ЛЕТНЯЯ ШКОЛА
по управлению интернетом

Мазай Ирэна

Суверенитет и digital – нет ли противоречия?

В последнее десятилетие понятие «технологический» или «цифровой суверенитет» стало центральным элементом политических дискуссий по цифровым вопросам. Серьезные опасения правительств как развитых, так и развивающихся стран, стало вызывать политическое, экономическое и социальное влияние международных технологических компаний, которые получили безграничный контроль не только над личными данными граждан, но и стали монополистами на многих национальных рынках, ограничив развитие технологий и инноваций локальных игроков. Таким образом, достижение цифрового суверенитета стало целью, которую разделяют заинтересованные стороны из государственных органов власти и коммерческих компаний. Однако в последнее время к ним также присоединились обычные пользователи - граждане и потребители, осознавшие свою уязвимость в Сети, ввиду постоянных скандалов с утечками персональных данных из банков и разнообразных интернет-платформ.

Термин «цифровой суверенитет», который возник в начале 2000-х годов, и вся концепция, выстроенная вокруг него, до сих пор вызывает споры, и необходимость в более тщательной проработке. Прилагательное ‘цифровой’ делает акцент на технической стороне вопроса, в то время как термин ‘суверенитет’, в классическом понимании является одной из фундаментальных категорий теории государства и права, и тесно связан с понятием политической власти, способностью субъекта, а именно государства проводить свою волю в политике и осуществлять контроль. Во многих странах мира растет беспокойство по поводу того, что государство, а также коммерческие компании и граждане, постепенно теряют контроль над своими данными, и право формировать и обеспечивать соблюдение и защиту своих прав в цифровой среде.

Понятие «технологический» или «цифровой суверенитет» появилось недавно как концепт продвижения лидерства и стратегической автономии страны в цифровой сфере. Государства не желают отказываться от своей монополии на политический, экономический и социальный контроль. В связи с этим они обращают повышенное внимание, и пытаются ограничить или зарегулировать то влияние, которое в последнее время получили отдельные компании, часто имеющие американское или китайское происхождение, однако по факту являющиеся автономными экономическими и политическими акторами. С точки зрения политиков многих стран, рост влияния данных компаний угрожает как государственным механизмам контроля, так и контролю граждан над личными данными; и ограничивает как рост новых национальных высокотехнологичных компаний, так и способность законодательных органов обеспечивать соблюдение нормативных требований. В этом контексте «цифровой суверенитет» относится к способности страны действовать независимо в цифровом мире и должен пониматься как с точки зрения защитных механизмов национальной безопасности, так и наступательных бизнес-инструментов для стимулирования цифровых инноваций в отдельно взятой стране и появлению новых технологических продуктов для глобального рынка.

Сегодня, крупные технологические компании собирают огромные массивы личных данных, и часто не подчиняются национальным и даже международным правилам в части хранения, обработки, защиты и использования этих данных (разработка национальных / международных стандартов и законов просто не поспевает за мировой цифровой трансформацией). Бизнес-модели таких крупных игроков как Google, Apple, Facebook, Amazon и Microsoft, которых в научной литературе и в СМИ окрестили аббревиатурой «GAFAM», в значительной степени основаны на сборе и использовании данных пользователей и получения доходов от рекламы. Однако скандал с Cambridge Analytica продемонстрировал, что данные онлайн-платформ могут использованы не только для бизнес-целей и монетизации, но также и в политических целях.

Широкую популярность получила теория ‘капитализма слежки’ (или по-другому еще надзорный капитализм или ‘шпионящий капитализм’ (surveillance capitalism) - экономическая система, сосредоточенная вокруг коммодификации личных данных для более точного нацеливания на потребителей, основной целью которой изначально было извлечения прибыли. Сегодня интернет-гиганты, мобильные операторы и компании, специализирующиеся на интернете вещей, не только собирают данные пользователей, но и пытаются влиять на их поведение в собственных целях. Они встраивают в страницы шпионские программы, выявляют с помощью алгоритмов привычки, улавливают эмоции, анализируют тексты, написанные пользователем, электронную почту, GPS-координаты, сообщения в социальных сетях, розничные покупки и прочее. Эти поведенческие данные превращаются в модели поведения, оценивающие кредитоспособность человека при помощи алгоритмов (а в некоторых странах и социальной благонадежности), который благодаря все новым и новым данным постоянно совершенствуется. В конечном итоге все это ведет к тому, что граждане по всему миру потеряли контроль над своей личной информацией и конфиденциальностью. Безусловно это не осталось без внимания со стороны государства. Правительства и политические лидеры все больше опасаются роста этого влияния, и того, что оно не только подрывает их монополию на власть, но и дает международным технологическим компаниями право создавать общественные тренды, политическую повестку, а также потенциально служить инструментом для “смены режимов”. С одной стороны они обеспокоены конкуренцией со стороны технологических гигантов, с другой видят потенциал цифровой массовой слежки, который может использоваться ими как еще один инструмент государственной власти. Создавая более полную картину общества и индивидуального поведения, чем это было возможно раньше, он может позволить создать государство, более прозрачное, а в некоторых случаях более репрессивное, чем любое из существовавших в прошлом.

С самого начала техническое управление Интернетом осуществлялось вне прямого государственного контроля, хотя на практике американские инженеры и компании де-факто имели полномочия по разработке инженерных протоколов. До 1998 года управление Интернетом не было фокусе внимания многих стран. Но это изменилось, когда правительство США добилось своего рода монополии и пролоббировал создание Интернет-корпорации по присвоению имен и номеров (ICANN), частной некоммерческой организации, которая взяла на себя роль лидера в

управлении доменами. С тех пор, правительства по всему миру начали обращать внимание на эту проблему. Страны по-разному подошли к вопросу регулирования Сети. Для правительства США было критически важно, чтобы Интернет управлялся группой неправительственных и частных организаций через ICANN. Вашингтон предпочел ориентированное на рынок решение, предполагающее саморегулирование Интернета частным сектором (которое защищало экономические интересы США). В США законы Конгресса до сих пор защищают “шпионящий капитализм”, вместо того чтобы ограничить его влияние. Раздел 230 Закона о коммуникациях 1996 года охраняет права не пользователей, а владельцев сайтов от судебных исков и государственного преследования за пользовательский контент. Пользователь или поставщик интерактивных услуг не рассматривается как издатель, это скорее посредник между источником информации и тем, кто в этой информации нуждается. Поэтому компании надзорного капитализма не отвечают за последствия своей деятельности. Интернет-компании рассматриваются как «саморегулируемые» и никому не подотчетные. В Европе дело обстоит по-другому. Европейский Союз выступает за государственно-частную систему, в которой правительства играли важную роль - многостороннюю институциональную основу. Китай, Россия и другие страны в идеале хотели бы иметь исключительно государственную систему управления Интернетом, но в современных реалиях, хотя бы ту, которая была бы привязана к заключенным договоренностям, в рамках работы профильных комиссий Организации Объединенных Наций.

На заре Интернета многие мыслители представляли себе цифровой мир, свободный от государственного контроля. Его первые создатели и защитники представляли его как пространство без гражданства, не подконтрольное правительству. Действительно, многие считали, что любое управление разрушит его сущность. На ранней стадии развития Интернета ученые, инженеры, представители бизнеса и пользователи, которые управляли процессом, были довольны созданием уникального инструмента коммуникации, не заботясь о том, как этот инструмент будет использоваться. Мало кто осознавал и предвидел потенциальный вред и угрозы, которые могут возникнуть в результате неограниченной свободы умноженной на анонимность: кибер-буллинг, троллинг, распространение детской порнографиии, преследование меньшинств, интренет-мошеничество, кибер-терроризм - лишь небольшой перечень вызовов и угроз с которыми мы столкнулись в процессе развития интернета. Интернет-теоретики и корпорации когда-то объявили себя свободными от государства и управления, но этот этап в развитии информационного общества подходит к концу. Сегодня государства планомерно работают над тем, чтобы вернуть себе контроль.

Можно утверждать, что в начале двадцать первого века началась новая эра. Правительства во всем мире стали предупреждать о потенциальных нарушениях, вызванных доступом к цифровым коммуникациям, будь то обмен текстовыми сообщениями с использованием мобильных телефонов, творческое использование социальных платформ, таких как Facebook и Twitter, потоковая передача видео непосредственно в Интернет или использование Интернет в обход цензуры. Правительства все чаще искали новые способы контроля и мониторинга онлайн-пространства. В то же время во всем мире все чаще звучали призывы взять эту нерегулируемую среду под контроль правительства - призывы, мотивированные в

демократических государствах страхом перед преступностью и терроризмом, а в авторитарных - стремлением правительств сохранить свою власть. Здесь следует отметить, что несмотря на то, что интернет-инфраструктура построена по принципу децентрализации управления, потоков данных и информации, географически инфраструктура (оборудование, сервера, дата-центры) - расположена на национальных территориях. Для функционирования интернет нуждается в физических и информационных ресурсах, размещенных на других территориях. В этой связи у стран есть все рычаги для постепенного усиления национального контроля над информационными потоками и инфраструктурой. Так, например, Россия прилагает усилия по продвижению своего «цифрового суверенитета» с 2012 года. По мнению российских законодателей, цель состоит в том, чтобы разработать способ изолировать российский Интернет по требованию, чтобы он мог быть самодостаточным и независимым от действий иностранных держав, и можно было гарантировать его непрерывное функционирование при любой ситуации. С другой стороны, такая конфигурация также облегчит возможность полной или частичной блокировки обмена данными. Россия здесь не единственное государство, которое стремится к усилению контроля над сетью. Иран пытался сделать то же самое в течение многих лет, как и Китай со знаменитым Великим китайским фаерволом. Многие государства стремятся усилить свою власть над «своим» Интернетом, вплоть до частичного или полного отключения сети. Автократии и гибридные режимы часто ограничивают доступ к телефону и Интернету в напряженные времена. Немногие правительства смогли полностью перекрыть доступ в сеть; например, в Мьянме (Бирме) сделала это в 2007 году, и совсем недавно в 2021 году во время протестов. Один из самых известных примеров - Египет, правительство которого перекрыло почти весь доступ к сети и отключило услуги мобильной связи во время революции 2011 года. Однако как показывает практика - такие экстремальные решения не всегда приводят к ожидаемому результату, а лишь вредят телеком-инфраструктуре и важному инструменту современной коммуникации. Согласно исследованиям, сегодня более 40 стран фильтруют определенные интернет-сайты или сервисы, запрещая доступ к некоторым иностранным источникам новостей, социальным сетям, опредленным сайтам итд. В эпоху Интернета правительства нашли множество способов контролировать поток информации - или, по крайней мере, попытаться это сделать, - вмешиваясь в цифровую коммуникацию или ограничивая ее. Таким образом, по мере роста размеров и возможностей Интернета резко возросла способность государств и негосударственных субъектов использовать цифровые технологии для вторжения и контроля над несанкционированными коммуникациями.

Интернет и его обитатели столкнулся с вызовом как государственного, так и частного манипулятивного контроля и влияния - а иногда их комбинацией. Хотя многие правительства осуждают очевидное отсутствие правил в Интернете, в сети есть управление. Такое управление обеспечивается крупными компаниями в соответствии с их пользовательский договорами, условиями обслуживания, стандартами сообщества и процедурами верификации и безопасности. Таким образом, проблема для многих правительств заключается не в том, что Интернет является бесконтрольным, а в том, что он в меньшей степени подотчетен непосредственно им, что его законы создаются частными компаниями с помощью их кодов и алгоритмов. И не просто частными

компаниями, а иностранными компаниями, компаниями стран- экономических и политических конкурентов. Именно на оспаривание этой монополии технологических гигантов направлены усилия некоторых государств, именно это они продвигают под эгидой ‘цифровой суверенитет’. И если для США выгоден глобальный Интернет, управляемый частным сектором, так как большая часть тех-компаний является резидентами именно этой страны, то для других стран - эта модель не является экономически и политически целесообразной. Например, Китай всеми своими действиями дает понять, что отвергает любое понятие о независимой коммуникационной сети, не находящейся под надзором государства. Главная цель китайской дипломатии - продвигать идею кибер-суверенитета (или интернет-суверенитета) - что означает «уважение права каждой страны выбирать свой собственный путь развития Интернета, свою собственную модель управления Интернетом [и] свою собственную государственную политику в отношении Интернета». И представляется, что сегодня позицию Китая разделяют многие другие страны.

Мы живем, как гласит китайская пословица, в интересные времена, по крайней мере для тех, кто задается вопросами вроде «Что такое суверенная власть?» и «Откуда государство получает право осуществлять эту власть?». Каким образом цифровая революция конца двадцатого века, и в частности появление Интернета и глобального киберпространства, повлияли на организацию глобальной политики и, повлияли ли вообще? Проблема с термином «цифровой суверенитет» заключается в том, что он имеет разное значение для разных государств. Для некоторых «суверенитет» равнозначно слову = «правительство», и является стратегическими активов экономической и политической борьбы, требующий государственного контроля. Для других — это чисто технический вопрос, касающийся протоколов, необходимых для обеспечения работы и развития инфраструктуры, а управление должно просто сосредоточиться на смягчении вреда, возникающего в результате функционирования глобальной Сети. С одной стороны, цифровизация всего и вся, и расширение киберпространства как будто ведет к закату института национального государства, после полувека доминирования на международной политической и правовой арене; с другой - возможно этот закат сильно преувеличен, и мы еще увидим, как государство возьмет под контроль и зарегулирует весь Интернет.

К лучшему или к худшему, мы все идем ко все более цифровому будущему, которое, вероятно, будет наполнено более умным искусственным интеллектом (ИИ), более быстрыми коммуникациями и более сложной информацией. Нет сомнений, что конкурентная борьба за цифровой суверенитет будет продолжаться. Любой стране, которая озабочена вопросами цифрового суверенитета, и не хочет попасть в положение, определяемое конкуренцией между США и Китаем, нужны инструменты для достижения своей относительной автономии. Для этого необходимо стимулировать увеличение государственных и частных инвестиций в следующее поколение ИИ; веб-сервисы, включая данные; полупроводники; и 6G. Это не только будет способствовать росту экономики, но и поможет государствам стать более автономными и эффективными в супер-индустриальном пост-информационном мире будущего.

Список источников:

1. Philosophy & Technology, The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU, Luciano Floridi, August 2020, Ссылка:https://link.springer.com/article/10.1007/s13347-020-00423-6
2. Fondapol, Digital sovereignty - Steps towards a new system of internet governance, Farid Gueham, January 2017, Ссылка:https://www.fondapol.org/en/study/digital-sovereignty-steps-towards-a-new-system-of-internet-governance/
3. French Economic, Social and Environmental Council, Towards a European digital sovereignty policy, March 2019, Ссылка:https://www.lecese.fr/sites/default/files/travaux_multilingue/2019_07_souverainete_europeenne_numerique_GB_reduit.pdf
4. Wilson Center, Digital Sovereignty on Paper: Russia's Ambitious Laws Conflict with Its Tech Dependence, Alena Epifanova, October 2020, Ссылка:https://www.wilsoncenter.org/blog-post/digital-sovereignty-paper-russias-ambitious-laws-conflict-its-tech-dependence
5. Berlin Social Science Center (WZB), Digital sovereignty, Julia Pohle, December 2020, Ссылка: https://policyreview.info/concepts/digital-sovereignty
6. The Heinrich Böll Foundation, Digital Sovereignty - The EU in a Contest for Influence and Leadership, Zora Siebert, February 2021, Ссылка:https://www.boell.de/en/2021/02/10/digital-sovereignty-eu-contest-influence-and-leadership
7. The Conversation, 'Digital sovereignty': can Russia cut off its Internet from the rest of the world? Francesca Musiani, Benjamin Loveluck, Françoise Daucé, Ksenia Ermoshina, October 2019, Ссылка:https://theconversation.com/digital-sovereignty-can-russia-cut-off-its-internet-from-the-rest-of-the-world-125952
8. EPRS | European Parliamentary Research Service, Towards a more resilient EU, Tambiama Madiega, July 2020, Ссылка:https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf
9. Эра надзорного капитализма — ключевые идеи книги Шошаны Зубофф, Konstantin Smygin, Февраль 2021, Ссылка:https://vc.ru/books/203887-era-nadzornogo-kapitalizma-klyuchevye-idei-knigi-shoshany-zuboff
10. Egypt Cuts Off Most Internet and Cell Service, The New York Times, Matt Richtel, January 2011, Ссылка:https://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html
11. A Struggle for Information Control Between China's Government and the Tech Giants, The Diplomat, Canghao Chen, August 11, 2021 Ссылка:https://thediplomat.com/2021/08/a-struggle-for-information-control-between-chinas-government-and-the-tech-giants
12. The End of Cyberspace, The Atlantic, Alexis C. Madrigal, May 2019, Ссылка:https://www.theatlantic.com/technology/archive/2019/05/the-end-of-cyberspace/588340/