

РИСКИ И УГРОЗЫ ЦИФРОВОМУ СУВЕРЕНИТЕТУ ЛИЧНОСТИ В КИБЕРПРОСТРАНСТВЕ

Артем Сергеевич Васекин^а

DOI: 10.22394/2070-8378-2024-26-5-72-77

а Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации

Аннотация: В настоящей статье выделены и проанализированы риски и угрозы цифровому суверенитету личности в киберпространстве. С увеличением объема собираемых и обрабатываемых данных возникает вопрос о праве индивидов контролировать свои данные и определять возможности их использования. Цифровой суверенитет можно рассматривать как ответ на вызовы, которые возникают в контексте массовой цифровизации. В условиях, когда личные данные становятся ценным товаром, важно, чтобы каждый пользователь осознавал свои права и возможности. Широкое применение «умных» устройств, технологий мобильности и связи, использование цифровых профилей и аккаунтов поднимает вопрос о необходимости защиты цифровых прав человека как одного из ключевых элементов цифрового суверенитета личности. В научно-практической литературе в последнее время уделяется значительное внимание цифровому и технологическому суверенитету государства, однако остается малоизученным целый ряд проблем, отражающих особенности развития личности в условиях цифровизации и глобального развития интернет-технологий и платформ. Хотя государство несет ответственность за нарушения прав человека и является основным носителем обязанностей по обеспечению прав личности, социальные платформы и крупные технологические компании в большинстве юрисдикций по-прежнему злоупотребляют своей властью. Тот факт, что социальные платформы являются корпоративными образованиями и могут причинить определенный вред правам человека, подтверждает необходимость признания их носителями обязанностей в области этих прав и привлечения к ответственности в случае их нарушения.

Ключевые слова: цифровой суверенитет, киберпространство, персональные данные, конфиденциальность, информационная безопасность, риски и угрозы

Дата поступления статьи в редакцию: 11 июня 2024 года.

RISKS AND THREATS TO THE DIGITAL SOVEREIGNTY OF THE INDIVIDUAL IN CYBERSPACE

Artem S. Vasekin^a

RESEARCH ARTICLE

a Russian Presidential Academy of National Economy and Public Administration

Abstract: This article highlights and examines the risks and threats to an individual's digital sovereignty in cyberspace. As more data is gathered and processed, the issue of people's right to control their data and decide how it can be used arises. Digital sovereignty can be viewed as a reaction to the difficulties presented by widespread digitalization. Given the increasing value of personal data, each user must recognize their rights and freedoms. Protecting digital human rights is a crucial component of an individual's digital sovereignty, as evidenced by the growing use of smart devices, mobility, and communication technologies, as well as digital profiles and accounts. Recently, the state's digital and technological sovereignty has received significant attention in the scientific and practical literature. However, there are still many issues that reflect the unique characteristics of personal growth in the context of digitalization and the worldwide growth of Internet technologies and platforms. Even though the state is responsible for individual rights and is accountable for human rights violations, social media platforms and major tech companies still misuse their influence in most jurisdictions. Given that social media platforms are businesses and have the potential to violate human rights, it is imperative that they be acknowledged as duty-bearers of those rights and held responsible when they do so.

Keywords: digital sovereignty, cyberspace, personal data, privacy, information security, risks and threats

Received: June 11, 2024.

Введение

С развитием технологий киберпространство постепенно превращается из аппаратной межсетевой инфраструктуры в виртуальную среду, в которой люди, бизнес и органы государственной власти взаимодействуют с помощью современных информационных и коммуникационных технологий. Как правило, процессы цифровизации инициируются крупными технологическими компаниями, контролирующими онлайн-платформы и большие массивы данных, где информация о пользователях легко доступна и может быть использована для целей анализа, в том числе для улучшения и модернизации существующих бизнес-операций. Нередко такие данные представляют собой индивидуальную (личную) информацию, включающую различные онлайн-профили, то есть «цифрового двойника» человека.

С увеличением объема собираемых и обрабатываемых данных возникает вопрос о цифровом суверенитете личности – об особом праве индивидов контролировать свои данные и определять возможности их использования. Цифровой суверенитет можно рассматривать как ответ на вызовы, которые возникают в контексте массовой цифровизации. В условиях, когда личные данные становятся ценным товаром, важно, чтобы каждый пользователь осознавал свои права и возможности.

Существует мнение, что одним из конститутивных признаков защиты цифрового суверенитета личности является обеспечение цифровых прав. Так, в докладе Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека отмечено, что «в своей совокупности “цифровые” права формируют “цифровой суверенитет” личности, в основе которого лежит понимание, что человек не равен “цифровому вектору”, то есть набору цифровых коэффициентов, вычисленных цифровыми платформами и помещенных в тот или иной реестр...»¹.

Несмотря на отсутствие нормативного закрепления цифрового суверенитета личности, существуют правовые и нормативные акты, обеспечивающие возможность независимой и автономной деятельности человека в цифровом пространстве [Гаврилов, 2020. С. 146–152], а также его защиту в данной сфере, в том числе статьи Конституции Российской Федерации по основным правам человека (ст. 19, 23, 28 и др.), ст. 141.1 ГК РФ о циф-

ровых правах, «право на забвение» в Интернете², Закон «О персональных данных»³ и т.д. [Мочалов, 2022. С. 27–39].

Нарушение цифрового суверенитета личности: риски и угрозы

Существует множество ситуаций, условий и факторов при использовании цифровых технологий, которые приводят к полной или частичной потере контроля человека над собственной конфиденциальной, приватной и чувствительной информацией и приводят к нарушению прав человека в киберпространстве. Такие ситуации в настоящей статье мы будем называть «рисками» или «угрозами» цифровому суверенитету личности. Перечислим и проведем краткий анализ некоторых из них.

Принудительное вовлечение граждан в цифровую среду.

Эта угроза была выделена в докладе Совета при Президенте Российской Федерации по развитию гражданского общества и правам человека⁴. Авторы доклада отмечают неоправданность в некоторых случаях принудительной цифровизации в сфере государственных и муниципальных услуг при проектировании и планировании национальных программ и стратегий, игнорирование прав граждан на сохранение традиционных способов взаимодействия с государством, а также медицинские, экономические и технологические ограничения некоторых людей.

Снижение правовой защиты в Интернете и ответственности государственных и частных структур за сохранение персональных данных.

Социальные платформы и сети оказывают большое влияние на цифровой суверенитет личности в связи с их неограниченными возможностями по сбору личных и чувствительных данных, по блокировке и фильтрации контента, по манипуляции с уязвимыми группами населения и т.д. Вместе с тем многие крупные социальные сети самостоятельно определяют политику, нормы и стандарты поведения для пользователей, обеспе-

1 Цифровая трансформация и защита прав человека в цифровом пространстве. Доклад Совета при Президенте РФ по развитию гражданского общества и правам человека. М., 2021. <https://ifap.ru/pr/2021/n211213a.pdf>

2 О внесении изменений в ФЗ «Об информации, информационных технологиях и о защите информации» и ст. 29 и 402 ГК РФ. ФЗ от 13 июля 2015 года № 264-ФЗ. *Российская газета*. 16 июля 2015 года. № 154.

3 О персональных данных. ФЗ от 27 июля 2006 года № 152-ФЗ. *Российская газета*. 29 июля 2006 года. № 4131.

4 Цифровая трансформация и защита прав граждан в цифровом пространстве: Доклад Совета при Президенте РФ по развитию гражданского общества и правам человека (Москва, 2021 г.). http://presidentsovet.ru/docs/doclad_SPCh.docx

Социум

чивают соблюдение этой политики, регулируют и разрешают конфликты.

Существует мнение, что такие сети представляют собой «квазигосударственный институт», обладающий многими основными характеристиками развитой политической системы [Busch, 2013]. Следовательно, социальные платформы обладают властью, представляющей собой особую угрозу для реализации гражданских прав и свобод, что может привести к нарушению и цифрового суверенитета личности.

Хотя государство несет ответственность за нарушения прав человека и является основным носителем обязанностей по обеспечению прав личности, социальные платформы и крупные технологические компании в большинстве юрисдикций по-прежнему злоупотребляют своей властью. Тот факт, что социальные платформы являются корпоративными образованиями и могут причинить определенный вред правам человека, подтверждает необходимость признания их носителями обязанностей в области этих прав и привлечения к ответственности в случае их нарушения.

Угроза интернет-зависимости или проблемного использования Интернета охватывает такие формы поведения в Интернете, как увлечение азартными играми, чрезмерное использование социальных сетей, «киберзапугивание» и «киберхондрия», которые могут иметь последствия для психического и физического здоровья человека. С точки зрения цифрового суверенитета личности эта угроза может повлиять на такие права, как право на здоровье и безопасность, а также на права конкретных уязвимых групп (например, права ребенка).

«Культура отмены» и социальная инженерия

Понятие «культура отмены» относится к действиям социальной «отмены» человека, формам социального ostracism, вызванного действиями других и направленного на то, чтобы обесценить мнения человека-жертвы и даже фактически его существование в некоторых сферах жизни общества. В специальной литературе это явление обычно упоминается в контексте взаимодействия в социальных сетях (например, публикация верных или ложных комментариев о социально предосудительном поведении, таком как жестокое обращение с детьми или гендерное насилие). Очевидно, что «культура отмены» является серьезной проблемой для формирования цифрового суверенитета личности.

С социальной отменой личности могут быть связаны и некоторые методы социальной инже-

рии. Например, когда за счет использования искусственного интеллекта и информации из социальных сетей формируется клеветническая кампания посредством выпуска фейковых новостей в отношении определенного человека.

Риски, связанные с этическими и образовательными аспектами цифрового суверенитета личности.

Для развития цифровой грамотности населения органы государственной власти разрабатывают образовательные программы и тренинги по вопросам этики цифрового взаимодействия, защиты персональных данных, защиты авторских прав, защиты от цифрового буллинга, ориентированные на все группы населения. Представляется, что цифровое образование должно учитывать этические, социальные и нормативные аспекты, а не только ориентироваться на обучение технологическим и информационным возможностям и навыкам людей.

Риски для конфиденциальности и безопасности в Интернете, связанные с искусственным интеллектом.

Системы искусственного интеллекта присутствуют во многих сферах частной и общественной жизни. В здравоохранении развивается роботизированная хирургия, внедряются ультразвуковые исследования сердца, распространяется клиническая диагностика на основе систем машинного обучения. Многие врачебные действия основаны на технологиях искусственного интеллекта с целью улучшения результатов лечения и повышения качества обслуживания пациентов.

Однако существует множество юридических и этических проблем, касающихся использования систем искусственного интеллекта, например, в части замены человеческого участия и личного доверия к полученным данным, выводам и т.п. Отмечается появление и развитие технологий доверенного искусственного интеллекта. Обеспечение правовой базы для технологических инструментов – это непростой процесс. За этим скрывается множество рисков, в том числе связанных с защитой цифрового суверенитета личности, поскольку технологии во многих случаях предшествуют формированию правовой базы, поэтому необходимо активно разрабатывать правовые основы для внедрения искусственного интеллекта. В своей Белой книге по искусственному интеллекту Европейская комиссия⁵ подчеркнула, что искусственный интеллект должен использоваться в сочетании с законодательством о правах

⁵ White Paper on Artificial Intelligence: a European approach to excellence and trust – European Commission (europa.eu).

человека, особенно с учетом защиты конфиденциальности и прав на данные.

Риски автоматизированного принятия решений, в том числе связанные с автоматизированной обработкой персональных данных (профилированием).

Прогресс в области алгоритмов машинного обучения облегчил использование данных как в государственном, так и в частном секторах для генерации / извлечения знаний, содействия принятию обоснованных решений, а в последствии – и для автоматизированного принятия решений.

Автоматизированное принятие решений, наряду с социальными и экономическими выгодами, может иметь и негативные последствия и риски для цифрового суверенитета личности, включая нарушение прав на неприкосновенность частной жизни, защиту персональных данных, ограничение свободы выбора, подрыв человеческого достоинства и автономии, увеличение предвзятости и дискриминации, а также возникновение социальной сегрегации. Во многом это связано с непрозрачностью используемых алгоритмов, вероятностным характером действий, связанных с качеством входных данных, и т.п.

Риски конфиденциальности, связанные с воздушным наблюдением и дронами.

С развитием технологий дронов и беспилотных летательных аппаратов появляются различные новые возможности бизнес-моделей, такие как доставка посылок по воздуху, аэрофотосъемка, воздушное такси, дронная журналистика и т.д.

Современные дроны обладают рядом технологических возможностей, связанных с захватом и хранением большого объема данных, перехватом сообщений, автономным отслеживанием цели, распознаванием изображений и звуков, а также могут взаимодействовать с другими устройствами и сетью Интернет. В этой связи персональные и приватные данные, полученные с использованием дронов, не только могут быть легко доступны, но и анонимно собраны в тех областях, где люди обоснованно ожидают приватности и конфиденциальности. Кроме того, дроны могут быть взломаны и перехвачены, в том числе с возможностью получения данных, хранящихся во внутренней памяти.

В этом контексте дроны – технология, обеспечивающая функциональность другим технологиям (например, камерам, звукозаписывающим устройствам, GPS) и позволяющая их использовать в совершенно новых условиях, предлагает совершенно новые возможности наблюдения, что представляет значительную угрозу цифровому суверенитету личности.

Представляется, что массовое внедрение дронов в общественную жизнь, несмотря на все новые возможности и преимущества, может привести к сдерживающему эффекту, когда люди почувствуют себя менее свободными и будут проявлять инстинкт самосохранения путем ограничения своего поведения в общественных и частных локациях.

Цифровая мобильность как угроза цифровому суверенитету личности

Ряд прямых и косвенных угроз цифровому суверенитету стал очевидным в условиях развития глобального рынка мобильной связи. Мобильность становится быстро развивающимся трендом и одновременно увеличивает потенциальные угрозы цифровым правам и суверенитету личности. Даже во время COVID-19, когда передвижения, социальные контакты были строго ограничены, возникли соответствующие угрозы в отношении цифрового суверенитета личности из-за использования цифровых мобильных приложений.

Цифровые мобильные приложения зачастую используются для отслеживания территориальных передвижений, наблюдения за сотрудниками с помощью систем видеонаблюдения, сбора персональных данных и могут работать без явного согласия пользователей. При этом платформы цифровой мобильности, продвигающие мобильность как услугу, включают в себя широкий спектр транспортных поставщиков, часто базирующихся в разных странах или даже континентах, предлагающих варианты поездок на такси, автобусе, поезде, велосипеде или электросамокате, что создает проблему юрисдикционной защиты прав человека в зависимости от выбранных технологий.

Появление больших баз данных в результате использования облачных сервисов, наряду с искусственным интеллектом, создает новые социальные и этические угрозы, например, общественной «слежки» в сочетании с рисками кибербезопасности. Поскольку большие наборы данных также продаются рекламным организациям за пределами национальных границ через различные платформы, очевидно, что для отдельных пользователей становится практически невозможным полностью обеспечить цифровой суверенитет личности. Последнее связано с неизбежными трудностями в определении того, кто несет ответственность и должен противодействовать таким угрозам. При этом некоторые нормативные требования трудно реализовать на практике, особенно в транспортном секторе, когда ответственность при передаче данных мобильных услуг выходит за пределы определенной юрисдикции.

Деплатформирование как принудительная блокировка или удаление пользователя

«Деплатформирование» означает исключение пользователя из конкретной технологической платформы или социальной сети путем закрытия его учетных записей, запрета или блокирования использования системы или ее услуг. Обычно это происходит из-за содержания высказываний или блогов пользователя платформы. В результате деплатформирования деятельность прерывается, и ее результаты не могут быть доведены до целевой аудитории [D’Orazio, 2022. Р. 269; Jhaver, Boylston, Yang, Bruckman, 2021. Р. 16–30]. Это рассматривается как некая форма цензурирования, как одностороннее навязывание власти с помощью нерегулируемых «больших технологий». Эта форма ограничения дает возможность технологическим компаниям манипулировать общественным дискурсом. Зачастую информационные платформы (социальные сети, торговые, платежные и сервисные платформы, услуги интернет-инфраструктуры (хостинг и т.п.) оправдывают удаление или блокировку пользователя и его контента нарушениями условий пользовательского соглашения.

Представляется, что деплатформирование отрицательно влияет на цифровой суверенитет личности и такие права, как свобода выражения мнений, и является крайней формой модерации контента, наказания за нарушение приемлемого поведения. Деплатформирование оправдано обращением к более широкой дискурсивной стратегии, которая пытается со временем остановить распространение потенциально вредных высказываний и сообщений [Там же. Р. 280].

Риски суверенитету личности, связанные с «умными» носимыми устройствами

Проблемы, которые порождают «умные» носимые устройства, можно разделить на две общие категории, с важным замечанием, что границы между ними могут быть размытыми: угроза автономии и угроза конфиденциальности. Угроза автономии касается возможности того, что носимые технологии могут повлиять на автономность пользователя таким образом, что снизят их способность принимать решения и направлять курс своей жизни в соответствии со своими желаниями и целями. Угроза конфиденциальности связана с риском того, что носимые устройства могут собирать, обрабатывать или хранить персональные данные, относящиеся только к их пользователям.

Носимые устройства обладают тремя особенностями, которые по отдельности и вместе увеличивают риски цифровому суверенитету личности. В частности, их присутствие непосредственно на человеке (близость) в сочетании с их легкой до-

ступностью (удобством) и вездесущностью (повсеместностью) может сделать их основными векторами вмешательства, влияющими на автономию пользователя и нарушающими его право на неприкосновенность частной жизни.

Индивид становится слишком зависимым от устройства, так что его собственные навыки и способность принимать решения атрофируются до такой степени, что автономия оказывается под угрозой. Такое явление часто называют «декалфикацией» [McKinlay, 2016]. Опасность зависимости возникает в двух случаях: во-первых, когда индивид попадает в ситуацию недоступности технологий или поломки самого устройства (телефона, планшета) и, во-вторых, когда зависимость приводит к уменьшению контроля над другими сферами жизни человека.

Что касается первого случая, то все меньше и меньше людей запоминают телефонные номера, перекладывая эту задачу на свои цифровые устройства, к которым все чаще относятся и будут причисляться «умные» носимые устройства. Это очень удобно и может быть интерпретировано как высвобождение когнитивных ресурсов для реализации более широких, более ценных и подлинных желаний и целей. Однако при возникновении ситуации недоступности устройств пользователи оказываются неспособными вспомнить информацию из-за отсутствия навыков в этой области. Это может варьироваться от легкого раздражения до серьезной опасности – в зависимости от ситуации, в которой происходит сбой навыка. Подобный пример – потеря навигационных навыков из-за чрезмерной зависимости от спутниковых навигационных систем. Логика аналогична: когда спутниковая навигация недоступна, пользователь из всех сил пытается найти дорогу, используя бумажные карты или альтернативные методы навигации.

Так, исследования Баумгартнера относительно влияния технологий на контроль других сфер жизни у подростков показали, что растущее использование и зависимость от различных технологий во многих случаях коррелируют с ухудшением способности внимания [Baumgartner, Schuur van der, Lemmens, Poel, 2018. Р. 24]. Снижение этих способностей представляет собой угрозу способности человека развивать автономную психическую жизнь, препятствуя саморефлексивному рассуждению и идентификации подлинных желаний и целей.

Заключение

Все это возлагает на разработчиков этих технологий эпистемический и моральный долг быть добросовестными и проявлять должную осмо-

трительность в доступе к косвенному влиянию на формирование зависимости от технологии. Это также требует, чтобы развитие цифрового суверенитета было направлено на минимизацию этого воздействия. Приведенная в статье систематизация рисков и угроз цифровому суверенитету личности не окончательна; она может по-

стоянно обновляться в связи с динамичным внедрением процессов цифровизации в различные сферы общественной жизни. Анализ цифровых угроз и рисков может послужить фундаментом для выработки направлений развития цифрового суверенитета личности и защиты его персональных данных.

Литература

- Гаврилов Е.О. Цифровой суверенитет в условиях глобализации: философский и правовой аспекты. *Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки*. 2020. № 2 (14). С. 146–152. <https://doi.org/10.21603/2542-1840-2020-4-2-146-152>. EDN: WCSQFR
- Мочалов А.Н. Об учреждении в России должности уполномоченного по защите прав человека в сфере информационно-телекоммуникационных технологий. *Правовое государство: теория и практика*. 2022. № 2 (68). С. 27–39. <https://doi.org/10.33184/Zpravgos-2022.23>
- Baumgartner S.E., Schuur van der W.A., Lemmens J.A., Poel te F. The relationship between media multitasking and attention problems in adolescents: Results of two longitudinal studies. *Human Communication Research*. 2018. No. 44 (1). P. 3–30. <https://doi.org/10.1111/hcre.12111>. In English
- Busch T. Fair Information Technologies: The Corporate Responsi-

- bility of Online Social Networks as Public Regulators 71 (2013). <https://www.alexandria.unisg.ch/228863/>. In English
- D'Orazio D. Deplatforming in Theory and Practice: The Ann Coulter Debacle // Macfarlane E. (eds.) *Dilemmas of free expression*. Toronto: University of Toronto Press, 2022. P. 269–298. In English
- Jhaver S., Boylston C., Yang D., Bruckman A. Evaluating the Effectiveness of Deplatforming as a Moderation Strategy on Twitter // *Proceedings of the ACM on Human-Computer Interaction*. 2021. Vol. 5. No. CSCW2, Article 381. P. 1–30. 10.1145/3479525. In English
- McKinlay R. Technology: Use or lose our navigation skills. *Nature*. 2016. P. 573–575. <https://doi.org/10.1038/531573a>. In English
- Zuboff P.S. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. London: Profile Books, 2019. In English

References

- Gavrilov E.O. Digital sovereignty in the context of globalization: philosophical and legal aspects. *Vestnik Kemerovskogo gosudarstvennogo universiteta. Seriya: Gumanitarnyye i obshchestvennyye nauki*. 2020. No. 2 (14). P. 146–152. <https://doi.org/10.21603/2542-1840-2020-4-2-146-152>. EDN: WCSQFR. In Russian
- Mochalov A.N. On the establishment of the position of ombudsman for the protection of human rights when using information technologies in Russia. *Pravovoye gosudarstvo: teoriya i praktika*. 2022. No. 2 (68). P. 27–39. <https://doi.org/10.33184/Zpravgos-2022.23>. In Russian

ИНФОРМАЦИЯ ОБ АВТОРЕ:

Артем Сергеевич Васекин, аспирант Института государственной службы и управления Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (Российская Федерация, 119606, Москва, проспект Вернадского, 84). E-mail: vasekin-as@ranepa.ru

Для цитирования: Васекин А.С. Риски и угрозы цифровому суверенитету личности в киберпространстве. *Государственная служба*. 2024. № 5. С. 72–77.

INFORMATION ABOUT THE AUTHOR:

Artem S. Vasekin, postgraduate student of the Institute of Public Administration and Civil Service Russian Presidential Academy of National Economy and Public Administration (84, Vernadsky Prospekt, Moscow, 119606, Russian Federation). E-mail: vasekin-as@ranepa.ru

For citation: Vasekin A.S. Risks and threats to the digital sovereignty of the individual in cyberspace. *Gosudarstvennaya sluzhba*. 2024. No. 5. P. 72–77.