Международный журнал Красного Креста (2021 г.), № 916–917
Борьба с терроризмом, санкции и война

МЖКК

Потоки биометрических данных и непредусмотренные последствия борьбы с терроризмом

Катя Линскоу Якобсен*
Катя Линскоу Якобсен — старший научный сотрудник факультета политологии в Копенгагенском университете, Дания.
Адрес электронной почты: kj@ifs.ku.dk.

Аннотация

Изучая непредусмотренные последствия сбора и обработки биометрических данных в контексте контртеррористической и гуманитарной деятельности, автор статьи предлагает двухкомпонентную систему анализа, применяя ее в контексте получения и распространения данных в Афганистане и Сомали. Введенное Тилли понятие «живой лаборато-

* Выражение признательности: написание статьи заняло некоторое время, и ее появлению так или иначе способствовало множество коллег автора — в ходе практикумов (благодарю Люси Сачмэн, Клаудию Арадау, Рокко Белланову, Линду Монсис и многих других) и семинаров (благодарю коллег из Копенгагенского университета, особенно Кевина Хеллера и Анине Хагеман). Исследование проводилось в рамках финансируемого Норвежским научно-исследовательским советом проекта (DoNoHarm), благодаря которому мне посчастливилось поработать с невероятными Кристин Сандвик (ведущий исследователь) и Ларисой Фаст. Благодарю Карла Штайнакера за чрезвычайно ценные материалы и многолетние беседы, благодарю за помощь двух практикантов Центра военных исследований и трех анонимных рецензентов за очень полезные конструктивные замечания, а также главного редактора Брюно Демейера.

рии» и предложенная Ларкиным концепция инфраструктуры объединены в систему, с помощью которой анализируются условия получения биометрических данных и последующие потоки данных, основанные на соглашениях об обмене данными либо ставшие следствием непредусмотренного доступа к данным. В процессе анализа непредусмотренных последствий обмена данными необходимо рассмотреть все многообразие акторов, использующих биометрические данные (каждый в своих целях), и возникающие несмотря на эти отличия потоки данных. С этой целью автор вводит понятие «инфраструктуры цифровых вмешательств», одним из компонентов которой является совокупность биометрических баз данных.

Ключевые слова: биометрические данные, инфраструктура, гуманитарные акторы, борьба с терроризмом, непредусмотренные последствия, «живые лаборатории», распространение данных.

: : : : : : : :

Инфраструктуры цифровых вмешательств: биометрия в контексте борьбы с терроризмом и в других сферах

Существует несколько типов ситуаций, в которых осуществляется сбор биометрических данных, то есть уникальных идентификационных биологических характеристик, таких как рисунок радужной оболочки глаза и отпечатки пальцев[1]. Так, биометрия стала важным техническим средством контртеррористической деятельности после терактов 11 сентября 2001 года. Представление о превосходстве биометрии как одной из технологий борьбы с терроризмом иллюстрируют слова бывшего сотрудника Центрального разведывательного управления США, который в ноябре 2001 года упомянул, что «благодаря биометрическим технологиям», защищающим граждан США от террористических атак, «Америка может стать безопаснее»[2]. Сегодня биометрия по-прежнему играет центральную роль в борьбе с терроризмом. Например, целью одной из новых программ США является разработка систем «дальней биометрической идентификации», которая позволит «устанавливать личность в сложных ситуациях», в том

1 Биометрические данные — это «персональные данные, полученные в результате специальной технической обработки, которые характеризуют физические, физиологические или поведенческие черты физического лица и позволяют произвести или подтверждают однозначную идентификацию этого физического лица»; см.: European Union (EU), *General Data Protection Regulation*, *Regulation (EU) 2016/679,* 27 April 2016, OJ L 119, 4.5.2016, pp. 1–88, Art. 4(14); EU, *Directive (EU) 2016/680*, 27 April 2016, OJ L 119, 4.5.2016, pp. 89–131, Art. 3(13). См.: Els Kindt, "A First Attempt at Regulating Biometric Data in the European Union", in Amba Kak (ed.), *Regulating Biometrics: Global Approaches and Urgent Questions*, AI Now Institute, September 2020, доступно по адресу: https://ainowinstitute.org/regulatingbiometrics.html (все ссылки на интернет-ресурсы приводятся по состоянию на декабрь 2021 г.).

2 John D. Woodward, "Biometrics: Facing up to Terrorism", Issue Paper IP-218, RAND Corporation, Santa Monica, CA, October 2001, доступно по адресу: https://www.rand.org/pubs/issue_papers/IP218.html.

числе при помощи беспилотных летательных аппаратов[3]. Еще одним примером убежденности в чрезвычайно важной роли биометрии в контртеррористической деятельности США служит цитата из доклада Счетной палаты правительства США, в котором отмечается, что в период с 2008 по 2017 гг. Министерство обороны США с помощью биометрии «обеспечило поимку или уничтожение 1700 человек»[4], предположительно представлявших угрозу для безопасности США[5].

После двух десятилетий использования биометрии в контексте контртеррористической деятельности проблемы этого подхода всплыли на поверхность. Ученые доказали, что «точность» технических средств обнаружения противника становится сомнительной, если под ней подразумевается точность политических решений о том, «кто может быть законной целью насильственных действий»[6]. Стали очевидными и проблемы самого биометрического метода. После вывода в августе 2021 года войск коалиции из Афганистана «Талибан» (*движение, запрещенное в России. — Прим. пер.*) получил доступ к оставленным силами США биометрическим устройствам, что открыло путь к получению биометрических данных и идентификации зарегистрированных силами коалиции физических лиц, проходивших подготовку, получавших заработную плату либо иным образом сотрудничавших с коалицией. В данном случае создание биометрических инфраструктур — понятие, которое мы разберем в настоящей статье, — повлекло за собой появление новых видов угроз для безопасности, поставив под сомнение представления о биометрии как о методе, безоговорочно служащем достижению самого высокого уровня безопасности. И хотя эта ситуация в силу ряда ее аспектов является уникальной, если проанализировать использование биометрии в других условиях и другими акторами — не только военными, но и гуманитарными, — обнаруживаются и другие примеры.

В ходе исследования применения биометрии в контексте двух различных операций — в Афганистане и Сомали — обозначились проблемные моменты, а также схожие динамика, логика процессов и их последствия. Обе

3 См.: BRIAR Program: Intelligence Advanced Research Projects Activity (IARPA), "Biometric Recognition and Identification at Altitude and Range", Office of the Director of National Intelligence, IARPA, доступно по адресу: https://www.iarpa.gov/research-programs/briar.

4 GAO, "DOD Biometrics and Forensics: Progress Made in Establishing Long-term Deployable Capabilities, But Further Actions are Needed", Washington, DC, 7 August 2017, доступно по адресу: https://www.gao.gov/products/gao-17-580. См. также: Nina Toft Djanegara, *Biometrics and Counter-Terrorism. Case Study of Iraq and Afghanistan*, Privacy International, London, May 2021, доступно по адресу: https://privacyinternational.org/sites/default/files/2021-06/Biometrics%20for%20Counter-Terrorism-%20Case%20study%20of%20the%20U.S.%20military%20in%20Iraq%20and%20Afghanistan%20-%20Nina%20Toft%20Djanegara%20-%20v6.pdf.

5 С критической оценкой «популяризации биометрических данных как уникального метода борьбы с угрозами XXI века» можно ознакомиться, например, в подробных докладах Privacy International: Privacy International, "Biometrics Collection Under The Pretext Of Counter-Terrorism", 28 May 2021.

6 Lucy Suchman, Karolina Follis and Weber, "Tracking and Targeting: Sociotechnologies of (In)security", *Science, Technology & Human Values*, Vol. 42, No. 6, 2017. См. также: Christine Agius, "Ordering Without Bordering: Drones, The Unbordering of Late Modern Warfare and Ontological Insecurity", *Postcolonial Studies*, Vol. 20, No. 6, 2017.

ситуации иллюстрируют, каким образом использование биометрии порождает новые риски и угрозы безопасности — будь то в результате попадания биометрических данных в руки противника, намеренной их передачи или тестирования непроверенных биометрических методов в реальных условиях. Кроме того, на примере обеих ситуаций можно понять, почему анализ рисков применения биометрии в условиях военных действий или гуманитарной деятельности, проведенный в отрыве от контекста, оставляет без внимания проблему потоков данных. В Афганистане огромные массивы биометрических данных производили не только военные, но и гуманитарные акторы. В определенных ситуациях источником потоков биометрических данных, которыми обмениваются гуманитарные акторы и государственная система безопасности, становятся соглашения об обмене данными. Рассмотрев проблему сквозь призму потоков, мы изучим многообразие путей, приводящих к умышленному или непредусмотренному взаимодействию потоков гражданских биометрических данных и инфраструктур контртеррористической деятельности, например в рамках соглашений об обмене данными (между Управлением Верховного комиссара Организации Объединенных Наций по делам беженцев (УВКБ ООН) и Министерством внутренней безопасности США в качестве одного из примеров).

Кроме того, разные акторы в различных обстоятельствах тестируют применение биометрии, порождая «истории успеха», которые в свою очередь подпитывают представления о точности и незаменимости сбора биометрических данных и обмена ими. Рассмотрение изолированных случаев не позволит оценить вклад военных и других акторов в становление инфраструктуры цифровых вмешательств. Предметом настоящей статьи являются в первую очередь биометрические инфраструктуры — как элемент инфраструктуры цифровых вмешательств — то есть производство биометрических данных и их потоки, которые лежат в основе инфраструктуры баз данных, используемых и создаваемых в разных целях субъектами различных вмешательств; порой они включают потоки, позволяющие использовать одни и те же данные, невзирая на обозначенные различия. Подобные биометрические базы данных представляют собой одно из измерений современной инфраструктуры вмешательств, которое часто упускается из виду, — «инфраструктуру для сбора, архивирования и идентификации цифровых биометрических данных»[7].

7 Согласно определению, предложенному Джасанофф, социотехнические мнимости представляют собой «коллективно разделяемые и реализуемые образы желаемого будущего, подкрепляемые общим пониманием форм общественной жизни и социального порядка, которые достижимы и поддерживаются с помощью успехов в науке и технологиях». См.: Sheila Jasanoff, “Future Imperfection: Science, Technology, and the Imaginations of Modernity”, in Sheila Jasanoff and Sang-Hyun Kim, *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*, The University of Chicago Press, Chicago and London, 2015, p. 25. Относительно обмена биометрическими данными в контексте борьбы с терроризмом см., например: Privacy International, *Briefing to the UN Counter-Terrorism Executive Directorate on the Responsible Use and Sharing of Biometric Data to Tackle Terrorism*, London, June 2019, доступно по адресу: https://privacyinternational.org/sites/default/files/2019-07/PI%20briefing%20on% 20biometrics%20final.pdf.

Под «инфраструктурами» мы понимаем концепцию Брайана Ларкина, который описывает их как платформы «не только для воды и машин» — в данном случае биометрических данных, — но и для желаний, мечтаний и мнимостей[8] — в данном случае историй успеха или страха. Но как и при каких условиях создаются биометрические инфраструктуры? Чтобы понять это, концепция инфраструктуры Ларкина объединена в статье с введенным Хелен Тилли понятием «живой лаборатории»; это позволяет обратить внимание на применение биометрии в реальных условиях различными акторами и в контексте различных вмешательств. Попытки применения биометрии приводят к созданию не только биометрических данных, но и «историй успеха», которые подпитывают представления акторов различных вмешательств о ценности биометрических (баз) данных, в перспективе поощряя попытки расширить производство биометрических данных и обмен ими. Объединяя обозначенные концепции инфраструктуры и живой лаборатории, статья ставит вопрос о том, при каких условиях создаются инфраструктуры биометрических вмешательств, из каких потоков они состоят и какие — порождают, включая потоки биометрических данных (производимые намеренно или неумышленно) и менее очевидные потоки историй успеха и страха.

За вводной частью следует объяснение концепций инфраструктуры и живой лаборатории. Затем вниманию читателя предлагается анализ производства биометрических данных и их потоков в Афганистане и Сомали. Статья завершается размышлениями о более широком значении этих двух примеров и о важности изучения процессов создания инфраструктур цифровых вмешательств, точнее, биометрических баз данных, с учетом соотношения сил и существующего неравенства, проявляющегося в том числе в процессе (в той или иной степени экспериментального) производства данных[9].

Методические замечания

В целях проведения анализа инфраструктур биометрических вмешательств были использованы различные источники информации. Проведено 11 полуструктурированных интервью с представителями Международного Комитета Красного Креста (МККК), Продовольственной и сельскохозяйственной организации Объединенных Наций (ФАО), Управления Организации Объединенных Наций по обслуживанию проектов (ЮНОПС), УВКБ ООН и Всемирной продовольственной программы (ВПП); все опрошенные имели опыт использования биометрии в Сомали, Афганистане или в целом в рамках реализации гуманитарных программ. В интервью

8 Brian Larkin, "The Politics and Poetics of Infrastructure", *Annual Review of Anthropology*, Vol. 42, No. 1, October 2013. См. также: Jana Hönke and Ivan Cuesta-Fernandez, "Mobilising Security and Logistics Through an African Port: A Controversies Approach to Infrastructure", *Mobilities*, Vol. 13, No. 2, January 2018.

9 Rocco Bellanova, Kristina Irion, Katja Lindskov Jacobsen, Francesco Ragazzi, Rune Saugmann and Lucy Suchman, "Toward a Critique of Algorithmic Violence", *International Politics Sociology*, Vol. 15, No. 1, March 2021.

приняли участие сотрудники разных категорий, работающие в разных географических точках. С учетом щекотливого характера вопросов об обмене данными и других аспектов интервью были анонимными. В дополнение к вышеперечисленному были изучены новостные статьи, отраслевые вебсайты, доклады экспертов и официальные документы, что позволило получить представление о производстве биометрических данных и организации их потоков. Источники охватывают период от начального этапа применения биометрии после 11 сентября до недавних примеров из Афганистана, последних регламентов по защите данных и соглашений об обмене ими. Ситуация в Афганистане и Сомали не изучалась подробно. В статье приводятся примеры из обеих стран, иллюстрирующие более общие тенденции, например: как потоки биометрических данных могут создать угрозу безопасности.

Информация по теме доступна лишь в малом объеме, секретными считаются не только биометрические технологии, используемые в контртеррористической деятельности, но и соглашения об обмене данными между донорами и гуманитарными учреждениями. Когда содержание соглашения об обмене данными неизвестно, невозможно установить, допустим ли обмен биометрическими данными, что не всегда имеет место, и какими именно биометрических данными разрешено обмениваться. Так, в Иордании биометрические данные раскрываются Министерству внутренней безопасности США, но не УВКБ ООН[10]. Разумеется, очень сложно представить неопровержимые доказательства наличия прямой связи между невоенными биометрическими данными и их использованием в борьбе с терроризмом, и мы не ставим перед собой такой задачи. В то же время, игнорируя возможную роль гражданских биометрических данных в усилиях по борьбе с терроризмом, мы продолжаем упускать из виду гипотетические связи такого рода и связанные с ними риски и угрозы безопасности. Еще одной причиной невнимания к проблематике потоков биометрических данных служит отсутствие информации о многочисленных пострадавших от непредусмотренных последствий обмена биометрическими данными и других нежелательных результатов применения биометрических технологий в контексте разнообразных вмешательств[11]. Важно не только разобрать процессы получения биометрических данных и потоков, но и разобраться в причинах подобного невнимания и устранить их, и такие попытки уже начинают предприниматься[12].

10 Анонимное интервью, ноябрь 2021 г.

11 Keren Weitzberg, *Biometrics and Counter-Terrorism: Case Study of Somalia*, Report, Privacy International, 28 May 2021; Karen Fog Olwig, Kristina Grünenberg, Perle Møhl and Anja Simonsen, *The Biometric Border World: Technology, Bodies and Identities on the Move,* 1st ed., Routledge, Oxon and New York, 2020; Katja Lindskov Jacobsen and Larissa Fast, "Rethinking Access: How Humanitarian Technology Governance Blurs Control and Care", *Disasters*, Vol. 43, No. 2, 2019; Mirca Madianou, "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies", *Television & New Media*, Vol. 20, No. 6, 2021.

12 Gus Hosein and Carly Nyst, *Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries*, Report, Privacy International, 2013;

Аналитические рамочные основы: инфраструктуры и живые лаборатории

Инфраструктурные продукты и потоки: данные и мечты

Рассматривая биометрические технологии в качестве элемента инфраструктуры цифровых вмешательств, мы вводим два элемента концепции инфраструктуры, предложенной Ларкиным.

Во-первых, это акцент на потоках, который делает Ларкин. Важнейшим элементом подхода Ларкина к толкованию понятия инфраструктуры как «социотехнической платформы мобильности» является то, что под мобильностью он понимает не только передвижение людей, но и материальные и нематериальные потоки, например автомобили и мечты, данные и слухи. Предложенный Ларкиным подход побуждает изучать инфраструктуры, не забывая об их функциях, которые находят отражение в потоках анализируемой инфраструктуры. Данная трактовка инфраструктуры предполагает, что анализ не ограничивается процессами, лежащими в основе продукта инфраструктуры, например биометрическими базами данных, но должен охватывать потоки, поддерживаемые инфраструктурами. Во-вторых, это внимание Ларкина к нематериальным элементам инфраструктуры, таким как мнимости и желания. Как сформулировал Ларкин, инфраструктуры «возникают из желаний и хранят их внутри себя»[13]. В нашем анализе акцент на нематериальных ценностях проявляется во внимании к историям успеха — строительному материалу для мечтаний и своего рода «потоку», который подпитывает представления о мнимой точности биометрических технологий и «оживляет» их.

Соответственно, в статье предлагается двухкомпонентный подход к анализу — с точки зрения продуктов инфраструктуры и с точки зрения потоков биометрических данных и историй успешного применения биометрических технологий. Акцент на потоках побуждает нас изучать — а не предполагать, — как появление биометрических инфраструктур влияет на отношения между акторами, например прослеживая путь, которым произведенные одним типом акторов биометрические данные попадают в распоряжение актора совершенно другого типа. В соответствии с этим

Human Rights Watch, "UN Shared Rohingya Data Without Informed Consent", 15 June 2021, доступно по адресу: https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-08/2021-guidelines-for-authors-irrc.pdf; Adam Moe Fejerskov, Maria-Louise Clausen and Sarah Seddig, *Risks of Technology Use in Humanitarian Settings. Avoiding Harm, Delivering Impact*, Policy Brief, Danish Institute for International Studies, 17 August 2021; Elise Thomas, "Tagged, Tracked and in Danger: How the Rohingya Got Caught in the UN's Risky Biometric Database", *WIRED*, 12 March 2018, доступно по адресу: https://www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh.

13 B. Larkin (примечание 8 выше). Отказавшись от более узкого толкования, сосредоточенного на материальных аспектах (дороги, трубы, кабели и т. д.), Ларкин, со всем вниманием к мечтам и мнимостям, выдвигает гипотезу о том, что нематериальные компоненты играют не менее важную роль. В данном случае истории успеха и мнимости, производимые и поддерживаемые биометрическими инфраструктурами, к примеру, влияют на создание (или отказ от создания) биометрических баз данных в будущем.

подходом мы предлагаем рассмотреть ряд потоков: между различными гуманитарными базами данных (на примере Сомали как лаборатории для исследования функциональной совместимости[14]), между гуманитарными организациями и корпорациями, между участниками гуманитарной и контртеррористической деятельности либо непредусмотренные потоки между силами коалиции и силами противника.

Живая лаборатория

Применение концепции «живой лаборатории» Тилли в рамках анализа инфраструктуры позволяет нам задать вопросы, предваряющие изучение потоков данных, — вопросы, касающиеся в первую очередь условий получения биометрических данных[15]. Концепция «живой лаборатории» акцентирует внимание на экспериментальном характере, который в той или иной степени носят многие случаи применения биометрических технологий как средства получения данных.

Концепция Тилли также обращает внимание на важность оценки более широких последствий применения технологии, носящей более или менее выраженный экспериментальный характер, и на сопутствующие доводы, такие как риски неявного превращения определенной местности во временную лабораторию, с учетом кажущейся приемлемости тестирования биометрических технологий в контексте различных вмешательств[16]. Важно отметить, что «живая лаборатория» — это не пространство и не условия, существующие в этом качестве. Тилли скорее предлагает нам проанализировать, как подобное пространство создают внешние акторы, применяя определенные допущения и аналогии, которые в свою очередь обеспечивают легитимизацию определенной практики[17]. Несмотря на то что методика Тилли разработана для стран колониальной Африки, концепция живых лабораторий обращает внимание на динамику, значимую

14 «В 2018 г. SCC [Somalia Cash Consortium] протестировал функциональную совместимость платформы для обмена биометрическими данными с технологиями проекта SCOPE, реализуемого ВПП»; см.: Boniface Owino, *Harmonizing Registrations and Identification in Emergencies in Somalia*, Development Initiatives, Nairobi, 29 August 2019, доступно по адресу: https://devinit.org/documents/67/Report_Harmonising-registrations-and-identification-in-emergencies-in-Somalia.pdf.

15 Говоря об условиях создания биометрических данных, следует выделить несколько ситуаций. Так, ученые изучали восприятие силы населением Сомали, взаимодействующим с биометрическими технологиями в европейских системах для беженцев за пределами Сомали: «Когда Мухтар силой принудили сдать отпечатки пальцев, она поняла, с какими последствиями европейской гуманитарной помощи могут столкнуться просители убежища»; см.: Anja Simonsen, "Fleeting (Biometric) Encounters: Care and Control at Italian Border Sites", in Karen Fog Olwig, Kristina Grünenberg, Perle Møhl and Anja Simonsen (eds), *The Biometric Border World: Technology, Bodies and Identities on the Move*, 1st ed., Routledge, Oxon and New York, 2019, p. 135.

16 Тилли изучает колониальную Африку и то, как глобальное неравенство сил (вос)производится в лабораториях за пределами стран Запада. Она препарирует исследования «для сбора фактов» (p. 8) и «разведку» колониальных времен (p. 4), показывая связь научной деятельности с более общими целями колониализма: Helen Tilley, *Africa as a Living Laboratory: Empire, Development, and the Problem of Scientific Knowledge, 1870–1950*, The University of Chicago Press, Chicago and London, 2011.

17 H. Tilley (примечание 16 выше), p. 2.

и для современных экспериментов в области биометрии. Так, Тилли отмечает, что применительно к странам Африки об информированном согласии в то время «редко действительно заботились» — и это замалчивание способствовало превращению Африки в будто бы интересную «живую лабораторию»[18]. Проблема согласия — которая часто заключается в отсутствии подлинного согласия — и возможных проистекающих из нее международно-правовых обязательств — важный аспект производства биометрических данных в контексте современных вмешательств[19]. Таким образом, проведенный Тилли анализ указывает на важность дополнения нашего анализа потоков биометрических данных вопросами создания лабораторных условий. Концепция «живой лаборатории» становится аналитической призмой, сквозь которую рассматриваются вопросы о различных противоречиях и недостатках временных лабораторий в реальных условиях.

Объединение двух подходов решает следующие задачи: Тилли предлагает обдумать важные темы, включая вопросы, предваряющие вдохновленный Ларкиным акцент на потоках биометрических данных и нематериальных компонентах, таких как истории успеха и страх, то есть прежде чем приступить к анализу этих потоков, следует задать вопрос о том, как получают биометрические данные, кто их получает и при каких условиях. Таким образом, объединив подходы Тилли и Ларкина, мы получили двухкомпонентную аналитическую систему. Соответственно, проведенный нами анализ в первую очередь отвечает на вопросы, связанные с «производством данных» (этап, предшествующий возникновению потоков данных), то есть a) кто и b) при каких условиях; а во вторую очередь рассматривает проблему потоков данных, разбирая и a) предусмотренные, и b) непредусмотренные потоки биометрических данных.

Афганистан и Сомали: анализ производства биометрических данных и потоков данных

Производство данных: a) кто

Афганистан

В ряде источников говорится, что к ноябрю 2019 года вооруженные силы США получили биометрические данные «7,4 миллиона человек», включая

18 H. Tilley (примечание 16 выше), pp. 1–2.

19 См., например: Naomi Cohen, "'Do No Digital Harm': A Conversation on Handling Sensitive Data", October 2018, *The New Humanitarian*; в статье эксперты обсуждают проблему согласия, отмечая, в частности, каким образом: a) «Мы взаимодействуем с людьми, которые иногда имеют очень низкий уровень образования или грамотности в вопросах данных. Как донести до них информацию о новой технологии или даже более базовые сведения? В то же время, если говорить о защите данных, как убедиться в том, что полученное согласие является информированным и действительным?» (эксперт Мария-Элена Чикколини); и b) «Гуманитарная деятельность, пожалуй, является средой для явления, которое можно назвать самым значительным дисбалансом сил между теми, кто собирает данные, и теми, чьи данные собираются… Думаю, дисбаланс проявляется в том, кому принадлежат данные» (эксперт Зара Рахман).

несколько лиц, подозреваемых в террористической деятельности[20]. В первом полугодии 2019 года эти данные «тысячи раз» помогали идентифицировать личность участников боевых действий[21]. О значении сбора биометрических данных говорит то, что в одном из документов вооруженных сил США («Применение биометрических технологий для поддержки оперативной деятельности») в разделе, посвященном «лицам, собирающим данные», отмечается, что: «Практически любая операция дает возможность сбора биометрических данных»[22]. Конкретно в Афганистане уже к 2011 году были получены биометрические данные «более 1,5 миллиона афганцев», которые хранились в «базах данных американских вооруженных сил, сил НАТО [Организация Североатлантического договора] и местных сил»[23]. С учетом состава этих данных становится очевидно, что сбор биометрических данных имеет определенную цель, а именно ориентирован на «мужчин призывного возраста, 15–64 лет», при этом в описываемой базе данных хранились биометрические показатели «примерно каждого шестого» мужчины призывного возраста[24]. Но каким образом были получены биометрические данные? Кто занимался их сбором и каким образом он был организован? Учитывая связь со сбором разведданных, следует отметить, что на биометрические данные приходится лишь малая доля мероприятий по сбору данных, реализуемых гораздо более обширной разведывательной инфраструктурой США[25]. Это, разумеется, относится и к участникам гуманитарной деятельности, которые собирают огромные объемы данных; цифровые биометрические данные — лишь один, но очень важный тип собираемых данных, учитывая то, насколько сложно изменить радужную оболочку глаз, голос и отпечатки пальцев и насколько просто распространить огромные массивы цифровых биометрических данных, в отличие от бумажных документов.

20 Наблюдатели отмечают, что перед Министерством обороны США стояла цель зарегистрировать 80% афганского населения; см.: Annie Jacobsen, *First Platoon A Story of Modern War in the Age of Identity Dominance*, Penguin, Dutton, 2021. Некоторые также утверждают, что Министерство обороны США «хранит биометрические данные более 7 миллионов человек, преимущественно из зон боевых действий»; см.: Matthias Monroy, "NATO Establishes Biometric Database, US Military has it Already", *Matthias Monroy*, 8 November 2019, доступно по адресу: https://digit.site36.net/2019/11/08/nato-establishes-biometric-database-us-military-has-it-already/; Thales, "Automated Fingerprint Identification System (AFIS) Overview — A Short History", *Thales*, 18 June 2021, доступно по адресу: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history; Delores M. Etter, Jeniffer Webb and John Howard, "Collecting Large Biometric Datasets: A Case Study in Applying Software Best Practices", *CrossTalk*, May/June 2014, доступно по адресу: http://jjhoward.org/pubs/collecting-large-biometric-datasets.pdf. Неизвестно, насколько была выполнена поставленная Министерством обороны цель в 80%.

21 Dave Gershgorn, "Exclusive: This is How the U.S. Military's Massive Facial Recognition System Works", *OneZero Medium*, 6 November 2019, доступно по адресу: https://onezero.medium.com/exclusive-this-is-how-the-u-s-militarys-massive-facial-recognition-system-works-bb764291b96d.

22 Army, Marine Corps, Navy and Air Force, "Biometrics: Multi-Service Tactics, Techniques, and Procedures for Tactical Employment of Biometrics in Support of Operations", Air Land Sea Application (ALSA), April 2014, p. 7, доступно по адресу: https://www.marines.mil/Portals/1/MCRP%203-33.1J%20BIOMETRICS%201.pdf.

23 Thom Shanker, "To Track Militants, U.S. has System that Never Forgets a Face", *New York Times*, 13 July 2011, доступно по адресу: https://www.nytimes.com/2011/07/14/world/asia/14identity.html.

24 Ibid.

25 Благодарим анонимного рецензента за то, что обратил внимание на это важное обстоятельство.

Как упоминалось выше, в Афганистане военные США собирали у ряда задержанных в зоне боевых действий лиц «отпечатки пальцев и рисунок радужной оболочки глаза», предполагая использовать их для точной «идентификации лиц, участвующих в боевых действиях на стороне неприятеля»[26], например путем сличения отпечатков пальцев с образцами, хранящимися в биометрических базах данных, включая «перечни лиц, признанных террористами или подозреваемых в участии в террористической деятельности»[27]. Помимо участников боевых действий, «военные и полиция» также собирали биометрические данные (отпечатки пальцев и рисунок радужной оболочки глаза) у заключенных и «местных жителей перед наймом в органы государственной власти, особенно в службу безопасности, полицию и американские структуры»[28]. Менее явной была работа по сбору отпечатков пальцев «с обезвреженных взрывных устройств и осколков разорвавшихся снарядов». Впоследствии полученные таким образом отпечатки пальцев использовались при проверке лиц, задержанных в зоне боевых действий, и при найме персонала. По словам генерала Петреуса, эта тактика «весьма эффективно помогала устанавливать личность ответственных за использование определенных боеприпасов при нападении, что впоследствии использовалось для определения целей»[29]. С помощью биометрических данных также контролировалось предоставление доступа к военным базам США.

Сбор биометрических данных осуществляли не только военные США, но и различные группы афганских должностных лиц. Так, служащие тюрьмы «Сарпоса», расположенной на юге Афганистана, используя предоставленные США технологии собирали рисунки радужной оболочки глаза и отпечатки пальцев у боевиков и заключенных[30]. Пользу полученных данных иллюстрируют их использованием в целях идентификации около 475 заключенных, совершивших побег из тюрьмы «Сарпоса» по тоннелю, прорытому «Талибаном» «прямо в тюрьму, в секцию для политических заключенных, где содержались сотни сторонников “Талибана”»[31]. Ряд источников утверждает, что биометрические данные сыграли важную роль

26 United States Government Accountability Office, “Defense Biometrics: Additional Training for Leaders and More Timely Transmission of Data Could Enhance the Use of Biometrics in Afghanistan”, GAO Report Number GAO-12-442, 23 April 2012, доступно по адресу: https://www.gao.gov/assets/600/590318.txt; см. также: Noah Schactman, “Army Reveals Afghan Biometric ID Plan; Millions Scanned, Carded by May”, *WIRED*, 24 September 2010, доступно по адресу: https://www.wired.com/2010/09/afghan-biometric-dragnet-could-snag-millions/.

27 U.S. DHS, “Enhancing Security Through Biometric Identification”, доступно по адресу: https://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_biometrics_brochure_english.pdf.

28 T. Shanker (примечание 23 выше).

29 Ibid.

30 Spencer Ackerman, “Biometrics Help Nab Afghan Prison Escapees”, *WIRED*, 14 July 2011, доступно по адресу: https://www.wired.com/2011/07/biometrics-help-nab-afghan-prison-escapees/; T’ash Spenser, “Afghanistan Using Biometrics on Wide Scale for Security”, *BiometricUpdate*, 9 July 2012, доступно по адресу: https://www.biometricupdate.com/201207/afghanistan-using-biometrics-on-wide-scale-for-security.

31 Jon Boone, “Afghanistan’s Great Escape: How 480 Taliban Prisoners Broke out of Jail”, *The Guardian*, 25 April 2011, доступно по адресу: https://www.theguardian.com/world/2011/apr/25/afghanistan-great-escape-taliban.

в идентификации сбежавших заключенных и их возвращении под стражу: «В течение нескольких дней после побега около 35 заключенных были пойманы на внутренних и пограничных контрольно-пропускных пунктах; они были возвращены после подтверждения личности при помощи биометрических досье»[32]. Многие другие афганские должностные лица также занимались сбором биометрических данных. В Афганистане было реализовано два основных проекта с применением биометрических технологий: по сбору биометрических данных у заключенных «и, в терминологии НАТО, "других лиц, представляющих интерес"»[33], и по сбору биометрических данных при приеме на службу в армию и полицию. Администрированием Афганской автоматизированной системы биометрической идентификации (AABIS)[34], разработанной Министерством внутренней безопасности США и НАТО, «занимались около 50 афганских служащих Министерства внутренних дел в Кабуле»[35], которые обеспечивали сбор «биометрических данных при приеме на службу в армию и полицию»[36] в целях «предупреждения проникновения диверсантов "Талибана" в афганскую армию»[37]. Модуль с биометрическими данными интегрирован и в Афганскую систему управления кадрами и оплатой труда (APPS), которая использовалась Министерством внутренних дел и Министерством обороны Афганистана для выплаты вознаграждения служащим национальной армии и полиции[38].

Сбор биометрических данных также осуществляет ряд других акторов. Так, Национальное информационно-статистическое управление Афганистана осуществляло сбор отпечатков пальцев и сканирование радужной оболочки глаза для системы удостоверения личности e-Tazkira[39],

32 T. Shanker (примечание 23 выше).

33 Steve Gold, "Military Biometrics on the Frontline", *Biometric Technology Today*, Vol. 2010, No. 10, 2010.

34 По информации NATO, AABIS предназначена для «контроля передвижения боевиков по Афганистану, а также предупреждения проникновения в армию Афганистана диверсантов "Талибана"» (ibid.). «Полученные в полевых условиях данные сличаются и используются в режиме реального времени и в полевых условиях, после чего партия данных обрабатывается и передается в Кабул для централизованного хранения и копирования другими базами данных в Афганистане и США» (ibid.).

35 База данных хранится Министерством внутренних дел; см.: Afghan War News, "Afghan Automated Biometrics Information System (AABIS)", доступно по адресу: https://afghanwarnews.info/intelligence/aabis.htm.

36 Federal Bureau of Investigation (FBI), "Mission Afghanistan: Biometrics. A Measure of Progress", 29 April 2011, доступно по адресу: https://www.fbi.gov/news/stories/mission-afghanistan-biometrics.

37 S. Gold (примечание 33 выше).

38 Eileen Guo and Hikmat Noori, "This is the Real Story of the Afghan Biometric Databases Abandoned to the Taliban", *MIT Technology Review*, 30 August 2021, доступно по адресу: https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/. По мнению критиков системы, ее нельзя назвать успешной: Zack Kopplin, "Afghanistan Collapsed Because Corruption had Hollowed Out the State", *The Guardian*, 30 August 2021, доступно по адресу: https://www.theguardian.com/commentisfree/2021/aug/30/afghanistan-us-corruption-taliban.

39 «Даже национальное цифровое удостоверение личности, тазкира, выдачу которого с 2018 г. поддерживал Всемирный банк, используемое для получения государственных услуг и участия в голосовании, может поставить под угрозу уязвимые этнические группы»; см.: Rina Chandran, "Analysis — Afghan Panic Over Digital Footprints Spurs Call for Data Collection Rethink", *Reuters*, 20 August 2021, доступно по адресу: https://www.reuters.com/article/afghanistan-conflict-tech-idUSL5N2OI06Y.

внедрявшейся при поддержке Всемирного банка[40]. Независимая избирательная комиссия Афганистана применяла биометрические технологии «в попытке предупредить подтасовку результатов голосования в ходе парламентских выборов 2019 года»[41]. Сбор биометрических данных также осуществляли другие акторы. В докладе 2019 года ВПП отмечает, что с момента создания системы SCOPE в Афганистане «было зарегистрировано более 2,5 миллиона получателей помощи»[42]. УВКБ ООН начало сбор биометрических данных получателей помощи еще раньше. В 2002 году УВКБ ООН ввело обязательное распознавание радужной оболочки глаза для миллионов афганцев, получивших помощь УВКБ ООН в связи с репатриацией в Афганистан из лагерей беженцев, созданных в соседнем Пакистане. По возвращении в Афганистан каждый беженец обязан был пройти процедуру регистрации радужной оболочки глаза, внедренную УВКБ ООН[43].

Приведенный и без того длинный список акторов, ведущих сбор биометрических данных у разных категорий населения Афганистана, тем не менее, не является исчерпывающим. Нашей целью было показать многообразие акторов, осуществляющих в самых разных целях сбор и хранение биометрических данных граждан Афганистана — субъектов, которые подозреваются в терроризме вооруженными силами США, лиц, сотрудничающих с силами США, заключенных, или бывших беженцев, зарегистрированных УВКБ ООН. При всем многообразии акторов, которые порой занимаются прямо противоположной деятельностью, у них есть одна общая черта — это твердая вера в то, что биометрические технологии способствуют более эффективному достижению их целей. Но как сбор и хранение биометрических данных приводят к установлению связи между разными акторами? Что происходит, когда биометрические данные от одного актора (преследующего свои цели) попадают к другому актору (также преследующему свои собственные цели)? Может ли подобная передача данных противоречить принципам защиты данных? Какое значение обмен биометрическими данными и их потоки имеют для противоречащих друг другу приоритетов в сфере безопасности — какому приоритету в итоге отдается предпочтение? Как организованы потоки биометрических данных, собираемых гуманитарными акторами? Все эти вопросы были актуальны уже 20 лет назад при проведении УВКБ ООН биометрической регистрации на границе Афганистана и Пакистана — территории, где, с точки зрения УВКБ ООН,

40 Frank Hersey, "25K Afghan Biometric Passports Ready to be Issued, 100K More to Follow", *BiometricUpdate*, 7 October 2021, доступно по адресу: https://www.biometricupdate.com/202110/25k-afghan-biometric-passports-ready-to-be-issued-100k-more-to-follow.

41 E. Guo and H. Noori (примечание 38 выше).

42 WFP, "Afghanistan Annual Country Report 2019. Country Strategic Plan 2018–2022", July 2020, p. 19, доступно по адресу: https://docs.wfp.org/api/documents/WFP-0000113807/download/.

43 УВКБ ООН поручило регистрацию беженцев пакистанскому Национальному управлению баз данных и регистрации (NADRA), то есть данные хранятся правительством Пакистана и передаются в УВКБ ООН. По сей день эта процедура является стандартной. См.: UNHCR, "Government Delivered First New Proof of Registration Smartcards to Afghan Refugees", *UNHCR*, 25 May 2021, доступно по адресу: https://www.unhcr.org/pk/12999-government-to-deliver-first-new-por-smartcards-to-afghan-refugees.html.

осуществлялась деятельность по репатриации афганского населения, тогда как с точки зрения других акторов, например войск США, — проводились контртеррористические мероприятия, одним из центральных компонентов которых была биометрическая идентификация. К некоторым вопросам мы вернемся позже, после изучения других характеристик производства биометрических данных, которыми обмениваются различные производящие их акторы, а именно — степени экспериментальности.

Сомали

В 2019 году США активизировали удары по Сомали с применением беспилотных летательных аппаратов (дронов)[44], и главной целью военных операций США остается предупреждение «использования Сомали в качестве базы международного терроризма»[45]. Но в отличие от Афганистана, в Сомали борьба с терроризмом ведется немногочисленными сухопутными силами США — а порой и без их участия[46]. В этой связи в контексте нашего анализа применения биометрических технологий в контртеррористических вмешательствах США возникают важные вопросы. Как и кто осуществляет сбор данных в Сомали, если там не присутствуют военные? Является ли биометрия сколько-нибудь значимым инструментом борьбы США с терроризмом в Сомали? Действительно — и вновь в отличие от ситуации в Афганистане — информации о том, каким образом и в какой степени войска США используют биометрические технологии в Сомали, немного. И все же некоторые данные указывают на то, что биометрия используется. В частности, снятие отпечатков пальцев с самодельных взрывных устройств, по всей видимости, практикуется не только в Афганистане. В мае 2010 года разведка с опорой на биометрические технологии сообщила, что «в США с территории Мексики пытался проникнуть предполагаемый член террористической организации “Аль-Каида” из *Сомали*»[47]. Сотрудники пограничной службы задержали человека, отпечатки пальцев

44 Kim Helfrich, “Top Islamic State Official Dies in Airstrike”, defenceWeb, 15 April 2019, доступно по адресу: https://www.defenceweb.co.za/security/national-security/top-islamic-state-official-dies-in-airstrike/.

45 Karl Wiest, “Commander of United States Africa Command Visits Somalia”, *United States Africa Command*, 27 November 2018, доступно по адресу: https://www.africom.mil/article/31366/commander-of-united-states-africa-command-visits-somalia.

46 В 2017 г. войска США вернулись в Сомали впервые с 1993 г., когда силы специального назначения США потеряли 18 человек убитыми. Недавно войска США были выведены из Сомали, но военные операции США в Сомали реализуются другими средствами, включая удары с применением беспилотных летательных аппаратов; см.: The Bureau of Investigative Journalism, “Drone Strikes in Somalia”, *The Bureau of Investigative Journalism*, доступно по адресу: https://www.thebureauinvestigates.com/projects/drone-war/somalia; Amnesty International, “Somalia: US Must Not Abandon Civilian Victims of its Air Strikes After Troop Withdrawal”, *Amnesty International,* 7 December 2020, доступно по адресу: https://www.amnesty.org/en/latest/news/2020/12/somalia-us-must-not-abandon-civilian-victims-of-its-air-strikes-after-troop-withdrawal/.

47 Anthony Kimery, “Biometrics Play Significant Role in New US Army Intelligence Doctrine”, *BiometricUpdate*, 22 September 2018, доступно по адресу: https://www.biometricupdate.com/201809/biometrics-play-significant-role-in-new-us-army-intelligence-doctrine.

которого указывали на то, что он представляет «чрезвычайный интерес для правительства США»[48]: считанные в пункте пропуска отпечатки пальцев «совпали с отпечатками пальцев подозреваемого в изготовлении используемых "Аль-Каидой" взрывных устройств, снятыми в ходе расследования с самодельного взрывного устройства и внесенными в основанный на биометрических технологиях список разыскиваемых лиц Министерства обороны США»[49]. Таким образом, даже отсутствие или очень ограниченное присутствие военных США в Сомали не препятствует сбору и хранению в базах данных США биометрических данных сомалийских членов «Аль-Каиды» (*организация, запрещенная в России. — Прим. пер.*). Приведенные и им подобные примеры позволяют предположить, что биометрия играет не последнюю роль в принимаемых США мерах по поиску подозреваемых в террористической деятельности лиц из Сомали.

Что касается военных акторов США, информации о возможном использовании ими биометрии в Сомали немного. В то же время относительно «Аш-Шабааб» бывший военнослужащий подразделения SEAL ВМС США отметил в 2017 году, что, «как только боевики попадают в плен, у них собирают биометрические данные»[50]. Сообщалось также о биометрической регистрации новобранцев частными военными компаниями[51]. Эта информация позволяет предположить, что военные акторы и компании производят биометрические данные частных лиц в Сомали. В то же время, как и в случае Афганистана, ограничиваясь сбором биометрии в военных целях, мы упускаем из виду все многообразие акторов, производящих биометрические данные для самых разных нужд. Так, в Сомали размещены многочисленные гуманитарные организации и учреждения по вопросам развития, осуществляющие сбор биометрических данных различных получателей помощи. О масштабах производства биометрических данных в Сомали свидетельствует проведенное ВПП на средства Европейского союза (ЕС) исследование по составлению карты «баз данных Сомали» включая биометрические базы данных[52]. Таким образом, сбор биометрии (малоизвестными способами) осуществляют не только военные акторы, различные участники гуманитарной деятельности также производят («идеально совместимые» — см. далее) базы данных, содержащие биометрические

48 Anthony Kimery, "Biometrics Play Significant Role in New US Army Intelligence Doctrine", *BiometricUpdate*, 22 September 2018, доступно по адресу: https://www.biometricupdate.com/201809/biometrics-play-significant-role-in-new-us-army-intelligence-doctrine.

49 Ibid.

50 Home Office, "Country Policy and Information Note. Somalia: Al Shabaab", UK Home Office, November 2020, p. 35, доступно по адресу: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/933800/Somalia-_Al_Shabaab_-_CPIN_-_V3.0e.pdf.

51 Kyle Rempfer, "US Troops, Non-Profit Trainers and a 'Lightning Brigade' Battle for Somalia", *Military Times*, 21 May 2019, доступно по адресу: https://www.militarytimes.com/news/your-army/2019/05/21/us-troops-nonprofit-trainers-and-a-lightning-brigade-battle-for-somalia/.

52 WFP Somalia, "Somalia Databases and Beneficiary Registries for Cash Transfer Programming", *World Food Programme*, October 2018, доступно по адресу: https://reliefweb.int/sites/reliefweb.int/files/resources/1555331373.Somalia%20Databases%20and%20Beneficiary%20Registries%20for%20Cash%20Transfer%20Programming.pdf.

данные разных категорий населения Сомали. УВКБ ООН осуществляет сбор и хранение биометрических данных сомалийских беженцев, получающих его помощь. К 2018 году ВПП провела биометрическую регистрацию 1,6 миллиона сомалийских получателей помощи[53].

Сбор и хранение биометрических данных также осуществляют другие учреждения системы ООН. В Пунтленде ФАО ведет «основанный на биометрических данных банк информации по лицам, занимающимся рыбным промыслом»[54]. ЮНОПС провело биометрическую регистрацию солдат Национальной армии Сомали, служащих на передовой. Любопытно, что некоторые учреждения ООН привлекают подрядчиков к созданию биометрических баз данных или получению биометрии — в частности, речь идет о регистрации населения в труднодоступных областях Сомали. По словам одного из интервьюируемых, биометрическую регистрацию для программы ЮНОПС осуществляли подрядчики. Это позволило обойти действующие в ООН строгие требования к обеспечению безопасности. В данном случае производство биометрических данных одновременно сопровождалось скрытым «аутсорсингом рисков». Наряду с подрядчиками к производству гражданских биометрических баз данных также привлекался местный персонал в Сомали: «Мы обучали сомалийцев применению оборудования [для сбора биометрических данных], поскольку в определенной местности персоналу ООН производить регистрацию было слишком опасно»[55]. Кроме того, Миссия Африканского союза в Сомали (АМИСОМ) обучала сомалийскую полицию методам биометрической регистрации. Международная организация по миграции (МОМ) оснастила биометрическими сканерами для считывания отпечатков пальцев восемь контрольно-пропускных пунктов в Сомали[56]. В дополнение к различным проектам

53 Более свежие данные получить непросто. Даже участники интервью, совместно с ВПП работавшие над биометрическими данными, не располагали готовыми актуальными цифрами.

54 FAO of the UN, "Biometrics Information Transfer System", *Food and Agriculture Organization of the United Nations*, доступно по адресу: https://www.itu.int/net4/wsis/archive/stocktaking/Project/Details?projectId=1386768611. В одном из документов Совета Безопасности ООН данный проект перечисляется среди инициатив по борьбе с пиратством, наряду с оказанием поддержки кенийским тюрьмам, и описывается как «создание в Пунтленде основанного на биометрических данных банка информации по лицам, занимающимся рыбным промыслом». См.: *Совет Безопасности ООН*. Доклад Генерального секретаря о ситуации с пиратством и вооруженным разбоем на море у берегов Сомали, док. ООН S/2013/623, 21 октября 2013 г., с. 10. Его дополняет база Интерпола, содержащая данные лиц, подозреваемых в пиратстве.

55 Анонимное интервью, декабрь 2019 г.

56 МОМ внедрила разработанную для Сахеля систему MIDAS: "IOM Upgrades Biometric Fingerprint Scanners to Enhance Somalia's Border Management", *Reliefweb*, 6 June 2018, доступно по адресу: https://reliefweb.int/report/somalia/iom-upgrades-biometric-fingerprint-scanners-enhance-somalias-border-management. Кроме того, она годами поддерживала выдачу удостоверений личности государством; см.: Canada: Immigration and Refugee Board of Canada, "Somalia: Identification Documents, Including National Identity Cards, Passports, Driver's Licenses, and Any Other Document Required to Access Government Services; Information on the Issuing Agencies and the Requirements to Obtain Documents (2013–July 2015)", SOM105248.E, 17 March 2016, доступно по адресу: https://www.refworld.org/docid/571f16dc4.html; FindBiometrics, "US-Backed NGO Project Enhances Biometric Border Screening in Mogadishu", *FindBiometrics*, 13 June 2018, доступно по адресу: https://findbiometrics.com/us-backed-ngo-project-enhances-biometric-border-screening-mogadishu-506133/.

ООН, а порой и в сотрудничестве с ними, биометрические данные получали исследователи, например в процессе тестирования новых инструментов биометрической регистрации избирателей в ходе выборов 2017 года в Сомалиленде. Это не исчерпывающий список примеров, а иллюстрация широты спектра военных и невоенных акторов, участвующих в создании баз данных, содержащих биометрическую информацию о лицах сомалийского происхождения, в том числе о тех, кто занимается рыбным промыслом, пересекает государственную границу, а также о беженцах и о солдатах, служащих на передовой.

Производство данных: b) при каких условиях

Афганистан

Первой «лабораторией» в реальных условиях, в которой военные США тестировали применение биометрии в борьбе с терроризмом, стал Ирак. Точнее, идея «массового применения биометрии в условиях военных действий впервые была опробована морской пехотой в 2004 году в Эль-Фаллудже»[57]. Ранее имели место мелкомасштабные пилотные проекты, например тестирование биометрических прототипов «в иракских центрах содержания под стражей в 2003 году»[58]. Несмотря на то что анализ ситуации в Ираке не является целью настоящей статьи, она представляется важной как источник «историй успеха», которые распространились за пределы Ирака и повлияли на применение биометрии в рамках контртеррористической деятельности в Афганистане. Как отметил генерал Петреус: «Основываясь на полученном в Ираке опыте, я активно отстаивал применение биометрии и в Афганистане»[59]. Хотя биометрия тестировалась в полевых условиях ранее, различные источники утверждают, что и в Афганистане применение биометрических технологий было в некотором смысле экспериментальным — например проверялось, как разработанные в других странах устройства покажут себя в сложных афганских условиях. В частности, было обнаружено, что «ручные [биометрические] устройства отказывают в условиях жаркого афганского лета»[60]. Еще одним параметром, ставшим объектом экспериментов, была функциональная совместимость: «…военные признаю́т, что новые системы, развертываемые американскими силами, коалицией и афганцами, не всегда совместимы друг с другом»[61].

57 Относительно этого «эксперимента»: «…убежище повстанцев было огорожено, входить и выходить разрешалось только тем, кто сдал биометрию»; см.: T. Shanker (примечание 23 выше).
58 N. Toft Djanegara (примечание 4 выше), p. 6.
59 T. Shanker (примечание 23 выше).
60 Ibid.
61 Ibid. Кроме того, отмечалось, что «войска США допускали ошибки в применении биометрических технологий; так, в Ираке военные собрали значительное количество данных гражданских лиц, и только после этого выяснилось, что одна база данных несовместима с другой»: S. Gold (примечание 33 выше).

Экспериментальный характер применения биометрических прототипов, масштабы их применения и другие неотработанные аспекты, такие как функциональная совместимость, были характерны не только для использования биометрии войсками США. Так, Всемирный банк оказывал «техническую помощь [афганскому] правительству в связи с тестированием проектов мобильных платежей для перечисления заработной платы»[62], предусматривавших регистрацию «биометрических данных и биографических сведений сотрудников Министерства образования, получающих заработную плату»[63]. Кроме того, тестирование биометрии производило УВКБ ООН[64]. В 2002 году УВКБ ООН приступило к реализации «первой подобной программы УВКБ ООН по применению биометрических технологий для афганских беженцев в Пакистане»[65]. Обезличенные копии радужной оболочки глаза, хранившиеся в системе, использовались для проверки получения возвращающимися в страну афганскими беженцами помощи УВКБ ООН. «Ложноположительный» результат, то есть ошибочное совпадение радужной оболочки глаза с шаблонами в базе данных УВКБ ООН, мог означать, что сбой биометрической технологии стал причиной отказа УВКБ ООН в помощи беженцу, имеющему на нее право, но неверно соотнесенному с хранящимися в системе данными[66]. В связи с применением биометрии респонденты также отмечали, и это касалось не только Афганистана, что «для развертывания подобных сложных технологий в трудных условиях характерен высокий коэффициент отказов»[67].

Не только УВКБ ООН, но и ВПП тестировала биометрические технологии в Афганистане: «В данный момент ВПП тестирует революционное решение, которое позволит применять новые технологии в деятельности по оказанию продовольственной помощи»; начиная с мая 2014 года «реализуется 6 проектов выдачи электронных ваучеров»[68]. То есть ВПП тестировала

62 Относительно этого пилотного проекта Всемирный банк отмечает: «Имеющуюся нормативно-правовую базу необходимо будет доработать в целях устранения недостатков, касающихся конфиденциальности данных и защиты потребителей». The World Bank, "Combined Project Information Documents/Integrated Safeguards Datasheet (PID/ISDS)", The World Bank, 18 February 2019, p. 8, доступно по адресу: https://documents1.worldbank.org/curated/en/591601550669552595/pdf/Project-Information-Document-Integrated-Safeguards-Data-Sheet-Payments-Automation-and-Integration-of-Salaries-in-Afghanistan-PAISA-P168266.pdf.

63 The World Bank, ibid., p. 8.

64 Katja Lindskov Jacobsen and Karl Steinacker, "Contingency Planning in the Digital Age. Biometric Data of Afghans Must Be Reconsidered", *PRIO Blogpost*, 26 August 2021, доступно по адресу: https://blogs.prio.org/2021/08/contingency-planning-in-the-digital-age-biometric-data-of-afghans-must-be-reconsidered/.

65 Irwin Loy, "Biometric Data and the Taliban: What are the Risks?" *The New Humanitarian*, 2 September 2021, доступно по адресу: https://www.thenewhumanitarian.org/interview/2021/2/9/the-risks-of-biometric-data-and-the-taliban.

66 Katja Lindskov Jacobsen, "Experimentation in Humanitarian Locations: UNHCR and Biometric Registration of Afghan Refugees", *Security Dialogue*, Vol. 46, No. 2, 2015.

67 G. Hosein and C. Nyst (примечание 12 выше), p. 81.

68 Katrin Fakiri, "Building a Gateway to Digital Payments in Afghanistan: The World Food Programme's E-Voucher Initiative", Case Study, Better Than Cash Alliance, New York, May 2016, доступно по адресу: https://btca-production-site.s3.amazonaws.com/documents/185/english_attachments/Afghanistan_Case_Study_May2016.pdf?1463507198.

электронные ваучеры в качестве «новой модели продовольственной помощи»[69]. Биометрические технологии были важным компонентом модели выдачи электронных ваучеров: «В целях проверки личности получателя помощи система биометрической регистрации снимает отпечатки пальцев получателя. <…> Это позволяет проверять и принимать платежи за продукты питания, приобретенные получателем электронного ваучера»[70]. Одной из проблем, выявленных в ходе пробного проекта распределения электронных ваучеров, который финансировался США, было то, что в ряде случаев, «касавшихся около 5% получателей помощи, считывание отпечатков пальцев устройством торговой точки было невозможным либо в силу пожилого возраста получателя помощи, либо вследствие попытки отоварить электронный ваучер ранее не зарегистрированным представителем получателя»[71]. Несмотря на обнаружение этих и других проблем — или скорее наряду с ними, — в ходе пилотного проекта ВПП были получены биометрические данные около «70 тысяч получателей продовольственной помощи». Преимущества новой системы для ВПП состояли в ее подотчетности и универсальности. В то же время, как отметил один из респондентов относительно информированного согласия, говоря о другой ситуации: «Какие гарантии можно дать получателям помощи относительно того, где окажутся полученные у них данные?» Вместе с тем существует международная нормативно-правовая база применения биометрических данных, в частности международные нормы в области прав человека и такие требования, как получение согласия и сбор данных в определенных целях. Мы вернемся к вопросу о рисках, связанных с потенциальными потоками биометрических данных, в следующем разделе.

Эксперименты в сфере биометрических технологий не только приводят к производству данных, которые впоследствии могут распространяться непредусмотренными путями. Если рассмотреть условия производства биометрических данных, станет очевидным еще одна группа рисков, включая риски технического отказа, а также менее заметная проблема — получение данных у субъектов, к чьей подверженности рискам, связанным с биометрическими технологиями, по всей видимости, относятся с большей толерантностью[72]. В то же время, несмотря на полученные за два десятка лет, в течение которых производятся биометрические данные, свидетельства рисков и отсутствия гарантий безопасности — как отмечалось и другими источниками, — часто «сопутствующие риски практически не принимались во внимание»[73], как и вопросы о том, каким образом будут

69 См. также: WFP SCOPE, "WFP's Beneficiary and Management System", WFP SCOPE, 16 January 2018, доступно по адресу: https://www.globalinnovationexchange.org/innovation/scope-wfp-s-beneficiary-and-management-system.

70 K. Fakiri (примечание 68 выше).

71 Ibid.

72 Katja Lindskov Jacobsen, "Making Design Safe for Citizens: A Hidden History of Humanitarian Experimentation", *Citizenship Studies*, Vol. 14, No. 1, 2010.

73 Keren Weitzberg, Margie Cheesman, Aaron Martin and Emrys Schoemaker, "Between Surveillance and Recognition: Rethinking Digital Identity in Aid", *Big Data & Society*, Vol. 8, No. 1, 2021.

удалены собранные данные и как они будут защищены от доступа неуполномоченных лиц, а также о том, как в отсутствие ответов на предыдущие вопросы получить осмысленное согласие субъекта данных. На что дают согласие субъекты данных, когда их сведения вносятся в биометрические базы данных гуманитарных и других организаций? На бессрочное хранение данных? На разглашение их биометрических данных? Как пояснил один из интервьюируемых (о применении биометрии не только в Афганистане): «Мы решили убрать из формы согласия раздел об удалении данных. Мы не можем этого гарантировать»[74]. Знают ли беженцы, зарегистрированные гуманитарными акторами, такими как УВКБ ООН или ВПП, о том, что их данные будут храниться вечно, и согласны ли они с этим? Какое значение имеют «лабораторные» условия — не только на пробном этапе, но и при последующем внедрении биометрических технологий?

Сомали

Многие из этих многочисленных акторов используют в Сомали биометрию в рамках более или менее экспериментальных программ. Например, в рамках инициативы по биометрической регистрации избирателей в Сомалиленде, в которой принимали участие специалисты из Университета Нотр-Дам, использовалась технология распознавания радужной оболочки глаза[75]. В ходе предыдущих экспериментальных проектов снятие отпечатков пальцев не решило проблему «двойной регистрации», то есть использования «системы» одним и тем же избирателем дважды, в данном случае для подачи более одного голоса. Одной из целей проекта распознавания радужной оболочки глаза было изучение проблемы двойной регистрации в ходе сбора биометрических данных, в том числе в целях создания достоверного контрольного списка избирателей[76]. Реализованные в Сомалиленде и других частях Сомали экспериментальные проекты не «просто» стали источником знаний о надежности технологии распознавания радужной оболочки глаза в контексте учета избирателей. Сомали рискует незаметно превратиться в «живую лабораторию», а все больше жителей Сомали — в «подопытных» этих экспериментов. Экспериментальное применение биометрии в сложных условиях позволяет «проверить» технологию, но и связано с рядом проблем, например с проблемой получения информированного согласия. Эта проблема не ограничивается проектами распознавания радужной оболочки глаза, а распространяется на широкий ряд в разной степени экспериментальных проектов применения биометрии в Сомали. Как отметил один

74 Анонимное интервью, сентябрь 2021 г.

75 ACE, "Iris Biometric Voter Registration in Somaliland", *ACE Electoral Knowledge Network*, 3 December 2014, доступно по адресу: https://aceproject.org/electoral-advice/archive/questions/replies/413937370.

76 Stephen Mayhew, "Notre Dame Researchers Using Iris Recognition to Improve Accuracy of Somaliland Election Process", *BiometricUpdate*, 21 August 2014, доступно по адресу: https://www.biometricupdate.com/201408/notre-dame-researchers-using-iris-recognition-to-improve-accuracy-of-somaliland-election-process.

из участников интервью в связи с невоенным использованием биометрии: «Это как дразнить ребенка конфетой», — указав на серьезные проблемы получения осмысленного информированного согласия (помощь беженцам, голосование и так далее) в ходе экспериментального применения биометрических технологий. Действительно, учитывая уязвимое положение и отсутствие альтернатив, стоит задаться вопросом, можно ли считать подлинным согласие, полученное в таких обстоятельствах. Как пояснил тот же интервьюируемый: «Предоставление согласия — это очень сложное понятие: согласие на хранение данных? На их распространение? В каких целях?» То есть проекты экспериментального применения биометрических технологий не только дают новые знания. Их продуктом также становятся получатели помощи (рыбаки и так далее) и другие регистрируемые субъекты данных (новорожденные, избиратели и так далее), которые являются якобы приемлемыми объектами эксперимента.

Еще один пример — снятие отпечатков пальцев у новорожденных. «Несмотря на многолетние усилия, достоверная биометрическая идентификация новорожденных и детей младенческого возраста остается недостижимой»[77]. Тем не менее, хотя критики метода среди прочих поводов для беспокойства, связанных с биометрическими данными детей младенческого возраста, отмечают, что их бы «удивило, если бы в богатых странах идея снятия отпечатков пальцев у детей раннего возраста относилась к разряду приемлемых или даже допустимых»[78], экспериментальное получение биометрических данных детей младенческого возраста практиковалось в Индии: «Лонгитюдная база данных отпечатков пальцев у населения столь раннего возраста была собрана впервые», — отметил г-н Джейн, специалист по биометрическим технологиям Мичиганского государственного университета. После реализации этого пробного проекта Джейн обсудил с ООН «применение системы Всемирной продовольственной программой»[79]. Позднее ВПП объявила о решении реализовать в партнерстве со специалистами Мичиганского государственного университета «пробный проект» для проверки использования детской биометрии в качестве решения ситуации, рассматриваемой ВПП как проблемной, а именно ситуации «предъявления разными семьями одних и тех же детей как своих собственных в целях получения дополнительных продовольственных пайков»[80]. В ходе проекта

77 Steven Saggese, Yunting Zhao, Tom Kalisky, Courtney Avery, Deborah Forster, Lilia Edith Duarte-Vera, Lucila Alejandra Almada-Salazar, Daniel Perales-Gonzalez, Alexandra Hubenko, Michael Kleeman, Enrique Chacon-Cruz and Eliah Aronoff-Spencer, "Biometric Recognition of Newborns and Infants by Non-Contact Fingerprinting: Lessons Learned", *Gates Open Research*, Vol. 3, 2019.

78 Ben Parker, "Betting on Biometrics to Boost Child Vaccination Rates", *The New Humanitarian*, 18 July 2019, доступно по адресу: https://www.thenewhumanitarian.org/news-feature/2019/07/18/betting-biometrics-boost-child-vaccination-rates.

79 Aviva Rutkin, "We Now Have the Tech to Fingerprint Babies — But Should We?", *New Scientist,* 15 June 2016, доступно по адресу: https://www.newscientist.com/article/mg23030782-200-we-now-have-the-tech-to-fingerprint-babies-but-should-we/.

80 The New Humanitarian, "Syria Cash Aid Freeze, Somali Biometrics, and Poverty Porn: The Cheat Sheet", *The New Humanitarian*, 26 April 2019, доступно по адресу: https://www.thenewhumanitarian.org/cheat-sheet/2019/04/26/syria-cash-aid-freeze-somali-biometrics-and-poverty-porn-cheat-sheet.

«в течение семи месяцев были взяты отпечатки пальцев у 150 детей из трех населенных пунктов в Сомали»[81]. Проект позволил получить «доказательства» надежности детской биометрии. Согласно сообщениям ВПП, проект продемонстрировал, что биометрические данные могут быть использованы для идентификации детей до пяти лет, и предоставил «подтверждения», которые подкрепляют идею о расширении регистрируемых групп населения, теперь включающих детей младше пяти лет. Еще одним следствием эксперимента ВПП стал призыв «активизировать научные исследования» для проверки надежности применения биометрических технологий среди детей младше пяти лет: «…несмотря на отдельные случаи применения биометрических технологий среди детей старше пяти лет, решения для более раннего возраста в основном носят экспериментальный характер и должны быть более тщательно исследованы»[82]. Призыв к проведению дополнительных исследований отвечает общей логике подобных проектов, когда для устранения недостатков и ограничений принимается больше все тех же мер: больше биометрических экспериментов, больше собранных биометрических данных, больше функциональной совместимости, больше обмена данными. И получение доказательств, и призыв к активизации научных исследований вторят видению будущего Министерства обороны США, в котором биометрия распространена повсеместно, и, таким образом, поддерживают идею расширения применения биометрических технологий как успешного и, предположительно, более этичного средства борьбы с терроризмом.

Ситуация в Сомали, как и «истории успеха» из Ирака, подпитывавшие более общие «мечты» и повлиявшие на применение биометрии в Афганистане, показывает в чем-то схожую динамику. В качестве примера того, как родилась идея использования биометрии в одном из проектов ООН, интервьюируемый описал использование биометрических технологий Службой ООН по вопросам деятельности, связанной с разминированием[83], на чью «историю успеха» ориентировались другие программы ООН[84]. Разные участники интервью описывали схожую динамику распространения историй успеха в сфере биометрических технологий: «Когда я работал(-а) с биометрией, она не была так популярна. Но успех проекта побудил многие другие учреждения ООН, скажем так, поддаться эффекту толпы». Интервьюируемый добавил, что информация об успешном применении биометрии в определенном проекте ООН «например, озвучивалась

81 The New Humanitarian, "Syria Cash Aid Freeze, Somali Biometrics, and Poverty Porn: The Cheat Sheet", *The New Humanitarian*, 26 April 2019, доступно по адресу: https://www.thenewhumanitarian.org/cheat-sheet/2019/04/26/syria-cash-aid-freeze-somali-biometrics-and-poverty-porn-cheat-sheet.

82 Unicef, "Biometrics: UNICEF Guidance on the Use of Biometrics in Children-Focused Services", *Unicef*, October 2019, доступно по адресу: https://data.unicef.org/resources/biometrics/.

83 Анонимный интервьюируемый указал, что Служба ООН по вопросам деятельности, связанной с разминированием, «прибыла в Сомали на самом раннем этапе в свете характера своей работы».

84 Интервью, декабрь 2019 г. См. также: U.S. Department of State, *Country Reports on Human Rights Practices for 2011*, Washington, DC, 2012, p. 538.

на заседании руководителей программ (ФАО, УНП ООН [Управление Организации Объединенных Наций по наркотикам и преступности] и так далее), то есть внутри ООН».

Изучение «историй успеха», служащих примером нематериальной составляющей биометрических инфраструктур, важно в силу ряда причин. К их последствиям можно отнести, например, укрепление уверенности в пользе применения данной технологии для разных проектов ООН и в применении биометрии все большим числом программ. Кроме того, истории успеха под эгидой ООН подкрепляют ожидания не только других программ ООН, но и акторов за пределами организации. Эти истории транслируются на специализированных веб-сайтах, демонстрируя ценность и надежность биометрических технологий. Как пояснил, к примеру, один из опрошенных, приводя пример технологии, оказавшейся полезной федеральному правительству Сомали: «Наша автоматизированная система биометрической идентификации (ABIS) была развернута МООНСОМ [Миссией Организации Объединенных Наций по содействию Сомали]»[85]. Подобные истории успеха в связи с применением биометрических технологий могут также укреплять веру в биометрию как средство борьбы с терроризмом. Этот подрядчик не только поставил свои системы ЮНОПС, но и «был награжден Министерством внутренних дел за работу над проектом по борьбе с терроризмом» как компания, «тесно связанная» с Министерством обороны и НАТО[86]. Таким образом «истории успеха» и другие «знания», полученные в ходе в той или иной степени экспериментального применения биометрии в Сомали, подкрепляют концепции использования биометрических технологий в целях борьбы с терроризмом. В то же время критики биометрии отмечали, что «инициативы применения биометрических технологий в Сомали различными международными акторами дали сомнительные результаты и отрицательно повлияли на местное население»[87]. Одним из подходов к изучению отдельных аспектов такого «отрицательного влияния» является анализ процессов, происходящих с биометрическими данными после их сбора.

Потоки данных и последующие процессы

Как применяется биометрическая инфраструктура после сбора биометрии всеми соответствующими акторами? Всех этих акторов объединяет вера в важную роль биометрии в достижении стоящих перед ними целей (защита беженцев, оказание чрезвычайной помощи, борьба с пиратством и терроризмом и так далее), но отправной точкой для исследования процессов, происходящих с полученными ими биометрическими данными,

85 Human Recognition Systems, "Case Study UN Somalia", доступно по адресу: https://www.hrsid.com/case-studyun-somalia?__hstc=90097796.566aa022561b6cdf11fa359f1b3a830f.1579511311374.1579511311374.1579511311374.1&__hssc=90097796.1.1579511311374&__hsfp=2488122038.

86 S. Gold (примечание 33 выше).

87 K. Weitzberg (примечание 11 выше).

становится предложенный Ларкиным акцент на потоках, в данном случае — потоках биометрических данных. Перейдя от анализа создания биометрических баз данных к изучению последующих потоков данных, далее мы приводим примеры предусмотренных и непредусмотренных потоков данных (существенно отличающихся с точки зрения получателей данных и процедур обмена данными).

Потоки данных и последующие процессы: а) предусмотренные — соглашения об обмене данными

Афганистан

Одним из примеров предусмотренного обмена биометрическими данными является уже упоминавшаяся система AABIS, в дизайн которой была заложена возможность передачи данных между Федеральным бюро расследований США (ФБР) и афганским Министерством внутренних дел. По данным ФБР, обмен информацией с партнерами, такими как ФБР, был одним из «ключевых компонентов программы [AABIS]», поддерживавшим потоки важнейших данных[88]. AABIS представляет собой пример решения, сама концепция которого предусматривает обмен биометрическими данными: «AABIS … разработана с учетом совместимости с автоматизированной системой биометрической идентификации Министерства обороны США и автоматизированной системой дактилоскопического учета ФБР»[89]. После вывода в августе 2021 года войск США и других сил коалиции из Афганистана возник ряд вопросов. Один из них: будет ли биометрическая база данных, которая, по данным одного из источников, содержит около «8,1 миллиона записей», сохранена или удалена?[90] Если база данных будет сохранена, как это повлияет на изменение границ биометрических инфраструктур, используемых в контртеррористической деятельности, с учетом вопроса о границах вмешательства и гипотетического доступа сторонних акторов к биометрическим данным миллионов афганских граждан. Этот и другие примеры обмена биометрическими данными в контексте борьбы с терроризмом важно анализировать с учетом поощрения обмена биометрическими данными широким спектром акторов и инициатив, среди которых можно выделить в том числе резолюцию 2396 (2017) Совета Безопасности, обязывающую государства «разрабатывать и внедрять системы сбора био-

88 FBI, "Mission Afghanistan: Biometrics. Part 4: A Measure of Progress", *FBI*, 29 April 2011, доступно по адресу: https://www.fbi.gov/news/stories/mission-afghanistan-biometrics.

89 AABIS: Afghan War News (примечание 35 выше). О центральной роли «обмена данными с Министерством обороны и Федеральным бюро расследований» также сообщают другие источники, включая доклад Министерства обороны; см.: Office of the Secretary of Defense, "Justification for FY 2022 Afghanistan Security Forces Fund (ASFF)", May 2021, p. 42, доступно по адресу: https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2022/FY2022_ASFF_Justification_Book.pdf.

90 E. Guo and H. Noori (примечание 38 выше).

метрических данных» для «ответственного и надлежащего выявления террористов»[91].

Говоря об Афганистане, привлечь внимание к последствиям попадания биометрических данных в руки «Талибана» (см. далее), которые могут быть фатальными, важно по ряду причин. В частности, это поможет обозначить срочную необходимость в обсуждении оптимальных способов ограждения субъектов биометрических данных, находящихся в Афганистане, от новых рисков, включая риск применения к ним карательных мер. В то же время в ходе подобной дискуссии нельзя забывать о том, что предусмотренный обмен данными, обусловленный «дизайном системы», также не лишен проблемных аспектов, пусть порой и менее явных. Так, разные акторы, осуществляющие сбор и хранение биометрических данных каждый в своих целях, могут разделять веру в пользу биометрии. Но подобные одинаковые убеждения нередко сопровождаются очень важными различиями в логике и приоритетах обеспечения безопасности, как, например, те, что наблюдаются между военными и гуманитарными акторами (но не только между ними). Признав, что логика, полномочия и приоритеты в области защиты, характерные для разных акторов, производящих биометрические данные, не всегда согласуются между собой, важно задать вопрос о том, какими путями — предусмотренными и непредусмотренными — распространяются биометрические данные. Важно и то, как потоки данных влияют на приоритеты в сфере безопасности, возможно не согласующиеся между собой, и то, как они в конечном счете сказываются на безопасности частных лиц, доступ к биометрическим данных которых может осуществляться без их согласия и даже без их ведома. В этой связи любопытно отметить, что в своем годовом отчете по Афганистану ВПП, говоря о соглашениях об обмене данными, подписанных с четырьмя партнерскими организациями — УВКБ ООН[92], Международный комитет спасения, Норвежский совет по делам беженцев (NRC) и Shelter Now International, — отмечает, что соглашения об обмене данными получателей помощи не распространяются на биометрические данные[93]. Значение этих данных и трудности, связанные с их защитой, даже при наличии соглашений об обмене данными, в явной

91 Krisztina Huszti-Orbán and Fionnuala Ní Aoláin, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?*, Human Rights Center at the University of Minnesota, July 2020; док. ООН S/RES/2396(2017), 21 декабря 2017 г.

92 С 1985 г. УВКБ ООН заключались и продлевались меморандумы о взаимопонимании (МоВ), действующие на глобальном уровне; последняя редакция МоВ датируется 2018 г. См.: UNHCR and WFP, "Addendum on Data Sharing to the January 2011 Memorandum of Understanding between the Office of the United Nations High Commissioner for Refugees (UNHCR) and the World Food Programme (WFP)", 17 September 2018, доступно по адресу: https://www.refworld.org/docid/5bbcac014.html. Впервые в документ были включены положения об обмене данными и о возможности предоставления сторонами «доступа к биометрическим данным главы домохозяйства и дополнительного получателя помощи, а также, в исключительных случаях, [обеспечения] передачи биометрических данных»; см.: UNHCR and WFP, "Annex 1: Matrix of Personal Data, Non-Personal Data and Information", 17 September 2018, доступно по адресу: https://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=5bbcac204.

93 WFP (примечание 42 выше).

форме исключающих обмен биометрией, становятся очевидными в свете следующих примеров непредусмотренных потоков данных.

Сомали

Некоторые биометрические инфраструктуры предназначены для поддержки потоков данных в пределах гуманитарного сектора, например для внутреннего обмена биометрическими данными между различными участниками гуманитарной деятельности в Сомали[94]. Повышение функциональной совместимости различных баз данных участников гуманитарной деятельности в Сомали было главной темой доклада, описывающего, в числе прочего, проекты тестирования «совместимости биометрических данных» ВПП и Somalia Cash Consortium. Отдельной целью вышеупомянутого анализа «баз данных Сомали», включая биометрические базы данных, была оценка «потенциала обмена данными и функциональной совместимости» и не просто производство биометрических данных, но и разработка «стандартов сбора биометрических данных»[95].

Заключение соглашений об обмене данными создает условия для возникновения еще одного типа предусмотренных потоков данных. В качестве примера соглашения об обмене данными, создавшего условия для возникновения потоков биометрических данных, можно привести принятое в 2010 году ЕС решение о передаче Интерполу данных «лиц, подозреваемых в морском пиратстве», включая отпечатки пальцев, полученные Военно-морскими силами ЕС в Сомали, для проверки биометрических данных «в сравнении с глобальной базой данных Интерпола»[96]. Что касается конкретных примеров соглашений об обмене данными, допускающих передачу собранных гуманитарными акторами биометрических данных за пределы их баз данных, организация Privacy Impact Assessment указывает на то, что Министерство внутренней безопасности США «обеспечивает неявный сбор биометрической информации десятков тысяч беженцев, многие из которых никогда не попадут в Америку»[97]. Министерство внутренней безопасности США получает биометрические данные «по соглашению об обмене данными с Управлением Верховного комиссара Организации Объединенных Наций по делам беженцев, которое направляет федеральным агентствам досье

94 B. Owino (примечание 14 выше).
95 K. Fakiri (примечание 68 выше).
96 K. Weitzberg (примечание 11 выше).
97 FindBiometrics, "The DHS and UNHCR are Sharing Biometric Data of Refugees", *FindBiometrics*, 23 August 2019, доступно по адресу: https://findbiometrics.com/dhs-unhcr-sharing-biometric-data-refugees-082304/. «По МоВ 2019 г. УВКБ ООН напрямую передает биометрическую и сопутствующую биографическую информацию в Автоматизированную систему биометрической идентификации (IDENT) Службы управления биометрической идентификацией при Министерстве внутренней безопасности США (которая вскоре будет заменена Национальной системой усовершенствованного распознавания (HART))»; см.: U.S. DHS, *Privacy Impact Assessment for the United Nations High Commissioner for Refugees (UNHCR) Information Data Share DHS/USCIS/PIA-081*, 13 August 2019, p. 1, доступно по адресу: https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis081-unhcr-august2019.pdf.

беженцев в целях их переселения [в США]»[98]. В то же время в 2018 году из почти 85 тысяч заявок УВКБ ООН на переселение было одобрено менее четверти[99]. На основании подобных соглашений об обмене данными биометрические данные «десятков тысяч беженцев, не допущенных в страну», попадают в базы данных Министерства внутренней безопасности и хранятся в «системе IDENT [Автоматизированная система биометрической идентификации] Службы внутренней безопасности», а также передаются различным федеральным агентствам[100]. IDENT представляет собой «постоянно пополняемую базу данных, содержащую биометрическую информацию и другие персональные данные более 200 миллионов человек, которые въезжали, предпринимали попытку въезда в Соединенные Штаты Америки и выезжали за их пределы»[101]. Не менее важным в свете вышеупомянутого соглашения об обмене данными с УВКБ ООН представляется и то, что в IDENT хранится информация о людях, которые никогда не бывали в США.

Анализ потоков данных, основанных на подобных соглашениях об обмене данными, наводит на ряд важных вопросов, включая вопросы охвата биометрических инфраструктур, используемых в контртеррористической деятельности: в какой степени биометрические инфраструктуры такого рода взаимодействуют с биометрическими данными, хранящимися невоенными структурами? Невоенные биометрические базы данных ценятся не только донорами, которые считают, что благодаря биометрической регистрации «помощь получают те, для кого она предназначена»[102], но и участниками контртеррористической деятельности[103]. Как отмечается

98 U.S. DHS, *Privacy Impact Assessment for the United Nations High Commissioner for Refugees (UNHCR) Information Data Share DHS/USCIS/PIA-081*, 13 August 2019, доступно по адресу: https://www.dhs.gov/publication/dhsuscispia-081-united-nations-high-commissioner-refugees-unhcr-information-data-share.

99 Eric Weiss, "DHS and UNHCR are Sharing Biometric Data of Refugees", *Find Biometrics*, 23 August 2019, доступно по адресу: https://findbiometrics.com/dhs-unhcr-sharing-biometric-data-refugees-082304/. Давая оценку этому явлению, интервьюируемый отметил, что «в период пребывания Трампа на посту президента ситуация изменилась. При Обаме одобрялось 90 и более процентов заявок» (интервью, ноябрь 2021 г.).

100 Ibid.

101 Thales Group, "DHS's Automated Biometric Identification System IDENT — The Heart of Biometric Visitor Identification in the USA", *Thales Group*, 19 January 2021, доступно по адресу: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/ident-automated-biometric-identification-system.

102 National Independent Electoral Commission, Federal Republic of Somalia. "Voter Registration Feasibility Study Report", UNSOM, UNDP, Mogadishu, Somalia, November 2017, p. 31, доступно по адресу: https://www.ec-undp-electoralassistance.org/wp-content/uploads/sites/24/2019/03/VR-Feasibility-Study-Report-Eng.pdf.

103 The New Humanitarian, "Head to Head: Biometrics and Aid. One Timely Topic, Two Opinionated Views", *The New Humanitarian*, 17 July 2019, доступно по адресу: https://www.thenewhumanitarian.org/opinion/2019/07/17/head-head-biometrics-and-aid. В этой статье, к примеру, отмечается: «В 2019 г. сотрудничество ВПП и «Палантир» (американская компания, сотрудничающая с контртеррористическими службами, ЦРУ, полицией и Иммиграционной и таможенной службой США) вызвало серьезные вопросы. Широко распространено мнение о том, что учреждения по оказанию помощи проявляют наивность, заключая с корпорациями соглашения о сотрудничестве в сфере данных, не вполне осознавая их последствия».

в политике обработки биометрических данных Международного Комитета Красного Креста, организации «известно, какую роль играют биометрические данные в обнаружении и идентификации лиц, представляющих интерес для государств и служб безопасности», а также, что МККК осознаёт, что государственные органы власти очень заинтересованы в получении подобных данных от организаций, осуществляющих деятельность в условиях чрезвычайных ситуаций гуманитарного характера. Подобная заинтересованность может распространяться на использование биометрических данных в целях… которые могут быть несовместимы с беспристрастным, нейтральным и независимым характером деятельности МККК, [включая] контртеррористическую деятельность[104].

Privacy International также утверждает, что ценность биометрических данных, полученных в рамках программ помощи, «не ускользнула от разведывательных служб»[105]. Схожее мнение выражает Макдональд: «Международные разведывательные службы осознаю́т уникальную ценность данных, собираемых гуманитарными организациями»[106]. Эти проблемы актуальны не только для Сомали, но и для сбора биометрических данных в процессе гуманитарной деятельности в целом, однако масштабы производства невоенных биометрических данных в Сомали в сочетании с постоянной контртеррористической деятельностью США на территории страны обусловили создание в Сомали условий, очень интересных с точки зрения изучения производства биометрических данных, их потоков и последствий распространения. На различные «проблемы, связанные с передачей данных государственным органам», также указывали другие ученые, анализировавшие применение биометрической регистрации гуманитарными акторами[107].

Несмотря на сложности доказывания возможных инфраструктурных взаимосвязей, их анализ приобретает особую значимость, когда речь идет не только о роли доноров (например, соглашения об обмене данными и соответствующие запросы), но и о роли корпораций наподобие «Палантира» (Palantir)[108]. Компания «Палантир» широко известна ввиду той роли, которую она играет в контртеррористической деятельности США:

104 ICRC, "Policy on the Processing of Biometric Data by the ICRC", 28 August 2019, доступно по адресу: https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_pdf.

105 Kevin P. Donovan and Carly Nyst "Privacy for the Other 5 Billion: Western-Backed Biometrics Programs for the Developing World Could Put Data in the Wrong Hands", *Slate*, 17 May 2013, доступно по адресу: https://slate.com/technology/2013/05/aadhaar-and-other-developing-world-biometrics-programs-must-protect-users-privacy.html.

106 Sean McDonald, "From Space to Supply Chains: A Plan for Humanitarian Data Governance", *SSRN*, 12 August 2019, доступно по адресу: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3436179.

107 Mirca Madianou, "The Biometric Assemblage: Surveillance, Experimentation, Profit, and the Measuring of Refugee Bodies", *Television & New Media*, Vol. 20, No. 6, 2019, доступно по адресу: https://journals.sagepub.com/doi/full/10.1177/1527476419857682.

108 Privacy International, "One of the UN's Largest Aid Programmes Just Signed a Deal with the CIA-Backed Data Monolith Palantir", *Privacy International*, 12 February 2019, доступно по адресу: https://privacyinternational.org/news-analysis/2712/one-uns-largest-aid-programmes-just-signed-deal-cia-backed-data-monolith.

ее программное обеспечение «использует ЦРУ в целях выявления террористических и повстанческих угроз»[109]. Как поясняет «Палантир», ее технологии «позволяют военным более адресно реагировать на угрозы»[110]. В то же время в отчете о своей благотворительной деятельности «Палантир» описывает применение решения Foundry для анализа данных в рамках трех экспериментальных проектов — один из которых был реализован в Сомали; данное решение обеспечило автоматизацию потоков данных ВПП и «принятие точных решений, основанных на данных, в целях обеспечения охвата получателей помощи ВПП»[111]. В феврале 2019 года ВПП объявила о заключении с «Палантир» пятилетнего соглашения о сотрудничестве[112]. Это значит, что топ-менеджмент «Палантира» осведомлен не только о военных, но и о гуманитарных данных из Сомали. Партнерство ВПП и «Палантир», которое критикуют в связи с тем, что оно могло привести к «злоупотреблению данными в "озере данных" ВПП, включая биометрические данные получателей помощи»[113], иллюстрирует значение анализа потенциальной роли невоенных биометрических данных в военных контртеррористических мерах. ВПП — единственный участник гуманитарной деятельности в Сомали, о сотрудничестве которого с «Палантир» достоверно известно. Но ВПП — не единственный невоенный актор, обеспечивающий сбор биометрических данных у разных категорий населения Сомали.

И хотя сотрудничество ВПП с «Палантиром» можно назвать исключением (ВПП — единственная гуманитарная организация, о сотрудничестве которой с корпорацией, содействующей контртеррористической деятельности вооруженных сил США, нам известно), роль корпораций в вопросах контроля биометрических данных интересна не только в контексте партнерских связей между ВПП и «Палантиром». Например, еще одной проблемной областью является использование данных коммерческими организациями — поставщиками услуг, в частности поддерживающими программы оказания денежной помощи. Программы могут быть ориентированы на определенные уязвимые группы населения, которым «Талибан» угрожает по причине участия этих людей в боевых действиях, принадлежности к сексуальным меньшинствам или по любой другой причине[114].

109 Charles W. Mahoney, "United States Defence Contractors and the Future of Military Operations", *Defense & Security Analysis*, Vol. 36, No. 2, 2020, p. 192.

110 Steven Overly, "Peter Thiel's Company Palantir Defense Could Win Contracts Under Donald Trump", *Financial Review*, 9 November 2016, доступно по адресу: https://www.afr.com/technology/peter-thiels-company-palantir-defense-could-win-contracts-under-donald-trump-20161109-gskz92.

111 См. описание проекта «Палантир» в Сомали по ссылке: https://www.palantir.com/philanthropy-engineering/learn-more/wfp.html. Два других проекта были реализованы в Южном Судане и Уганде.

112 WFP, "Palantir and WFP Partner to Help Transform Global Humanitarian Delivery", *World Food Programme*, 5 February 2019, доступно по адресу: https://www.wfp.org/news/palantir-and-wfp-partner-help-transform-global-humanitarian-delivery.

113 Linda Raftree, "A Discussion on WFP-Palantir and the Ethics of Humanitarian Data Sharing", *Medium*, 5 March 2019, доступно по адресу: https://medium.com/data-stewards-network/a-discussion-on-wfp-palantir-and-the-ethics-of-humanitarian-data-sharing-4fc1499f81d8.

114 I. Loy (примечание 65 выше).

Рассуждая на более общую тему, интервьюируемый, представлявший сектор оказания гуманитарной помощи, поднял следующий вопрос: «Каким образом обеспечить эффективное удаление данных, которые передаются стольким различным акторам?» Важно отметить, что, даже если утечки крупных массивов данных не имели места, к неблагоприятным последствиям могла приводить сама вероятность утечки данных. Наряду с данными возникали и распространялись нематериальные объекты, такие как слухи и страх (в противовес мечтам), которые могли повлиять на сотрудников на местах в свете риска «восприятия в качестве коллаборанта — подрядчика ЦРУ» при сборе биометрических данных у получателей помощи, и на жителей Сомали, которые, «зная об этом партнерстве», могли отказаться от получения помощи ВПП[115].

Если взять потоки биометрических данных не только между гуманитарными организациями, а в целом в пределах Афганистана и Сомали, можно выделить еще один тип потенциального потока данных, обусловленный вероятностью непредусмотренной передачи собранных гуманитарными организациями биометрических данных вооруженным группам, и связанные с ним риски.

Потоки данных и последующие процессы: b) непредусмотренные — в руках противника

Афганистан

Особенно примечательный случай возникновения непредусмотренных потоков биометрических данных имел место после ухода войск коалиции из Афганистана в августе 2021 года. После вывода войск «“Талибан” изъял биометрические устройства вооруженных сил США, с помощью которых может быть установлена личность жителей Афганистана, сотрудничавших с международными силами, сообщает организация Intercept»[116]. «27 августа “Талибан” заявил об использовании американских цифровых технологий идентификации личности в целях преследования афганцев, сотрудничавших с силами международной коалиции»[117], — речь шла о портативных устройствах идентификации личности (биометрических устройствах), принадлежавших вооруженным силам США. Такое развитие событий связано с серьезными рисками для многих афганцев, чьи биометрические данные регистрировались и хранились системами биометрической идентификации. Для них это означало, что «“Талибан” завладел важными данными,

115 Andrew Young, “A Discussion on WFP-Palantir and the Ethics of Humanitarian Data Sharing”, *MEDIUM*, 5 March 2019, доступно по адресу: https://medium.com/data-stewards-network/a-discussion-on-wfp-palantir-and-the-ethics-of-humanitarian-data-sharing-4fc1499f81d8.

116 I. Loy (примечание 65 выше).

117 Emrys Schoemaker, “Digital Identity for Development — and Protection”, *Global Policy*, 14 September 2021, доступно по адресу: https://www.globalpolicyjournal.com/blog/14/09/2021/digital-identity-development-and-protection.

позволяющими устанавливать личность, которые, по словам "Талибана", будут использованы против тех, кого они считают противником или угрозой»[118]. Различные источники сообщали, что «Талибаном» «было создано специальное подразделение "Аль-Иша" для преследования афганцев, помогавших США и их союзникам», а после того как стало известно о том, что «Талибан» завладел биометрическими устройствами, оставленными силами коалиции, один из командиров спецподразделения отметил в интервью, «что его подразделение использует американские ручные сканеры для подключения к огромной базе биометрических данных и установит личность каждого, кто помогал союзникам НАТО»[119].

Другие авторы обращали внимание на то, что афганские граждане, чьи биометрические данные могут оказаться в распоряжении «Талибана», подвергаются опасности наказания за действия, которые режим «Талибана» расценивает как предательство. Когда речь идет о биометрии, «стереть» определенные характеристики, чтобы обеспечить свою безопасность в Афганистане, которым руководит «Талибан», не представляется возможным — нельзя изменить рисунок радужной оболочки глаза. Как «Талибан» распорядится этими данными и устройствами, покажет время. Каким образом и где «Талибан» воспользуется, если воспользуется, «данными и устройствами, чтобы установить факт сотрудничества с союзническими силами»?[120] Впервые об этой истории заговорили в августе 2021 года, но опасения такого рода высказывались уже десятью годами ранее: «Некоторые афганцы обеспокоены, что в будущем растущая биометрическая база данных может быть использована как оружие»[121]. Важно отметить, что обеспокоенность в связи с влиянием на гражданских лиц непредусмотренных последствий потоков данных выражала Специальный докладчик ООН по вопросу о поощрении и защите прав человека и основных свобод в условиях борьбы с терроризмом, профессор Финнула Ни Илан. Так, в ее докладе отмечается, что «наряду с опасностью злоупотреблений, в частности со стороны репрессивной и/или авторитарной государственной власти, вызывает озабоченность проводимый в разных обстоятельствах сбор биометрических данных уязвимых категорий населения и лиц, оказавшихся в сложной ситуации». Говоря об Афганистане, Специальный докладчик отметила не только то, что «Соединенные Штаты Америки и некоторые их союзники продолжали собирать биометрические данные населения в зонах конфликта, таких как Ирак и Афганистан», но и что правозащитные организации с 2007 года предостерегают: биометрические базы данных в непра-

118 Emrys Schoemaker, "Digital Identity for Development — and Protection", *Global Policy*, 14 September 2021, доступно по адресу: https://www.globalpolicyjournal.com/blog/14/09/2021/digital-identity-development-and-protection.

119 Siddharthya Roy and Richard Miniter, "Exclusive: First-Ever Interview With Terror Leader who's Hunting Americans and Allies in Afghanistan", *Zenger News*, 28 August 2021, доступно по адресу: https://www.zenger.news/2021/08/28/taliban-team-is-using-us-made-biometric-database-and-scanners-to-hunt-american-and-afghan-enemies/.

120 K. L. Jacobsen and K. Steinacker (примечание 64 выше).

121 T. Shanker (примечание 23 выше).

вильных руках могут стать “расстрельным списком”»[122], подвергнув опасности «миллионы афганских и иракских граждан, не совершавших ничего противозаконного»[123].

Концепция Ларкина напоминает нам о том, что мы должны изучать не только материальные потоки, но и нематериальные компоненты инфраструктур. Даже если бы «Талибан» не завладел огромными массивами биометрических данных и тем более не мог бы их активно использовать, потенциальные инфраструктурные связи, которые стали заметными с появлением историй о получении «Талибаном» доступа к биометрическим базам данных коалиции, могли породить нематериальные «потоки» в виде «слухов» и «страха» (в противовес желаниям и мечтам)[124]. Действительно, со всей тщательностью стоит подходить не только к анализу неблагоприятных последствий потоков данных, но и к изучению последствий страха: например, из страха проверки биометрических данных «Талибаном» субъект таких данных может отказаться от обращения за помощью в больничное учреждение. В подобных случаях, даже если потенциальные потоки биометрических данных и возможности их применения не обретают материальную форму, важно не забывать о возникновении и потоке страха, который может отрицательно повлиять на безопасность лиц, прошедших биометрическую регистрацию. Подобные вопросы имеют отношение ко всем акторам, обеспечивающим сбор биометрических данных в Афганистане (и других странах). Могут ли быть даны гарантии, что собранными важными данными (нельзя заменить радужную оболочку глаза) не завладеет «неприятель» и другие лица, которые могут использовать их не по назначению?

Обобщая приведенные примеры на основе афганского опыта с учетом всего многообразия военных, гуманитарных и прочих акторов, как того требует рассмотрение проблемы сквозь призму инфраструктуры, мы можем выделить важные проблемные задачи. Например, ни хранение силами коалиции биометрических данных, позволяющих установить личность их субъекта, ни обезличивание данных в базах данных УВКБ ООН не дают простых ответов на сложный вопрос о том, что из себя представляет «безопасная» биометрическая регистрация. Обезличенные данные были связаны с рядом рисков, воздействовавших на УВКБ ООН (от сбоев чтения данных до непредоставления гуманитарной помощи). Возникают новые вопросы, например: как (предусмотренные и непредусмотренные) потоки биометрических данных влияют на цели в области безопасности, лежащие в основе использования подобной информации? Вопросы функциональной совместимости находятся не в технической плоскости и относятся не только к платформам, поддерживающим потоки данных, но и к процессам распро-

122 K. Huszti-Orbán and F. Ní Aoláin (примечание 91 выше), pp. 6–7.
123 K. Huszti-Orbán and F. Ní Aoláin (примечание 91 выше).
124 Thomas Macaulay, “Fears Grow Over Taliban Using Biometric Systems to Identify US Collaborators”, *TNW News*, 18 August 2021, доступно по адресу: https://thenextweb.com/news/fears-taliban-has-seized-us-biometric-systems-will-target-vulnerable-people-afghanistan.

странения и создания мнимостей на основе потоков данных, включая иерархические представления о ценности или отсутствия ценности жизни в разрезе различных проблем безопасности. Какие разносторонние, порой диаметрально противоположные задачи безопасности «стирают» потоки биометрических данных и какие иерархии поддерживают, создают и изменяют эти потоки? Как распространяются истории успеха и какие последствия влечет за собой внедрение биометрических технологий в новых условиях или расширение существующих систем?

Сомали

Применение биометрических данных в Сомали также сопровождается рисками непредусмотренной передачи биометрии, полученной гуманитарными организациями, акторам, которые могут их использовать не в целях обеспечения безопасности, а способами, угрожающими безопасности лиц, чьи связи с западными акторами могут оцениваться негативно. Как отметил один из участников интервью, сотрудничавший с учреждением ООН в Сомали: «Если бы у "Аш-Шабааб" была возможность установить личность, к примеру, получателей помощи западных организаций (которых они считают своим противником), эти сведения могли бы быть использованы не по назначению». Учитывая данный риск, это учреждение ООН приняло решение заменить биометрические устройства: «Мы использовали массивные аппараты для регистрации. Но они выглядели подозрительно, поэтому мы нашли регистрационные устройства другого типа, которые не так бросались в глаза и вызвали бы меньше подозрений, если бы кого-то из сотрудников, использующих устройство, остановили члены "Аш-Шабааб"».

Помимо соглашений об обмене данными и партнерстве, потоки данных между гуманитарными организациями и государственными службами безопасности могут возникнуть в результате совершенно иных недобровольных связей. Проверить эти сведения невозможно, но и интервьюируемые, и новостные источники утверждают, что сотрудники служб безопасности могут участвовать в кибератаках на базы данных ООН в целях получения данных. По мнению Макдональда, проблема не только в ограниченных возможностях гуманитарных организаций в области защиты хранящихся у них биометрических данных. Но и в том, что они являются «целью для ряда подкованных в цифровых технологиях групп», включая «международные разведывательные службы»[125]. Как отметил один из интервьюируемых, занимающий высокий пост в важной гуманитарной организации: «Я не удивлюсь, если те, кто занимается контртеррористической деятельностью, и те, кто взламывает наши [гуманитарные] базы данных, — это одни и те же люди. Атаки на наши базы данных — постоянная проблема, и обеспечение хотя бы минимального уровня кибербезопасности

125 Sean McDonald, "From Space to Supply Chains: A Plan for Humanitarian Data Governance," *SSRN*, 12 August 2019, доступно по адресу: https://ssrn.com/abstract=3436179.

дается нам нелегко»[126]. Обратив внимание на эту проблему, журналист узнал о том, что в 2019 году сети ООН в Женеве подверглись «массивной хакерской атаке»[127]. По словам специалиста в области кибербезопасности, атака «по всем признакам, была совершена очень опытным злоумышленником»; он также добавил, что «часто самые опытные киберпреступники работают на государство»[128]. Этот инцидент иллюстрирует уязвимость биометрических баз данных гуманитарных организаций перед несанкционированным доступом[129], следствием которого становятся непредусмотренные потоки данных. Несмотря на то что такое явление, как несанкционированный доступ к базам данных гуманитарных организаций, знакомо техническим компаниям и гуманитарным организациям[130], о степени их уязвимости известно немногое. Гуманитарные организации, «как и любая другая организация, в репутации которой заложена функция защиты, не заинтересованы в том, чтобы признавать факт хакерской атаки»[131]. Различные утечки данных — «Аш-Шабааб», Министерству внутренней безопасности или хакерам — не афишируются по ряду причин, таких как конфиденциальность программ, обусловленный обнародованием сведений о хакерской атаке подрыв репутации и возможные сложности в связи с противоречием подобных инцидентов широко распространенному представлению о биометрии как ценном инструменте борьбы с терроризмом, оказания помощи беженцам и многих других вмешательств.

Следует отметить, что несколько источников обратили внимание на то, что обозначенные проблемы и важные непредусмотренные последствия характерны не только для Афганистана и Сомали, а указывают на гораздо более масштабные задачи. В этой связи Специальный докладчик ООН обращает внимание на то, что «передача данных государствам, в которых действуют менее строгие нормы верховенства права и права прав человека, связано с риском содействия нарушению прав человека, что противоречит обязательствам государств по международному праву прав человека и [внутреннему] законодательству»[132]. Другие критики биометрии, например, отмечали, что «сбор цифровых данных, позволяющих установить личность, и биометрических данных подвергает уязвимые группы населения в условиях конфликта или притеснения особым

126 Анонимное интервью, август 2020 г.

127 Ben Parker, "Exclusive: The Cyber-Attack the UN Tried to Keep Under Wraps", *The New Humanitarian*, 29 January 2020, доступно по адресу: https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack.

128 Ibid.

129 Katja Lindskov Jacobsen and Larissa Fast, "Rethinking Access: How Humanitarian Technology Governance Blurs Control and Care," *Disasters*, Vol. 43, No. 2, 2019.

130 Ben Parker, "Security Lapses at Aid Agency Leave Beneficiary Data at Risk", *The New Humanitarian*, 27 November 2017, доступно по адресу: https://www.thenewhumanitarian.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk.

131 Anja Kaspersen and Charlotte Lindsey-Curtet, "The Digital Transformation of the Humanitarian Sector," *Humanitarian Law & Policy*, 5 December 2016, доступно по адресу: https://blogs.icrc.org/law-and-policy/2016/12/05/digital-transformation-humanitarian-sector/.

132 K. Huszti-Orbán and F. Ní Aoláin (примечание 91 выше), p. 11, footnote 67.

рискам: в результате передачи неприятелю или утечки их данные могут быть использованы против них»[133]. Таким образом, несмотря на то что Афганистан и Сомали играют важную роль в изучении непредусмотренных последствий производства биометрических данных и их потоков, возникающие в связи с применением биометрических технологий опасения указывают на гораздо более широкие проблемные области.

Афганистан, Сомали и другие страны

Несмотря на то что ситуация в Афганистане и Сомали по целому ряду причин уникальна, изучение производства биометрических данных и их потоков с учетом полученного в условиях этих двух стран опыта может привести к выводам, имеющим значение и для других стран[134]. Примером может служить парадоксальная ситуация: несмотря на различные проблемы экспериментального применения биометрических технологий, производства данных и умышленных/непредусмотренных потоков данных, — в частности, несмотря на риски, воздействующие на безопасность и конфиденциальность гражданских лиц, — вера в центральную роль биометрии в борьбе с терроризмом и в технических вмешательствах другого характера, по всей видимости, почти не пострадала. Многие акторы в рамках различных вмешательств продолжают осуществлять порой очень масштабный сбор биометрических данных, их хранение и передачу. К каким последствиям для акторов, участвующих в создании инфраструктур биометрических вмешательств, приведет в перспективе эта стойкая вера в биометрию — стойкая, несмотря на растущее число примеров (из Афганистана, Сомали и других стран) рисков и угроз безопасности, проистекающих из применения биометрических данных? С другой стороны, мы наблюдаем появление новых

133 B. Parker (примечание 78 выше).

134 Примером другой ситуации, в которой внедрение биометрии сопровождалось появлением новых угроз безопасности, служит получение биометрических данных, подвергшее опасности беженцев этнической группы рохинджа. Не только в Афганистане и Сомали потоки биометрических данных, полученные гуманитарными акторами, приводили к неблагоприятным последствиям. Как говорится в докладе организации Human Rights Watch, УВКБ ООН подвергло беженцев-рохинджа «риску принудительного возвращения», передав биометрические данные государственным органам Мьянмы — государства, из которого бежали рохинджа: Human Rights Watch, "UN Refugee Agency Data Sharing Puts Rohingya at Risk of Forced Return", 2021, доступно по адресу: https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent. Несмотря на отличия этой ситуации, она, тем не менее, иллюстрирует, как заключение соглашений об обмене данными с УВКБ ООН (в данном случае с Бангладеш, которое впоследствии заключило соглашение об обмене данными с Мьянмой) ставит под угрозу тех, кого УВКБ ООН должно защищать. О том, как «биометрические данные, полученные УВКБ ООН от беженцев-рохинджа, были переданы Мьянме — стране, из которой они бежали», см. также: Zara Rahman, "The UN's Refugee Data Shame", *The New Humanitarian*, 21 June 2021, доступно по адресу: https://www.thenewhumanitarian.org/opinion/2021/6/21/rohingya-data-protection-and-UN-betrayal; Kate Hodal, "UN put Rohingya 'at Risk' by Sharing Data Without Consent, Says Rights Group", *The Guardian*, 15 June 2021, доступно по адресу: https://www.theguardian.com/global-development/2021/jun/15/un-put-rohingya-at-risk-by-sharing-data-without-consent-says-rights-group.

правил в отношении биометрии, явно предусматривающих отказ от сбора биометрических данных. Так, в политике Oxfam в отношении биометрических технологий указано, что при принятии решений о приемлемости обработки биометрических данных в обязательном порядке следует удостовериться в том, что «вероятные потоки данных поддаются анализу и известны», то есть необходимо понимать, «кто будет получать доступ к данным на протяжении всего их жизненного цикла»[135]. В аналогичной политике МККК (2019 года) содержится требование «ограничить применение биометрических данных конкретными целями»[136], что, к примеру, отличается от политики УВКБ ООН, для которого биометрическая регистрация является «стандартной процедурой»[137] и стратегически важным решением[138]. На схожую тенденцию указывает недавняя активизация полемики об удалении данных и праве на забвение[139], как и «участившиеся призывы ряда организаций обратить более пристальное внимание на риски новых цифровых технологий»[140]. В то же время биометрические данные до сих пор не только собирают и хранят многие акторы, но и их удаление не всегда возможно: «Когда речь идет об официальных базах данных, в частности об APPS [финансировавшаяся США "Афганская система управления кадрами и оплатой труда"], удалить пользователя невозможно»[141]. Еще один интервьюируемый отметил: «Регистрационные системы УВКБ ООН в силу своей архитектуры не позволяют удалять досье. Досье может быть "деактивировано", но не удалено»[142].

Инфраструктуры биометрических вмешательств: неоднозначность, а не точность

Забегая вперед, еще одной проблемой, связанной с расширением инфраструктур биометрического вмешательства, является вопрос о том, каким образом эта инфраструктура, до сих пор не вполне явная, влияет на ряд важных различий и границ, таких как военное/мирное время, друг/неприя-

135 Oxfam, "Oxfam Biometric & Foundational Identity Policy", 2021, доступно по адресу: https://oxfam.app.box.com/v/OxfamBiometricPolicy.

136 ICRC (примечание 104 выше).

137 См., например: UNHCR, "Planning and Preparing Registration and Identity Management Systems: 3.6. Registration Tools", доступно по адресу: https://www.unhcr.org/registration-guidance/chapter3/registration-tools/.

138 Katja Lindskov Jacobsen, "On Humanitarian Refugee Biometrics and New Forms of Intervention", *Journal of Intervention and Statebuilding*, Vol. 11, No. 4, 2017.

139 I. Loy (примечание 65 выше). Говорилось также о том, что биометрические данные должны «удаляться после того, как были использованы по назначению»; см.: Kerrie Holloway, Reem Al Masri and Afnan Abu Yahia, "Digital Identity, Biometrics and Inclusion in Humanitarian Responses to Refugee Crises", Humanitarian Policy Group (HPG) Working Paper, ODI, London, October 2021, pp. 34–5, доступно по адресу: https://cdn.odi.org/media/documents/Digital_IP_Biometrics_case_study_web.pdf.

140 E. Schoemaker (примечание 117 выше).

141 На это также обращал внимание участник анонимного интервью: анонимное интервью, сентябрь 2021 г.

142 Анонимное интервью, ноябрь 2021 г.

тель и правящая власть/интервенция[143]. В определенных ситуациях потоки биометрических данных способствуют повышению точности, но важно отметить и то, что распространение биометрических данных (на основании официальных соглашений или недобровольными средствами) в иной ситуации усугубляет неоднозначность. Неоднозначность проявляется на двух уровнях. Во-первых, что касается процедур, которые используются различными органами власти для отнесения частных лиц к законным беженцам, законным целям контртеррористической деятельности и/или объектам эксперимента, проведенный анализ указывает на важность вопросов о том, как и кто осуществляет сбор биометрических данных, их распространение и обработку для определения подобных категорий людей. Акцент на потоках данных подталкивает к анализу того, как предположительная точность биометрии не всегда трансформируется в однозначность потоков данных, а биометрические данные порой получают сомнительными методами. Иными словами, соглашения об обмене биометрическими данными и случаи взлома баз биометрических данных представляют собой различные инфраструктурные взаимосвязи военной и невоенной биометрии, в изучении последствий которых необходимо отталкиваться не от мнимой точности данного метода, а от его способности порождать растущую неопределенность; эта неопределенность воздействует на прошедших биометрическую регистрацию лиц, не осведомленных о методах обработки их биометрических данных и о том, кто и с какой целью производит их обработку. Предпринятую в статье попытку выделить неоднозначности и угрозы безопасности на уровне биометрической инфраструктуры следует рассматривать в контексте существующей литературы о ложной точности современной контртеррористической деятельности[144].

Во-вторых, изучение процессов производства данных и потоков данных привлекает внимание к вопросу о том, как расширение инфраструктуры биометрических вмешательств может усиливать неоднозначность в еще одной важной сфере — в проведении различий между войной и миром, когда речь заходит о сборе биометрических данных и их использовании. Что происходит с проведением различий между вооруженным конфликтом и мирным временем, когда биометрические данные, полученные в ходе вооруженного конфликта, передаются государству или хранятся им, в том числе государственными разведывательными службами, и, возможно, будут использованы для операций в мирное время? Если биометрические данные, собранные вооруженными силами США во время военного вмешательства в Афганистан, будут храниться бессрочно, то есть в том числе после официального окончания военных действий, как подобные

143 Возможно, еще одно распространенное разграничение, которое также может поставить под сомнение биометрическая система, это разграничение частного лица и связей, учитывая то, что новые биометрические системы допускают идентификацию не только отдельных лиц, но и родственных связей.

144 Lucy Suchman, "Algorithmic Warfare and the Reinvention of Accuracy", *Critical Studies on Security*, Vol. 8, No. 2, 2020.

потоки данных и хранение данных повлияют на безопасность их субъектов? Практика хранения биометрии после «окончания войны» расширяет сферу контртеррористической деятельности, включая в нее «мирное время», как свидетельствует следующее высказывание специалиста по биометрическим технологиям: «Мы должны применять комплексный подход к нашим базам данных, поскольку это мощное оружие, которое может быть использовано и в мирное время, и на поле боя»[145]. Представления о биометрии как о ценном инструменте борьбы с терроризмом способствуют закреплению практики хранения данных, что в свою очередь становится очередным источником неоднозначности, подчеркивающей границы «трансформации» точности биометрических технологий в более точную и якобы более легитимную форму контртеррористической деятельности. Вышеприведенный анализ дополняет некоторыми нюансами текущую полемику о противоречиях и заблуждениях в современной контртеррористической деятельности, а также показывает, что рассмотрение биометрических инфраструктур со всем вниманием к военным и невоенным акторам становится отправной точкой для вскрытия более общих сложностей и противоречий.

Заключительные замечания

Как показывает вышеприведенный анализ, наряду с рисками новых случаев непредусмотренного распространения биометрических данных (которые могут быть получены акторами, диаметрально противоположно подходящими к проведению различий между друзьями и неприятелями в сравнении с учреждениями, которым получатели помощи и другие субъекты данных изначально доверили свои важные данные), важно углублять понимание процессов, которые приводят к угрозе для безопасности вследствие применения биометрических технологий. В дальнейшем, разумеется, будет крайне важно изучить имеющиеся потоки данных, но не менее пристального внимания заслуживают процессы возникновения и потоки различных нематериальных элементов инфраструктуры, таких как истории успеха или страх, с учетом того, что и те, и другие оказывают различное влияние на безопасность получателей помощи и других субъектов, прошедших регистрацию биометрии. Например, обязательная биометрическая регистрация в отсутствие изменений в политике хранения и передачи данных связана с риском отказа потенциальных получателей помощи от прохождения регистрации в ВПП, УВКБ ООН и других гуманитарных организациях по причине страха, возникающего у этих людей в связи с возможными последствиями распространения их биометрических данных. Могут ли данные попасть в руки лиц, чьи методы использования данных создадут дополнительные угрозы для безопасности субъектов данных, и без того находящихся в уязвимом положении? Как показано в настоящей статье, это вполне реальные

145 S. Gold (примечание 33 выше).

риски — с учетом недавних примеров и масштабов, в которых ряд участников мер вмешательств — военных и прочих — производят биометрические базы данных, не защищенные от рисков и непредусмотренного распространения содержащихся в них сведений. Кроме того, истории о непредусмотренном доступе к данным порождают страх. А информация о доказанных в реальных условиях надежности и масштабируемости биометрических технологий приводит к появлению историй успеха. Несмотря на нематериальность как историй успеха, так и страха, и то, и другое, хотя и действуя разнонаправленно, формирует будущие контуры сбора биометрических данных. Истории успеха поддерживают более общую мнимость «больше биометрии — больше безопасности» и представления о центральной роли биометрии в текущей и будущей контртеррористической деятельности в качестве «мощного оружия в мирное время и на поле боя»[146]. С другой стороны, страх и тревога угрожают безопасности и косвенно — например, безопасности беженцев, которые отказываются от регистрации и получения помощи ВПП, имея на нее право, либо безопасности прошедших биометрическую регистрацию афганцев, чей рисунок радужной оболочки глаза хранится в базе данных, о получении доступа к которой заявляет «Талибан»[147]. На других примерах мы убедились в том, что биометрическая регистрация «может быть связана с опасениями по поводу безопасности, которые для некоторых беженцев становятся препятствием для прохождения регистрации в УВКБ ООН. В такой ситуации оказались сирийские беженцы в Ливане»[148]. Использование биометрии может повлиять на передвижение беженцев, что в свою очередь может привести к непредусмотренным отрицательным последствиям для их безопасности. Например, применение биометрии может усилить «страх быть задержанными при пересечении внутренних контрольно-пропускных пунктов»[149] у беженцев, которые «в силу опасений за свою безопасность пересекали ливанскую границу не через официальный пропускной пункт»[150].

Важно отметить углубляющийся разрыв между воображаемой безопасностью биометрических технологий и (замалчиваемым) появлением угроз для безопасности. В связи с замалчиваемыми угрозами для безопасности также следует отметить, что наряду с рассмотренными в настоящей статье определенными типами последствий существует множество других, чаще всего нерассказанных историй о непредусмотренных последствиях

146 S. Gold (примечание 33 выше).

147 Даже до распространения биометрических технологий многие беженцы отказывались проходить регистрацию, предлагаемую гуманитарными организациями. Биометрия — лишь один из многих факторов, влияющих на решение беженца проходить или не проходить регистрацию; существует целый ряд причин, в силу которых беженцы отказываются регистрироваться.

148 Katja Lindskov Jacobsen, "UNHCR, Accountability and Refugee Biometrics", in Kristin Bergtora Sandvik and Katja Lindskov Jacobsen (eds), *UNHCR and the Struggle for Accountability*, Routledge, London and New York, 2016.

149 K. L. Jacobsen (примечание 148 выше).

150 NRC, "The Consequences of Limited Legal Status for Syrian Refugees in Lebanon", NRC Lebanon Field Assessment, NRC Lebanon, March 2014, p. 6.

применения биометрических технологий, с которыми сталкиваются различные маргинализированные группы населения. Так, УВКБ ООН и ВПП в совместной оценке оказания помощи кенийским беженцам отмечают, что «школьники и возглавляемые детьми семьи» были вынуждены «пропускать школьные занятия, чтобы соблюсти требования системы распределения продовольственной помощи на основе биометрической регистрации»[151]. Примеры того, как применение биометрии в рамках гуманитарной деятельности может непреднамеренно привести к отрицательным последствиям для беженцев, также отмечались в ряде других ситуаций. Например, использование биометрической идентификации может усилить «страх быть задержанными при пересечении внутренних контрольно-пропускных пунктов»[152] у сирийских беженцев из городов, которые «в силу *опасений за свою безопасность* пересекали ливанскую границу не через официальный пропускной пункт»[153]. В действительности опасения относительно возможного неумышленного отрицательного воздействия, которое сбор биометрических данных и их раскрытие оказывают на передвижение и безопасность беженцев, озвучиваются уже несколько лет. В неопубликованном исследовании отмечается несколько рисков, включая риск того, что «попав не в те руки, данные могут стать причиной судебного преследования, дискриминации и даже неминуемой угрозы для свободы и жизни субъекта данных», а также что данные, «полученные государственными органами принимающей страны», могут использоваться «в рамках мероприятий по заключению под стражу и преследованию определенных групп населения»[154]. Многие другие примеры и мнения тоже заслуживают внимания, если мы хотим понять мириады путей, приводящих к непредусмотренным последствиям производства и распространения биометрических данных, включая риски дублирования некорректных данных в разных системах, что может стать причиной отказа от подачи заявки на переселение или регистрации рождения ребенка[155]. Обобщение имеющейся информации, дополненной примерами последствий производства и распространения биометрических данных для лиц, чьи данные обрабатываются и распространяются, будет способствовать учету мнений субъектов данных, что, возможно, еще более явно обозначит причины, по которым нам стоит уделять внимание

151 WFP/UNHCR, "Joint Assessment Mission — Kenya Refugee Operation: Dadaab (23–27 June 2014) and Kakuma (30 June–1 July 2014) Refugee Camps", 2014, p. 18, доступно по адресу: https://www.unhcr.org/54d3762d3.pdf. Внимания заслуживают и другие примеры, в том числе более свежие. См., например: Belkis Willie, "A Cautionary Tale: When Humanitarian Data Collection/Transfer Harms Beneficiaries", NetHope 20th Anniversary Summit, 15–19 November 2021, доступно по адресу: nethopeglobalsummit.org.

152 K. L. Jacobsen (примечание 148 выше).

153 NRC (примечание 150 выше).

154 Simon Davies, "How a United Nations Agency Buried a Security Report that Warned of Potential Genocide", *The Privacy Surgeon*, 2012, доступно по адресу: http://www.privacysurgeon.org/blog/incision/ howa-united-nations-agency-buried-a-security-report-that-warned-of-potentialgenocide/.

155 Я очень признательна двум анонимным рецензентам, отдельно отметившим значение внимательного разбора последствий обработки и передачи биометрических данных для их субъектов, а также более тщательного изучения проблемы с точки зрения пострадавших, особенно в свете того, что их мнение нередко игнорируется.

непредусмотренным последствиям расширения инфраструктур биометрических вмешательств.

Проведенный нами анализ, в основу которого легла концепция «живой лаборатории», предложенная Тилли, также показал, что важным аспектом мнимости биометрии как центрального инструмента контртеррористической деятельности является неустанное тестирование новых биометрических систем в реальных условиях, включая новые методы сбора биометрических данных и взаимодействия биометрических технологий. Подобно тому, как в ситуации с ВПП ограничения в биометрии среди детей младенческого возраста стали поводом призвать к интенсификации исследований, другие ограничения данного метода также оформляются в приглашение добавить больше: новых исследований, новых регистрационных устройств, новых биометрических данных. В этом смысле в анализе упоминается еще один фактор расширения: внутренняя логика непрерывности, согласно которой недостатки «компенсируются» умножением одних и тех же сущностей. Неспособность найти доказательства надежности применения биометрии среди детей младше пяти лет представляется как возможность активизации экспериментальной младенческой биометрии в реальных условиях. Неспособность обеспечить «совместимость» биометрических баз данных в Ираке и других странах не стала поводом для сомнений в повсеместном применении биометрии и точности идентификации противника на глобальном уровне, а напротив, способствовала реализации новых проектов тестирования функциональной совместимости. Упоминая об «ограниченной совместимости и возможностях обмена данными между гуманитарными организациями», работающими в Сомали, авторы недавнего доклада говорят о попытках изучить «методы создания совместимых баз данных»[156]. Еще раз отметим, что это не нечто уникальное, характерное только для биометрии в контексте контртеррористической деятельности, а тенденция, которая прослеживается и в других контртеррористических мерах. Анализируя контртеррористическую деятельность Франции в Сахеле, Гишауа отмечает: «Это можно назвать максималистской логикой: неудача становится поводом не для того, чтобы отказаться от инициативы, а чтобы разработать новую»[157].

Обращаясь к этой логике, мы замечаем другую взаимосвязь: применение биометрии в гуманитарной и контртеррористической деятельности опирается на «самоподдерживающуюся динамику» — ограничения и недостатки приводят не к сомнениям в технических средствах или мнимых результатах, а к призывам провести дополнительные эксперименты в реальных условиях. Так, когда на восьми контрольно-пропускных пунктах сканеры отпечатков пальцев, рассчитанные на считывание одного отпечатка, были заменены МОМ сканерами, позволяющими считывать отпечатки десяти

156 B. Owino (примечание 14 выше).
157 Yvan Guichaoua, "The Bitter Harvest of French Interventionism in the Sahel", *International Affairs*, Vol. 96, No. 4, 2020.

пальцев[158], это было представлено как техническое «усовершенствование» существующих систем, без упоминания о том, что внедрение новых систем позволяет сверять «данные с национальными и международными списками лиц, подозреваемых в совершении преступлений». Продуктивность «неудач» наводит на мысль, что биометрические эксперименты не бывают неудачными, в том смысле что никогда не указывают на отсутствие доказательств универсальности биометрии как контртеррористического инструмента. Это неудача другого рода: продуктивное стремление провести новые эксперименты, получить новые биометрические данные и повысить совместимость систем[159]. В какой степени эта логика провоцирует расширение инфраструктуры, подвергнутое критическому анализу в данной статье? Рассматривая вопросы производства данных, потоков данных и инфраструктурных взаимосвязей биометрических технологий, используемых как военными в борьбе с терроризмом, так и невоенными акторами, мы обратили внимание на неоднозначность и слабое разграничение понятий, которые ставят под сомнение воображаемую точность биометрии и популярное мнение о том, что биометрические данные, полученные самыми разными акторами, играют центральную роль в планировании контртеррористических операций.

И наконец, можем ли мы полноценно изучать постоянное расширение биометрических баз данных, не задаваясь вопросом о роли доноров и их влиянии на практику сбора и распространения биометрических данных гуманитарными акторами? Как отмечает Специальный докладчик ООН в уже упоминавшемся отчете, «доноры систематически настаивают на интеграции биометрии, используемой при оказании помощи»[160]. В какой степени производство биометрических данных как условие получения выделенного донорами финансирования может стать проблемой для гуманитарных акторов? В будущем необходимо будет учесть это при рассмотрении вопросов об условиях производства биометрических данных, для того чтобы понять, каким образом гуманитарные акторы принимают сложные решения, учитывая, что «“нет” биометрии» может означать «“нет” финансированию», а значит, «нет» и помощи людям, чья подверженность рискам, связанным с биометрическими данными, тесно связана с их уязвимым положением, которое в отсутствие помощи только усугубляется. В то же время эти рассуждения не должны умалять значения, которое имеет пересмотр практики гуманитарных и других акторов в сфере производства данных и обмена ими.

158 Chris Burt, “IOM Installing 10-Digit Fingerprint Readers at Somalian Ports of Entry”, *BiometricUpdate.com*, 7 June 2018, доступно по адресу: https://www.biometricupdate.com/201806/iom-installing-10-digit-fingerprint-readers-at-somalian-ports-of-entry.

159 Благодарю Марейн Хойтинк за организацию семинара для обсуждения этой темы. Благодарю Дебби Лисл за то, что обратила на это внимание в процессе плодотворной дискуссии в ходе семинара.

160 K. Huszti-Orbán and F. Ní Aoláin (примечание 91 выше), p. 7; The Engine Room and Oxfam, “Biometrics in the Humanitarian Sector”, March 2018, доступно по адресу: https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf; Kristin Bergtora Sandvik, Katja Lindskov Jacobsen and Sean Martin McDonald, “Do No Harm: A Taxonomy of the Challenges of Humanitarian Experimentation”, *International Review of the Red Cross*, Vol. 99, No. 904, 2017.