

Неофобия российской власти

Вы испуганы за ваших собственных детей, так как они - аборигены в том мире, где вы всегда будете иммигрантами

Джон Перри Барлоу, Декларация независимости киберпространства

Российские правители боятся перемен. С опаской относятся к несанкционированным инициативам, видят угрозу в новых технологиях, не строят далеко идущих планов, не имеют образа будущего. Этот консерватизм проявляется как на законодательном уровне, так и в правоприменительной практике, препятствуя развитию, увеличивая издержки и причиняя страдания людям.

Неофобия – боязнь новизны, которая в крайней патологической форме представляет собой иррациональный и неконтролируемый страх перед новым (пусть даже новое это на самом деле давно и успешно используется другими). Этот страх российской власти проявляется не только, когда дело касается технологических новинок в узком смысле, но в самых различных сферах жизни, в которых российское государство сопротивляется внедрению позитивных практик.

В настоящем докладе мы не претендуем на всеобъемлющее описание и анализ логики отношений российского государства к новым технологиям, однако хотим сформулировать и предложить для обсуждения несколько следующих тезисов.

Мы полагаем, что российские власти, препятствуя техническому и социальному прогрессу, чаще всего действуют импульсивно, и лишь впоследствии под уже принятое таким образом решение формулируется объяснение, представляемое обществу. При этом, поскольку потребность в технологии или продукте, доступ к которым искусственно ограничен, сохраняется, граждане вынуждены искать обходные пути – использовать VPN и прокси для доступа к заблокированным сайтам и сервисам, возить из-за рубежа несертифицированные в России лекарственные препараты, игнорировать требования об обязательной регистрации дронов и т.п.

Государственная неофобия может принимать форму протекционизма, иметь коррупционный элемент или основываться на стремлении заручиться поддержкой консервативной части общества и обеспечить информационный, биологический, продовольственный или какой-то

иной суверенитет. Однако в основе своей это по-прежнему инстинктивный страх изменений, иррациональное чувство опасности.

Практически единственная сфера, в которой инновациям дан «зеленый свет», — разнообразные технологии слежки, цензуры и пропаганды: распознавание лиц, автоматизированные системы мониторинга интернета, централизованное распространение фейковых новостей и т.п. В этом же ряду и технологии, упрощающие контроль, – электронные государственные услуги и унификация государственных баз данных.

Мы исходим из того, что российское государство не однородно, отдельные его представители могут иметь собственные интересы или действовать, руководствуясь альтернативными соображениями. Однако результирующая разнонаправленных векторов государственной политики при этом стремится к ограничению развития и пресечению инициативы.

Интернет и связь

Наиболее наглядно описываемая тенденция проявляется в регулировании ИТ-сферы. До 2010-2012 годов Рунет развивался свободно и регулировался крайне выборочно. Пожалуй, именно отсутствие государственного вмешательства стало одним из определяющих факторов российского прорыва в области интернет-технологий. К примеру, суточная аудитория Рунета за период с 2008 по 2013 год [увеличилась](#) с 13,1 до 50,1 млн. человек.

Тем не менее, либеральный период закончился еще до возвращения Владимира Путина в Кремль, и после этого регулирование свелось к введению все новых ограничений, запретов и криминализации прежде вполне легальной деятельности под предлогом защиты традиционных ценностей от внешней угрозы*.

Принято считать, что ужесточение регулирования Рунета и, прежде всего, социальных сетей стало реакцией Владимира Путина на события «Арабской весны». Однако признаки радикального изменения подхода к сетевой активности появились раньше.

Так, 15 июня 2009 года в Екатеринбурге правительства государств-членов Шанхайской организации сотрудничества заключили

* Подробно об ограничении свободы интернета в России можно прочитать в ежегодных [докладах](#) Международной Агоры.

Соглашение о сотрудничестве в области международной информационной безопасности, выразив озабоченность угрозами, которые несет «прогресс в развитии и внедрении новейших информационно-коммуникационных технологий и средств, формирующих глобальное информационное пространство».

Одной из таких угроз названо *«появление и тиражирование в электронных (радио и телевидение) и прочих средствах массовой информации, в сети Интернет и других сетях информационного обмена информации: искажающей представление о политической системе, общественном строе, внешней и внутренней политике, важных политических и общественных процессах в государстве, духовных, нравственных и культурных ценностях его населения».*

Этот тезис, закрепленный в документе, подписанном Правительством России, которое на тот момент возглавлял Владимир Путин, лег в основу всех последующих мер, предпринятых в отношении российского интернета.

Николай Патрушев, секретарь Совета безопасности России: «Интернет и другие современные технологии все чаще применяются в процессе дестабилизации государств для вмешательства в их внутренние дела и подрыва национального суверенитета».

Последовавшая спустя полтора года цепь революций в арабском мире, в которых действительно важную мобилизующую роль сыграли социальные сети Facebook, Twitter и YouTube, должна была убедить российских руководителей в правильности избранного курса.

Примечательно, что примерно с этого же времени Организация Объединенных Наций и ее институты обратились к формулированию и закреплению стандартов свободы слова в интернете и гарантий права на приватность и анонимность. Российское правительство сопротивлялось как могло. Ужесточение национальной цензуры все еще нуждалось в международно-правовом обосновании.

В 2011 году Россия отказалась поддержать Резолюцию «Поощрение, защита и осуществление прав человека в интернете». В ней Совет по правам человека ООН признал *глобальный и открытый характер Интернета, который является одной из движущих сил ускорения прогресса по пути развития в его различных формах.*

Тогда же Россия подготовила и попыталась продвинуть на глобальном уровне проект Конвенции об обеспечении международной информационной безопасности, в которой предлагалось гарантировать свободу обмена информацией *с учетом уважения суверенитета*

государств и их существующих политических, исторических и культурных особенностей, среди основных угроз называлась эрозия традиционных культурных, нравственных, этических и эстетических ценностей.

Предусмотренное проектом право стран-участниц *устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством* стало бы юридической основой для «балканизации» интернета и распада Глобальной сети на замкнутые локальные пространства полностью подконтрольные национальным властям.

В 2016 году российская делегация вместе с Ираном, Китаем и Беларусью [предлагала](#) исключить из обсуждаемого проекта [Резолюции](#) о свободе слова онлайн указание на необходимость правозащитного подхода к регулированию интернета.

Однако после фактического провала попыток изолировать Рунет юридически российские власти попытались решить проблему свободного распространения информации техническими способами.

В июле 2014 года Минсвязи совместно с Минобороны, ФСБ и ФСО провело [учения](#) «по обеспечению устойчивости работы национального сегмента интернета». Официально объявленная цель – «предотвращение деструктивных действий» извне, однако наиболее вероятным сценарием выглядит тестирование технологии блокировки сайтов и фильтрации трафика.

Ранее в 2013 году Минсвязи [опубликовало](#) «Тезисы концепции развития мультисервисных сетей связи РФ», согласно которым осуществлять трансграничную передачу трафика предполагалось разрешить только так называемым «федеральным операторам связи». Для получения подобного статуса, в частности, требовалось иметь собственную коммуникационную инфраструктуру (включая физические каналы связи) в каждом субъекте Федерации, а также не менее двух трансграничных переходов (в Европе и Азии). Очевидно, что таким требованиям даже в среднесрочной перспективе могли бы соответствовать лишь крупнейшие телекоммуникационные компании (прежде всего, государственные Ростелеком и Транстелеком), которые было бы гораздо легче контролировать в экстренной ситуации.

Тогда дальше дискуссии чиновников, экспертов и представителей отрасли дело не пошло, однако исполнительный директор Общества Защиты Интернета Михаил Климарев считает, что идея допуска к

трансграничной передаче трафика только избранных операторов связи в будущем может быть реанимирована для упрощения блокировки сайтов по китайскому или иранскому образцу.

В 2017 году Владимир Путин [утвердил](#) новую Стратегию развития информационного общества, предполагающую *приоритет традиционных российских духовно-нравственных ценностей и соблюдение основанных на этих ценностях норм поведения при использовании информационных и коммуникационных технологий*, а также требующую на международном уровне *отстаивать суверенное право государства определять информационную, технологическую и экономическую политику в национальном сегменте сети «Интернет»*.

Стремление к физической и технологической изоляции Рунета подтверждают и планы Правительства и Минсвязи, анонсированные в национальной программе «Цифровая экономика», принятой на основе Стратегии. Согласно этому [документу](#), к примеру, до 2024 года предполагается до 5% ограничить передачу внутреннего российского интернет-трафика через иностранные серверы.

При этом фактически единственной гарантией безопасности цифровых отношений признается использование российских технологий обработки информации, в том числе российского программного обеспечения и оборудования, а также исключительно национальных криптографических стандартов и технологий защиты информации.

На основе описанных выше подходов и концепций, начиная с 2012 года, в российское законодательство (прежде всего – базовый Федеральный закон «Об информации, информационных технологиях и о защите информации») вносились все новые и новые поправки, направленные на ограничение свободного распространения информации и усиление контроля за теми, кто ее распространяет.

Тогда в России началось массовое ограничение доступа к интернет-сайтам, и к настоящему времени общее число заблокированных ресурсов превысило 10 миллионов. Причем, если первоначально необходимость столь радикальных мер объяснялась стремлением защитить детей от вредной информации, то спустя 6 лет открытый перечень оснований для блокировки включает в себя призывы к участию в митингах, отказ интернет-сервиса сообщить Роскомнадзору контактную информацию, нарушение прав интеллектуальной собственности, рекламу запрещенных к обороту товаров, описание личного опыта дачи взятки и т.п.

Расширение практики блокирования веб-сайтов и интернет-сервисов, в том числе таких популярных ресурсов, как RuTracker.Org (русскоязычный торрент-трекер) и Flibusta (независимая онлайн-библиотека), впервые привело к тому, что пользователи начали активно использовать средства обхода блокировок. К примеру, с 1 ноября 2012 года, когда вступил в силу первый закон о внесудебных блокировках веб-сайтов, до настоящего времени российская аудитория Tor [увеличилась](#) с 20 до 250 тысяч. А после попытки заблокировать Telegram весной 2018 года некоторые VPN-сервисы [сообщали](#) о многократном росте российской аудитории.

[Признавая](#) неэффективность блокировок, российские власти пытаются повлиять на граждан, которые распространяют или ищут «противоправный» контент. Расширяется практика применения антиэкстремистского законодательства в отношении пользователей социальных сетей – увеличивается количество дел, ужесточаются приговоры (до 5 лет лишения свободы за один эпизод).

Статьи 280 (призывы к экстремистской деятельности) и 282 (возбуждение ненависти и вражды) Уголовного кодекса РФ переведены в категорию преступлений средней тяжести, что позволяет избирать меру пресечения в виде содержания под стражей, а также означает увеличение с 2 до 6 лет срока давности привлечения к уголовной ответственности. Большинство обвиняемых по этим статьям также заносят в специальный перечень Росфинмониторинга, в результате чего все их банковские операции по умолчанию блокируются.

Еще одно направление государственной политики – давление на сервисы, прежде всего крупнейшие глобальные платформы, такие как YouTube, Twitter и Facebook, а также интернет-мессенджеры, составляющие серьезную конкуренцию сотовым операторам, однако в отличие от последних, не подключенные к системе перехвата коммуникаций СОРМ. Цель – заставить их выполнять запросы о фильтрации контента и раскрытии личных данных пользователей, а также предоставить доступ к переписке.

Поскольку большая часть интернет-трафика передается в зашифрованном виде, простой перехват его не имеет смысла. В этой связи в 2016 году был принят так называемый «пакет Яровой»* - корпус

* Федеральный закон от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части

поправок в законодательные акты, в частности, обязывающий интернет-сервисы хранить пользовательскую переписку и предоставить Федеральной службе безопасности «информацию, необходимую для декодирования передаваемых и обрабатываемых сообщений». Сервисам также [запрещается](#) разглашать информацию о правительственных запросах.

За отказ зарегистрироваться в специальном реестре Роскомнадзора в 2017 году были [заблокированы](#) сервисы Imo, Line, Blackberry Messenger и интернет-рация Zello, а в 2018 году за отказ предоставить ФСБ доступ к переписке пользователей – мессенджер Telegram.

Фундаментальная причина конфликта – несоответствие претензий органов власти современному уровню развития технологий передачи и защиты информации. Положения «пакета Яровой» и вытекающее из них требование ФСБ предоставить доступ к переписке пользователей Telegram базируются на предположении о том, что оператор сервиса имеет полный доступ к передаваемой с его помощью информации, а следовательно – может при желании поделиться этим доступом со спецслужбой, например, предоставив ключи шифрования или прямой доступ с по выделенному каналу.

Однако то, что было справедливо в XIX веке при прокладке телеграфного кабеля, не применимо к интернет-сервисам, использующим сквозное шифрование. Технология, ставшая фактически «золотым стандартом» отрасли и используемая в разных вариантах всеми крупнейшими интернет-сервисами, предполагает, что ключи шифрования генерируются непосредственно на устройствах пользователей, а, кроме того, как правило, регулярно обновляются.

Однако представители российских телекоммуникационных властей продолжают [настаивать](#) на том, что архитектура сервиса должна быть изменена, чтобы отвечать требованиям российского законодательства.

Помимо «пакета Яровой» в связи с появлением принципиально новых интернет-сервисов в России был принят еще целый ряд ограничительных мер.

установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»

В январе 2017 года поправки, внесенные в Федеральный закон «Об информации...» (т.н. «закон о новостных агрегаторах»)*, вынудили Яндекс [изменить](#) правила сервиса Яндекс.Новости. После того как на новостные агрегаторы возложили ответственность за достоверность публикуемой информации, в топ-5 российских новостей, а также в тематических подборках перестала отображаться информация от незарегистрированных в качестве СМИ новостных ресурсов. Очевидно, что информационная картина дня, которую по умолчанию видят на своих экранах миллионы российских пользователей сервиса, значительно изменилась.

В блестящей книге журналистов Андрея Солдатова и Ирины Бороган [«Битва за Рунет»](#) описывается, в частности, как в 2008-2009 годах администрация президента Медведева пыталась заставить Яндекс исключить из алгоритма подбора новостей оппозиционные сайты, а Владислав Сурков и Константин Костин требовали предоставить им доступ к интерфейсу сервиса и дать возможность влиять на выбор заголовков. Они не хотели (!) поверить в то, что подбор новостей осуществляется автоматически**.

Летом 2016 года, после запуска Netflix в России, министр культуры Владимир Мединский [заявил](#), что сервис используется правительством США, чтобы *«войти ... в каждый дом, залезть в каждый телевизор, а через этот телевизор — в голову каждому жителю Земли»*. Спустя год, в июле 2017 вступил в силу закон об онлайн-кинотеатрах***, согласно которому на популярные «аудиовизуальные сервисы» распространяются ограничения, применимые к средствам массовой информации, в том числе связанные с иностранным контролем. Несоответствие требованиям грозит блокировкой.

За последнее десятилетие структура и формат интернет-коммуникации претерпели революционные изменения, в том числе благодаря появлению сервисов мгновенного обмена сообщениями, сформировавшими к настоящему времени собственную экосистему и в значительной степени перехватившими наиболее активную аудиторию

* Федеральный закон от 23 июня 2016 № 208-ФЗ «О внесении изменений в Федеральный закон Об информации, информационных технологиях и о защите информации и Кодекс Российской Федерации об административных правонарушениях»

** Андрей Солдатов, Ирина Бороган. Битва за Рунет. М., 2016

*** Федеральный закон от 1 мая 2017 № 87-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации»

у «традиционных» социальных сетей, а также вытеснив еще более «традиционные» SMS.

Два миллиарда пользователей WhatsApp, Viber, Facebook Messenger, WeChat, Line, Telegram и других подобных сервисов, благодаря развитию мобильного интернета получившие возможность буквально круглые сутки находиться онлайн, получая информацию из тысяч выбранных ими самостоятельно источников, не только перевернули рынок, но и лишили эффективности привычные средства пропаганды и манипулирования общественным мнением, используемые авторитарными режимами.

По [данным](#) Mediascope, в начале 2018 года только мобильными мессенджерами в России пользовались более 50 млн. человек. Одним из наиболее востребованных свойств мессенджеров стала возможность анонимного общения с помощью зашифрованных сообщений.

Безопасность, анонимность и отказ от произвольного предоставления национальным властям пользовательских данных стали одним из основных

[Александр Бортников](#), директор ФСБ: «Только в минувшем году в России было предотвращено 25 терактов, совершено четыре. Все они координировались через глобальную сеть посредством мессенджеров, в том числе с территории Сирии и Ирака»

конкурентных преимуществ, наряду с удобным интерфейсом и дополнительными опциями вроде стикеров, групповых чатов и публичных каналов.

В этой связи летом 2017 года Роскомнадзор принудительно включил Telegram в реестр организаторов распространения информации, что дало Федеральной службе безопасности основания потребовать от компании-администратора сервиса предоставить доступ к переписке пользователей. Одновременно был принят т.н. «закон о мессенджерах»^{*} - очередные дополнения к Федеральному закону «Об информации», обязывающие сервисы мгновенного обмена сообщениями идентифицировать пользователей по номеру сотовой связи и ограничивать передачу сообщений по требованию властей. Взаимодействие с мессенджерами и организаторами распространения информации должна осуществлять Федеральная служба безопасности, которая, судя по всему, и была [инициатором](#) принятия закона.

^{*} Федеральный закон от 29 июля 2017 года №241-ФЗ «О внесении изменений в статьи 10.1 и 15.4 Федерального закона «Об информации, информационных технологиях и о защите информации»

С весны 2018 года в Госдуме рассматривается «закон о соцсетях»*, согласно которому все популярные сервисы обмена сообщениями должны открыть в России представительства, а также в течение суток по запросу удалять «запрещенную» информацию, идентифицировать пользователей, «не допускать использование публичной сети в целях сокрытия или фальсификации общественно значимых сведений, распространения недостоверной общественно значимой информации под видом достоверных сообщений». Несоблюдение обязанностей является основанием для ограничения доступа к сервису операторами связи. Авторы законопроекта ссылаются на то, что социальные сети в качестве неконтролируемого источника информации, в том числе из-за рубежа, становятся более эффективными, чем традиционные СМИ.

В этом же ряду находятся [поправки](#) в закон об информации, касающиеся ограничения деятельности VPN и анонимайзеров, [попытки](#) заблокировать сервис райдшеринга BlaBlaCar, [закон](#) о локализации пользовательских данных и т.п.

Как видно, российские власти готовы допускать деятельность любых интернет-сервисов при условии соблюдения ими двух ключевых условий – безоговорочное и оперативное выполнение требований по удалению или ограничению доступа к запрещенной информации, а также идентификация пользователей и предоставление всей личной информации, включая переписку, спецслужбам. За неисполнение требований, как правило, предусматриваются штрафы, однако основной механизм давления – блокировка ресурсов. Однако этот план может провалиться в случае появления устойчивой глобальной системы доступа в интернет.

Поэтому еще несколько лет назад, когда стало известно о планах сразу нескольких международных компаний развивать такие системы на основе группировок низкоорбитальных спутников, аэростатов или дронов, угрожающих национальным системам контент-фильтрации, российские власти задумались о [разработке](#) аналога советских «глушилок» радиосигнала.

* Законопроект № 223849-7 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» (в части установления особенностей распространения информации в публичной сети)

Поскольку свободное трансграничное распространение информации рассматривается российскими властями как угроза национальной безопасности, а социальные сети воспринимаются в качестве одного из средств ведения «информационной войны», в борьбе за «цифровой суверенитет» несомненно будут применяться военные технологии. Все современные средства радиоэлектронной борьбы и противоспутниковое оружие будет нацелено в том числе и на глобальный интернет.

Представитель «Ростелеком» на круглом столе в Правительстве: «Компания OneWeb планирует обеспечить доступ в Интернет в любой точке земли, есть такие планы у Samsung и других. У наземных операторов могут появиться проблемы. Если здесь выигрывают иностранные игроки, будут вопросы с суверенитетом. Кто управляет информацией, тот управляет миром»

Медицина и биотехнологии

Одна из наиболее проблемных и конфликтных тем связана с наркополитикой, в том числе с лечением наркотической зависимости, а также применением и доступностью обезболивающих средств.

Не имеющее никакого разумного и логичного объяснения сопротивление введению программ заместительной терапии на фоне официального применения «кодирования» и вспышек принудительного тестирования школьников и студентов, так же как уголовное преследование врачей, выписывающих пациентам болеутоляющие средства и «кетаминные дела» (преследование ветеринаров, использующих препараты кетамина для обезболивания животных) – лишь некоторые примеры карательного подхода, обусловленного отказом воспринимать (а в ряде случаев даже обсуждать) современные практики.

В 2015 году в Госдуму вносился законопроект о принудительном медицинском освидетельствовании несовершеннолетних при наличии неопределенных «видимых признаков наркотического или иного токсического опьянения».

Для частичной либерализации порядка назначения пациентам обезболивающих препаратов понадобилась целая серия самоубийств онкобольных, и громкое уголовное дело врача Алевтины Хориняк, сначала осужденной, а потом оправданной по обвинению в подделке документов и сбыте сильнодействующего вещества в составе организованной группы. Хориняк выписала два рецепта на

приобретение трамадола (опиоидный анальгетик, включенный в Список сильнодействующих веществ). Работавшая в поликлинике терапевтом Хориняк в нарушение инструкции выписала очередной рецепт на обезболивающий препарат, который больной постоянно принимал.

Правовой основой российской наркополитики является Федеральный закон «О наркотических средствах и психотропных веществах», принятый более двадцати лет назад и с тех пор в базовых положениях не менявшийся. Закон, в свою очередь, основан на конвенции ООН о наркотических средствах 1961 года. Он нацелен на «установление строгого контроля за оборотом наркотических средств», «раннее выявление незаконного потребления наркотических средств», «сокращение количества правонарушений, связанных с незаконным оборотом наркотических средств». За исключением формального указания на необходимость обеспечить доступность наркотических средств гражданам, которым они необходимы в медицинских целях, закон не содержит ни одного положения, требующего гуманного отношения к больным, нуждающимся в обезболивании, и применения правозащитного подхода при лечении зависимости.

К примеру, закон помимо абсолютного запрета любого оборота веществ, включенных в Список I (метадон), запрещает также лечение наркотической зависимости средствами, внесенными в Список II (бупренорфин).

Meduza [приводит](#) слова одного из сотрудников представительства ООН в Вене, который подтвердил, что Россия постоянно блокирует любые международные документы, посвященные «пропаганде наркотиков», и тем самым фактически лишает Всемирную организацию здравоохранения запустить глобальную программу помощи странам, желающим реализовать у себя программы снижения вреда.

[Евгений Брюн](#), главный нарколог Минздрава: «В отличие от западной наркологии у нас государство взяло на себя обязательства предоставлять любую наркологическую помощь любому больному. На Западе за каждого больного кто-то должен заплатить. И это создает массу проблем»

При этом заместительная поддерживающая терапия с использованием метадона и бупренорфина [считается](#) одним из наиболее эффективных методов лечения опиоидной зависимости и применяется в десятках стран мира. На 2017 год это лечение получают более миллиона человек с опиоидной зависимостью. Заместительная терапия доступна и применяется во всех странах Европы, в США, Канаде, Австралии, Китае,

Иране, Юго-Восточной и Центральной Азии, в ЮАР. В странах бывшего СССР она доступна в 12 из 15 республик. Запрещена только в России, Туркменистане и Узбекистане.

Кстати, власти Узбекистана [обосновывают](#) фактический запрет метадонной терапии тем, что она «противоречит национальным интересам и менталитету узбекского народа».

После аннексии Крыма весной 2014 года без доступа к заместительной терапии на полуострове остались более 800 человек. По [оценкам](#) экспертов ООН, около сотни из них могли погибнуть уже несколько месяцев спустя.

Представители медицинских и полицейских властей неоднократно заявляли, что медицинское назначение наркозависимым людям метадона не имеет отношения к лечению и в России никогда

[Виктор Иванов](#), руководитель расформированной Федеральной службы по контролю за оборотом наркотиков: «Метадоновые программы внедряются за гранты от разных неправительственных зарубежных организаций. Кажется, что псевдолечение бесплатное. Но когда люди крепко «подсядут» на эту дрянь, финансирование заканчивается»

применяться не будет. Именно поэтому недавнее [высказывание](#) заместителя руководителя Федеральной службы исполнения наказаний Анатолия Рудого о необходимости внедрения программ заместительной терапии вызвало столь бурную реакцию. Никто просто не ожидал такого от представителя одного из самых консервативных учреждений страны.

Судя по всему, в ряде случаев ограничения разработки и использования медицинских и биотехнологий обусловлены идеологически.

К примеру, отдельный [раздел](#) Основ социальной концепции Русской православной церкви посвящен биоэтике, в которых РПЦ выступает не только против абортов и контрацепции, но признает недопустимыми целый ряд медицинских технологий, связанных с искусственным оплодотворением, в том числе ЭКО, суррогатным материнством, донорством и эвтаназией.

Учитывая, насколько глубоко РПЦ интегрирована в различные государственные структуры, влияние ее представителей на принятие решений в этой сфере может в некоторых случаях иметь определяющее значение.

К примеру, не смотря на то, что формально законодательного запрета абортов или [выведения](#) процедуры искусственного прерывания беременности из системы обязательного медицинского страхования

добиться не удалось, Министерство здравоохранения на федеральном и региональном уровнях продвигает различные [инициативы](#), направленные на затруднение доступа к абортам.

Вот еще один пример, явно обусловленный влиянием религиозных соображений. В июле 2016 года Владимир Путин

Патриарх [Кирилл](#): «Все это ведет в сторону расчеловечивания, гипертрофированной индивидуализации, а значит - разрушению социума и концу истории»

подписал Федеральный закон N 358-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части совершенствования государственного регулирования в области генно-инженерной деятельности». Совершенствование регулирования свелось в итоге к наделению Правительства РФ полномочиями по ограничению ввоза в страну генно-модифицированных организмов, установлением административной ответственности за оборот и использование генно-инженерно-модифицированных организмов, не прошедших государственную сертификацию, а также полным запретом выращивания и разведения генетически модифицированных растений и животных.

Слежка и контроль

Есть, впрочем, сфера, в которой инновации всячески поощряются государством. Это слежка за гражданами, цензура и манипулирование общественным мнением.

В [докладе](#) «Россия под наблюдением 2017: как власти выстраивают систему тотального контроля за гражданами» мы описывали развитие технологий массовой слежки, включающей в себя сбор, хранение и обработку биометрической информации, видеонаблюдение и идентификацию граждан, мониторинг интернета и перехват коммуникаций.

Одна из ключевых общемировых тенденций развития информационных технологий последних лет – «интернет вещей» (IoT) - для российских властей прежде всего является способом усовершенствовать слежку за гражданами. Так, по результатам исследования компании iKS-Consulting и оценкам Национального исследовательского института технологий и связи, государственные закупки [составляют](#) до 80% всего российского оборота IoT, причем 90% из них приходится на финансирование систем безопасности, прежде всего – АПК «Безопасный город», в основе которой лежит распределенная сеть камер видеонаблюдения.

Начиная с 2015 года, в рамках системы «Безопасный город» по всей стране – прежде всего на транспортных узлах и спортивных объектах – активно [устанавливаются](#) системы видеонаблюдения, включающие к настоящему времени сотни тысяч видеокамер, которые постепенно оснащаются функцией распознавания лиц. Только в Москве установлено более 100 тысяч таких камер, а бюджет программы составляет почти 200 млрд рублей.

Видеомониторинг с распознаванием лиц [используется](#) полицией на протестных мероприятиях – чтобы попасть на территорию митинга, необходимо пройти через рамку металлодетектора, на котором установлена камера видеонаблюдения.

Российские власти явно заинтересованы в развитии подобных технологий – поощряют отечественных разработчиков и привлекают зарубежных. К примеру, *Meduza* недавно [заметила](#), что единственное европейское представительство китайской государственной корпорации CEIEC, занимающейся разработкой и экспортом систем электронной слежки, расположено в Москве.

В 2013 году компания «Вокорд СофтЛаб» получила 20-миллионный грант от Фонда «Сколково» на реализацию проекта по созданию системы распознавания лиц. «Технология позволяет проводить биометрическую авторизацию при доступе в помещения, искать людей в толпах и т.п.» - [говорится](#) на сайте Фонда.

Только за последние месяцы тендеры на закупку специального программного обеспечения объявляли органы внутренних дел [Тверской](#), [Ивановской](#), [Московской](#) областей, [Пермского](#) края и [Хакасии](#). Стандартное техническое задание содержит требования о том, что сбор данных пользователей должен осуществляться с детализацией до уровня малых населенных пунктов в ретроспективе, начиная с 2006 года, с возможностью ежесуточной автоматической актуализации контента и метаданных пользователей, а также постоянного хранения всей информации, включая удаленные материалы.

Ранее об использовании автоматической системы мониторинга СМИ для выявления экстремистского и прочего запрещенного контента [объявлял](#) Роскомнадзор, который также [использует](#) программный комплекс «Ревизор» для контроля выполнения операторами связи обязанностей по блокировке сайтов из «черных списков».

Ради возможности усилить контроль или упростить слежку российские власти готовы искусственно поддерживать устаревающие технологии и

требовать этого от разработчиков, как в случае с интернет-мессенджерами, использующими сквозное шифрование.

В августе 2018 года СМИ сообщили о проекте приказа Минсвязи, обязывающие заменить абсолютно все sim-карты российских операторов на «симки» нового образца – использующие российскую криптографическую защиты и сертифицированные ФСБ. Причем повторять эту процедуру предлагалось ежегодно. Позже [сообщалось](#), что разработка приказа временно приостановлена. История очень показательна – в то время как мир постепенно [отказывается](#) от физических sim-карт, Россия готова потратить миллиарды ради призрачной защиты от воображаемой угрозы.

Точно так же прокуратура [требует](#) запретить материалы, размещенные в ранее запрещенном и, по утверждению Роскомнадзора, заблокированном на основании судебного решения Telegram. При покупке билета на самолет вы предоставляете все свои паспортные данные, которые мгновенно попадают в базу «Розыск-Магистраль», а в аэропорту проходите несколько сканеров, попадаете в объектив видеокамеры, подключенной к системе распознавания лиц, однако на предварительно распечатанный посадочный талон вам должны поставить размазывающейся краской штамп контроля авиационной безопасности.

С другой стороны, усилия властей по аккумулярованию разнообразной личной информации в государственных базах данных в сочетании с коррупцией и игнорированием минимальных стандартов безопасности хранения данных приводят к таким курьезным историям, как [разоблачение](#) сотен агентов главной военной разведки журналистами. Причем именно тех агентов, чья деятельность – хакерские атаки – казалось бы предполагает особо тщательное отношение к вопросам кибербезопасности.

Очевидная причина крупнейшего провала в истории – архаичный взгляд руководителей государства и спецслужб на мир и их отказ признать реальность того, что новые технологии меняют окружающую действительность.

Заключение

В 2011 году правительство России [утвердило](#) Стратегию инновационного развития Российской Федерации на период до 2020 года. В ней, в частности, отмечается, что ни частный, ни государственный сектор не проявляют достаточной заинтересованности во внедрении инноваций.

Одна из причин государственного устарения – страх перед технологиями, не поддающимися контролю. Рост и развитие наблюдаются как правило в отдельных отраслях, не привлечших пока государственного интереса либо в редкие периоды либерализации, как произошло, например с регулированием интернета и развитием электронного правительства и государственных услуг при Дмитрии Медведеве.

Приведенные выше эпизоды – лишь некоторые примеры такого подхода. В этом же ряду сложности с регистрацией и сертификацией лекарственных средств, приводящие к регулярным перебоям в поставках жизненно-необходимых лекарств и вакцин, противоречивое отношение к криптовалютам, выражающееся в метаниях от прокурорских [предложений](#) запретить «денежные суррогаты» и ввести ответственность за их оборот до [надежд](#) заработать на майнинге и [идей](#) использовать биткойн для обхода международных санкций, и многое другое.

Всемерное поощрение российскими властями традиционализма и обскурантизма, маргинализация либеральных концепций развития рыночной экономики, гражданских и политических свобод явно препятствуют догоняющему развитию в сфере технологий. В результате, попытки введения всеохватного государственного контроля, создание системы разнообразных «Роснадзоров» и культивирование неприятия прогресса не только подавляют развитие публичной сферы, гражданского общества, медиа, но и создают труднопреодолимые барьеры на пути экономического развития.



Дамир ГАЙНУТДИНОВ
кандидат юридических наук,
правовой аналитик Международной Агоры



Павел ЧИКОВ
кандидат юридических наук,
руководитель Международной Агоры



Международная правозащитная группа Агора – объединение десятков юристов из нескольких стран, специализирующихся на правовой защите гражданских свобод на постсоветском пространстве