических систем, правосубъектностью, правами и свободами, 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 граждан РФ в их реализации в цифровом пространстве.

Например, поэтому мы не обсуждаем здесь некое «право на доступ в Интернет» или «на доступ к цифровым технологиям», которое пытаются ввести в некоторых странах мира – мы считаем, что это правомочие входит в содержание конституционного права гражданина на получение и распространение информации.

Переживаемый нами опыт пандемии свидетельствует, что гарантировать безопасность гражданам может только эффективное государство, а безопасность вкупе со свободой и правами человека может гарантировать только эффективное правовое государство. Поэтому исходя из фундаментальных принципов достоинства, свободы и прав человека, мы должны найти современную эффективную модель правового государства,

которая обеспечит их реализацию одновременно в новых технологических условиях и в контексте актуальных вызовов и угроз. В том числе – в контексте «пандемии цифровизации».

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

Итак, конституционный порядок и, прежде всего, его основополагающие принципы: достоинства, свободы, прав человека и гражданина; принадлежности суверенитета народу России; правового государства, – должны рассматриваться нами в качестве руководящих ценностей, не подверженных влиянию технологических факторов, изменению общественных настроений.

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

– формирование условий для защиты конституционных прав и свобод человека и гражданина, реализуемых в цифровом пространстве Российской Федерации;

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

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

– целенаправленное использование потенциала цифровых технологий для укрепления единства многонационального народа Российской Федерации, гражданского мира, согласия и солидарности в российском обществе.

Обеспечение защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации должно осуществляться на основе принципов:

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

– признания, соблюдения и защиты достоинства личности, прав и свобод человека и гражданина в цифровом пространстве как конституционной обязанности государства, институтов гражданского общества и граждан Российской Федерации;

– защиты суверенитета Российской Федерации 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;

– осуществления власти многонациональным народом Российской Федерации – носителем суверенитета и единственным источником власти в Российской Федерации непосредственно, а также через органы публичной власти;

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

– единства правового пространства Российской Федерации, в том числе в цифровой среде;

– приоритета федерального законодательства в правовом регулировании цифрового пространства Российской Федерации;

– признания и защиты в цифровом пространстве Российской Федерации всей полноты правовых, культурных, этических и иных норм, принятых российским обществом и государством;

– системного подхода к правовому регулированию вопросов защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации;

– формирования цифрового пространства России в качестве среды, благоприятной для становления и развития личности человека и гражданина в соответствии с традиционными духовно-нравственным ценностям российского общества;

– заботы о безопасности, нравственном, культурном, образовательном, гражданском и патриотическом развитии детей и молодёжи в цифровом пространстве Российской Федерации;

– неотвратимости наказания за противоправные деяния в цифровом пространстве Российской Федерации;

– запрета на принудительное вовлечение граждан в цифровую среду - в том числе, под угрозой невозможности полноценной реализации их прав, свобод и законных интересов;

– признания права гражданина на сохранение традиционных, нецифровых способов взаимодействия с государством и обществом с возможностью полноценной реализации прав и свобод человека и гражданина;

– опережающего регулирования развития цифрового пространства в Российской Федерации 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 граждан в цифровом пространстве имеют подходы, положенные в основу комплекса концептуальных документов в области национальной безопасности и стратегического планирования.

Согласно Стратегии национальной безопасности Российской Федерации[63], достижение цели обеспечения информационной безопасности

[63] Утверждена Указом Президента РФ от 02.07.2021 г. № 400.

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 установленных российским законодательством требований по защите такой информации и персональных данных; обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий[64].

В соответствии с п. 3 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы[65] основными принципами настоящей Стратегии 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, следует отметить «развитие технологий электронного

[64] Подпункты 6, 8 пункта 57 Стратегии национальной безопасности Российской Федерации.

[65] Утверждена Указом Президента РФ от 09 мая 2017 г. № 203.

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).

Как отмечено в принятой в ходе всенародного голосования 1 июля 2020 года ст. 75.1. Конституции РФ **«В Российской Федерации создаются условия … для взаимного доверия государства и общества гарантируются защита достоинства граждан и уважение человека труда…».**

Таким образом, одним из главных условий, которое позволит обеспечить социальную стабильность и доверие граждан государству, является чёткое соответствие федерального законодательства и подзаконных актов Конституции РФ, вышеприведённым положениям стратегических документов и неукоснительное их соблюдение на практике.

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

Мы убеждены: **защите и реализации в цифровом пространстве Российской Федерации подлежит весь объём 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 существующие права и свободы** человека и гражданина, установленные законодательством Российской Федерации.

Защита прав и свобод человека и гражданина в цифровом пространстве должна быть целевым и ценностным ориентиром развития отечественной информационно-коммуникационной отрасли, разработки отечественных технологий обработки больших данных и искусственного интеллекта.

К числу **специфических** прав и свобод человека и гражданина, подлежащих защите в цифровом пространстве Российской Федерации, относятся:

– право на защиту цифровой идентичности;

– право на обеспечение цифрового суверенитета человека;

– право на защиту от ментальной (информационно-психологической) манипуляции;

– право на защиту от цифровой дискриминации;

– право на защиту биометрических и иных персональных данных;

– право на отзыв данных, право на забвение в цифровом пространстве;

– право на защиту от противоправных деяний в цифровом пространстве;

– право на оспаривание решений и действий цифровых систем в отношении себя;

– 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, в том числе:

– от противоправного контента в цифровом пространстве;

– от сетевого манипулирования;

– от цифровой дискриминации;

– от передачи образовательной функции от учителя автономным системам искусственного интеллекта;

– от замены традиционных образовательных и воспитательных функций педагога автономными системами искусственного интеллекта;

– от цифровой зависимости;

– от причинения вреда их здоровью при использовании цифровых технологий.

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

2.1.4. Обеспечение суверенитета РФ над национальным цифровым пространством

Мы исходим из того, что цифровое пространство Российской Федерации является частью суверенного пространства России, в котором наша страна имеет право и возможность самостоятельно определять законы, правила, правоприменение, национальную стратегию и безопасность, как сказано в Части I настоящего Доклада.

Под цифровым информационным пространством мы понимаем всё медийное пространство России, 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 законодательной и иной практической деятельности по защите прав и свобод человека и гражданина в цифровом пространстве Российской Федерации предлагается определять «цифровое пространство» 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» и «цифровая

среда», «цифровая сфера» мы предлагаем считать синонимами в рамках данного Доклада.

Важнейшим принципом обеспечения суверенитета Российской Федерации в цифровом пространстве выступает **приоритет конституционных норм и национального законодательства над международными нормами в случае их противоречия**.

Поскольку многие страны мира, а также международные организации, включая ЮНЕСКО и Совет Европы, в настоящий момент также озабочены регулированием цифровой среды, нам нужно ответить на естественно возникающие важные вопросы о соотношении российского и международного регулирования:

- нужно ли вообще России применять внутри страны мировой опыт регулирования цифрового пространства?
- нужно ли стремиться участвовать в создании международных соглашений и законов о регулировании «цифры» 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 ЮВА – также вырабатывают собственные подходы, часто с интересными и оригинальными законодательными решениями (наподобие «приземления» цифровых экосистем и «цифрового налога» на них). Нужно внимательно изучать мировой опыт в этой области. Однако здесь необходимо понимать, что все упомянутые крупные игроки цифровой среды, исповедуя **разные цивилизационные ценности**, идут в области регулирования цифровой сферы в принципиально разные стороны. Скажем, Китай движется в сторону **всё более полного 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, со всё 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.

Этот разнобой объясняется в первую очередь различными представлениями о благом и должном социальном порядке, то есть разными цивилизационными установками и целями.

Кроме того, довольно сильно влияет и реальное положение игрока в цифровом мире: США – абсолютный лидер цифровой сферы и обладатель полноценного цифрового суверенитета; ЕС – напротив, полностью 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 промежуточном 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 страну во власть «цифровых экосистем».

Сказанное означает, что России придётся искать баланс, свой собственный «срединный цифровой путь». Впрочем, это не мешает изучать мировой опыт законотворчества и заимствовать наиболее подходящие идеи и механизмы регулирования.

Следует также обратить внимание на достаточно популярную 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 «цифровое» законодательство в соответствие с ними.

Мы считаем эту позицию неверной по следующим причинам:

- **перспективы создания адекватного международного «цифрового» законодательства весьма туманны.** В настоящее время лидерами в развитии цифровых «экосистем» и технологий искусственного интеллекта являются США и Китай. Ни при каких обстоятельствах страны, стремящиеся быть лидерами и ощущающие себя лидерами в такой критически значимой области, не будут добровольно накладывать на себя какие-либо серьёзные ограничения и обязательства.
- **предыдущие попытки регулирования цифровой среды провалились:** двадцатилетний опыт попыток создать международное законодательство в сфере информационной безопасности или взять управление маршрутизацией Интернета в руки международного сообщества[66] оказался неудачным, что служит модельным примером того, какие есть шансы на появление «международного цифрового законодательства».
- **подходы к регулированию цифровой среды у США, Китая и ЕС разнятся**: уже сейчас они если не противоположны, то как минимум «перпендикулярны», имеют разные этические установки и цели. Вряд ли получится сгладить эти противоречия при выработке международных норм.

[66] Эти попытки неизменно торпедировались американцами, являющимися главным источником киберугроз для всего мира.

- **перспективы международного правоприменения в цифровом пространстве – ещё более туманны.** Есть большие сомнения в том, что США, например, согласятся на международное расследование компьютерных инцидентов, имеющих «американский след», а тем более – выдачу киберпреступников, действующих с территории США[67]. Нет никаких сомнений, что и Китай также будет проявлять твёрдость в этом отношении. Конституция Российской Федерации также запрещает экстрадицию российских граждан по любым зарубежным уголовным делам, запросам и основаниям.
- **глобальные цифровые платформы можно «приземлять» только локально.** Перспективы создания общемирового законодательства, регулирующего деятельность глобальных цифровых «экосистем» наподобие Google, Meta (Facebook), Twiiter, TikTok и др. – близки к нулю. Национальные представления о приемлемом и неприемлемом контенте и поведении цифровых платформ кардинально отличаются в разных странах, что легко прослеживается по политике и основаниям блокировок аккаунтов в Meta (Facebook), Twitter, Instagram и др.

  Все возможные средства принуждения цифровых платформ к исполнению национальных законодательств – также локальны, по сути, сводятся к штрафам и блокировкам по национальному законодательству. Подобных международных средств и механизмов для ограничения деятельности мировых цифровых гигантов – не существует, и сейчас даже не просматриваются пути к их созданию.
- **самое главное: при создании и ратификации международных соглашение и норм в «цифровой» сфере, нам может быть**

[67] Между тем, последнюю четверть века подавляющее число (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 МО США и разведсообщества.

навязана чужая и чуждая этическая и юридическая модель. Как уже много раз бывало в истории (например, с ВТО или Киотским протоколом), «международное сообщество» может под давлением «лидеров свободного мира» закладывать в международные законы довольно смещённые представления о законности и справедливости, «сдвинутые» в пользу отдельных стран, главных организаторов такого законотворчества.

Безусловно, нужно проявлять добрую волю к сотрудничеству в области создания международных правил и норм по регулированию цифрового пространства и участвовать во всех разумных международных инициативах, однако рассчитывать на полезные результаты в ближайшее время и откладывать формирование собственного подхода и собственных законов – нельзя. Национальное законодательство нужно исправлять и дорабатывать параллельно участию в международных инициативах и с существенным опережением, при этом присоединение к международным соглашениям в этой сфере и их последующая ратификация должны осуществляться не в ущерб национальным интересам Российской Федерации.

2.1.5. Принципы работы с данными

В целях защиты прав и свобод человека и гражданина, обеспечения суверенитета Российской Федерации, необходимо сформулировать и законодательно закрепить новые принципы использования персональных данных.

Как мы говорили выше, несмотря на различные подходы к регулированию, правам граждан и общей системе ценностей, мы вполне можем заимствовать некоторые идеи и методы у наших зарубежных соседей, с последующей их адаптацией под российские реалии и стратегические национальные приоритеты.

В частности, мы можем разработать российский аналог довольно разумных принципов работы с данными, имеющихся в современном европейском законе о правилах работы с данными (General Data Protection Regulation - GDPR), среди которых:

- **законность, справедливость и прозрачность.** Персональные данные должны обрабатываться законно, справедливо и прозрачно. Любую информацию о целях, методах и объёмах обработки персональных данных следует излагать максимально открыто, доступно и просто;
- **ограничение цели.** Данные должны собираться и использоваться исключительно в тех целях, которые заявлены компанией или организацией (онлайн-сервисом);
- **минимизация данных.** Нельзя собирать личные данные в большем объёме, чем это необходимо для заявленных целей их обработки;
- **точность и достоверность.** Личные данные, которые являются неточными или ложными, должны быть удалены или исправлены (в том числе по требованию пользователя);
- **ограничение хранения.** Личные данные должны храниться в форме, которая позволяет идентифицировать субъекты данных на срок не более, чем это необходимо для целей обработки;
- **целостность и конфиденциальность.** При обработке данных пользователей компании и органы публичной власти обязаны обеспечить защиту персональных данных от несанкционированной или незаконной обработки, уничтожения и повреждения.

Представляется, что обсуждение и выработка таких принципов может стать:

– основой для консолидации ответственных представителей «цифровой» сферы, политиков, экспертов, общественников;

– одной из стартовых стратегий ценностной «перезагрузки» цифровизации страны.

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 упомянутых 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, уважения к достоинству человека, его 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», 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.

Поэтому ключевой вопрос нашего времени: **что необходимо сделать в области применения информационно-коммуникативных («цифровых») технологий для того, чтобы наши конституционные идеалы были защищены и реализованы**?

Мы считаем, что сегодня необходимо принять в качестве руководящего принципа «**принцип высокой планки» (или презумпцию высокого достоинства человека) как основу, например, для:**

– диалога государства и общества, бизнеса и общества, бизнеса, государства и общества;

– государственной культурной политики, государственной системы образования;

– функционирования сферы медиа, для всех процессов, которые происходят в информационном («цифровом») пространстве.

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 цифрового пространства, а именно об уважении высокого достоинства личности человека и гражданина, его права 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 все сказанное означает, что перед элитой российского гражданского общества, перед российскими политиками, интеллектуалами, представителями бизнеса стоит задача – выработать такую модель организации информационного пространства, которая соответствует нашим конституционным ценностям, модели правового государства, принципу

уважения к человеческому достоинству, **является 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, в том числе – требование хранить культурное наследие. Соответственно, эта модель должна решать одну из важнейших проблем нашего общества – проблему отчуждения значительной части сограждан, особенно – новых поколений от собственного культурного наследия как фактора формирования личности и трендов общественного развития.

2. **Модель развития цифровой среды России должна соответствовать закреплённым в Конституции правам и свободам граждан**, что исключает идеологическую цензуру, но означает необходимость соответствия цифровой среды фундаментальным ценностям Конституции и российского общества.

3. Наше государство должно развиваться как социальное. Например, важно, чтобы публичное пространство не было тотально коммерциализировано, рынок имел границы, а граждане - равный доступ к культурным ценностям и 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 прямая 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 Российской Федерации осуществляется посредством решения комплекса задач на следующих направлениях:

– **совершенствование и развитие законодательства** в сфере обеспечения защиты прав и свобод человека и гражданина в цифровом пространстве Российской Федерации;

– **институциональное развитие** цифрового пространства Российской Федерации, а также развитие **саморегулирования** в данной сфере;

– формирование устойчивой и достаточной для безопасного развития **цифровой грамотности граждан** Российской Федерации;

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

– **научные исследования** процессов формирования и развития цифрового пространства.

2.2.1. Совершенствование и развитие российского законодательства

Согласно пункту «м» ст. 71 Конституции РФ в ведении Российской Федерации находится обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных. Согласно ч. 1 ст. 76 Конституции РФ, по предметам ведения Российской Федерации принимаются федеральные конституционные законы и федеральные законы, имеющие прямое действие на всей территории Российской Федерации.

Очевидно, что 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 Российской Федерации, наиболее актуальными представляются следующие меры по совершенствованию и развитию российского законодательства:

1. Дальнейшее развитие законодательства в области защиты суверенитета Российской Федерации в цифровом пространстве, в том числе, по развитию правовых механизмов регулирования деятельности зарубежных и транснациональных акторов цифрового пространства в соответствии с требованиями российского законодательства.
2. Разработка Цифрового кодекса, систематизирующего правовое регулирование отношений в цифровом пространстве Российской Федерации, обеспечивающего правовую защиту прав и свобод человека и гражданина в цифровом пространстве Российской Федерации, а также информационную безопасность страны – сначала в виде поправок к существующим нормативным правовым актам, а затем в формате самостоятельного кодекса.
3. Дальнейшее совершенствование законодательных гарантий доступа граждан к культурным ценностям, образованию, просвещению в цифровом пространстве.
4. Дальнейшее законодательное обеспечение развития инфраструктуры электронной демократии.
5. Сохранение бумажного документооборота в критически значимых сферах защиты интересов государства, гражданского общества, коммерческих и некоммерческих организаций, общественных объединений, человека и гражданина.

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 граждан, а также установление ответственности за создание, внедрение таких систем и причинённый ими ущерб.
9. Совершенствование правовых механизмов, регулирующих сбор персональных данных граждан.
10. Усиление 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 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, 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. Совершенствование правовых механизмов противодействия мошенническим, коррупционным, иным преступным деяниям в цифровой среде.
19. Ужесточение ответственности за противоправное изготовление, использование и оборот цифровых документов.
20. 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.).
21. Повышение эффективности правовых механизмов противодействия манипулированию в цифровом пространстве общественным мнением, сознанием и поведением граждан.

22. Совершенствование законодательства об особых экспериментальных режимах (так называемых «законодательных песочницах)» в целях недопущения создания предпосылок к нарушению прав и свобод человека на региональном и местном уровнях.
23. Системное развитие правовых механизмов защиты и реализации специфических прав, возникающих в ходе развития цифрового пространства (право на защиту цифровой идентичности, право на обеспечение цифрового суверенитета человека и гражданина, право на защиту от информационно-психологической манипуляции, право на отзыв данных, право на забвение в цифровом пространстве, право на защиту от противоправных деяний в цифровом пространстве, право на использование традиционных форм взаимодействия граждан, бизнеса и государства, право на защиту от негативных социальных последствий цифровизации и иных прав).
24. 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.
25. Развитие законодательства о государственно-частном партнёрстве в решении задач развития цифрового пространства и обеспечения защиты в цифровом пространстве интересов государства и общества, прав и свобод человека и гражданина.
26. Совершенствование законодательства Российской Федерации в части уточнения условий и порядка дачи информированного добровольного согласия граждан на сбор данных.
27. Развитие законодательства в области установления (использования) режима тайны и категории защищаемых данных.

28. Законодательное закрепление категорий особо защищаемых граждан в ходе цифровой трансформации жизнедеятельности личности, общества и государства.
29. Законодательное закрепление порядка раскрытия информации цифровыми сервисами, а также порядка сбора и хранения данных.
30. Установление упрощённого режима оспаривания гражданами данных о себе в частных и государственных базах данных.
31. Установление запрета на ограничение информационного суверенитета человека.
32. Установление запрета цифровой слежки, цифровых «двойников», «профилей», «траекторий» и «рейтингов».
33. Установление квалификационных требований к специалистам по обработке данных и мер ответственности за их нарушения.
34. Разработка единых стандартов пользовательских соглашений и политики цифровых сервисов для всех цифровых сервисов, как отечественных, так и зарубежных, на территории Российской Федерации.
35. Установление запрета на присвоение единого номера-идентификатора человеку в общенациональном цифровом пространстве.
36. Минимизация состава обрабатываемых персональных данных, необходимых для решения возлагаемых на государственные, муниципальные и частные информационные системы задач.
37. 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 не может не включать в себя решение комплекса задач по развитию институциональной

структуры цифрового пространства Российской Федерации, а также саморегулирования в данной сфере. К числу этих задач следует отнести:

1. Дальнейшее развитие публичной инфраструктуры электронной демократии в цифровом пространстве Российской Федерации.

Строительство эффективного правового государства в условиях нового технологического уклада и роста глобальных угроз безопасности личности, общества и государства, требует создания развитой инфраструктуры электронной демократии. Здесь необходимо преодолеть имеющийся дисбаланс, при котором существующая система государственных и муниципальных сервисов и система государственного контроля и мониторинга 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.

2. Дальнейшее развитие публичной инфраструктуры образования, культуры, массового просвещения в цифровом пространстве Российской Федерации.

3. Разработку и развитие системы этических кодексов использования цифровых технологий как основы для саморегулирования субъектов цифрового пространства, работающих с данными пользователей на территории Российской Федерации. Стандартизацию и развитие саморегулирования отрасли больших данных и искусственного интеллекта на основе отраслевых этических кодексов соответствующих отраслей

4. Проведение информационных кампаний в целях развития социальной ответственности бизнес-структур и представителей бизнеса при внедрении новых цифровых технологий.

5. Создание института аудита и независимой экспертизы цифровых технологий и систем хранения и передачи данных, а также использование механизмов саморегулирования в данной сфере.

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

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

1. Проведение массовых просветительских кампаний по повышению осведомлённости граждан об их правах и свободах в условиях цифровой трансформации, формирования цифрового пространства Российской Федерации.

2. Проведение массовых просветительских кампаний по повышению осведомлённости граждан о возможностях реализации их гражданских, культурных, образовательных, социально-экономических и иных прав и свобод в цифровом пространстве Российской Федерации.

3. Проведение массовых просветительских кампаний по повышению и осведомлённости о цифровой гигиене и правилах безопасности в цифровой среде.

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

5. Включение в образовательные программы, реализуемые в государственных и муниципальных учреждениях общего и высшего образования, знаний и навыков, необходимых для реализации прав и свобод

новых поколений граждан, развития у представителей новых поколений 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, 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. Нужна обязательная экспертиза законодательства, выявление пробелов, несовершенств правового регулирования отношений, возникающих в цифровом пространстве.

Проекты цифровизации, затрагивающие широкий круг граждан России или уязвимые категории граждан, такие как цифровизация образования, создание реестров персональных данных и пр., создающие риски, угрожающие правам граждан РФ, должны проходить обязательную экспертизу со стороны общественных правозащитных организаций, Общественной палаты Российской Федерации, Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека при Президенте Российской Федерации, РОЦИТа, 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 в цифровом пространстве. Активное выражение гражданского мнения и гражданской

позиции по различным аспектам цифровой трансформации, формирования цифрового пространства.

4. **Защита особо незащищенных и уязвимых групп граждан в реализации их прав и свобод в условиях цифровой трансформации**.

5. **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 Российской Федерации.

6. **Использование различных форм изучения общественного мнения** (опросы, общественные слушания, голосования) по ключевым вопросам цифровизации, затрагивающим основные права и свободы граждан, таким как: цифровизация образования, цифровизация медицины, создание единых реестров граждан, цифровая трансформация рынка труда, цифровая трансформация 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 самых различных сферах бытия личности, общества и государства. Соответственно, его изучение должно носить междисциплинарный характер, включать в себя 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, рост безработицы, рост социальной напряжённости. Прогнозирование угроз личности, правам и свободам человека и гражданина в цифровом пространстве.
4. Выявление гуманитарных и культурных последствий цифровизации.
5. Изучение опыта и модели регулирования реализации прав и свобод граждан в ведущих странах мира.
6. Создание альтернативных сценариев развития цифрового пространства для России.

Заключение

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

Здесь уместно провести аналогию с появлением автомобилей в начале XX века. Первые три десятилетия существования автомобилей и эксплуатации их 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 XX века. Появление ПДД никаким образом не ограничило развитие автомобильной отрасли: напротив, оно 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 Российской Федерации 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 нам нужно ввести «Правила 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 Российской Федерации 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 Российской Федерации, задач развития безопасного информационного пространства, защиты российского общества от деструктивного информационно-психологического воздействия, культурного развития граждан и роста человеческого потенциала Российской Федерации, 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

Авторы и редакторы:

Ашманов Игорь Станиславович, кандидат технических наук, специалист по информационным технологиям и искусственному интеллекту, президент аналитической компании «Крибрум», член Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека;

Волобуев Сергей Григорьевич, философ, автор гражданской интеллектуальной инициативы «Хартия Рунета», координатор проекта «Гражданский экзамен», эксперт Центра социально-консервативной политики;

Наумов Виктор Борисович, доктор юридических наук, специалист по цифровому праву, управляющий партнёр российского офиса компании Dentons, член Экспертного совета при Федеральной антимонопольной службе по развитию конкуренции в области информационных технологий;

Швабауэр Анна Викторовна, адвокат, кандидат юридических наук, эксперт Уполномоченного по защите семьи в Санкт-Петербурге, член экспертно-консультативного совета по семейному законодательству при Совете Федерации;

Цветков Юрий Дмитриевич, исполнительный секретарь Комитета по искусственному интеллекту Комиссии Российской Федерации по делам ЮНЕСКО, советник Президента Сколковского института науки и технологий (Сколтех).

Соавторы, члены рабочей группы Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека:

Вагнер Милош Эдуардович, заместитель руководителя Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор);

Дейнеко Алексей Геннадьевич, к.ю.н., профессор департамента теории права и междисциплинарных юридических исследований факультета права НИУ «Высшая школа экономики»;

Денисенков Андрей Владимирович, президент компании «Урбантех», сопредседатель Московского регионального отделения общероссийской общественной организации «Деловая Россия»;

Кабанов Кирилл Викторович, член Совета при Президенте РФ по развитию гражданского общества и правам человека, председатель Национального антикоррупционного комитета;

Касперская Наталья Ивановна, специалист по информационной безопасности, глава Рабочей группы по информационной безопасности Национального проекта «Цифровая экономика», член Рабочей группы по разработке предложений для внесения изменений в Конституцию в 2020 г. (автор поправки в ст. 71 о защите данных граждан в цифровом пространстве);

Киркора Ирина Владимировна, заместитель председателя Совета при Президенте РФ по развитию гражданского общества и правам человека, председатель Постоянной комиссии по социальным и культурным правам, директор АНО «Авторский центр «Мир Семьи», член Рабочей группы по разработке предложений для внесения изменений в Конституцию 2020 г.;

Короткевич Алексей Сергеевич, ИТ-предприниматель, сокоординатор проекта «Гражданский экзамен»;

Лафитский Владимир Ильич, профессор Московского государственного юридического университета имени О.Е. Кутафина, член Научного совета и приглашённый профессор Международной антикоррупционной академии (Лаксенбург, Австрия), член-корреспондент Международной академии сравнительного права (Париж, Франция), заслуженный юрист Российской Федерации;

Максимова Виолетта Борисовна, директор Департамента государственного консалтинга АО «Аудиторско-консультационная группа «Развитие бизнес-систем»», директор проекта по информационно-технологическому и методологическому сопровождению Минэкономразвития России в части мониторинга развития сети МФЦ в Российской Федерации, эксперт по вопросам цифровизации государственных услуг;

Фёдоров Максим Валериевич, доктор физ.-мат. наук, профессор, ректор Научно-технологического университета «Сириус», представитель России в рабочей группе ЮНЕСКО по этике искусственного.