DOI: 10.31857/S0321507525020023

Цифровой суверенитет африканских стран: угрозы и способы защиты

© Суфиянова Г.Р.[a], 2025

[a] Тюменский государственный университет,
Тюмень, Россия
ORCID: 0000-0002-9020-7771; g.r.sufiyanova@utmn.ru

Резюме. В статье анализируются последствия цифровизации Африканского континента в контексте технологического, экономического и политического соперничества между США и КНР и роста зависимости Африки от внешних партнеров. Центральное место занимает проблема защиты данных, использование которых рассматривается экспертами через понятия «колониализм данных», «цифровой колониализм» и «цифровой суверенитет».

Отмечается, что, с одной стороны, цифровые технологии могут способствовать повышению производительности, динамичному росту, структурным изменениям и реализации Целей устойчивого развития на Африканском континенте, с другой – они создают новые проблемы и вызовы. Делается вывод, что цифровому суверенитету государств Африканского континента кроме технологических, экономических проблем препятствует соперничество в киберпространстве внерегиональных акторов, прежде всего США, КНР и ЕС, в нормативно-правовой сфере, принимающей политико-идеологический характер.

Достичь цифрового суверенитета, понимаемого как право государства регулировать и осуществлять контроль над технологиями, услугами и цифровыми данными, используемыми на суверенной территории, в текущих обстоятельствах крайне сложно в связи с тем, что преодоление многих проблем невозможно без инвестиций и участия западных и азиатских цифровых гигантов, которые в условиях активного соперничества за Африку сами являются их причиной.

Ключевые слова: Африка, цифровой колониализм, цифровой суверенитет, суверенитет данных, цифровая экономика, защита данных, цифровое противостояние

Для цитирования: Суфиянова Г.Р. (Тюмень). Цифровой суверенитет африканских стран: угрозы и способы защиты. *Азия и Африка сегодня*. 2025. № 2. С. 14–22. DOI: 10.31857/S0321507525020023

Digital Sovereignty of African Countries: Threats and Ways to Protect Them

© Gulnur R.Sufiyanova[a], 2025

[a] University of Tyumen, Tumen, Russia
ORCID: 0000-0002-9020-7771; g.r.sufiyanova@utmn.ru

Abstract. The article analyzes the consequences of digitalization of the African continent in the context of technological, economic and political rivalry between the United States and China, and Africa's growing dependence on external partners.

The central issue is data security, the process of using the data is considered by the experts through the concepts of "data colonialism", "digital colonialism" and "digital sovereignty".

The author notes that, on the one hand, digital technologies can contribute to increased productivity, dynamic growth, structural changes and the implementation of the Sustainable Development Goals on the African continent; on the other hand, they create new problems and challenges. It is concluded that the digital sovereignty of the states of the African continent, in addition to technological and economic problems, is hampered by competition in cyberspace of extra-regional actors, primarily the United States, China and the EU, in the regulatory and legal field, which is taking on a political and ideological nature.

It is extremely difficult to achieve digital sovereignty, understood as the right of states to regulate and exercise control over technologies, services and digital data used on sovereign territory in the current circumstances due to the fact that overcoming of quite a few issues is impossible without investment and participation of Western and Asian digital giants, which, in the context of active competition for Africa, are themselves the cause of them.

Keywords: Africa, digital colonialism, digital sovereignty, data sovereignty, digital economy, data protection, digital confrontation

For citation: Sufiyanova G.R. (Tyumen). Digital Sovereignty of African Countries: Threats and Ways to Protect Them. *Asia and Africa today*. 2025. № 2. Pp. 14–22. (In Russ.). DOI: 10.31857/S0321507525020023

ВВЕДЕНИЕ

Африка – второй по величине и численности населения континент в мире – переживает значительный рост спроса на интернет-подключение и развитие информационно-коммуникационных технологий (ИКТ) в целом. Решением этих проблем являются проекты внерегиональных акторов в области цифровизации континента (прокладка «цифровых коридоров» – сети подводных оптоволоконных кабелей, которые проходят вдоль восточного и западного побережий континента, проекты в сфере облачных технологий, центров хранения данных, умных городов и т.п.).

ЦИФРОВЫЕ ПРОЕКТЫ В АФРИКЕ

В цифровизации африканских государств участвуют, прежде всего, американские (*Google, Apple, Facebook, Amazon* и *Microsoft*) и китайские (*Baidu, Alibaba, Tencent, Xiaomi*) гиганты. Так, компания *Google* в 2021 г. объявила о плане инвестировать $1 млрд в течение следующих 5 лет для поддержки цифровой трансформации Африки. Один из ключевых проектов компании – проект *Equiano*, подводный оптоволоконный кабель протяженностью 15 000 км от Португалии до Южной Африки с двумя стратегическими точками подключения в Нигерии и Намибии. Кабель был запущен в 2022 г.[1] По предварительным подсчетам, *Equiano* увеличит возможности подключения в Нигерии в 5 раз, в 2 раза – в Южной Африке и Намибии. Он способствует созданию 1,6 млн рабочих мест в период с 2022 по 2025 г. и снижению цен на передачу данных на 16–21%[2].

Кроме этого, компания объявила о запуске в Южной Африке первого на континенте «облачного региона». «Облачные регионы» *Google* позволяют пользователям развертывать облачные ресурсы, размещенные на серверах *Google*, в определенных географических точках. Физический центр обработки данных *Google* будет размещен недалеко от Кейптауна.

О реализации еще одного крупного проекта *2Africa* – подводной магистрали длиной 37 тыс. км 4 мая 2020 г. объявили *Meta, China Mobile International, MTN GlobalConnect, Orange, Vodafone* и *WIOCC*. «Крупнейшая в истории подводная оптоволоконная кабельная система»[3], как называет ее *Meta*, будет опоясывать континент, соединит 16 африканских стран и «произведет экономический эффект в размере от $26,4 до $36,9 млрд (по ППС) для Африки в течение 2–3 лет»[4], что эквивалентно ВВП Сенегала в 2022 г.

В 2021 г. Европейская комиссия объявила о стратегии *Global Gateway*, направленной на поддержку развития инфраструктуры по всему миру[5]. Проект предусматривает прокладку подводного оптоволоконного кабеля *EurAfrica Gateway*, который соединит Европейский и Африканский континенты, и создание внутриконтинентальных сетей оптоволоконных кабелей.

[1] https://www.submarinecablemap.com/submarine-cable/equiano (accessed 15.02.2024)
[2] https://african.business/2023/07/technology-information/can-africa-achieve-digital-sovereignty-in-an-era-of-big-tech (accessed 04.04.2024)
[3] https://www.2africacable.net/ (accessed 10.03.2024)
[4] https://furtherafrica.com/2023/08/23/mozambiques-nacala-linked-to-largest-submarine-cable-in-the-world/ (accessed 10.03.2024)
[5] https://www.eeas.europa.eu/delegations/russia/%D0%B8%D0%BD%D0%B8%D1%86%D0%B8%D0%B0%D1%82%D0%B8%D0%B2%D0%B0-global-gateway (accessed 18.03.2024)

Компании *Alcatel Submarine Networks* (*ASN*), *Elettra Tlc* и *Orange* объявили о начале реализации проекта *Medusa,* в рамках которого планируется прокладка самого длинного в Средиземном море подводного интернет-кабеля протяженностью более 8700 км, который соединит Европу и Северную Африку[6]. Подсистема *Via Tunisia*, часть кабеля *Medusa*, финансируется Европейским союзом в рамках программы *Connecting Europe Facility* (*CEF*).

В создании цифровой инфраструктуры в Африке активно участвуют китайские фирмы. *Huawei* и *ZTE* построили почти 80% сетевой инфраструктуры третьего поколения (*3G*) в Африке, *Huawei* построила 70% всех сетей четвертого поколения (*4G*) и конкурирует за создание всех будущих сетей *5G* в Африке.

Стоит отметить, что за последнее десятилетие фокус внимания Китая постепенно переместился с создания сетей на передачу знаний, развитие облачных технологий, решения в области искусственного интеллекта и проекты «умных городов» [1]. Примерами могут стать два проекта – технологический город Конза в Кении и дата-центр *Zamengoe* в Камеруне. Кроме того, при технической поддержке *Huawei* запланировало строительство Национального центра обработки данных Диамниадио в Сенегале, который станет местом хранения данных государственных и правительственных учреждений [1].

Технологические гиганты утверждают, что подобные проекты в конечном итоге укрепят цифровой суверенитет стран Африканского континента. Однако как эксперты, так и представители общественных организаций рассматривают их как стратегические долгосрочные шаги по расширению базы пользователей на континенте. Поскольку, по прогнозам, к 2050 г. в африканских странах будет проживать не менее 25% населения мира, а технологические компании теряют активных пользователей в Европе и Америке, Африка представляет собой значительную возможность для роста. Увеличивающийся спрос на цифровые услуги в сочетании с растущим объемом генерации данных позволил экспертам Международного союза электросвязи прогнозировать развитие цифровой экономики Африки до $180 млрд к 2025 г.[7]

С этой точки зрения Африка является перспективным партнером и для российских *IT*-компаний. Тем более что сами африканские страны проявляют интерес к опыту России, которая за последние пару лет серьезно укрепила свой цифровой суверенитет. Заметим, что на территории Африканского континента уже работают российские *IT*-компании («Яндекс», «Лабратория Касперского», «Вымпелком», *Razio Group* и др.) и используются российские разработки (так, для обеспечения кибербезопасности в ряде стран используется решение российской компании *StormWall*). Являясь одним из лидеров по развитию информационных технологий в органах государственной власти, образовании, телемедицины, РФ предлагает сотрудничество в области *IT*-технологий и готова к нему (прежде всего в области программного обеспечения), информационной безопасности, подготовки кадров, в т.ч. специалистов по управлению данными[8].

СОДЕЙСТВИЕ РАЗВИТИЮ ИЛИ ЦИФРОВОЙ КОЛОНИАЛИЗМ?

Анонсирование и реализация подобных крупномасштабных проектов актуализировали и усилили дебаты среди исследователей относительно последствий цифровизации континента. Цифровые стратегии и проекты США, ЕС, КНР и других стран в области ИКТ рассматриваются в экономическом, социальном, политическом и геоэкономическом аспектах. Африка стала не только полем технологической конкуренции между мировыми лидерами. Как справедливо отмечает профессор, завкафедрой американских исследований СПбГУ Н.А.Цветкова, в настоящее время «решаются вопросы о том, на компьютеры какой страны… будет собираться информация о пользователях в других странах, кто из них будет

[6] https://medusascs.com/alcatel-submarine-networks-elettra-tlc-medusa-and-orange-announce-the-beginning-of-the-construction-of-medusa-submarine-cable-system-in-the-mediterranean-sea/ (accessed 28.03.2024)

[7] https://gga.org/navigating-digital-sovereignty-in-africa-a-review-of-key-challenges-and-constraints/ (accessed 20.03.2024)

[8] В 2023 году на саммите Россия – Африка Центр изучения Африки ВШЭ и компания «Иннопрактика» представили Программу по обмену знаниями в сфере цифровизации государственного управления. https://innopraktika.ru/news/2649/ (accessed 14.01.2025)

передавать свои технологии, мобильные телефоны и платформы социальных сетей в третьи страны» [16].

Широко обсуждаются такие последствия политики крупных внерегиональных игроков, как появление новых геополитических альянсов и акторов, растущее накопление власти в крупных платформенных компаниях [2]; угроза исключения из цифровой экономики местных компаний [3, 4]; угрозы цифровому суверенитету африканских государств [5]; рост затрат на инновации, приток хищнических фирм [6, 7]; социально-политические и этические последствия обработки данных [8–10]; информационный/культурный империализм [11, 12]; проблема извлечения и коммодификации данных [13–15].

Цифровая трансформация увеличила риски неправомерного использования личных данных (о финансовых транзакциях, о местонахождении и др.), несанкционированного наблюдения. Вопросы защиты данных и суверенитета данных, особенно персональных, весьма актуальны в условиях, когда данные хранятся за пределами континента, в центрах обработки данных зарубежных стран.

В странах Африканского континента имеется лишь несколько центров обработки данных, которые обеспечивают владение и контроль данных. Согласно исследованию Африканской ассоциации центров обработки данных, по итогам 2020 г. в Африке располагалось лишь 1,3% мировых дата-центров, т.е. менее сотни. В то же время потребности сегодня составляют 700 новых объектов такого рода[9].

Процесс обработки данных, получаемых прежде всего европейскими корпорациями, исследователи предлагают рассматривать через широкие концептуальные рамки колониализма, которые позволяют понять весь происходящий социальный процесс, связанный с цифровизацией континента.

В публицистике и журналистике, а затем и в научной литературе для описания процесса «освоения» стран Глобального Юга зарубежными технологическими гигантами стали все чаще использоваться понятия «цифровой колониализм», «колониализм данных», под которыми понимается децентрализованное извлечение данных у граждан без их явного согласия через сети связи, разработанные и принадлежащие западным технологическим компаниям.

Идея «цифрового колониализма» / «колониализма данных» / «информационного колониализма», а позднее «алгоритмического колониализма» / «колониализма искусственного интеллекта» возникла как продолжение дискуссий о «цифровом империализме» и «цифровом капитализме». В основе этих понятий лежит идея, что данные о поведении и действиях человека – это сырье/ресурс, которые можно бесплатно извлекать и использовать для получения прибыли.

Одной из первых эту идею высказала американский экономист и политолог, профессор Гарвардской школы бизнеса Ш.Зубофф. В своих работах она вводит понятие «надзорный капитализм», под которым понимает «новый экономический порядок, использующий в качестве капитала человеческий опыт как сырье и характеризующийся распространением коммерческого мониторинга – тотального наблюдения за поведением граждан». В основе «надзорного капитализма» лежат, прежде всего, формирующиеся в результате человеческой деятельности данные, которые «извлекаются, анализируются узкоспециальными вычислительными системами», а во-вторых, возможность прогнозировать поведение людей на основе анализа этих данных [13].

По мнению Ш.Зубофф, пионером и одним из ведущих представителей «надзорного капитализма» стал *Google*. «Идея монетизации поведенческого излишка и сделала *Google* ключевым игроком на рынке пользовательских данных» [17].

В статье «Информационный колониализм: переосмысление отношения больших данных к современному предмету» Н.Кудри, специалист в области медиа и культуры, глава департамента медиакоммуникаций и культуры Лондонской школы экономики и политических наук, и У.Мехиас, профессор в области медиакоммуникаций Государственного университета Нью-Йорка [18, p. 352], используют понятие социальной датафикации, под которой они понимают «перевод» человеческой жизни в наборы данных, который стал возможным благодаря эксплуатации отношений индивидов с данными, то есть связей, которые они ежедневно устанавливают с другими субъектами, институтами и частными компаниями,

[9] https://resilient.digital-africa.co/en/blog/2023/10/12/digital-sovereignty-africa-is-giving-itself-the-means/ (accessed 15.03.2023)

особенно с помощью цифровых технологий и устройств. По их мнению, созданные как «социальные сети для капитала» [18, p. 338], эти отношения с данными можно отслеживать, превращая отдельных людей в субъектов данных, и извлекать выгоду из их ценности с помощью методов персонализированного таргетинга и прогнозной аналитики.

Кудри и Мехиас проводят прямую аналогию между цифровым колониализмом XXI в. и колониализмом XVI–XIX вв. По мнению Мехиаса и Кудри, «вместо земли и труда новый колониализм присваивает саму человеческую жизнь, которая отражена в данных» [18]: «подобно тому, как колонизаторы строили железные дороги, чтобы вывозить ресурсы, цифровые колонизаторы XXI века создают цифровую инфраструктуру и цифровую экосистему, позволяющие им извлекать данные Глобального Юга, обрабатывать их и возвращать информационные услуги колонизируемому населению. Впоследствии данные используются для манипулирования отдельными людьми, группами и организациями в своих интересах, с целью получения корпоративной прибыли, прежде всего такими корпорациями, как *Facebook, Twitter, Amazon, Google*» [18].

Исследователь из Йельского университета Майкл Квейт считает, что «именно доступ к данным, а не к деньгам, природным ресурсам или современному вооружению, теперь является наиболее ценным активом, причем доступным не только государствам, но и крупным технологическим корпорациям. Ассимиляция технологических продуктов, моделей и идеологий иностранных держав во главе с Соединенными Штатами представляет собой форму колонизации XX века» [15].

Этот ряд проблем можно изучить через призму цифрового суверенитета, достижение которого невозможно без обеспечения безопасного хранения и защиты пользовательских данных и суверенитета данных, подразумевающих хранение данных на территории государств, и их защита должна регулироваться национальным законодательством.

Из-за нехватки оборудования на местах, отсутствия конкретного законодательства и ограниченной уверенности в надежности существующей инфраструктуры конфиденциальные африканские данные хранятся за границей. Лишь единицы африканских государств могут самостоятельно обеспечить хранение данных. В Сенегале благодаря платформе *Senix*, точке обмена интернетом, страна серьезно работает над хранением своих данных в национальном масштабе. По мнению Ш.Бахума, управляющего директора *Sénégal Numérique*, благодаря такому подходу интернет-обмен между сенегальцами больше не будет проходить через маршрутизаторы за рубежом.

В Марокко с марта 2021 г. в дополнение к уже существующей инфраструктуре создан Африканский суперкомпьютерный центр с самым мощным суперкомпьютером в Африке на базе Политехнического университета Мухаммеда VI. В июле 2021 г. правительство Марокко приняло решение запретить размещение конфиденциальных данных за рубежом. В Руанде компания *Africa Data Centers* построила дата-центр мощностью 2 МВт. Алжир, Тунис, Гвинея и даже Кот-д'Ивуар следуют по тому же пути[10]. Однако до настоящего времени большая часть африканских стран допускают свободный поток данных, в т.ч. за пределы своих границ, прежде всего из-за отсутствия законов о защите данных.

ЗАЩИТА ДАННЫХ: ПРОБЛЕМЫ И ПРЕПЯТСТВИЯ

Эксперты выделяют несколько групп проблем, связанных с обеспечением цифрового суверенитета и кибербезопасности, защитой данных в масштабах континента и на уровне отдельных регионов.

Прежде всего, это финансовые и инфраструктурные барьеры (отсутствие собственных средств для обеспечения технических условий защиты данных). Пока африканские правительства, за небольшим исключением, нуждаются в международной помощи в создании необходимой цифровой инфраструктуры, что ведет к зависимости от внешних акторов. Такая односторонняя зависимость серьезно ограничивает способность Африки обеспечивать безопасность своих цифровых технологий, инфраструктуры и контроль над своим цифровым развитием.

[10] https://resilient.digital-africa.co/en/blog/2023/10/12/digital-sovereignty-africa-is-giving-itself-the-means/ (accessed 21.08.2024)

Серьезным препятствием является отсутствие согласованности в сфере законодательства. Многообразие и разнообразие правовых систем и традиций, политических и правовых режимов усложняет процесс гармонизации законодательства в области защиты данных [21–23].

Несмотря на консенсус среди государств – членов Африканского союза (АС) о том, что гармонизация нормативно-правовой базы имеет решающее значение для цифровой экосистемы Африки, стратегической необходимости создания единого цифрового рынка в Африке к 2030 г. при одновременной защите информации и данных, формирование нормативной базы продвигается сложно.

Еще в 2014 г., во время 23-й очередной сессии Ассамблеи АС в Малабо (Экваториальная Гвинея), была принята Конвенция Африканского союза о кибербезопасности и защите персональных данных (*African Union Convention on Cyber Security and Personal Data Protection*) (Конвенция Малабо)[11]. Эта Конвенция, содержащая различные аспекты защиты данных, включая создание органов по защите данных, принципы обработки персональных данных и положения о трансграничной передаче данных, вступила в силу только в июле 2023 г.

Общерегиональные конвенции, такие как Конвенция АС, принятый в 2010 г. Закон A/SA.1/01/10 о защите персональных данных в ЭКОВАС, являются свидетельством быстро растущего признания важности и неотложности принятия законов о защите данных. Но в то же время до сих пор отсутствуют согласованные механизмы трансграничной передачи данных, что могло бы дать странам возможность извлекать выгоду из экономики, основанной на данных. Еще одним важным аспектом стала публикация Основ политики АС в области защиты данных в 2022 г. Эта перспективная концепция рекомендует региональный подход к решению проблем защиты данных, направленный на преодоление разрозненных эффектов в подходах к регулированию. Есть надежда, что планы континента по гармонизации законодательных усилий осуществятся. Эта консолидация должна уменьшить торговые барьеры и проблемы, связанные с передачей данных в Африке, способствуя единому подходу к соблюдению нормативных требований.

Ситуация осложняется отсутствием комплексных законов о защите данных в части африканских стран. Если до 2016 г. только 16 из 55 стран приняли специальные законы о защите данных (примерами могут послужить Алжир, Египет, Кения, Нигерия, Уганда, Руанда, ЮАР)[12], то на сегодняшний день в 36 из 54 африканских стран действуют законы и/или правила о защите данных. Отсутствие национальных законов о защите данных может препятствовать эффективному выполнению Конвенции. Без таких законов могут отсутствовать необходимые правовые инструменты для обеспечения соблюдения ее положений.

Четвертая проблема – это соблюдение правильного баланса между вопросами национальной безопасности и защиты прав личности на неприкосновенность частной жизни, что особенно важно для трансграничной передачи данных при взаимодействии между правоохранительными органами и спецслужбами[13].

Важным препятствием является также отсутствие единой позиции среди правительств африканских государств относительно суверенитета в цифрой среде и управления интернетом в целом. Примером в этом вопросе могли бы послужить государства БРИКС, которые «последовательно координируют внешнеполитическую позицию и голосуют сходным образом по вопросам международной информационной безопасности и защиты цифрового суверенитета как нового принципа международного права в ООН»[14] и исходят из того, что основополагающим принципом международного сотрудничества в сфере информационной безопасности является «суверенное право каждого государства на обеспечение безопасности национального информационного пространства, установление норм и механизмов управ-

[11] https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed 03.04.2024)

[12] См., например: The Republic of Uganda: Data Protection and Privacy Act, 2019. https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.pdf; The Kenya Data Protection Act can be accessed at Government of Kenya, "Data Protection Act, 2019," Kenya. Gazette Supplement. No. 181 (Acts No. 24), November 18, 2019. https://www.dataguidance.com/notes/eu-kenya-gdpr-v-kenya-data-protection-act (accessed 02.04.2024)

[13] https://www.accessnow.org/wp-content/uploads/2024/01/Strengthening-data-protection-in-Africa-key-issues-for-implementation-updated.pdf (accessed 15.03.2023)

[14] https://russiancouncil.ru/analytics-and-comments/analytics/tsifrovoy-suverenitet-v-povestke-obedineniya-briks/?sphrase_id=172401928 (accessed 15.01.2025)

ления своим информационным и культурным пространством в соответствии с национальным законодательством»[15].

Трудности согласования политики в области защиты данных и управления интернетом в целом, осложняются тем, что США, ЕС, КНР вместе со своими технологическими разработками продвигают также свои ценности и нормы взаимодействия с сетевыми ресурсами [24]. Трансфер китайских, европейских, американских подходов влияет на законодательство и политические стратегии стран в области кибербезопасности, управления социальными сетями, использования данных и т.д.

Американские и европейские политики склонны развивать и защищать систему, которая продвигает неограниченный поток информации. Так, в силу заинтересованности в сохранении свободного обмена личными данными, ЕС предлагает африканским правительствам полагаться на европейский опыт и опираться на принятый в 2016 г. Общий регламент по защите данных (*General Data Protection Regulation*)[16], считая, что он может послужить основой для национального и регионального регулирования данных в Африке. Регламент предоставляет пользователям больше свободы и контроля над информацией, которой они делятся с компаниями. В частности, этот закон предполагает, что граждане могут давать согласие на сбор и обработку их данных (в т.ч. иностранным организациям и компаниям) либо не давать его, а также контролировать личную информацию, которую собирают компании в бизнес-целях. Следует отметить, что законы в области защиты данных Кении, Руанды и ЮАР имеют похожие статьи, предполагающие возможность при определенных условиях сбора и обработки данных зарубежными компаниями[17].

Другого подхода в отношении хранения и обработки данных придерживается китайское правительство. В КНР еще в 2017 г. был принят закон о кибербезопасности, который требует хранения и обработки данных граждан исключительно на территории государства. Похожие требования о локализации данных на территории страны содержатся в законах Кении, Руанды и Замбии.

ЗАКЛЮЧЕНИЕ

Цифровой суверенитет в настоящее время является стратегическим императивом для большинства африканских стран. Однако его достижение осложняется рядом проблем и ограничений экономического, технического и политического характера.

По нашему мнению, решение проблем цифрового и технологического суверенитета возможно при условии укрепления нормативно-правовой базы путем пересмотра и обновления существующих законов о конфиденциальности данных; закрытия пробелов в действующем законодательстве; повышения технического и инфраструктурного потенциала путем инвестирования в ИК-инфраструктуру, способствующую повышению конфиденциальности. Необходимы также гармонизация законодательства на региональном и континентальном уровне.

Хотя внешние партнеры будут продолжать играть важную роль, характер отношений с ними должен меняться – от традиционных патерналистских моделей к моделям, поощряющим взаимную поддержку. Важнейшим императивом для Африки, по нашему мнению, должно стать создание надежной цифровой экосистемы, открытой для партнерства с различными заинтересованными сторонами. Такой подход гарантирует, что континент не будет чрезмерно зависеть от одного партнера.

Достичь цифрового суверенитета, понимаемого как право государства регулировать и осуществлять контроль над технологиями, услугами и цифровыми данными, используемыми на суверенной территории, в текущих обстоятельствах крайне сложно в связи с тем, что преодоление многих проблем невозможно без инвестиций и участия западных и азиатских цифровых гигантов, которые в условиях активного соперничества за Африку зачастую сами являются их причиной.

[15] https://russiancouncil.ru/analytics-and-comments/analytics/tsifrovoy-suverenitet-v-povestke-obedineniya-briks/?sphrase_id=172401928 (accessed 15.01.2025)
[16] https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html (accessed 15.11.2023)
[17] https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/digital-rights-in-africa-national-overview/) (accessed 20.02.2024)

ЛИТЕРАТУРА / REFERENCES

1. Calzati S. 2022. 'Data sovereignty' or 'Data colonialism'? Exploring the Chinese involvement in Africa's ICTs: a document review on Kenya. *Journal of Contemporary African Studies*. Vol. 40, Iss. 2. Pp. 270–285. DOI: 10.1080/02589001.2022.2027351
2. Кутюр С., Тоупин С. Что означает понятие «суверенитет» в цифровом мире? *Вестник международных организаций*. 2020. Т. 15. № 4. С. 48–69. DOI: 10.17323/1996-7845-2020-04-03
   Couture S., Toupin S. 2020. What Does the Notion of "Sovereignty" Mean When Referring to the Digital? *International Organisations Research Journal*. Vol. 15, № 4. Pp. 48–69. (In Russ.). DOI: 10.17323/1996- 7845-2020-04-03
3. Floridi L. 2020. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*. Vol. 33, Pp. 369–378.
4. Polatin-Reuben D., Wright J. 2014. An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. In: *IEEE Symposium on Foundations of Computational Intelligence.* University of Oxford.
5. Pinto R.Á. 2018. Digital sovereignty or digital colonialism? New tensions of privacy, security and national policies. *International Journal on Human Rights*. Iss. 27. https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/
6. O'Neil C. 2016. Weapons of math destruction: How big data increases inequality and threatens democracy. New York: Crown.
7. Abebe R., Aruleba K., Birhane A., Kingsley S. 2021. Narratives and counternarratives on data sharing in Africa. Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency. DOI: 10.1145/3442188.3445897
8. Dencik L., Hintz A., Cable J. 2016. Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*. 3 (2). DOI: 10.1177/2053951716679678
9. Kitchin R. The Data Revolution: Big data, Open data, Data infrastructures and their consequences. Los Angeles, London, New Delhi, Singapore, Washington DC: SAGE, 2014. 222 p.
10. Metcalf J., Crawford K. Where are human subjects in Big Data research? The emerging ethics divide. January 2016. *Big Data & Society*. 3(1). DOI: 10.1177/2053951716650211
11. Грибанова В.В., Усачева В.В. Неоколониализм в сфере образования и СМИ в Африке: некоторые итоги перехода от культурного к цифровому империализму. *Электронный научно-образовательный журнал «История».* 2023. Т. 14.
    Gribanova V.V., Usacheva V.V. 2023. Neocolonialism in the field of education and media in Africa: some results of the transition from cultural to digital imperialism. *Electronic scientific and educational journal "History".* Vol. 14. (In Russ.)
12. Панцерев К.А. Страны Африки южнее Сахары в цифровую эпоху: к вопросу обеспечения информационного суверенитета. *Азия и Африка сегодня*. 2019. № 10. С. 10–16.
    Pantzerev K.A. 2019. Sub-Saharan African Countries in the Digital Age: Towards Ensuring Information Sovereignty. *Asia and Africa today.* № 10. Pp. 10–16. (In Russ.)
13. Zuboff Sh. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: Public Affairs, 2019. 704 p.
14. Couldry N., Mejias U. 2018. Data colonialism: rethinking big data's relation to the contemporary subject. *Television and New Media*. https://modelviewculture.com/pieces/technology-colonialism
15. Kwet M. 2019. Digital colonialism: US empire and the New Imperialism in the Global South. *Race & Class.* Vol. 60. Iss. 4. DOI: 10.1177/0306396818823172
16. Цветкова Н., Сытник А. Цифровое противостояние США и КНР: экономическое и политическое измерения. *Мировая экономика и международные отношения.* 2023. № 11. С. 15–23.
    Tsvetkova N., Sytnik A. 2023. Digital Confrontation between the USA and China: Economic and Political Dimensions. *World Economy and International Relations.* № 11. Pp. 15–23. (In Russ.)
17. Сафронов Э.Е. Трансформации капитализма в XXI веке: концепция «надзорного капитализма» Шошаны Зубофф. *Социологические исследования*. 2021. № 4. С. 165–172. (In Russ.)
    Safronov E.E. 2021. Transformations of capitalism in the 21st century: Shoshana Zuboff's concept of "surveillance capitalism". *Sociological Studies.* № 4. Pp. 165–172. (In Russ.)
18. Couldry N., Mejias U.A. 2019. The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism. Stanford University Press, 2019. 352 p.
19. Birhane B. 2020. Algorithmic Colonization of Africa. *SCRIPTed*: *A Journal of Law, Technology & Society*. Vol. 17. Iss. 2. DOI: 10.2966/scrip.170220.389
20. Birhane A. 2017. Descartes was wrong: "A person is a person through other persons"'. Aeon. https://aeon.co/ideas/descartes-was-wrong-a-person-is-a-person-through-other-persons

21. Makulilo A.B. 2012. Privacy and data protection in Africa: A state of the art. *International Data Privacy Law*. 2 (3). Pp. 163–178. DOI: 10.1093/idpl/ips014
22. Makulilo A.B., Mophethe K. 2016. Privacy and Data Protection in Lesotho. *African Data Privacy Laws*. Springer Cham. Pp. 337–347. DOI: 10.1007/978-3-319-47317-8
23. Babalola O. 2023. Data Protection Legal Regime and Data Governance in Africa: An Overview. In: *Ndemo B., Ndung'u N., Odhiambo S., Shimeles A.* (eds). *Data Governance and Policy in Africa. Information Technology and Global Governance*. Palgrave Macmillan, Cham. DOI: 10.1007/978-3-031-24498-8_4
24. Цифровой поворот в международных отношениях: как новые технологии меняют мировую политику и науку о ней. Под ред. М.А.Сучкова, И.В.Болговой. М.: МГИМО – Университет, 2023. 232 с.
The Digital Turn in International Relations: How New Technologies Are Changing World Politics and the Science of It. 2023. Ed. by M.A.Suchkov, I.V.Bolgova. Moscow, 2023. 232 p.

ИНФОРМАЦИЯ ОБ АВТОРЕ/ INFORMATION ABOUT THE AUTHOR

Суфиянова Гульнур Рафаэлевна, кандидат исторических наук, заведующая кафедрой международных отношений и регионоведения, Тюменский государственный университет, Тюмень, Россия.

Gulnur R. Sufiyanova, PhD (History), Head, Department of International Relations and Regional Studies, University of Tyumen, Tyumen, Russia.

Поступила в редакцию (Received) 06.09.2024
Доработана после рецензирования (Revised) 16.01.2025
Принята к публикации (Accepted) 22.01.2025