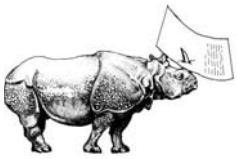

Александра Куликова

# О ФРАГМЕНТАЦИИ ИНТЕРНЕТА: СТАРЫЕ ВОПРОСЫ И НОВЫЕ ВЫЗОВЫ

Последние законодательные инициативы в Российской Федерации, касающиеся запрета на хранение персональных данных россиян за пределами РФ, необходимости хранить метаданные о коммуникациях пользователей в течение как минимум 6 месяцев, а также дискуссия о возможности дублирования корневых структур сети для устойчивости Рунета, часто обсуждаются в русле опасений о нарастающей фрагментации интернета. Такая деятельность многим экспертам видится как некое покушение на *единый и открытый* интернет.

С одной стороны, попытки подогнать киберпространство под цели и задачи различных участников функционирования в нем — процесс, который начался не вчера, и Россия в нем далеко не пионер. Важно помнить, что и интернет едва ли когда-то был неделимым и универсальным, что только подчеркивает постепенно усложняющиеся отношения между его пользователями. Россия же сравнительно недавно заняла ощутимо активную позицию в национальном и глобальном управлении интернетом и сразу на всех уровнях, как в лице государственных органов, так и на уровне бизнеса и институтов гражданского общества и др. Учитывая несбалансированность взаимодействия этих групп внутри страны и разногласия с международными участниками глобального управления интернетом, пожалуй, лучшей иллюстрацией к создавшейся ситуации могла бы послужить басня И. А. Крылова *Лебедь, рак и щука.* И все же нельзя не заметить рост запретительных мер в онлайн-пространстве по инициативе властей, что и приводит в конечном итоге к формированию особых правил жизнедеятельности Рунета в глобальном интернете.

С другой стороны, недавние события, связанные с проявлением экстремизма в Европе, а также с глобальными киберугрозами, диктуют новые реалии и толкают различные государства, ранее не поддерживавшие активное регуляторное вмешательство в онлайн-сферу, к решениям, мотивированным именно государственными интересами и ограничивающим гражданские свободы в интернете.

Ввиду этих развитий стоит еще раз переосмыслить понятие *фрагментация интернета*, которое до сих пор использовалось именно в контексте управления онлайн-контентом и именно в отношении стран с более жестким законодательством в этой области.

## О ЧЕМ МЫ ГОВОРИМ?

В рассуждениях о фрагментации интернета есть тенденция к идеализации того, чем он якобы был раньше. Так, Тим Бернерс-Ли (Tim Berners-Lee), один из отцов-основателей мировой паутины, говорит о том, что хотел бы видеть сеть «открытой,

работающей по всему миру так хорошо, как это только возможно, и не подчиняющейся национальным принципам», упоминая, в частности, стремление Бразилии к национализации персональных данных как пример ситуаций, которых следует избегать. Однако процесс фрагментации начался не вчера, и едва ли интернет был универсален для всех даже в начале своего развития. В том его сила, что с эволюцией функционала киберпространства, интернет проник буквально во все области человеческой жизни, служа тем самым очень разным целям и задачам. Фрагментация — это процесс, сопутствующий адаптации интернета к этим целям различных заинтересованных сторон, а их вовлеченность в процесс управления и развития интернета также значительно изменилась — от полного безразличия до заявок на лидерство в этой роли. Так, например, значительно возрос интерес правительств разных стран к использованию национального сегмента интернета для внутриполитических целей. Концентрация персональных данных пользователей по всему миру в руках небольшого числа глобальных компаний, базирующихся в основном в США и работающих в различных юрисдикциях, создает феномен государства в государстве, а значит, не минуем конфликт интересов, что, в частности, продемонстрировал скандал вокруг разоблачений Эдварда Сноудена.

Сама сеть неоднородна, соответственно и фрагментация также не едина и выражается различными процессами в разных *слоях* интернета. В академическом и техническом сообществах принято несколько схем уровневого строения интернета. Наиболее развернутый эталонный вариант — это базовая система взаимодействия открытых систем, сетевая модель OSI, состоящая из семи уровней. Тим Бернерс-Ли в 2000 г. в своей книге *Weaving the Web* предложил несколько упрощенный вариант системы сетевой архитектуры из всего четырех уровней: уровень передачи, компьютерный уровень, уровень программного обеспечения и контента. Обе системы характеризуют функциональные свойства сети, а для удобства их регуляторного осмысления часто используется схема архитектуры сети, предложенная профессором Гарвардской школы права Йохаи Бенклером (Yochai Benkler) в статье *From Consumers to Users*, состоящая из трех уровней: физического, логического и контентного. Аналогичную систему предлагает его коллега Лоуренс Лессиг (Lawrence Lessig) в своей книге *Future of Ideas* (находится в свободном доступе под Creative Commons), переформулировав уровни как физический, уровень кода и контента. Лессиг, основатель *Creative Commons*, приверженец открытых систем, знаменит своей формулой регулирования интернета, гласящей, что код есть закон (*Code is law*), т. е. регулирование в интернете коренится в кодовом инфраструктурном уровне (с учетом того, что физический остается неизменным), даже если конечная цель регуляторного вмешательства — контентный уровень. Иначе говоря, если, например, правообладатель видео- или аудиоконтента обращается к *Google* с требованием снять какой-либо ролик с *YouTube*, ссылаясь на положения DMCA[1], оно может быть удовлетворено через обращение к программным инструментам. Таким образом, регулирование на более высоких уровнях обеспечивается снизу вверх — через управление базовыми уровнями, причем принцип сверху вниз работать не будет: изменение контента не влияет на логический уровень или корневые структуры интернета.

Профессор Джонатан Зиттрейн (Jonathan Zittrain), директор Центра интернета и общества имени Беркмана при Гарвардском университете, визуализирует устройство сети в виде песочных часов, которые могут состоять из различных слоев, как было указано выше, от физического до содержательного. Но главное — это *талия* часов, уровень IP-протоколов, обеспечивающих одновременно относительную автономность и взаимосвязь базовых и верхних уровней. Это механизм передачи данных, он универсален и мало подвергается инновационному развитию и пересмотру как физическая инфраструктура или уровень приложений и контента. Этим обеспечивается принцип генеративности сети (generativity) — ее «способности к непредсказуемым (‘*unfiltered*’) переменам, благодаря неограниченному участию в ее развитии широкого спектра участников»[2]. Генеративность

лежит в корне бурного развития уровня приложений, но она же является причиной формирования закрытых систем типа Apple, например, с целью обеспечения безопасности пользователей и защиты информации, что сложно сделать в открытых системах. Иными словами, в силе генеративности лежит ее же слабость, как мы увидим ниже.

Таким образом, разговор о фрагментации/сегментации/*балканизации* следует начинать с уточнения уровня, о котором идет речь. Если мы говорим о физическом уровне, к примеру, до недавнего времени процессы дробления DNS-системы на национальные языковые сегменты скорее говорили о развитии и диверсификации сети, включения все большего количества пользователей и доступности для языковых меньшинств. Впрочем, это в целом позитивное развитие также используется для решения внутриполитических задач сообществ, получающих национальные языковые домены, связанных с укреплением государственности. Языковая локализация национальных сегментов в свою очередь также часто видится инструментом большего контроля над цифровыми коммуникациями в данных сообществах.

На логическом уровне, например, в США продолжаются баталии вокруг так называемой сетевой нейтральности (*net (work) neutrality*)[3], несмотря на то что в начале 2014 г. в Штатах было вынесено судебное решение, по сути, положившее ей конец, позволив провайдерам связи брать дополнительную плату с интернет-сервисов за высокоскоростной трафик. Противники дифференцированного подхода к трафику обеспокоены делением инфраструктурных мощностей интернета по принципу *paywall*: для тех, кто может платить больше, и для всех остальных, — а также тем, что более мелкие игроки не смогут конкурировать в доступе к высоким скоростям с такими гигантами, как *YouTube*. Аналогичные ограничения доступа к контенту могут появиться и для некоторых групп пользователей, потому что для них определенный контент, скорее всего, в таком случае станет дороже. Это могло бы стать реальностью уже в 2014 г., если бы не беспрецедентный общественный протест, в результате которого президент Барак Обама лично выступил в ноябре 2014 г. в поддержку принципа сетевой нейтральности ('Obamacare for the Internet', как выразился техасский сенатор Тед Круз), что неожиданно стало важным козырем в его в остальном ослабевшей политической повестки дня.

Другое решение в мае 2014 г., уже Европейского суда, признало за гражданами ЕС давно обсуждаемое *право на забвение* (*right to be forgotten*), обязующее *Google* удалять из результатов поисковой машины информацию, не соответствующую или переставшую соответствовать действительности по запросу граждан через специальную форму. Следует все же уточнить, что данная информация при этом не стирается из самой сети и может быть найдена на соответствующих страницах. Но данный прецедент, с одной стороны, подчеркивает, насколько наш доступ к определенной информации определяется поисковиками[4] (причем в основном первой-второй страницами), а с другой стороны, фрагментирует уровень контента тем, как обрабатывается информация о гражданах ЕС в отличие от остальных пользователей сети.

До сих пор активные действия российских властей по регулированию онлайн-пространства последовательно критиковались интернет-либертарианцами как приводящие к *балканизации* интернета и разрушающие его единство. Хотя большинство мер, предпринятых в России, так или иначе уже были опробованы другими странами (из последних, например, дифференциация трафика, предложенная ФАС с учетом мирового опыта). Некоторая уникальность российского кейса состоит, пожалуй, в том, что наступательное движение началось всего пару лет назад и стремительно охватило практически все системные уровни интернета. Точкой отсчета в его легитимации является принцип верховенства роли государства в области глобального управления интернетом в целом и российской юрисдикции в отношении национального сегмента сети в частности.

Россия не первой стала добиваться суверенности национального сегмента — в мире не первый день существует *Великий китайский файрвол (the Great Firewall of China)*, где *Google* перестал бороться с фильтрацией своего сервиса еще в 2009 г., но занимается этим планомерно при малоэффективных рычагах продвижения интересов ИКТ-индустрии, в отсутствие механизмов саморегулирования и при слабости общественных организаций. Не углубляясь в исторические предпосылки такой архитектуры решения вопросов общественной важности, стоит заметить, что многие процессы в области интернета, запущенные в России за последние 2–3 года, во многих европейских странах действуют в порядке саморегулирования соответствующих бизнес-сегментов при участии институтов гражданского общества.

Внешнеполитическая конъюнктура, в последнее время определяемая украинским конфликтом, на первый план выносит вопросы национальной безопасности, что плотно увязывается властями с информационной, собственно цифровой безопасностью и безопасностью критической инфраструктуры. Таким образом, решение внутриполитических задач после осознания стремительно возрастающей роли ИКТ-сектора в жизни и развитии общества требует максимального над ним контроля — цель, требующая легитимации и в плоскости глобального управления интернетом. Поэтому учения по выявлению уязвимостей Рунета летом 2014 г., выводы о необходимости защитных мер, а возможно, и о создании структур, дублирующих корневые, на территории России, планы по передаче функций Координационного центра национального сегмента интернета госструктурам создают фундамент для главенствующей роли государства в управлении интернетом на своей территории. Этакая *крымизация Рунета* на физическом уровне. Министр коммуникаций Н.А. Никифоров в очередной раз озвучил соответствующую позицию России относительно глобального управления интернетом на Полномочной конференции Международного союза электросвязи.

Этой же позицией подкрепляется закон о необходимости локализации хранения персональных данных россиян, а также *закон о блогерах*, предусматривающий хранение метаданных в течение как минимум 6 месяцев. Декларируемые задачи обеспечения национальной безопасности в самом широком смысле, в том числе в киберпространстве, инспирировали ряд законодательных актов, требующих фильтрации и блокировки определенного контента в доступе россиян (пропаганда экстремизма, терроризма, детская порнография и т. п.), разрабатываемые требования к идентификации в интернете. Им предшествовал первый из серии ограничений антипиратский закон, действие которого было расширено на авторские права в литературе, музыке, программном обеспечении и других сферах, кроме фотографии, в ноябре 2014 г. и который вступит в силу с 1 мая 2015 г. Взятые все вместе, эти ограничения на уровне контента (исполняемые, разумеется, через логический уровень кода) теоретически создают пользовательский опыт в интернете, отличный от получаемого в других географических точках, что и позволяет говорить о дальнейшей фрагментации интернета. Впрочем, выстраиваемая система не герметична благодаря появляющимся техническим решениям обхода запретов — пока, по крайней мере, базовый, физический уровень архитектуры сети находится под распределенным контролем.

## ГРАЖДАНСКИЕ СВОБОДЫ vs БЕЗОПАСНОСТЬ: НОВЫЕ ПРАВИЛА ИГРЫ?

В свете всего вышесказанного важно отметить, что последние мировые события внесли свои коррективы в возможные сценарии развития глобального Интернета и национальных сегментов, что позволит говорить о фрагментации онлайн-контента, а возможно, и физической инфраструктуры, уже на новом качественном уровне.

Как известно, ранее вопросом *суверенности данных* после разоблачений Эдварда Сноудена об электронной слежке уже озаботились и Германия, и Бразилия, и прочие страны. Под лозунгом борьбы с глобальной электронной слежкой соз-

даются те же самые автономные системы, об уязвимости которых говорит Джонатан Зиттрейн, уже на национальном уровне и в ущерб глобальности бизнесов интернет-гигантов, которые стали к настоящему моменту *суверенами сети*, по терминологии Ребекки МакКиннон. Их же ответ на кризис доверия в сети — еще более замкнутые системы: так, Apple и Google по умолчанию вводят шифрование данных на девайсах. Развитие криптографии — это естественная реакция на почти неограниченный доступ к данным пользователей во многих государствах, что также способствует фрагментации.

*Дискурс приватности* доминировал как в европейских, так и в американских общественных дискуссиях последние 2 года после первой утечки сведений о деятельности Агентства национальной безопасности, призывая к большей соразмерности усилий по обеспечению безопасности, предпринимаемой властями различных стран, стандартам защиты гражданских прав. Но некоторые события вновь вынесли на первый план вопросы безопасности граждан, дав соответствующим ведомствам новый рычаг для лоббирования расширения своих полномочий.

Так, как стало очевидно после террористической атаки на редакцию *Charlie Hebdo* в Париже, некоторые европейские государства, в первую очередь Франция и Великобритания, готовы пересмотреть свою политику регулирования онлайн-пространства в национальных сегментах интернета для повышения эффективности антитеррористических мер. По иронии, предлагаемые меры повышенной слежки за цифровыми коммуникациями и принятие мер по идентификации в интернете очень созвучны российскому законодательству в этой области последних лет, т. е. тем самым требованиям по хранению метаданных коммуникаций операторами связи, расширению полномочий спецслужб по перехвату электронных коммуникаций в рамках СОРМ и т. п., за которые российские законодатели традиционно подвергались критике западных правозащитников. Не углубляясь в детали событий, спровоцировавших такие заявления, возможно, пока довольно популистские, можно с большой долей вероятности предположить, что тенденция к суверенизации интернета, приведению его в соответствие с национальным законодательством в разных уголках света будет только нарастать. Скорее всего, утверждение жестких досудебных мер все-таки менее вероятно в странах Европы, но важен тот факт, что тенденция так или иначе уже намечается и уже не только в странах, считающихся авторитарными, но и в западных демократиях, что само по себе может еще больше раздробить всемирную сеть и не только на уровне контента.

В то же время мир явно стоит на пороге новой гонки вооружений — на этот раз кибервооружений. После, предположительно, северокорейской кибератаки на *Sony Pictures* США планирует уделять еще более пристальное внимание вопросам национальной кибербезопасности (т. е. и до того приоритетное направление получило публичное подтверждение своей важности), о чем было сказано в ежегодном обращении президента к конгрессу 20 января 2015 г. Барак Обама предложил ужесточить общефедеральное законодательство по защите персональных данных граждан, а также укрепить защиту онлайн-ресурсов банков и кредитных организаций. Подобные атаки, как и развитие новых национальных стратегий кибербезопасности, затрагивают логический уровень интернета, что отражает фундаментальный характер как самих угроз, так и последствий борьбы с ними. К тому же, если учесть продолжающиеся публикации Эдварда Сноудена о кибершпионаже Агентства национальной безопасности за другими странами, а также, как стало известно из последних обнародованных документов, о разработке и внедрении вредоносных программ, нацеленных на вывод из строя объектов критически важной инфраструктуры потенциального противника, усилия, прежде всего европейских стран, видимо, будут балансировать между сотрудничеством с *главным стратегическим партнером* и защитой от него, наращивая собственные кибервооружения. Все эти противоречия могут только усугубить уже сформировавшиеся разногласия относительно новых моделей управления глобальным интернетом после истечения контракта ICANN и NTIA (Департамента телекоммуникаций и информации Министерства торговли США) по выполнению функций IANA, обеспечивающих функ-

*Подробнее с материалами по управлению интернетом вы можете ознакомиться в разделе «Международная информационная безопасность и глобальное управление интернетом» на сайте ПИР- Центра по адресу:* ***net.pircenter.org***

ционирование глобального интернета. Сегодня фрагментация интернета, пожалуй, наиболее сильно проявляется именно в отсутствии единства мнений о будущем модели с привлечением участия всех заинтересованных сторон *(multistakeholder approach)* в контексте все более агрессивно проводимых национальных политик.

На этом фоне интересен вопрос, поднятый Милтоном Мюллером, профессором Школы информационных исследований Университета Сиракуз, на закрытии 9-го Форума по глобальному управлению интернетом (IGF), о необходимости признания *интернет-нации* и ее суверенности. Иными словами, в ситуации до сих пор доминировавшего принципа управления при участии всех заинтересованных сторон неправительственные игроки оказываются на одном уровне с суверенными государствами, что мешает последним заявлять о своем безоговорочном авторитете в принятии решений. Предложив вновь обратиться к небезызвестной Декларации о независимости киберпространства Джона Перри Барлоу 1996 г., Милтон Мюллер буквально заявил о необходимости борьбы за освобождение и суверенитет *интернет-нации*, которая сможет на равных говорить с государствами стран. Не совсем ясно, кого именно Милтон Мюллер включает в эту нацию, как она будет управляться, развиваться и т. п., но главный посыл ясен — у нее будет политический вес, а ключевые решения по управлению интернета должны быть надгосударственными.

По прошествии всего полугода после этого выступления очевидно, что для либертарианского подхода к управлению сетью наступают сложные времена, тогда как то, что в западной терминологии называется *multistakeholder approach*, подвергается все большему давлению с возрастанием роли национальных правительств в управлении глобального интернета, причем в том числе ряда европейских государств. Сейчас сценарий Милтон Мюллера звучит утопично, так как в ближайшей перспективе нас, скорее всего, ждет дальнейшая суверенизация и более ярко выраженная фрагментация киберпространства на национальные сегменты. Причем если раньше наибольшее беспокойство вызывала сегментация глобального контента, сегодня этот процесс перемещается на базовые уровни, а это представляет реальную угрозу для связности того, что мы привыкли звать *глобальным* интернетом.

**Примечания**

[1] *Digital Millennium Copyright Act* — закон США об авторском праве в цифровую эпоху. Подробнее см.: THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998. U. S. Copyright Office Summary. December 1998. http://www.copyright.gov/legislation/dmca.pdf (последнее посещение — 21 января 2015 г.).

[2] The Future of the Internet and How to Stop It, Jonathan Zittrain, Yale University Press & Penguin UK 2008. http://yupnet.org/zittrain/archives/13 (последнее посещение — 21 января 2015 г.).

[3] Принцип регулирования провайдеров связи, обеспечивающий недискриминационный подход к контенту, приложениям, сайтам, платформам и т. п.

[4] Как известно, существуют компании, занимающиеся управлением репутации личностей, компаний, брендов через управление результатами поиска о них в главных поисковых системах интернета.