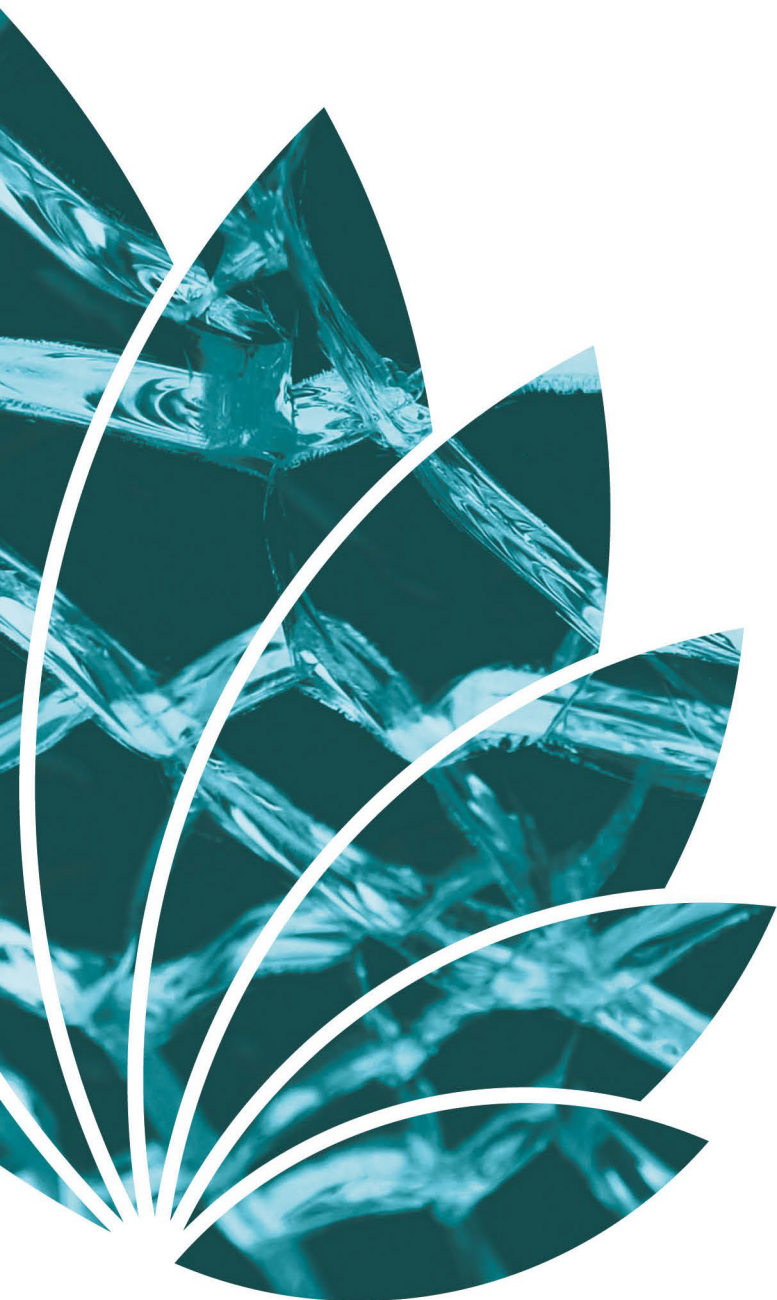


АКТУАЛЬНОЕ ИССЛЕДОВАНИЕ

Фрагментация интернета: почему этот вопрос важен для Европы

*Константинос Комаитис
Январь 2023 г.*



EU CYBER DIRECT

Инициатива ЕС по кибердипломатии

Данная публикация подготовлена в рамках Инициативы ЕС по кибердипломатии «EU Cyber Direct» – проекта при финансовой поддержке Европейского союза. Ответственность за содержание данного документа лежит исключительно на его авторах, и ни при каких обстоятельствах он не может считаться отражающим позицию Евросоюза или любых других институтов.

Автор изображения на обложке: Доминик Хофбауэр/Unsplash

Организация-исполнитель:
Институт ЕС по изучению вопросов безопасности
Фонд Карнеги за международный мир
Лейденский университет



Universiteit
Leiden
Institute of Security
and Global Affairs



При финансовой поддержке Европейского союза



Оглавление

Аннотация	3
Введение	3
1. Почему важно открытое киберпространство	5
2. Определение фрагментации и ее последствия	6
3. Измерения фрагментации	9
3.1 Угрозы системе доменных имен (DNS)	9
3.2 Медленный переход от адресов IPv4 к IPv6	9
3.3 Блокировка и/или фильтрация контента в Интернете	9
3.4 Анализ пиринговых соглашений и взаимосвязи	10
3.5 Опыт локализации данных	10
3.6 Закрытые экосистемы	10
3.7 Провал стандартизации Интернета	11
4. Чем грозит фрагментация Европе?	12
5. Борьба с фрагментацией	13
6. Выводы	16
Об авторе	17

Аннотация

Можно ли говорить о закате открытого интернета? Процесс глобализации переживает серьезную трансформацию. Реагируя на различные глобальные проблемы, государственные власти ставят во главу угла именно интернет. Сама концепция открытого интернета за последние несколько лет претерпела существенные изменения: государство все больше вмешивается в работу интернета, по большей части путем внутреннего регулирования и надзора. Фрагментация интернета уже стала реальностью, проявившись совокупностью действий технического и коммерческого плана, а также государственных мер.

Европейский подход к фрагментации нельзя считать прямолинейным. На международной арене Европа активно выступает за открытый и глобальный интернет и в целом уделяет большое внимание этой идее в своих отношениях с партнерами. Но когда дело касается внутренних правил, Европа своими действиями напротив способствует фрагментации. В силу крайне загруженной законотворческой повестки в Европе созданы условия для движения интернета к большей закрытости и разобщенности. В центре этой повестки находится выбранный Европой подход к обеспечению своего «цифрового суверенитета», который в определенной степени несовместим с идеей открытого интернета.

Европе необходимо сделать важный выбор. Какой интернет ей нужен? Открытый, глобальный, взаимосвязанный – или же фрагментированный интернет с ограниченным выбором?

Введение

Можно ли говорить о том, что наступил конец эпохи открытого, глобального и взаимосвязанного интернета? Ожидать ли нам в будущем, что глобальный интернет, с его открытостью и децентрализованной структурой, сдастся под натиском фрагментации? И что это означает для Европы?

Процесс глобализации, несомненно, претерпевает серьезные изменения, испытывая на себе влияние таких важных глобальных проблем как изменение климата, высокая инфляция и энергетический кризис в Европе. В последние годы востребованность демократических принципов по всему миру постоянно снижалась¹, что во многом объясняется волной захлестнувшего страны национализма, под влиянием которого власти стали замыкаться на внутренней повестке. Однако просто взять и отвергнуть сформировавшуюся под влиянием глобализации за последние десятилетия взаимозависимость стран друг от друга невозможно. Международная торговля товарами и услугами, постоянное передвижение людей по миру (добровольное и вынужденное), трансграничное движение данных – все эти факторы продолжают поддерживать определенный уровень глобальной координации. В настоящий момент государственные субъекты борются за то, чтобы стать более автономными и устранить зависимость от глобальной конъюнктуры, сохранив при этом уровень взаимосвязанности, который бы позволил эффективно реагировать на непредвиденные экстренные ситуации, такие как недавняя пандемия коронавируса.

Интернет – сеть сетей, в которой осуществляется вся деятельность в киберпространстве – играет ключевую роль в уравнивании этой борьбы. Интернет стал для государственных субъектов тем инструментом, который позволяет им сохранять связи, при этом обеспечивая суверенитет над их технологическими аспектами. С годами накопилось немало внутригосударственных законов, создающих препятствия для взаимодействия сетей.²

Хотя архитектура интернета в целом позволяет данным обходить препятствия, это становится невозможным, когда вмешивается государство. Таким образом, есть ощущение, что интернет фрагментируется, то есть распадается на маленькие «интернет-островки», которые, как правило, существуют как изолированные островки.

¹ Sarah Repucci and Amy Slipowitz, *Freedom in the World 2022: The Global Expansion of Authoritarian Rule*, Freedom House (2022), available at: https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf

² Неплохой пример – Индия. Будучи на первом месте по намеренной блокировке интернета властями, Индия также требует, чтобы кабелепрокладочные суда, заходящие в ее воды, устанавливали оборудование для мониторинга широкополосных сетей, которые заканчиваются в Индии, тем самым создавая препятствия в международных коммуникациях.

Дискуссии по поводу фрагментации начались не вчера. На самом деле, они ведутся с 1990-х годов, но в поле зрения широкой общественности попали после инцидента с Эдвардом Сноуденом, который раскрыл информацию о программе правительства США по ведению массовой слежки. Вскоре после его разоблачений власти сразу нескольких стран принялись обсуждать и предлагать правила и политики, требующие локализации определенных видов данных в пределах своих юрисдикции. Некоторые даже рекомендовали дать государству возможность определять структуру интернет-трафика.³ Смысл состоял в том, чтобы контролировать потоки коммуникаций таким образом, чтобы предотвратить несанкционированный перехват информации извне. Фрагментация интернета возникла как часть политического дискурса в противовес этому нарративу.⁴ С тех пор вопрос фрагментации преобладает в разговорах об управлении интернетом.

Тем не менее, проблема фрагментации не ограничивается вмешательством государства. За прошедшие годы наблюдались и другие проявления фрагментации, как коммерческие, так и технические, и считается, что они сыграли определенную роль в том, что интернет стал менее глобальным и взаимосвязанным. Фрагментация наблюдается в различных ипостасях и проявлениях на всем пространстве интернет-экосистемы, от базовой инфраструктуры и вплоть до приложений и контента, из-за чего исчезает единообразие с точки зрения использования интернета. Следовательно, важно осознавать масштаб и глубину фрагментации, особенно если речь идет о результатах этой фрагментации.

“

Отчасти сложность проблемы фрагментации заключается в том, что среди непосредственных участников дискуссий об управлении интернетом нет единого понимания этого термина.

Отчасти сложность проблемы фрагментации заключается в том, что среди непосредственных участников дискуссий об управлении интернетом нет единого понимания этого термина. Для технических специалистов под фрагментацией понимаются препятствия в инфраструктуре интернета, которые мешают взаимодействию и взаимосвязанности между сетями.⁵

С точки зрения частного сектора, фрагментация часто видится как форма государственной политики, направленная на локализацию данных

или ограничивающая каким-либо образом свободный поток данных. И, наконец, гражданское общество понимает фрагментацию через призму правил, нацеленных на ограничение доступа к контенту или его цензуру в интересах коммерческих организаций или государственной власти. Все эти толкования имеют место быть и важны для поиска решений, но они должны дополнять друг друга. В противном случае заинтересованные стороны не придут к единому знаменателю.

В текущей ситуации ценность открытого и глобального интернета легко потерять из виду. Международный порядок становится все менее упорядоченным. На первый план выходит непрекращающаяся борьба за сохранение последних признаков спокойствия. Растет соблазн замкнуться в себе и оградиться от внешнего мира, чтобы удержать контроль и снизить степень неопределенности, которую создает взаимосвязанность. Но это лишь только усугубит и без того хрупкую ситуацию. Если и есть возможность движения вперед, то только через сотрудничество. И этому способствует открытый интернет: он становится общей платформой. Европе следует бороться со стремлением к фрагментации и вместо этого сосредоточиться на поиске путей

³ Matthew Taylor, Nick Hopkins and Jemima Kiss, 'NSA surveillance may cause breakup of internet, warn experts, The Guardian (1 November 2013), available at: <https://www.theguardian.com/world/2013/nov/01/nsa-surveillance-cause-internet-breakup-edward-snowden>

⁴ Когда Сноуден обнародовал информацию о программе слежки, крупнейший телеком-провайдер Германии Deutsche Telekom предложил сделать так, чтобы региональный трафик проходил только через соединения внутри страны ('Deutsche Telekom hopes to hide German internet traffic from spies', Reuters, available at: <https://www.reuters.com/article/germany-spying-telekom-idCNL6N01209320131012>). Хотя эта идея так и не ушла дальше предложения, Европа создала более строгую систему для маршрутизации данных через США. Эта мера вызвала серьезные сложности с управлением потоками данных между двумя союзниками, и недавно президент США Байден подписал указ, создающий предпосылки для нового соглашения о передаче данных между ЕС и США (White House, 'Fact Sheet: President Biden signs executive order to implement the European Union-U.S. Data Privacy Framework', available at: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/>).

⁵ Примеры: несовместимые файлы корневой зоны, проблемы с разрешением DNS-имен, несовместимость между адресами IPv4 и IPv6 и т.д.

формирования собственной цифровой повестки, при этом обеспечивая соблюдение принципа открытости интернета. В главах данной работы изложено общее понимание фрагментации, ее уровней, а также разъясняется, почему Европе необходимо как можно скорее решить, какой именно интернет ей нужен.

1. Почему важно открытое киберпространство

Ранее существовало расхожее мнение, что интернет делает общество более открытым и свободным – объединяет людей, позволяет преодолевать культурные и политические препятствия, создавая новые возможности для самовыражения и позволяя людям расширять свои права и возможности. Люди получают беспрецедентно широкий доступ к информации и инновациям, что, в свою очередь, еще больше вовлекает их в общественную деятельность и делает общество более открытым.

С самых первых дней структура интернета представляла логическую сеть, призванную объединить существовавшие на тот момент разрозненные сети, при этом не лишая их возможности работать независимо. Предполагалось, что интернет будет выполнять роль конструктора по отношению к этим сетям и обеспечивать их взаимосвязанность.⁶ Для этого требовалось обеспечить возможность подключения к интернету с любого устройства. Любой компьютер должен был иметь возможность подключиться к сети, при условии, что он готов к взаимодействию, а технически это несложно.⁷

Эти характеристики завоевали интернету звание «генеративной технологии» – «системы, которая создает неожиданные изменения благодаря «неотфильтрованным» – ничем не регулируемым – действиям широкой и разнородной аудитории». ⁸Эти характеристики и соответствующие протоколы остаются неизменными с тех времен, когда интернет состоял из двух сетей подписчиков, и по сегодняшний день, когда доступ в интернет имеет половина населения планеты. Эта «неотфильтрованная» деятельность подарила нам веб-браузеры, поисковые системы, протокол VoIP, потоковую передачу данных в режиме реального времени, электронную коммерцию, Wi-Fi, электронную почту и даже систему GPS. Она стала главным источником невиданных инноваций – залогом экономического роста и социального развития на современном этапе.

Еще одно важное замечание касательно интернета заключается в том, что его нельзя воспринимать как некий монолит, то есть как единый, целостный объект. Он претерпевает постоянную трансформацию под влиянием множества действующих лиц – частного сектора, властей, технического сообщества, гражданского общества, научных кругов. Отчасти данная трансформация касается опыта пользователя, то есть пространства, в котором размещается контент посредством веб-приложений, мобильных приложений и магазинов приложений. В этом измерении также процветают интернет вещей и стандартизированное программное обеспечение. Тем не менее, это еще и место, в котором общество сталкивается с определенными угрозами, что порождает споры и необходимости вмешательства государства. Часто такие угрозы воспринимаются как «интернет-угрозы», создавая благоприятную почву для фрагментации интернета.

С технической точки зрения в отношении развития интернета изначально преобладало мнение, что любое устройство в интернете должно иметь возможность обмениваться пакетами данных с любым другим устройством, которое готово эти данные принять. Эта степень взаимодействия обеспечивала органическое развитие открытого интернета без какой-либо фрагментации. Интернет – это распределенная система, экосистема из множества пересекающихся сетей, устройств, приложений, людей, коммерческих и государственных интересов. Но главное, у него имеются и невидимые атрибуты, также известные как «постоянные величины»⁹ в силу того, что они не меняются, хотя сам интернет продолжает свое развитие. Можно выделить следующие атрибуты:

⁶ Neil Randall, *The Soul of the Internet* (London: Thomson Learning, 1997).

⁷ Brian Carpenter, 'Architectural principles of the internet' (1996), available at: <https://www.rfc-editor.org/rfc/rfc1958>

⁸ Jonathan Zittrain, *The Future of the Internet and How to Stop It* (Yale University Press, 2008).

⁹ 'Internet invariants: what really matters', Internet Society (2012), available at: <https://www.internetsociety.org/internet-invariants-what-really-matters/>

- > Интернет имеет глобальный охват и целостность, он поддерживает неограниченное количество и виды приложений и сервисов;
- > Интернет существует для всех, без централизованного руководства, которое бы определяло или санкционировало различные категории деятельности в интернете;
- > Интернет требует наличие базовых договоренностей на техническом уровне и следования людьми определенным нормам социального поведения;
- > Хотя нет конкретной технологии, которая бы определяла интернет, существуют базовые характеристики, описывающие его работу;
- > Наконец, чем дольше интернет остается прежним, тем больше он меняется.

Идея об открытости интернета и его глобальном характере имеет глубокое и очень большое значение. Интернет предоставляет значительные экономические преимущества и может способствовать улучшению благосостояния людей по всему миру. У людей появляются новые способы взаимодействия, самовыражения и участия. Возникают новые каналы доступа к сервисам и продуктам, возможность пользоваться огромным объемом знаний и информации. Принцип открытого интернета приносит пользу всем без исключения, включая социально неблагополучные и уязвимые слои населения, среди которых обычно меньше всего пользователей интернета. Согласно «Отчету о глобальной связанности»¹⁰ Международного союза электросвязи, «обеспечение всеобщего и реального доступа» к сети Интернет «стало новым императивом на десятилетие с 2020 по 2030 год».

В целом, по состоянию на сегодняшний день интернет соответствует принципу глобальности, по крайней мере в том, что касается его инфраструктуры. «На сетевом уровне можно с полной уверенностью сказать, что интернет имеет глобальный охват: в принципе, по-прежнему верно то, что любая конечная точка может отправлять пакеты в другую конечную точку».¹¹ Но на практике в своем стремлении к глобальному охвату интернет сталкивается с техническими, политическими и коммерческими факторами, которые приводят к его фрагментации.

В следующей главе кратко разъясняется понятие фрагментации и ее последствия.

2. Определение фрагментации и ее последствия

Фрагментацию интернета можно рассматривать как движущую силу в развитии миропорядка, а также как отражение этого процесса. Например, в последние годы правительство США пытается запретить¹² китайскую видеоплатформу TikTok, и это лишь очередной раз подтверждает наблюдение: рост напряженности в отношениях между США и Китаем подрывает принцип глобальности в функционировании интернета. То же касается и других проявлений геополитического напряжения как регионального, так и международного плана.

С точки зрения управления фрагментация представляет непосредственную угрозу глобальному интернету, в связи с чем в центре внимания международного сообщества оказались вопросы координации и сотрудничества на глобальном уровне. «Различия в работе интернета, наблюдаемые в разных странах, предвосхищают изменения в международной торговле и военной сфере», – гласит исследование¹³ Лаборатории по изучению вопросов безопасности Калифорнийского университета в Беркли. Существует мнение,¹⁴ что споры о фрагментации

¹⁰ Global Connectivity Report, International Telecommunications Union (2022), available at: <https://www.itu.int/itu-d/reports/statistics/2022/05/29/gcr-chapter-1/>

¹¹ Leslie Daigle, The Internet Invariants: The Properties Are Constant, Even as the Internet Is Changing (2019), available at: <https://www.thinkingcat.com/wordpress/wp-content/uploads/2020/08/2019-InvariantsUpdated.pdf>

¹² В США возобновились начавшиеся в период президентства Трампа призывы к запрету TikTok. Bethany Allen-Ebrahimian, 'FCC Commissioner says government should ban TikTok', Axios (2022), available at: <https://www.axios.com/2022/11/01/interview-fcc-commissioner-says-government-should-ban-tiktok>

¹³ Nick Merrill and Steve Weber, 'Website blocking as a proxy of policy alignment' (2020), available at: <https://daylight-lab.github.io/blocking-proxy-paper/writeup.html>

¹⁴ Milton Mueller, Will the Internet Fragment? Sovereignty, Globalization and Cyberspace (Cambridge: Polity Press, 2017).

интернета сводятся к вопросу о суверенитете в цифровой среде, а это уже касается не только самого интернета, но и мирового порядка и роли государственной власти в нем.

Поэтому дискуссии о фрагментации часто выливаются в обсуждение вопроса об открытости интернета: фрагментированный интернет нельзя считать открытым.

Как и фрагментация, термин «открытость» часто используется очень широко и может означать разные вещи для разных людей. Самым простым языком это способность любого человека стать участником интернет-экосистемы. Для технического сообщества понятие открытости подразумевает «архитектуру, которая позволяет создавать общие взаимодействующие сервисы, обеспечивающие повсеместность и общедоступность инноваций. Процесс массовой стандартизации и внедрения необходимых решений обеспечивает проведение полезных изменений, в то время как все ненужное отсеивается».¹⁵ С другой стороны, с экономической точки зрения «открытость» – это возможность пользователей получать доступ к интернету и использовать его для расширения своих возможностей на цифровых рынках. По мнению Организации экономического сотрудничества и развития (ОЭСР), «экономическая открытость повышается по мере развития инфраструктуры широкополосного интернета, но сужается, если среди провайдеров отсутствует конкуренция, и, как следствие, они начинают повышать тарифы или предоставлять некачественные услуги».¹⁶ Наконец, социально-общественная открытость достигается, когда пользователи могут свободно образовывать сообщества и получать информацию, не сталкиваясь при этом с какими-либо ограничениями и предписаниями. Понятие социально-общественной открытости во многом созвучно идеи расширения прав и возможностей людей.

Совокупность всех перечисленных аспектов делает открытость чрезвычайно важным свойством интернета. Любые ограничения открытости интернета, будь то технические, экономические или социально-политические, свидетельствуют о том, что мы называем фрагментацией интернета. К такому же выводу пришли авторы доклада,¹⁷ подготовленного по заказу Всемирного экономического форума (ВЭФ) и опубликованного в 2016 году. В докладе анализируется вопрос о масштабе фрагментации применительно к трем обширным категориям, которые отражают наше видение открытости.

- > Техническая фрагментация – это «условия базовой инфраструктуры, которые мешают способности систем полноценно взаимодействовать и обмениваться пакетами данных, а интернету – функционировать слаженно во всех конечных точках».
- > Фрагментация в силу факторов государственного управления – это «правила и действия, которые ограничивают использование интернета определенным образом или препятствуют деятельности по созданию, распространению информационных ресурсов или ознакомлению с ними».
- > Коммерческая фрагментация – это «подходы к коммерческой деятельности, которые ограничивают использование интернета определенным образом или препятствуют деятельности по созданию, распространению информационных ресурсов или ознакомлению с ними».

Пользуясь интернетом, люди ожидают, что у них будет доступ к его глобальной, а не ограниченной версии. Например, нормативные правила, фильтрующие или блокирующие контент определенного рода, требования по локализации данных и контроль корпораций над крупными контент-платформами и сервисами обмена сообщениями свидетельствуют о фрагментации или возможности ее нарастания.

¹⁵ The internet way of networking: defining the critical properties of the internet', Internet Society (2020), available at: <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/>

¹⁶ Economic and Social Benefits of Internet Openness (Paris: OECD, 2015), available at: [https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP\(2015\)17/FINAL&docLanguage=En](https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP(2015)17/FINAL&docLanguage=En). На момент написания данного доклада обсуждение этой темы в Европе может обернуться непосредственным сокращением экономической открытости. Предложение о принципе «Сторона-отправитель отвечает за расходы», которое рассматривается в Евросоюзе, скорее всего, приведет к менее открытому интернету и некоторой форме фрагментации.

¹⁷ William J. Drake, Vinton G. Cerf and Wolfgang Kleinwächter, Internet Fragmentation: An Overview (Cologne: World Economic Forum, 2016), available at: https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

Исходя из этого, последствия фрагментации могут варьироваться в зависимости от того, где именно она происходит и в чем ее суть. Представьте, например, что обмен данными запрещен, или что, в силу вмешательства государственных органов, появляются альтернативные корневые серверы. Эффект ощутит большинство пользователей, если не все. Чтобы справиться с такой ситуацией, придется пересмотреть процессы и операции. Между тем, в некоторых случаях фрагментация происходит более точно, оказывая влияние только на ограниченное число участников и/или процессов. Например, пользовательские соглашения магазинов приложений превращают их пользователей в узников соответствующих экосистем, и это тоже следует считать фрагментацией, но она влияет только на пользователей конкретных магазинов приложений.

По причине существования множества измерений фрагментации ее последствия с трудом поддаются оценке. Во-первых, фрагментация не возникает мгновенно: напротив, она развивается системно, годами по мере того, как определенные правила и процессы создают предпосылки для нее. Во-вторых, реальные последствия фрагментации всегда чувствуют на себе именно пользователи. Фрагментированный интернет позволяет лучше контролировать, что пользователи видят и посещают. Это, в свою очередь, может привести к дезинформации, глобальной разобщенности и дополнительному контролю со стороны государства. Например, если сравнить опыт интернет-пользователей в Китае и в Европе, то нельзя не заметить существенные отличия.

Еще один важный параметр фрагментации – утрата доверия. Как правило, большая часть каждодневных операций в интернете основана на доверии. Об интернете говорят, что это надежное целое, собранное из ненадежных частей. Другими словами, интернет хрупок, а его устойчивость держится на доверии. Вообще вся система, которая обеспечивает корректную маршрутизацию трафика в интернете, основана на доверии или на «кодексе чести»¹⁸ интернета. Фрагментация не только подрывает это доверие, но и дает возможность нажиться на этом, создавая необходимые условия для дополнительного контроля за потоком трафика. Фрагментация затрудняет доступ, повышает стоимость ведения бизнеса и приводит к тому, что компании покидают цифровые рынки.

Фрагментация интернета также может создавать риски в области безопасности. Кибербезопасность недаром называют «злободневной проблемой». Кибербезопасность «по природе своей трансгранична, работает на нескольких уровнях в различных секторах, между институтами, и влияет на всех участников, как государственных, так и частных, в комплексе и во взаимосвязи, а зачастую этот процесс существенно политизирован».¹⁹ «Злободневные проблемы», как правило, чрезвычайно сложны и требуют совместных усилий, сосредоточенности и межфункционального взаимодействия для поиска решений.²⁰ Как политическая проблема кибербезопасность находится на стыке развития интернета и его стратегического и политического использования государственными и негосударственными субъектами. Фрагментация интернета мешает любым мерам по обеспечению кибербезопасности, так как перечеркивает многие взаимосвязанные факторы и препятствует сотрудничеству.

“

Фрагментация интернета мешает любым мерам по обеспечению кибербезопасности, так как перечеркивает многие взаимосвязанные факторы и препятствует сотрудничеству.

В странах с фрагментированным интернетом люди могут оказаться заложниками геополитических устремлений собственных властей, которые определяют, что может быть доступно, а что нет. В менее открытом интернете правительство может «направить» пользователей в колею определенной повестки, нарушив необходимый уровень доверия, который имеет первостепенную важность для функционирования демократии.

¹⁸ Craig Timberg, 'Net of insecurity: the long life of a quick fix', Washington Post (31 May 2015), available at: <https://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/>

¹⁹ Madeline Carr and Feja Lesniewska, 'Internet of Things, cybersecurity and governing wicked problems: learning from climate change governance', International Relations 34 (3) (2020), 391–412.

²⁰ Leslie Daigle, Konstantinos Komaitis and Phil Roberts, 'Keys to successful collaboration and solving wicked problems', Internet Society (2016), available at: <https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-Collaboration-Behavior-20161122.pdf>

3. Измерения фрагментации

Обозначить четкие измерения фрагментации, как правило, сложно. По мере того, как государственные субъекты все больше отдаляются от принципов глобализации, возникают и развиваются все новые угрозы открытому и глобальному интернету. Тем не менее, за прошедшие годы выявлен ряд действий, которые усугубляют фрагментацию экосистемы интернета.²¹ Эти действия не являются исчерпывающими, и их не следует считать таковыми. Они также не поддаются тщательному анализу без должного изучения правовой среды, в которой они осуществляются. Тем не менее, они дают представление о том, как тем или иным директивным органам следует подходить к вопросу об обеспечении открытости интернета.

3.1 Угрозы системе доменных имен (DNS)

Система доменных имен (DNS) выступает тем «клеем», который скрепляет глобальный интернет. DNS отвечает за преобразование IP-адресов в понятные пользователю алфавитно-числовые доменные имена. Функции управления и координации DNS осуществляет Корпорация по управлению доменными именами и IP-адресами (ICANN). Попытки любых участников установить альтернативные корневые серверы в обход ICANN могут привести к фрагментации. Там, где будут существовать такие альтернативные корневые серверы, пользователи будут отрезаны от глобального интернета. Например, несколько лет назад Международный союз электросвязи предложил Архитектуру цифровых объектов, которая была воспринята как конкурент DNS.²² По той же причине есть опасения, что европейская Директива о сетевых и информационных системах 2 (NIS) может нарушить функционирование глобальной DNS.²³

3.2 Медленный переход от адресов IPv4 к IPv6

IPv4-адреса исчерпали себя²⁴ уже довольно давно.²⁵ Если страны не будут продвигать протокол IPv6, а компании не станут на него переходить, то есть вероятность, что пользователи не смогут получить доступ к некоторым новым сервисам и приложениям. Мы можем получить «Интернет IPv6», изолированный от всех плодов «Интернета IPv4». Даже при стабильно прогрессирующем внедрении IPv6-адресов результата ждать еще долго. «Только 32 страны могут похвастаться уровнем внедрения IPv6 выше общемирового среднего показателя в 30%. Если смотреть по регионам, то наиболее широко IPv6 используется в Южной Азии, Северной Америке и Западной Европе, а меньше всего – в Африке и Тихоокеанском регионе (Океании)».²⁶ В будущем для поддержания глобальности интернета очень важно обеспечить внедрение IPv6-адресов по всему миру.

3.3 Блокировка и/или фильтрация контента в интернете

В самом простейшем случае определенная степень фрагментации интернета приводит к тому, что страны непоследовательно фильтруют контент, исходя из своего понимания того, какие высказывания допустимы, а какие нет. Власти применяют различные технические и правовые средства для блокировки сайтов и платформ и удаления контента. Используя такие инструменты как фильтрация DNS, блокировка по IP-адресу, DDoS-атаки и удаление результатов поиска, власти корректируют способы подключения пользователей и их участие в глобальном интернете. Самый яркий пример – Китай, где работает очень сложная система фильтрации для контроля доступного пользователям контента. Тем не менее, блокировка контента происходит

²¹ Jonah Force Hill, *Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for US Policy Makers* (Harvard, MA: John F. Kennedy School of Government, 2012), available at: https://www.belfercenter.org/sites/default/files/legacy/files/internet_fragmentation_jonah_hill.pdf

²² Chip Sharp, 'Overview of the Digital Object Architecture (DOA)', *Internet Society* (2016), available at: https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-DOA-Overview-20161025-A4-3_0.pdf

²³ 'ICANN org comments on the Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the EU, repealing Directive (EU) 2016/1148 (NIS 2 Directive)', available at: <https://www.icann.org/en/system/files/files/icann-org-comments-proposed-nis2-directive-19mar21-en.pdf>

²⁴ APNIC, 'IPv4 exhaustion details', available at: <https://www.apnic.net/community/ipv4-exhaustion/ipv4-exhaustion-details/>

²⁵ RIPE NCC, 'The RIPE NCC has run out of IPv4 addresses', available at: <https://www.ripe.net/publications/news/about-ripe-ncc-and-ripe/the-ripe-ncc-has-run-out-of-ipv4-addresses>

²⁶ Geoff Huston, 'The transition to IPv6: Are we there yet?', *APNIC* (2022), available at: <https://blog.apnic.net/2022/05/04/the-transition-to-ipv6-are-we-there-yet/>

и за счет других процессов – например, с целью защиты авторских прав или борьбы с материалами, демонстрирующими сексуальное насилие над детьми, поэтому блокировка широко применяется и в демократических странах.²⁷

3.4 Анализ пиринговых соглашений и взаимосвязей

Как говорилось выше, интернет представляет «сеть сетей», которые связаны друг с другом благодаря использованию открытых стандартов. Традиционно сложилось, что в интернете вопросы оплаты регулировались двусторонними пиринговыми соглашениями. При этом возможны случаи, когда крупные интернет-провайдеры ущемляют интересы конкурирующих сервисов или отдают предпочтение определенным типам данных. Это может ограничивать виды доступных пользователям приложений и сервисов, в зависимости от того, услугами какого провайдера они пользуются. Это тоже вид фрагментации интернета. Хороший пример этого явления – споры о модернизации инфраструктуры и плате за развитие сетей, которые в настоящее время ведутся в Европе. Европейская комиссия рассматривает предложения по кардинальному изменению взаимодействия сетей в Европе и хочет ввести новые обязательства для сторон, заключающих пиринговые соглашения.²⁸ По опыту Южной Кореи можно сказать, что такие ничем не оправданные изменения делают экосистему интернета обременительной, затратной и некачественной. В итоге вполне может выйти, что таким интернетом никто не захочет пользоваться.²⁹

3.5 Опыт локализации данных

Страны вводят все больше ограничений в отношении хранения и передачи данных местными компаниями, руководствуясь географическим принципом по целому ряду причин, будь то забота о неприкосновенности частной жизни своих граждан, стремление защититься от слежки со стороны иностранных спецслужб или обеспечить безопасный доступ к данным с целью охраны правопорядка. Введение дополнительных мер правовой защиты персональных данных действительно может решить проблему сохранения конфиденциальности онлайн, но если многие страны будут вводить свои собственные требования по охране частной жизни, то каждая компания, работающая в интернете, теоретически может столкнуться с необходимостью следовать множеству противоречащих друг другу законов. Если компании окажутся не в состоянии выполнить требования каждой отдельной страны, потому что эти требования противоречат друг другу или по причине дополнительных затрат на выполнение множества несовместимых правил, компании могут быть вынуждены уйти с некоторых рынков, что скажется на пользователях и сделает интернет еще более фрагментированным. Законы о локализации данных особенно активно принимаются в Китае, России и Индии. Страны Африки (например, Нигерия) и Азиатско-Тихоокеанского региона (например, Индонезия, Бруней) тоже ввели жесткие требования по локализации данных. Европейская облачная инициатива GAIAx,³⁰ «Закон об управлении данными» и «Закон о данных»³¹ также нацелены на локализацию данных.³²

3.6 Закрытые экосистемы

В том, чтобы пытаться «запереть» пользователей в собственной экосистеме, нет ничего нового. В 1980-е и 1990-е годы компании Prodigy, CompuServe и America Online в США занимались

²⁷ Paul Bischoff, 'Internet censorship 2022: a global map of internet restrictions' (2022), available at: <https://www.comparitech.com/blog/vpn-privacy/internet-censorship-map/>; see also 'Internet Society perspectives on internet content blocking: an overview' (2017), available at: <https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/>

²⁸ Konstantinos Komaitis, 'Europe's risky plan for the internet', Directions Cyber Digital Europe (2022), available at: <https://directionsblog.eu/europes-risky-plan-for-the-internet/>

²⁹ Kyung Sin Park and Michael R. Nelson, 'Korea's challenge to the standard internet interconnection model', Carnegie Endowment for International Peace (2021), available at: <https://carnegieendowment.org/2021/08/17/afterword-korea-s-challenge-to-standard-internet-interconnection-model-pub-85166>

³⁰ Olaf Kolkman and Andrei Robackevsky, 'Technical architecture of the GAIA-X project', Internet Society (2021), available at: <https://www.internetsociety.org/resources/2021/internet-impact-brief-technical-architecture-of-the-gaia-x-project/>

³¹ Luca Bertuzzi, 'Is data localization coming to Europe?', The International Association for Privacy Professionals (23 August 2022), available at: <https://iapp.org/news/a/is-data-localization-coming-to-europe/>

³² 'Internet way of networking use case: data localization', Internet Society (2020), available at: <https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/>

именно этим – помещали пользователей в ограниченную и, в отличие от интернета, закрытую экосистему. Однако в дальнейшем все изменилось, так как компании начали осознавать преимущества открытой среды. Стены пали, появились новые сервисы. В последние годы все вновь стало меняться. Пользователи все чаще выходят в интернет с мобильных устройств, сделав магазины приложений новым рубежом, по периметру которого стали возводиться новые заграждения. В то же время некоторые компании теперь служат исключительным средством доступа в интернет в силу эффекта масштаба. Эти компании также помещают пользователей в свою закрытую экосистему. Как отметила лауреат Нобелевской премии Мария Ресса, на Филиппинах «интернет, по сути, сводится к Фейсбуку».³³

3.7 Провал стандартизации интернета

В последние годы наблюдается рост интереса властей к разработке стандартов, что представляет угрозу для организаций, в задачи которых входит разработка технических стандартов интернета. В некоторых странах, особенно в Китае³⁴ и России,³⁵ утверждают, что эти организации, с 1980-х годов отвечающие за основные стандарты интернета и протоколы, не несут никакой ответственности за свои действия и ущемляют интересы неамериканских компаний. Однако такие предположения не соответствуют реальному положению дел в интернете. Здесь любой может принять участие в разработке стандартов и любой может добровольно их внедрять. Но в последнее время наблюдаются попытки забрать полномочия по разработке стандартов у соответствующих учреждений и передать их в ведение организованных по директивному принципу многосторонних площадок. Китай продвинулся в этом направлении посредством создания собственных технологий, отражающих внутригосударственные правила и политику.³⁶

Некоторые из этих угроз являются особенно злободневными, некоторые вызваны действиями самих властей и бизнеса, другие носят скорее экзистенциальный характер. Но факт остается фактом: полным ходом идет слом идеи открытого и глобального интернета, да и сам интернет тоже меняется. Власти разных стран меняют интернет, способствуя его большей фрагментации, как правило, даже не отдавая себе в этом отчет. Некоторые изменения продиктованы резонной обеспокоенностью, например, когда дело касается обеспечения неприкосновенности частной жизни или конкуренции. Но негативные последствия от таких изменений будут минимальными, если не торопиться с их внедрением и обеспечить сотрудничество с заинтересованными сторонами. Хороший пример – Общий регламент ЕС по защите данных: хотя в самом начале он создал условия для того, чтобы многие компании перестали показывать свой контент европейским пользователям,³⁷ со временем эти компании нашли способ привести свою деятельность в соответствие с новыми нормативно-правовыми требованиями, поскольку регламент охватывает очень широкий круг вопросов. Другие изменения более очевидные. Хороший пример – меры, принятые в Южной Корее по стоимости обмена трафиком, особенно с учетом влияния этих мер на интернет-экосистему страны.³⁸ Фрагментация интернета может очень дорого обойтись Европе.

В следующем разделе речь пойдет о том, чем именно грозит фрагментация Европе и ее внутреннему рынку.

³³ Maria Ressa, 'Facebook let my government target me. Here's why I still work with them', Time (17 January 2019), available at: <https://time.com/5505458/facebook-maria-ressa-philippines/>

³⁴ Luca Bertuzzi, 'China rebrands proposal on internet governance, targeting developing countries', Euractiv (6 June 2022), available at: <https://www.euractiv.com/section/digital/news/china-rebrands-proposal-on-internet-governance-targeting-developing-countries/>

³⁵ Ewen MacAskill, 'Putin calls internet a "CIA project" renewing fears of web breakup', The Guardian (24 April 2014), available at: <https://www.theguardian.com/world/2014/apr/24/vladimir-putin-web-breakup-internet-cia>

³⁶ Stacie Hoffmann, Dominique Lazanski and Emily Taylor, 'Standardizing the splinternet: how China's technical standards could fragment the Internet', Journal of Cyber Policy 5 (2) (2020), 239–264

³⁷ Konstantinos Komaitis 'GDPR: going beyond borders', Internet Society (2018), available at: <https://www.internetsociety.org/blog/2018/05/gdpr-going-beyond-borders/>

³⁸ Konstantinos Komaitis and K.S. Park, 'The global trend that could kill the Internet: the Sending-Party-Network-Pays', TechDirt (2022), available at: <https://www.techdirt.com/2022/11/22/the-global-trend-that-could-kill-the-internet-sender-party-network-pays/>

4. Чем грозит фрагментация Европе?

В том, что касается фрагментации интернета, для Европы наступил переломный момент. ЕС принял амбициозную программу «Цифровые цели к 2030 году»³⁹, уверенно заявив, что к 2030 году «все будут иметь доступ в интернет». Более того, в 2015 году Евросоюз закрепил на законодательном уровне⁴⁰ свою приверженность принципу открытого интернета, заявив, что «недопустима дискриминация, блокировка, ограничение интернет-трафика или предпочтение одного вида трафика другому». На международном уровне Европейская комиссия неоднократно заявляла о той непреклонности, с которой будет отстаивать ценности открытого и глобального интернета, а в числе последних инициатив вместе с США и другими международными партнерами подписала декларацию⁴¹ о том, что интернет будущего должен быть открытым, глобальным и взаимосвязанным.

В то же время на повестке ЕС стало появляться все больше законодательных предложений, подрывающих принципы открытости и глобальности интернета. Некоторые нормативные инициативы, например, «Закон о цифровых сервисах» или Общий регламент по защите данных, представляют собой попытку упорядочить регулирование интернета на уровне ЕС. В таких случаях фрагментация представляется не основным, а побочным следствием принимаемых мер, а значит, решать такие проблемы будет проще. Но есть и другие предложения, преимущественно в контексте стремления Европы обеспечить свой цифровой суверенитет, и такие инициативы несут в себе гораздо более высокие риски с точки зрения фрагментации интернета.

В качестве примера можно привести инициативу DNS4EU. В рамках политики по обеспечению кибербезопасности ЕС рекомендовал создать собственный публичный рекурсивный DNS-сервис, что, в случае неудачного внедрения, может сделать функционирование DNS как единой системы невозможным.⁴² Еще один пример – предложение о «справедливой доле»: это значит, что контент-провайдеры платят поставщикам телекоммуникационных услуг за используемый трафик. Реализация такого предложения, скорее всего, приведет к аннулированию⁴³ пиринговых соглашений и радикально изменит весь рынок обмена трафиком, как сказано выше. Наконец, Директива сетевой и информационной безопасности (NIS 2) на сегодняшний день представляет, возможно, наибольшую угрозу с точки зрения фрагментации интернета. Проект директивы предусматривает чрезвычайно широкое поле для применения и территориальный охват (эффект экстратерриториальности). В сущности Европа претендует на юрисдикцию над всеми сетевыми и информационными сервисами по всему миру, и велика вероятность, что это как минимум приведет к перестройке всей DNS,⁴⁴ а как максимум побудит другие страны ответить тем же, «что существенно усложнит работу основополагающего компонента глобальной инфраструктуры интернета, которая была чрезвычайно устойчивой, надежной и безопасной на протяжении всей истории своей работы».⁴⁵

Таким образом, Европа оказалась на перепутье. Она может стать проводником положительных перемен или создать препятствия, которые усугубят фрагментацию интернета. В дальнейшем Европе предстоит определиться, какой интернет ей нужен: открытый, глобальный, способный к взаимодействию или же фрагментированный с ограниченным выбором?

³⁹ European Commission, 'Europe's Digital Decade: digital targets for 2030', available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

⁴⁰ Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2015%3A310%3ATOC&uri=uriserv%3AOL_2015.310.01.0001.01.ENG

⁴¹ U.S. Department of State, 'Declaration for the Future of the Internet', available at: <https://www.state.gov/declaration-for-the-future-of-the-internet>

⁴² Geoff Huston, 'Some thoughts on DNS4EU – the European Commission's intention to support the development of a new European DNS resolver', CircleID (2022), available at: <https://circleid.com/posts/20220213-some-thoughts-on-dns4eu-new-european-dns-resolver>

⁴³ Komaitis and Park (см. сноску 37 выше).

⁴⁴ ICANN org comments (см. сноску 23 выше).

⁴⁵ 'RIPE NCC Response to the European Commission's Proposed NIS 2 Directive', available at: https://www.ripe.net/participate/internet-governance/multi-stakeholder-engagement/ripe-ncc-response-to-nis-2-directive_march-2021.pdf

В недавнем исследовании⁴⁶ Группы по развитию науки и технологии Европейского парламента по оценке сценариев научно-технического развития (STOA) определены три сценария для Европы. Первый – это сохранение статуса-кво: интернет и внутренний цифровой рынок рассматриваются

“

В дальнейшем Европе предстоит определиться, какой интернет ей нужен: открытый, глобальный, способный к взаимодействию или же фрагментированный с ограниченным выбором?

ЕС как структуры, обладающие достаточным запасом прочности перед лицом угрозы фрагментации. Согласно второму сценарию, Европа принимает фрагментацию как данность. Ей придется адаптировать свою повестку по цифровому суверенитету к условиям фрагментированного интернета, и тогда будет легче оправдать некоторые из ее собственных нормативных инициатив. Наконец, третий сценарий предполагает, что Европа будет бороться с тенденцией к фрагментации и займется введением правил, руководствуясь принципами глобального и открытого интернета.

Эти три сценария подразумевают разный уровень риска. Реальность такова, что Европа в своих действиях не может ограничиться поддержкой текущего статус-кво. Как правильно подмечено в исследовании STOA, «инициативы России и Китая, в сочетании с ухудшением международной обстановки в части поддержания открытого и глобального многостороннего процесса, неизбежно вынесут фрагментацию на повестку дня – как нечто, несущее возможности или риски».⁴⁷ В то же время серия принятых самой Европой законодательных инициатив свидетельствует об отходе от идеи о том, что государству не следует вмешиваться в функционирование интернета. Аналогичным образом принятие фрагментации может потребовать от Европы пойти на компромисс, но она может не желать этого или оказаться не готовой к такому развитию событий. Фрагментация определенно затруднит использование интернета в Европе и дестабилизирует ее внутренний рынок, создаст риски для отношений с международными торговыми партнерами, не обеспечив при этом должный уровень кибербезопасности.⁴⁸

Следовательно, борьба с фрагментацией видится как единственный реальный сценарий для Европы. Он подразумевает принятие внутренних и внешних правил в соответствии с принципами открытого и глобального интернета. Тем не менее, Европа столкнулась с невиданной ранее проблемой: ей необходимо найти способы достичь этого, не саботируя собственную цифровую повестку.

5. Борьба с фрагментацией

Не стоит рассматривать фрагментацию в качестве одного из возможных путей развития интернета. Европе следует избегать директивного подхода, который может привести к раздроблению интернета на несколько не связанных между собой и несогласованных подсетей. Как по экономическим соображениям, так и из соображений безопасности строить виртуальные стены – это не выход, а введение искусственных нормативно-правовых ограничений только усугубляет негативные последствия фрагментации.

Первоочередным средством избежать фрагментации выступает поддержка стратегии сотрудничества в области управления интернетом и ее поощрение, чтобы участники совместными усилиями определили будущее интернета. Способность к сотрудничеству со стороны многочисленных субъектов лежит в основе работы интернета и его развития. «По мере движения по интернету, информация проходит через множество сетей, и сеть исходящего трафика, возможно, никак не связана с сетью, получающей этот трафик. Эта схема работает благодаря сотрудничеству как в части обмена, так и в части передачи трафика из других сетей, а также в части

⁴⁶ Clément Perarnaud, Julien Rossi, Francesca Musiani and Lucien Castex, Splinternets: Addressing the Renewed Debate on Internet Fragmentation (Brussels: European Parliament, 2022), available at: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU\(2022\)729530](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2022)729530)

⁴⁷ Там же.

⁴⁸ Там же.

решения проблем, которые могут возникать на расстоянии нескольких этапов».⁴⁹ Интернет транснационален по своей сути, и это свойство должно находить отражение в процессе разработки европейских правил регулирования интернета. Европа уже задала тон в области регулирования интернета в глобальном масштабе, приняв Общий регламент по защите данных и «Закон о безопасности данных», но при этом действовала в отрыве от всех остальных. По мере того, как другие юрисдикции начнут пользоваться возможностью регулировать интернет в соответствии с экстерриториальным принципом, Европа может встать во главе совместной деятельности по систематизации и повышению эффективности принимаемых мер. В этом случае очень важно создавать центры разработки нормативно-правовых правил и формировать процессы, способствующие сотрудничеству.

“

Интернет транснационален по своей сути, и это свойство должно находить отражение в процессе разработки европейских правил регулирования интернета. Европа уже задала тон в области регулирования интернета в глобальном масштабе, приняв Общий регламент по защите данных и «Закон о безопасности данных», но при этом действовала в отрыве от всех остальных.

Кроме того, Европа может внимательнее отнестись к возможному влиянию регулирования на интернет. Обеспечение эффективности любого процесса регулирования предполагает оценку его воздействия. Это касается и интернета.⁵⁰ Оценка воздействия – проверенный способ собрать вместе множество участников, задействованных в планировании, внедрении и мониторинге любых улучшений в системе регулирования. Независимо от того, осуществляется ли фрагментация намеренно или стала побочным следствием других действий, правила должны быть сбалансированными, предметными, последовательными и предсказуемыми. Для этого при разработке регламентов Европе следует задать несколько вопросов, особенно учитывая, что институты ЕС стремятся найти равновесие между соблюдением принципа открытого интернета и необходимостью его регулировать. Решает ли предлагаемое новое правило проблему? Соблюден ли баланс между

необходимостью решить проблему и избежать фрагментации? Ведет ли это решение к справедливому распределению затрат и преимуществ для всех участников? Является ли решение законным, надежным и заслуживающим доверия? Скажутся ли новые правила на соблюдении принципов открытого и глобального интернета? Например, Европейской комиссии следует требовать проведения оценки воздействия принимаемых мер в рамках своего нормотворчества, внимательно анализируя то, как предлагаемые законы могут препятствовать соблюдению принципа открытости интернета.

Еще один способ обеспечить сохранение открытого интернета и удовлетворить потребность в государственном регулировании заключается в задействовании международного права, в первую очередь, в области защиты прав человека и торговли. Международные договоры определяют степень сотрудничества, и в случае с интернетом пространство для дальнейшего углубления взаимодействия есть. Как говорилось выше, интернет – это технология людей; возможность участвовать, выражать себя и создавать что-либо является неотъемлемой частью его концепции и развития. Если рассматривать фрагментацию интернета с точки зрения прав человека, то «единство в интернете вытекает из основополагающих прав, таких как свобода доступа к информации, и устанавливает, что любое ограничение этого права может осуществляться, только если это необходимо и действительно отвечает целям демократического общества».⁵¹

⁴⁹ Olaf Kolkman, 'Internet is all about collaboration, Internet Society (2015), available at: <https://www.internetsociety.org/blog/2015/04/internet-is-all-about-collaboration/>

⁵⁰ Konstantinos Komaitis, 'The silver lining of internet regulation: a regulatory impact assessment', TechDirt (2020), available at: <https://www.techdirt.com/2020/08/11/silver-lining-internet-regulation-regulatory-impact-assessment/>; Кроме того, Обществом Интернет подготовлено руководство по оценке воздействия, призванное способствовать более эффективной оценке политических решений и нормативно-правовых действий. Руководство не затрагивает вопрос о существовании разных видов фрагментации и ограничивается рассмотрением возможных проблем с точки зрения технической фрагментации. См. подробнее: <https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/>

⁵¹ Там же.

Европе следует обеспечить соблюдение прав человека и принципа соразмерности при внедрении всех правил регулирования интернета. ЕС должен сотрудничать с международными организациями, особенно с Советом по правам человека, для укрепления правовой базы по защите прав человека применительно к интернету. Закреплению принципа открытого интернета может способствовать проведение в 2025 году обзорной конференции Всемирной встречи на высшем уровне по вопросам информационного общества.

Аналогичным образом ряд торговых соглашений⁵² содержит формулировки, указывающие на приверженность принципу открытого интернета и отвергающие любые действия, которые способствуют фрагментации, например, локализацию данных. Такие соглашения преимущественно носят двухсторонний или региональный характер, но они играют роль важных ступенек на пути к достижению глобального консенсуса по вопросу об обеспечении открытости интернета. Пока Европа ведет переговоры о заключении новых соглашений о свободной торговле, существующие соглашения могут служить моделью и подсказывать правила, касающиеся запрета на тарифы и дискриминационную политику в отношении зарубежных цифровых продуктов, защиты от несправедливых требований по передаче исходного кода государственным органам и противодействия локализации данных. Европе также следует стать во главе движения в поддержку открытости интернета и вести работу через Всемирную торговую организацию (ВТО).

Наконец, Европе необходимо вернуться к активному взаимодействию и вспомнить о его преимуществах. Это означает приверженность идее открытых стандартов и их добровольное применение. С самого появления интернета существование открытых стандартов обеспечивало развитие интернета и не сводилось к следованию чьим-то политическим или коммерческим интересам:

Интернет – это результат рыночной дисциплины, которая отражает предпочтения потребителей, а те, в свою очередь, служат ориентиром для производителей цифровых товаров и услуг. Потребитель может не нуждаться во всех возможных услугах в отдельно взятый момент времени, но должен иметь возможность воспользоваться всей совокупностью предложений, доступных в рамках определенной услуги, и каждый поставщик хочет, чтобы его услуги были доступны каждому потребителю. Упорядоченная сетевая среда всегда работает одинаково: непрерывный доступ ко всем серверам, отображение идентичного процесса взаимодействия с сервисом для всех потребителей. И производитель, и потребитель имеют возможность универсального доступа.⁵³

«Закон о цифровых рынках», в основе которого лежит возможность взаимодействия – хорошая точка отсчета для развития конкуренции, столь важной для эффективного взаимодействия. Следовательно, корректное внедрение этого закона приобретает особое значение. Более того, Европе следует и дальше поддерживать развитие открытых стандартов, например, работу Инженерного совета Интернета (Internet Engineering Task Force, IETF), и противостоять попыткам перевести обсуждение в ведение межправительственных организаций, включая Международный союз электросвязи.

Наконец, Европа должна вести более решительную внешнюю политику в отношении тех, кто выступает против принципов открытого и глобального интернета на международной арене. Наличие внутренних правил и инфраструктуры для обеспечения открытости интернета имеет огромное значение, но не менее важно поддерживать другие страны на этом пути. Например, Европе следует содействовать инфраструктурному развитию для повышения проникновения интернета там, где это требуется. Такие инициативы, как Инвестиционный пакет «Глобальный шлюз ЕС-Африка»⁵⁴ можно масштабировать на другие регионы, чтобы помочь им с расстановкой приоритетов, разработкой программ и внедрением процессов, связанных с реализацией совместных инфраструктурных проектов. Европе следует сформировать столь необходимую стратегию цифровой внешней политики, в основе которой лежала бы идея отказа от фрагментации интернета.

⁵² Например, Всеобъемлющее и прогрессивное соглашение о Транстихоокеанском партнерстве и Соглашение США, Мексики и Канады содержат отсылки к принципу открытого интернета.

⁵³ Geoff Huston, 'Reexamining internet fragmentation', CircleID (2022), available at: <https://circleid.com/posts/20220926-reexamining-internet-fragmentation>

⁵⁴ European Commission, 'EU-Africa: Global Gateway Investment Package', available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/global-gateway/eu-africa-global-gateway-investment-package_en



Европа должна вести более решительную внешнюю политику в отношении тех, кто выступает против принципов открытого и глобального интернета на международной арене. Наличие внутренних правил и инфраструктуры для обеспечения открытости интернета имеет огромное значение, но не менее важно поддерживать другие страны на этом пути.

Один из ключевых аспектов фрагментации заключается в ее многоликости: иногда ее причины очевидны, а иногда угроза фрагментации возникает как будто неоткуда. При этом сам феномен фрагментации постоянно меняется. Следовательно, не стоит ожидать, что приведенные в данной работе рекомендации позволят полностью решить проблему фрагментации интернета. Европе также следует понимать, что для дальнейшего соблюдения принципа открытости интернета его придется имплементировать в своей нормативно-правовой базе. Начинать следует с себя, но и на международном уровне Европе следует рассматривать фрагментацию интернета как важный вопрос внешней политики.

6. Выводы

В недавнем отчете⁵⁵ Совет по международным отношениям заявил, что «эра глобального интернета закончилась» и что США стоит отказаться от существовавшей долгое время идеи об открытом и глобальном интернете. В отчете говорится, что, под влиянием геополитических вызовов, исходящих от Китая и России, которые все больше используют принцип открытого интернета как оружие, США следует сосредоточиться на реагировании на эти вызовы.

Действительно, действия России и Китая подталкивают Европу к похожему поведению и более строгому контролю над интернетом. Тем не менее, «контролируемого интернета» как такового не существует, по крайней мере, в той форме, в какой его представляют Китай и Россия. Это не интернет, а просто еще одна форма взаимодействия сетей, которой не свойственны ни развитие, ни инновации, ни создание новых возможностей.

У Европы уже есть инструменты по борьбе с фрагментацией интернета. Она инициировала на международном уровне дискуссию по вопросу о регулировании интернета, доказывая, что может играть ведущую роль в этом процессе, добившись равновесия между регулированием интернета и соблюдением принципа его открытости. Более того, Европе следует оптимизировать процессы содержательного взаимодействия с различными субъектами. Многосторонняя модель уже существует, и у Европы есть возможность применить ее к интернету. Европе также следует руководствоваться нормами международного права в киберпространстве и способствовать их закреплению, особенно в сфере защиты прав человека. И, наконец, Европа должна продолжить поддерживать процесс развития открытых стандартов и вновь заявить о своей приверженности идеям совместимости и взаимосвязанности. Другой путь – это изоляция, чем, по сути, и является фрагментированный интернет.

Интернет сохраняет свою устойчивость, пока соблюдается минимальный набор норм, и одна из них – открытость. Борьба за открытый, нефрагментированный интернет стоит желаемого результата. Европа вновь и вновь доказывает свою приверженность демократическим ценностям и стремлению развивать благоприятную среду для их продвижения. Одним из воплощений такой среды выступает интернет.

⁵⁵ Nathaniel Fick, Jami Miscik, Adam Segal and Gordon M. Goldstein, *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*, Council of Foreign Relations (2022), available at: https://www.cfr.org/report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf

Об авторе

Константинос Комаитис – эксперт по разработке и анализу мер по соблюдению принципов открытого и глобального интернета. Занимался разработкой правил и стратегий на посту старшего директора фонда Общество Интернет и старшего преподавателя Университета Стратклайда (Великобритания), где изучал вопросы интернет-регулирования и преподавал этот предмет. В настоящий момент является внештатным научным сотрудником Лиссабонского совета. Также является внештатным научным сотрудником Таллиннского университета технологий.

О проекте EU Cyber Direct

Проект EU Cyber Direct оказывает поддержку кибердипломатии ЕС и вносит свой вклад в развитие безопасного, стабильного и основанного на правилах международного порядка в киберпространстве за счет ведения широкого диалога со стратегическими странами-партнерами, региональными и международными организациями. EU Cyber Direct получает финансирование Европейской комиссии в рамках проекта «Инструменты партнерства, международное цифровое сотрудничество: доверие и безопасность в киберпространстве».

АКТУАЛЬНОЕ ИССЛЕДОВАНИЕ

Серия исследований в поддержку политик Евросоюза в сфере киберпространства, обеспечивающая своевременный и релевантный анализ.

