Текст · 4 февраля 2020, 07:37
Давид Френкель,

Контроль, цензура и изоляция. Российская власть против интернета: итоги 2019 года

В России сохранилась тенденция на установление государственного контроля над интернетом, констатируют правозащитники: вступили в силу законы об «изоляции интернета», «фейковых новостях» и «неуважении к власти», от официальных лиц звучали угрозы блокировки *VPN*-сервисов, социальных сетей *Twitter* и *Facebook* и даже окончательной и бесповоротной блокировки мессенджера *Telegram*. Новые тенденции: распространение практики региональных и локальных шатдаунов — отключений доступа к интернету на определенной территории по требованию государства — усиление давления на *IT*-бизнес, в том числе с помощью уголовных дел, а также первая в истории российского интернета цензура компьютерной игры.

Политические шатдауны

Хотя федеральный закон «О связи» разрешает приостановку услуг связи для обеспечения безопасности или для осуществления оперативно-разыскной деятельности, систематически и в политических целях эта возможность стала использоваться только в 2019 году.

По требованию ФСБ мобильный интернет отключался во время митингов в Ингушетии против передачи части территории республики Чечне. Подобные же отключения зафиксированы в Шиесе во время протестов против строительства мусорного полигона и в Улан-Удэ во время митингов за отмену результатов выборов мэра. Впервые подобные отключения затронули и Москву во время летних протестов против недопуска независимых кандидатов на выборы в Мосгордуму.

Были зафиксированы и локальные ограничения, например, журналисты жаловались на отключение связи в Люблинском суде во время допроса одного из ключевых свидетелей обвинения по делу «Нового величия».

Уголовные дела

Авторы доклада отмечают, что в 2019 году резко снизилось число случаев уголовного преследования за действия в интернете: с 384 дел в 2018 году до 200 в 2019-м. При этом количество осужденных на реальное лишение свободы уменьшилось незначительно: с 45 до 38 приговоров. Основным фактором снижения числа дел правозащитники называют частичную декриминализацию статьи 282 УК (возбуждение ненависти), после которой она практически перестала применяться: число приговоров по первой части статьи снизилось практически в десять раз.

Самым заметным примером применения 282-й статьи стало дело менеджера Владислава Синицы — суд приговорил его к 5 годам лишения свободы за

резкий комментарий в твиттере о детях силовиков, участвовавших в избиениях демонстрантов в Москве.

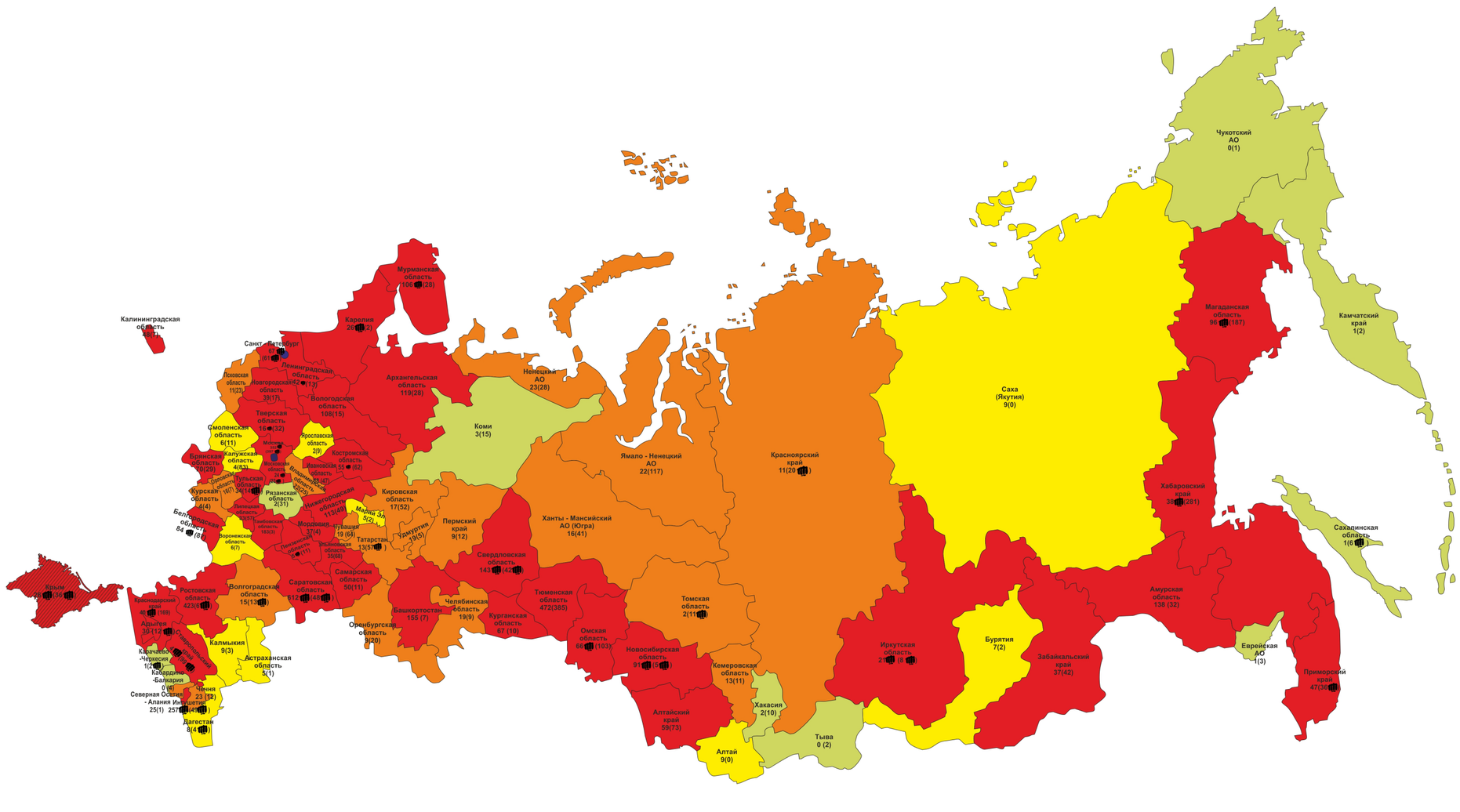
Запрет связанной с работой в интернете деятельности стал использоваться как дополнительное наказание для осужденных активистов — так, студенту-блогеру Егору Жукову, осужденному за свои видеоролики на 3 года условно, суд дополнительно запретил администрировать страницы в сети в течение двух лет. Используется это и как мера пресечения — Роману Удоту из «Голоса», который попал под уголовное преследование из-за конфликта с журналистами НТВ, суд заменил домашний арест на запрет пользоваться интернетом и мобильной связью.

Уголовные дела стали использоваться и для давления на *IT*-бизнес и программистов, отмечается в докладе. Так, 12 декабря 2019 года в рамках уголовного дела о нарушении авторский прав прошел обыск в московском офисе компании-разработчика веб-сервера *NGINX*[1]. Основателей компании Игоря Сысоева и Максима Коновалова задержали и после многочасового допроса отпустили в статусе свидетелей, изъяв мобильные телефоны. Заявление подала компания *Rambler*, утверждавшая, что Сысоев создавал *NGINX* в то же время, когда работал в компании, а значит, все права на результат его деятельности принадлежат бывшему работодателю. Коновалов в разговоре с РБК назвал произошедшее рейдерским захватом компании. Крупнейшие российские *IT*-компании выступили в поддержку создателей *NGINX*, после чего *Rambler* отказался от своих претензий.

В качестве еще одного примера подобного давления авторы доклада приводят уголовное преследование бывшего замминистра связи России и одного из основателей российского сегмента интернета Алексея Солдатова. Против него и еще двух предпринимателей возбудили уголовное дело по статье 159 УК(мошенничество), обвинив в организации схемы по выводу за рубеж 470 тысяч IPv4-адресов[2], которые ранее администрировал Российский научно-исследовательский институт развития общественных сетей (РосНИИРос).

«Эксперты предполагают, что причиной уголовного преследования мог стать отказ Солдатова передать государству контроль над доменной зоной *.su*, которая в рамках суверенизации Рунета должна стать частью национальной доменной зоны», — отмечается в докладе.

Карта ограничения свободы интернета в 2019 году



- 0-3 факта (относительная свобода)
- 4-9 фактов (тревожная тенденция)
- Территория Крымского полуострова включена в настоящий мониторинг, поскольку фактически контролируется властями Российской Федерации
- 10-29 фактов либо реальное лишение свободы (систематическое давление)
- 30 и более фактов или применение насилия (серьезное давление)
- ( ) - в скобках приведены данные за 2018 год
- отмечены факты насилия

Административные дела

В докладе особое внимание уделяется новой статье 20.3.1 КоАП (возбуждение ненависти либо вражды), которая появилась в начале 2019 года в результате частичной декриминализации статьи 282 УК — теперь уголовная ответственность наступает лишь в том случае, когда человек в течение года был уже привлечен по этой административной статье.

Только в первом полугодии 2019-го было привлечено к ответственности по этой статье 158 человек (из них — 138 оштрафовали, девять попали под административный арест, 11 получили обязательные работы). Правозащитники отмечают короткие сроки рассмотрения и неопределенность со сроками давности привлечения к ответственности и ожидают увеличения числа дел по этой статье.

Еще одной популярной статьей в 2019 году стала часть 3 статьи 20.1 КоАП, которая наказывает за неуважение к власти в сети — в законе это описывается как распространение в интернете информации, выражающей явное неуважение к обществу, государству, официальным государственным символам, Конституции или органам государственной власти. Чаще всего эта статья используется против тех, кто грубо отзывался о Владимире Путине в социальных сетях (44 из 78 дел в 2019 году).

Регулирование интернета

«В 2019 году мы насчитали 62 различных предложения по регулированию интернета, в том числе уже принятые нормативные правовые акты, включающие в себя не только дополнительные

основания запрета информации, но и санкции в отношении пользователей, новые обязанности *IT*-компаний, а также меры по централизации интернет-трафика», — пишут авторы доклада.

Среди нововведений они указывают на вступившие в силу пакеты законов о «фейковых новостях» и о «неуважении к власти», предусматривающие, помимо прочего, блокировку интернет-ресурсов, а также закон, позволяющий признавать иностранными агентами не только некоммерческие организации, но и отдельных граждан.

Кроме того, в 2019 году были увеличены штрафы за распространение контента: например, за повторное нарушение «владельцем аудиовизуального сервиса» — в их число закон включает, например, онлайн-кинотеатры и стриминговые платформы — порядка распространения информации среди детей (статья 13.36 КоАП, до 1 млн рублей для юридических лиц), распространение призывов к терроризму или экстремизму (статья 13.37 КоАП, до 5 млн рублей для юридических лиц), а для поисковых систем — за повторное нарушение запрета на выдачу ссылок на сайты с запрещенной информацией (13.40 КоАП, до 5 млн рублей для юридических лиц).

Однако главным законом в сфере регулирования интернета эксперты считают закон «о суверенном интернете», предусматривающий установку технических средств противодействия угрозам (-*DPI*[3]), создание центра мониторинга и управления сетями связи общего пользования, ориентацию на отечественные методы криптографии

и национальную систему доменных имен. Ключевой проблемой закона в докладе названа неопределенность тех угроз, от которых он призван защищать. В качестве примера приводится мессенджер *Telegram*, работа которого может рассматриваться властями как угроза получения гражданами доступа к запрещенной информации.

Цензура

«За девять месяцев прошлого года Роскомнадзор по собственной инициативе, а также по решениям МВД, Федеральной налоговой службы, Генеральной прокуратуры, Роспотребнадзора, судов и ряда других ведомств включил в реестры запрещенных ресурсов больше 270 тысяч сайтов и указателей страниц — это почти на треть превышает аналогичные показатели 2018 года. На 100 тысяч больше поручений было направлено операторам связи для ограничения доступа к ресурсам», — констатируется в докладе.

Авторы отмечают, что одновременно с этим под блокировку попадают более 4.74 миллионов сайтов, которые сами по себе не заблокированы, но находятся на внесенных в реестр блокировки IP-адресах.

Среди примеров блокировок в докладе приведены не только российские ресурсы, но и блокировка норвежского издания *Barents Observer*, часть материалов которого выходит на русском языке. Блокировкам подверглись и сервисы защищенной электронной почты, например, *Protonmail*.

Роскомнадзор провел как минимум две кампании по блокировке ресурсов: одна коснулась около

тысячи публикаций, посвященных отношениям президента государственного банка ВТБ Андрея Костина и сотрудницы ВГТРК Наили Аскер-заде, другая затронула публикации в СМИ на тему наркотиков, ограничения коснулись таких изданий как *Meduza*, *Baza*, *The Village* и «Батенька, да вы трансформер».

Неоднократно подвергались блокировкам публикации об обходе блокировок, а издание «Фергана» было полностью заблокировано за материал с информацией о самоубийствах.

С одной стороны, замечают правозащитники, в России пока нет запрета на использование методов обхода блокировок и люди активно ими пользуются, с другой стороны, в 2019 году Роскомнадзор впервые разослал десяти *VPN*-компаниям требование о фильтрации трафика. Большая часть *VPN*-сервисов, за исключением *Kaspersky Lab*, ответила отказом.

«Инструмент политической борьбы»

Подводя итоги, авторы доклада отмечают, что «чиновники перестают считать ограничение свободы слова исключительной мерой, применяемой в крайних случаях, рассматривая блокировки сайтов, преследование пользователей и ограничение прав российских и зарубежных СМИ как инструмент политической борьбы и способ противостоять Западу в информационной войне».

«Власти после ряда колебаний несколько лет назад определились с основным вектором политики в отношении российского сегмента интернета —

контроль, цензура и изоляция», — констатируют они. Конечной целью властей, по мнению авторов, является «создание суверенного интернета наподобие китайско-северокорейского», и в 2019 году были приняты «ключевые нормативные акты в этом направлении».

Правозащитники ожидают, что вслед за подготовкой возможной изоляции российского сегмента интернета будет усилено и давление на интернет-бизнес, причем не только на российский, но и зарубежный, с тем, чтобы принудить его к сотрудничеству. Они предполагают, что это затронет и аполитичные сервисы и компании.

Главным вопросом остается, что из запланированного удастся осуществить российским властям, говорится в докладе. Сейчас новые инициативы либо не исполняются (хранение и расшифровка трафика из «пакета Яровой»), либо не достигают цели или обходятся (как, например, блокировка телеграма и многочисленных сайтов), а технологии постоянно развиваются, расширяя возможности пользователей в борьбе с ограничениями.

Редактор: Егор Сковорода

---

1. NGINX — один из наиболее распространенных веб-серверов в интернете, он был разработан программистами из России и в марте 2019 года продан американской компании F5 за $670 миллионов.

2. Это наиболее широко распространенная в интернете версия IP--адресов, общее число которых ограничено четырьмя миллиардами. На сегодняшний день все свободные адреса в Европе и многих других

регионах исчерпаны, в связи с чем разработана новая версия — IPv6 — в которой на каждого жителя Земли приходится около 300 млн IP-адресов.

3. DPI — Deep Packet Inspection — метод анализа трафика в интернете, использующий не только заголовки пакетов с данными, но и их содержимое. Применяется для блокировки или переадресации запросов, например, если заголовки пакетов недоступны, как в случае с шифрованным HTTPS-трафиком.