Принцип «не навреди» в цифровую эпоху: как цифровизация денежных расчетов влияет на гуманитарную деятельность

Джо Бёртон*

Джо Бёртон — специалист по денежным переводам и рынкам, имеет более 12 лет практического опыта работы в странах, пострадавших от конфликтов. Начала работать в программе предоставления денежной помощи и ваучеров (CVA) в 2004 году, специализируется на оказании такой поддержки в конфликтных и постконфликтных условиях. Сейчас занимает должность руководителя направления по предоставлению денежной помощи и ваучеров в МККК, следит за тем, чтобы эта поддержка была междисциплинарной и составляла неотъемлемую часть реагирования МККК на потребности людей, пострадавших от вооруженных конфликтов и иных ситуаций насилия. Адрес электронной почты: joburton@icrc.org.

Аннотация

С появлением денежных переводов изменился формат помощи, которую оказывают гуманитарные организации; в то же время цифрови-

* В этой статье выражаются исключительно взгляды автора, которые не обязательно совпадают с позицией Международного Комитета Красного Креста.

зация вызывает глубинные преобразования в жизни всего нашего мира. Цифровизация денежных расчетов привела к тому, что простым нажатием кнопки можно в течение нескольких минут передать деньги сотням тысяч, если не миллионам людей. Электронные платежи стали революционным решением, которое позволило ускорить оказание жизненно важной помощи и повысить ее эффективность. С развитием электронных платежей наличные никуда не денутся, но важно обеспечить баланс между пользой такой цифровизации и сопутствующим ей риском. Мы как гуманитарные организации должны сформулировать, что означает принцип «не навреди» в цифровую эпоху, и применить его к использованию нами электронных платежей для оказания поддержки людям, пострадавшим от вооруженных конфликтов и других ситуаций насилия.

Ключевые слова: предоставление помощи в виде денежных средств и ваучеров (CVA), денежные переводы, цифровизация, электронные платежи, принцип «не навреди» в цифровую эпоху, цифровой риск, защита данных, ответственность за данные.

Деньги правят миром — так считают многие. Но почему денежные средства — такая знакомая часть нашей повседневной жизни — стали столь актуальной темой в гуманитарной сфере?

Это связано с тем, что использование денежных средств, как часто называют предоставление денежной помощи и ваучеров (CVA)[1], стало одним из основных изменений в гуманитарной деятельности за последнее десятилетие. За период с 2016 по 2019 год объем их использования вырос вдвое — в 2019 году международная гуманитарная помощь в размере 5,6 млрд долларов США, или 17,9% всего бюджета на подобного рода поддержку, была предоставлена в виде денежных средств или ваучеров[2], что приводит к изменению формата оказания гуманитарной помощи.

Этот акцент на предоставление отдельным лицам, домохозяйствам или сообществам помощи в виде денежных средств[3] и/или ваучеров, чтобы они могли получить доступ к необходимым товарам и услугам[4] вместо раз-

1 Понятие помощи в виде денежных средств и/или ваучеров (Cash and Voucher Assistance, CVA) является на данный момент самым ходовым в гуманитарном секторе; ранее вместо него использовались синонимы «программа денежных переводов» (Cash Transfer Programming), «помощь в виде денежных средств» (Cash-Based Assistance) и «вливание денежных средств» (Cash-Based Interventions). См.: Cash Learning Partnership (CaLP), "Glossary of Terms", доступно по адресу: www.calpnetwork.org/library-andresources/glossary-of-terms/ (все ссылки на интернет-ресурсы приводятся по состоянию на декабрь 2020 года).

2 CaLP, *The State of the World's Cash 2020: Cash and Voucher Assistance in Humanitarian Aid*, July 2020, p. 9, доступно по адресу: www.calpnetwork.org/publication/the-state-of-the-worlds-cash-2020-full-report/.

3 Понятие «денежные средства» в этом определении помощи в виде денежных средств и/или ваучеров относится как к наличным, так и к электронным платежам.

4 Определение, сформулированное Международным Комитетом Красного Креста (МККК) в соответствии с определениями CaLP и других организаций, оказывающих подобную помощь, ориентировано на прямую передачу средств нуждающимся людям, семья и сообществам. МККК не учитывает более крупные денежные переводы в адрес партнеров, таких как нацио-

дачи товаров, изменил наше понимание и формат оказания гуманитарной помощи, сместив приоритет в сторону предоставления пострадавшим возможности самостоятельно делать выбор и перераспределив силы в гуманитарном секторе. В то же время с увеличением объемов помощи в виде денежных средств или ваучеров наблюдается активизация процессов перехода на цифровые технологии во всем гуманитарном секторе, которую еще больше подтолкнула пандемия COVID-19. Цифровизация вызывает глубинные преобразования в жизни всего нашего мира: меняются форматы общения, объединения в группы, путешествий, принятия решений и высказывания своей точки зрения. Коротко говоря, цифровизация меняет способ взаимодействия людей со своей социальной, политической и выстроенной средой не только в цифровом, но и в физическом пространстве.

Применительно к оказанию помощи в виде денежных средств и/или ваучеров цифровизация изменила способ предоставления жизненно важной поддержки, позволив значительно увеличить скорость оказания помощи и охват людей, нуждающихся в ней.

Цель этой статьи — выяснить, как оказание помощи в виде денежных средств и/или ваучеров совместилось с процессом цифровизации, и исследовать принцип «не навреди» в отношении использования электронных платежей для предоставления поддержки людям, пострадавшим от вооруженных конфликтов и иных ситуаций насилия. Мы начнем с общего обзора некоторых тенденций в развитии цифровых технологий, влияющих на работу гуманитарного сектора, дадим определение электронных платежей и изучим феномен роста их использования гуманитарными организациями. Затем мы рассмотрим, как должен развиваться принцип «не навреди» в мире, который все больше опирается на цифровые технологии, — с учетом опасностей и возможных ловушек, связанных с электронными платежами, особенно в отношении защиты данных; здесь мы подробнее остановимся на роли Международного Комитета Красного Креста (МККК) как организации, в течение последнего десятилетия занимавшей в этой сфере ведущую позицию. Кроме того, мы проанализируем, как можно смягчить действие перечисленных видов риска, сопряженных с оказанием помощи в виде денежных средств и/или ваучеров в электронном формате. Статья завершается обращенным к гуманитарным организациям призывом более вдумчиво подходить к принятию решений по поводу электронных платежей и взаимодействия в цифровом мире, чтобы интересы пострадавших всегда стояли для нас на первом месте.

нальные общества Красного Креста и Красного Полумесяца и крупные предприятия, или доплаты сотрудникам соответствующих государственных органов, с которыми работает организация. Кроме того, из помощи в виде денежных средств и/или ваучеров исключаются пересылка заработка эмигрантов и микрофинансирование, хотя микрофинансовые организации могут привлекаться для непосредственной выдачи помощи в виде денежных средств и/или ваучеров. ICRC, *Cash Transfer Programming in Armed Conflict: The ICRC's Experience*, Geneva, November 2018, p. 14, доступно по адресу: www.icrc.org/en/publication/cash-transfer-programming-armed-conflict-icrcs-experience.

Почему гуманитарные организации рассуждают о цифровизации денежных средств?

Для того чтобы выяснить, какую пользу приносит цифровизация денежных средств и какие ловушки она может в себе таить, необходимо рассмотреть три основных понятия: цифровизация, электронные платежи и принцип «не навреди».

Цифровизация и электронные платежи

Понятие цифровизации охватывает широкий спектр различных областей, многие из которых рассматриваются в статьях, опубликованных в этом номере журнала. Неполный перечень основных тенденций, влияющих на гуманитарную деятельность и на весь мир, включает в себя повсеместную связность; большие данные; воздействие революционных технологий на традиционные модели ведения бизнеса; распространение вводящих в заблуждение сведений, дезинформации и риторики ненависти; кибервойны; слежку; искусственный интеллект. Повсеместная связность означает, что доступ к услугам связи у людей стал шире, чем когда бы то ни было; в 2019 году более чем у 53% мирового населения имелся выход в интернет[5], а услугами мобильной связи в той или иной форме пользовались 67% населения Земли[6].

Такая цифровая связность — в том числе расширение использования электронных платежей — требует большого объема данных и сама их порождает. Цифровизация этих данных, в том числе финансовой информации, позволяет наращивать слежку, которую могут сегодня осуществлять государственные органы — на законном основании и без такового — и крупные компании, которые оказывают услуги и с их помощью собирают и обрабатывают информацию или делают из нее выводы. Кроме того, поскольку оборудование для шпионажа становится дешевле и доступнее, возникает вполне реальный риск, выходящий за рамки простого нарушения неприкосновенности частной жизни. Существуют доказательства того, что, несмотря на долг государств соблюдать и защищать права граждан, «практически беспрепятственно ведется слежка за отдельными лицами — в том числе за теми, кто критикует действия властей, журналистами и правозащитниками, — результатом чего становятся задержания, пытки и убийства без суда и следствия»[7]. Помимо данных как таковых, нашему цифровому миру требуется и физическая, и электронная инфра-

5 International Telecommunication Union, *Facts and Figures 2019: Measuring Digital Development*, Geneva, 2019, доступно по адресу: https://itu.foleon.com/itu/measuring-digital-development/home/.

6 GSMA, *The Mobile Economy 2020*, London, 2020, p. 3, доступно по адресу: https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf.

7 Siena Anstis, Ron Deibert, Miles Kenyon and John Scott-Railton, "The Dangerous Effects of Unregulated Commercial Spyware", *Citizen Lab*, 24 June 2019, доступно по адресу: https://citizenlab.ca/2019/06/the-dangerous-effects-of-unregulated-commercial-spyware/.

структура. Количество кибератак, понимаемых как враждебные действия, которые осуществляются через потоки данных в отношении компьютеров, компьютерных систем, связанных устройств или сетей, растет год от года, и пандемия COVID-19 лишь усугубила эту ситуацию[8]. Мишенью кибератак может стать любая инфраструктура, опирающаяся на связанные сети, а их последствия ощутимы в реальном мире; в том числе, как поясняется ниже, это касается финансовых систем.

В результате цифровизации изменились и способы использования денег. Спроси я вас сейчас, сколько наличных у вас в кармане, что бы вы ответили? Доллар? Десять долларов? Нисколько? Люди все чаще стали прибегать к электронным платежам — с помощью карты, мобильного телефона или онлайн-банка, — чтобы приобрести необходимые товары и услуги, будь то оплата продуктов, счета в ресторане, оплата аренды или медицинской страховки. Много раз мне приходилось видеть замешательство на лицах людей в тех случаях (все более редких), когда продавец сообщал: «Мы не принимаем к оплате карты». Однако это не значит, что наличные перестанут существовать. В многочисленных докладах центральных банков и финансовых специалистов, где признается развитие электронных платежей, говорится и о том, что, перефразируя Марка Твена, «слухи о смерти наличных денег сильно преувеличены»[9].

Хотя по мере развития этой технологии терминология, скорее всего, изменится, важно определить, что имеется в виду под цифровизацией денежных средств и электронными платежами, чтобы прийти к единому пониманию темы наших рассуждений и получить возможность проанализировать воздействие этого явления на гуманитарную деятельность. По сути, речь идет об «электронных платежах» или «электронных переводах», посредством которых деньги передаются электронным способом — например, с помощью банковского перевода или мобильного платежа. Сеть изучения и осуществления электронных денежных переводов (Electronic Cash Transfer Learning Action Network, ELAN), которая стала первопроходцем в области применения электронных платежей в гуманитарной сфере, определяет их как «электронный перевод денег или ваучеров от организации-исполнителя участнику программы. Электронные переводы обеспечивают

8 Maggie Miller, "FBI Sees Spike in Cyber Crime Reports during Coronavirus Pandemic", *The Hill*, 16 April 2020, доступно по адресу: https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic.

9 Проведенное в 2014 году Европейским центральным банком исследование наличных и безналичных (в том числе электронных) платежей в семи европейских странах показало, что наличные деньги по-прежнему активно используются, несмотря на существование множества других механизмов оплаты. Важно отметить, что, по данным исследования, использование наличных расчетов в значительной степени коррелирует с демографическими характеристиками и характеристиками конкретной торговой точки. Поскольку исследование проводилось в промышленно развитых странах, важно сделать поправку на то, как можно экстраполировать эти результаты на те условия, в которых работают гуманитарные организации. См.: John Bagnall, David Bounie, Kim P. Huynh, Anneke Kosse, Tobias Schmidt, Scott Schuh and Helmut Stix, *Consumer Cash Usage: A Cross-Country Comparison with Payment Diary Survey Data*, Working Paper Series No. 1685, European Central Bank, June 2014.

доступ к денежным средствам, товарам и/или услугам с помощью мобильных устройств, электронных ваучеров или карт (например, предоплаченных, принимаемых банкоматами, кредитных или дебетовых карт)»[10].

Электронные платежи не следует путать с цифровыми валютами, такими как биткоин — одна из самых популярных криптовалют. Криптовалюты представляют собой электронную форму валюты, созданной общедоступной сетью, а не государством, и поэтому не являются законным платежным средством[11]. В некоторых странах, например в Канаде, рассматривается возможность внедрения законного платежного средства в электронной форме с упразднением бумажных и металлических денег[12]. Однако, как показывает недавнее исследование гуманитарной помощи в виде денежных средств и/или ваучеров, несмотря на возросший интерес к технологии распределенных реестров и к цифровой валюте, «до их масштабного применения в реальной жизни пока далеко»[13].

Для целей этой статьи я буду пользоваться термином «электронные платежи» применительно к операциям, которые совершаются полностью в электронной форме. Это означает, что и плательщик, и получатель используют электронные средства передачи (такие как банковский или мобильный перевод) и что платежный инструмент (способ исполнения платежного поручения) имеет электронную, а не бумажную форму (т. е. без использования наличных средств, чеков или почтового перевода).

Разумеется, электронная форма платежей не означает, что в них никак не задействована валюта в физическом выражении. Например, после зачисления средств на лицевой счет получателя он может полностью или частично снять деньги в банкомате; в случае мобильных расчетов средства могут быть переведены в электронный кошелек получателя, а затем использованы для совершения электронных платежей (например, в магазине) либо также обналичены (т. е. сняты в виде наличных средств в любой торговой точке).

В целом, давно уже прошли те времена, когда гуманитарным организациям приходилось отправлять внедорожник, набитый купюрами, чтобы осуществить выплаты сообществу для удовлетворения их потребностей, будь то покупка продуктов, одежды и бытовых товаров или оплата транспорта, ночлега или медицинской помощи. На планете еще действительно остались места, куда перевести деньги в электронной форме не получится, но гуманитарные организации все чаще осуществляют выплаты

10 ELAN, “Vocabulary and Usage”, доступно по адресу: www.calpnetwork.org/wp-content/uploads/2020/01/elan-vocab-and-usage-expanded-jan-2017.pdf.

11 Законным платежным средством считается все, что признается законом в качестве способа погашения долга перед государством или частным лицом либо в качестве средства исполнения финансового обязательства, в том числе для уплаты налогов, внесения платежей по договору и погашения законных штрафов или пеней.

12 Better Than Cash Alliance (BTCA), “Payments Measurement Toolkit”, доступно по адресу: www.betterthancash.org/tools-research/toolkits/payments-measurement/focusing-your-measurement/introduction.

13 CaLP (примечание 2 выше), p. 116.

в электронном виде — на пластиковые карты, мобильные телефоны или банковские счета. Ситуацию поменяла именно цифровизация передачи денег, а не денежные средства как таковые. Простым нажатием кнопки можно в течение нескольких минут передать деньги сотням тысяч, если не миллионам людей, что привело к преобразованию процессов, существовавших десятилетиями, и позволило ускорить оказание жизненно важной помощи и повысить ее эффективность.

Эволюция обязательства «не навредить»: пример из практики МККК

Рука об руку с распространением электронных платежей идет необходимость минимизировать возможные побочные действия этого процесса цифровизации. Понимая, что риск будет присутствовать в нашем мире всегда, гуманитарные организации, которые обязаны заботиться о пострадавших, должны, тем не менее, думать и о последствиях своей работы, пользуясь представившимися возможностями, но одновременно с этим прогнозируя и уменьшая их возможное отрицательное воздействие. Именно здесь обязательство «не навредить»[14] играет ключевую роль. Принцип недопущения нанесения вреда требует от гуманитарных организаций стремления не причинять своими действиями еще большего ущерба и страданий.

Эта концепция, введенная в обращение Мэри Б. Андерсон, воплощена в первом принципе обеспечения защиты, приведенном в Гуманитарной хартии и Минимальных стандартах, применяемых при оказании гуманитарной помощи[15]. Со своей стороны МККК подчеркивает принцип «не навреди» в своей Политике в области предоставления защиты[16], где указано, как необходимо действовать, чтобы не оказывать отрицательного влияния на население и отдельных людей и не создавать для них новые опасности. За прошедшие десятилетия многие гуманитарные организации наряду с МККК внедрили принцип «не навреди» в свою работу и политику, в том числе в отношении процессов перехода на цифровые технологии, таких как цифровизация денежных средств. Одним из первых учреждений, разработавших четкую политику в области ответственного обращения с данными, стал Оксфам[17], который также обеспечил инструментарий и обучение своих сотрудников, чтобы внедрить принципы ответственного обраще-

14 Mary B. Anderson, *Do No Harm: How Aid Can Support Peace or War*, Lynne Rienner, Boulder, CO, 1999. В качестве недавнего основополагающего текста см.: Hugo Slim, *Humanitarian Ethics: A Guide to the Morality of Aid in War and Disaster*, Oxford University Press, Oxford, 2015.

15 *Проект «Сфера»*. Руководство проекта «Сфера»: Гуманитарная хартия и минимальные стандарты, применяемые при оказании гуманитарной помощи, 2018, Принцип обеспечения защиты № 1, доступно по адресу: https://spherestandards.org/wp-content/uploads/2018/06/Sphere_Handbook_2011_Russian.pdf.

16 *МККК*. Политика МККК в области предоставления защиты // Международный журнал Красного Креста. Т. 90, № 871, 2008. С. 371. Доступно по адресу: https://international-review.icrc.org/sites/default/files/reviews-pdf/2020-11/554.pdf.

17 Oxfam, "Responsible Program Data Policy", February 2015, доступно по адресу: https://policy-practice.oxfam.org.uk/publications/oxfam-responsible-program-data-policy-575950.

ния с данными во все свои программы[18]. Из недавних примеров можно привести работу Центра гуманитарных данных Управления Организации Объединенных Наций по координации гуманитарных вопросов (УКГВ) в сфере ответственного обращения с данными, в рамках которой через призму принципа «не навреди» создаются инструменты и руководства, помогающие сотрудникам разбираться в технических и этических вопросах работы с гуманитарными данными, в том числе с данными, созданными при осуществлении электронных платежей, но не только с ними[19].

Исследование цифровизации денежных средств с помощью механизма недопущения нанесения вреда — который иначе называют принципом недопущения нанесения *цифрового* вреда — играет ключевую роль, поскольку оно позволяет гуманитарным организациям внедрять цифровые технологии этично.

Недопущение нанесения цифрового вреда — ключевое обязательство, особенно в отношении того, как гуманитарные организации и их партнеры работают с данными, осуществляют деятельность и взаимодействуют с пострадавшими в цифровом пространстве. Это также относится и к применению электронных платежей для оказания поддержки людям, пострадавшим от кризиса. В случае МККК это значит, что организация не только использует денежные средства и ваучеры (как в физическом, так и в электронном виде) в рамках принимаемых мер реагирования, но и четко осознает, каким образом цифровизация денежных средств может повлиять на гуманитарную деятельность, особенно в условиях вооруженного конфликта. МККК знает, что «недостаточно понимать только физическую среду вооруженного конфликта. Важно сопоставлять это понимание с данными, полученными из виртуального или цифрового пространства»[20]. Для того чтобы воспользоваться преимуществами, которые дает цифровизация — в отношении денежных средств и не только, — реализация принципа «не навреди» со стороны МККК строится таким образом, чтобы на первом месте в нашем анализе стояли интересы людей, которым мы помогаем.

Предоставление помощи в виде денежных средств и/или ваучеров как мера реагирования в интересах людей

Преимущества оказания помощи в виде денежных средств и/или ваучеров хорошо известны: она дает пострадавшим чувство собственного достоинства, полномочия, самостоятельность и возможность выбора стратегии

18 Oxfam, “Responsible Data Management”, 2017, доступно по адресу: https://policy-practice.oxfam.org.uk/our-approach/toolkits-and-guidelines/responsible-data-management.

19 OCHA, Centre for Humanitarian Data, “Data Responsibility”, доступно по адресу: https://centre.humdata.org/data-responsibility/.

20 ICRC, *Symposium Report: Digital Risks in Situations of Armed Conflict, London, 11–12 December 2018*, Geneva, 2019, p. 1, доступно по адресу: https://www.icrc.org/en/publication/4403-symposium-report-digital-risks-armed-conflicts.

выживания и восстановления[21]. Когда мы говорим о том, что интересы пострадавших должны стоять у нас на первом месте, такая помощь становится чрезвычайно важным инструментом, поскольку предоставляет людям, пострадавшим от кризиса, финансовые средства, позволяющие им оправиться от пережитого так и тогда, как они пожелают. Тем самым мы даем пострадавшим возможность самостоятельно принимать решения, и эти решения могут значительно отличаться от тех, что приняла бы за них гуманитарная организация. Помощь в виде денежных средств и/или ваучеров может оказать преобразующее воздействие, поскольку она начинает менять соотношение сил между гуманитарными организациями и людьми, пострадавшими от кризиса, а также многими другими заинтересованными лицами, участвующими в гуманитарной деятельности: донорами, правительствами и гражданским обществом. При хорошей подготовке агентства помощь в виде денежных средств и/или ваучеров может быть оказана быстро и в больших объемах. Кроме того, такая форма помощи дает больше гибкости и, помимо решения конкретной задачи, позволяет достичь более масштабного социально-экономического мультипликативного эффекта по сравнению с помощью в натуральной форме (через непосредственную раздачу товаров). Это связано с косвенным воздействием передачи денежных средств: рост расходов получателей способствует росту доходов тех, кто не получил помощь, расширению рынков сбыта товаров местного производства и росту спроса на услуги.

В то же время оказание помощи в виде денежных средств и/или ваучеров сопряжено с опасностями, аналогичными тем, что сопутствуют предоставлению помощи в натуральной форме: вмешательством в рыночную экономику, отслеживанием подотчетности, социальной напряженностью, проблемами защиты — с ними необходимо тщательно работать. В этом отношении цифровизация помощи в виде денежных средств и/или ваучеров может привести к росту как пользы, так и риска для пострадавших. В дальнейшем мы будем анализировать именно этот вопрос — как цифровизация денежных средств влияет на гуманитарную деятельность, в чем состоят те виды риска, с которым сопряжена такая цифровизация, и что могут сделать представители гуманитарного сектора, чтобы сократить этот риск.

Как цифровизация денежных средств меняет гуманитарную деятельность

Как бы мы ни относились к электронным платежам, они будут использоваться — и в обществе в целом, и в гуманитарной деятельности. По данным анализа, проведенного компанией MasterCard, «за последние 15 лет способы оплаты изменились сильнее, чем за предыдущие 150, и почти все нов-

21 Overseas Development Institute (ODI), *Doing Cash Differently: How Cash Transfers can Transform Humanitarian Aid. Report of the High Level Panel on Humanitarian Cash Transfers*, London, September 2015.

шества, которые нам довелось наблюдать, способствовали отказу от наличных расчетов»[22]. Хотя в масштабах всего мира наличные расчеты остаются основным способом оплаты, отмечается значительное увеличение темпов роста электронных платежей, а некоторые страны быстро идут к тому, чтобы стать «безналичными».

Чем хороши электронные платежи?

В гуманитарном секторе эта тенденция проявляется через переход от наличных платежей к электронным. Например, сегодня более половины всех выплат Международного движения Красного Креста и Красного Полумесяца в адрес пострадавших совершается в электронной форме[23]. Отчасти это связано с общемировым переходом к цифровым технологиям, а отчасти с тем, что, по мнению многих участников гуманитарного сегмента, таких как Всемирный банк, использование электронных платежей, денежных переводов и пересылок заработка эмигрантов на родину способствует достижению целей Группы двадцати — всеохватному экономическому росту, всеобщему доступу к финансовым услугам и расширению экономических прав и возможностей женщин[24]. Объединение Better than Cash Alliance (BTCA)[25] исследовало пять основных стимулов роста электронных платежей и пришло к выводу о том, что электронные платежи дают следующие преимущества:

- экономия расходов за счет повышения эффективности и скорости;
- прозрачность и безопасность за счет более удобной отчетности и отслеживания, в результате чего сокращается коррупция и число краж;
- расширение пользования финансовыми услугами за счет обеспечения доступа к ряду финансовых услуг, в том числе к сберегательным счетам и страховым продуктам;
- участие женщин в экономической деятельности за счет предоставления им большего контроля над финансовой стороной своей жизни и расширения их экономических возможностей;
- всеохватный рост за счет создания институтов, формирующих основу экономики, и кумулятивного эффекта экономии расходов, повышения прозрачности, расширения пользования финансовыми услугами и активизации участия женщин в экономике[26].

22 Hugh Thomas, "Measuring Progress towards a Cashless Society", MasterCard Advisors, доступно по адресу: https://newsroom.mastercard.com/wp-content/uploads/2014/08/MasterCardAdvisors-CashlessSociety-July-20146.pdf.

23 См. интерактивные карты денежных выплат на платформе Cash Hub по адресу: www.cash-hub.org/resources/cash-maps.

24 Leora Klapper and Dorothe Singer, *The Opportunities of Digitizing Payments*, World Bank, Washington, DC, 28 August 2015, p. 91.

25 Объединение BTCA представляет собой партнерство 75 государств, компаний и международных организаций, направленное на ускорение «перехода от наличных средств к электронным платежам с целью сократить нищету и способствовать всеохватному росту». См. веб-сайт BTCA по адресу: www.betterthancash.org.

26 BTCA, "Why Digital Payments?", доступно по адресу: www.betterthancash.org/why-digital-payments.

В переходе к электронным платежам сыграли свою роль и дополнительные факторы, в том числе соображения безопасности, поскольку перевозка больших денежных сумм может привлекать к себе много внимания и создавать для получателей помощи или сотрудников гуманитарных организаций риск кражи или грабежа — то же, кстати, касается предоставления поддержки в натуральной форме. Для получателя обычно безопаснее хранить деньги на банковском счете, а не под матрасом. Еще одним важным фактором являются предпочтения получателей — в тех случаях, когда люди уже пользуются электронными платежами в повседневной жизни, имеет смысл придерживаться привычных и удобных для них механизмов.

На момент написания этой статьи, спустя почти год после начала пандемии COVID-19, наверное, можно добавить еще один стимул для использования электронных платежей — убежденность в том, что они сокращают риск передачи вируса. Хотя по итогам ранее проведенных исследований в отношении гриппа было установлено, что «на практике избежать хождения банкнот и монет невозможно, и оно не сопряжено с хоть сколько-нибудь ощутимым повышением риска по сравнению почти с любым другим бытовым предметом, используемым в повседневной жизни»[27], во время пандемии COVID-19 предпочтение в целом отдается электронным платежам. Электронные платежи, например использование мобильных расчетов либо дебетовых или кредитных карт, требуют меньше касаний, чем наличные деньги. Кроме того, все предметы, необходимые для совершения электронных платежей (карты, мобильные телефоны, терминалы и так далее), можно регулярно обрабатывать простым дезинфицирующим средством. Всемирная организация здравоохранения (ВОЗ) и Глобальный кластер здравоохранения опубликовали руководство по оказанию помощи в виде денежных средств и/или ваучеров в условиях пандемии COVID-19, в котором подчеркивается, что предпочтение следует отдавать электронным платежам, поскольку это сокращает необходимость собираться в пунктах раздачи и позволяет регулярно дезинфицировать поверхности, такие как клавиатура банкоматов; кроме того, руководство содержит рекомендацию «по возможности осуществлять бесконтактные электронные или мобильные платежи для сокращения риска передачи инфекции»[28].

Как гуманитарные организации внедряют электронные платежи

Различные гуманитарные организации вот уже несколько десятилетий занимаются оказанием поддержки в денежной форме, однако структуриро-

27 European Centre for Disease Prevention and Control, *Technical Report of the Scientific Panel on Influenza in Reply to Eight Questions concerning Avian Flu*, Stockholm, 5 June 2006, p. 26, доступно по адресу: https://www.ecdc.europa.eu/sites/default/files/media/en/publications/Publications/0606_TER_Eight_Questions_Concerning_Avian_Flu.pdf.

28 WHO and the Global Health Cluster, *Guidance Note on the Role of Cash and Voucher Assistance to Reduce Financial Barriers in the Response to the COVID-19 Pandemic, in Countries Targeted by the Global Humanitarian Response Plan COVID-19*, Geneva, April 2020, p. 8, доступно по адресу: www.who.int/health-cluster/about/work/task-teams/Guidance-note-CVA-COVID.pdf?ua=1.

ванное обсуждение помощи в виде денежных средств и/или ваучеров, а вместе с тем и электронных платежей началось только с созданием в 2005 году Партнерства по изучению денежных средств (Cash Learning Partnership, CaLP), цель которого состояла в содействии развитию и совершенствовании такой помощи. К началу 2010-х годов и с появлением все большего числа фактов, подтверждающих эффективность помощи в виде денежных средств и/или ваучеров, произошло сближение и появилось несколько совместных инициатив. Объединение BTCA, которое было сформировано в 2012 году в ответ на запрос со стороны общественного и частного секторов, по-прежнему занимается стратегической информационно-пропагандистской деятельностью, исследованиями и подготовкой инструкций по переходу на электронные платежи. В 2016 году была сформирована сеть ELAN, за четыре года работы которой был создан целый ряд ценных ресурсов для практикующих специалистов, проведены учебные мероприятия и оказано содействие развитию и прогнозированию в рамках работы гуманитарного сектора, связанной с электронными платежами. Кроме того, за этот период крупнейшая в мире гуманитарная сеть, Международное движение Красного Креста и Красного Полумесяца, осуществила значительные капиталовложения в наращивание потенциала оказания помощи в виде денежных средств и/или ваучеров[29], причем большинство выплат производятся в электронной форме. Такой подход требует определенного уровня совместимости различных гуманитарных организаций, выполняющих эту работу, и с точки зрения анализа пользы и риска это означает, что использование электронных платежей в обычной деятельности повлияло на весь гуманитарный сектор.

Как указано выше, электронные платежи получают все большее распространение в гуманитарном секторе. Однако в связи с этим возникает вопрос: в чем состоят риск и польза этого направления цифровизации? В следующем разделе будет дан ответ на этот вопрос через описание действующего в МККК процесса принятия решения о целесообразности использования электронных платежей в каждом конкретном случае.

Как МККК использует электронные платежи в условиях вооруженных конфликтов и других ситуаций насилия

Как и многие другие организации гуманитарного сектора, МККК работает и с физическими, и с электронными платежами, делая выбор на основе тщательного анализа риска и пользы для людей, пострадавших от вооруженных конфликтов или иных ситуаций насилия. Как будет показано в следующих разделах, МККК не только вот уже более ста лет оказывает помощь в виде денежных средств и/или ваучеров, но и уделяет большое внимание анализу

29 International Red Cross and Red Crescent Movement, *Cash Transfer Programming: Guidelines for Mainstreaming and Preparedness*, Geneva, 2015, доступно по адресу: https://cash-hub.org/wp-content/uploads/sites/3/2020/10/Cash-Transfer-Programming-Guidelines-for-Mainstreaming-and-Preparedness.pdf.

риска, связанного с цифровыми технологиями, и защите данных[30]. Таким образом, работа МККК может послужить примером того, как следует изучать риск, сопутствующий оказанию помощи в виде денежных средств и/или ваучеров.

Как выяснилось в результате исследования архивов МККК, выдача денежных средств практиковалась еще во время Первой мировой войны, когда действующее при Комитете Агентство по делам военнопленных занималось обработкой поручений о переводе денежных средств и пересылкой заказных писем, в том числе с деньгами, которые отправляли интернированным гражданским лицам и военнопленным их родственники[31]. Сегодня МККК оказывает помощь в виде денежных средств и/или ваучеров в рамках большинства из своих 80 с лишним операций, и его опыт показывает, что предоставление такой поддержки в условиях вооруженных конфликтов или иных ситуаций насилия вполне возможно[32]. За период с 2012 по 2020 год число получателей помощи в виде денежных средств и/или ваучеров в рамках всех программ — будь то небольшие денежные пособия, покрывающие дорожные расходы на посещение родственников, содержащихся под стражей, или более крупные гранты на восстановление жилья или на поиск источника заработка — выросло на 600%. За это время количество электронных платежей существенно увеличилось, и большинство крупных денежных переводов — предназначенных для оказания помощи большому числу людей — осуществляется в электронной форме.

Сотрудники МККК делают выбор между наличными и электронными платежами на совершенно определенных основаниях в зависимости от того, какие ресурсы и услуги доступны в конкретной стране. Так, в Южном Судане, где возможности для проведения электронных платежей очень ограничены, небольшие выплаты, например на покрытие транспортных расходов человека, разлученного со своей семьей и желающего воссоединиться с близкими, производятся наличными непосредственно пострадавшему. Для сравнения: в Сомали МККК осуществляет почти все выплаты в электронной форме, поскольку население этой страны давно пользуется мобильными расчетами. МККК выясняет, какие платежные инструменты знакомы людям, доступны им и обеспечивают оперативность, эффективность и безопасность для пострадавших и для сотрудников МККК. Иногда это означает, что в одной стране используется сразу несколько способов оплаты. Например, в Демократической Республике Конго МККК использует три вида платежей: выдачу наличных непосредственно получателям помощи, электронные платежи с помощью мобильных расчетов и электронные платежи на лицевые счета, открытые в кооперативах.

30 См.: Интервью: гуманитарные операции, распространение вредоносной информации и защита данных (опубликовано в этом выпуске журнала).
31 ICRC, *L'agence internationale des prisoners de guerre, Genève, 1914–1918*, Geneva, 1919, p. 105.
32 ICRC (примечание 4 выше), p. 7.

Разумеется, невозможность проведения электронных платежей не означает отказ от выплат; во многих случаях наличный расчет остается полноценным платежным инструментом. На Украине в дополнение к оказанию родственникам пропавших без вести содействия в поисках, укреплению потенциала органов власти для проведения поисков в соответствии с международными стандартами и предоставлению психосоциальной, юридической и административной помощи семьям МККК также производил ежемесячные выплаты, чтобы помочь семьям удовлетворять свои базовые потребности. Эти выплаты сотрудники МККК передавали наличными напрямую семьям, отчасти потому что это давало им предлог для регулярного посещения этих семей. Сотрудники МККК отмечали, что им было бы некомфортно приходить в семьи каждый месяц, не имея никаких новостей о пропавшем, а выплаты наличными давали им хороший повод для визита. По мнению персонала, при использовании электронных платежей это столь необходимое общение происходило бы гораздо реже, и на выстраивание отношений с семьями и завоевание их доверия могло бы уйти больше времени.

В чем состоит риск при осуществлении электронных платежей в гуманитарной деятельности?

Осознание возможных видов риска и ловушек, которые могут таить в себе электронные платежи в гуманитарной сфере, и принятие мер к их уменьшению составляют ключевую часть работы по переосмыслению принципа «не навреди» в мире, который все больше опирается на цифровые технологии. На самом деле, технология электронных платежей уже помогла снизить уровень некоторых опасностей, которые традиционно приписываются оказанию помощи в виде денежных средств и/или ваучеров: оценка эффективности программ, в которых используются электронные платежи, показала, что при их реализации реже наблюдаются хищения, сотрудники меньше рискуют, чем при перевозке денег, а сами программы пользуются большей популярностью у получателей помощи благодаря тому уровню конфиденциальности, который они обеспечивают[33]. Однако важно с самого начала понимать, что полностью исключить любой риск нельзя; так, риск, присущий электронным платежам, можно только снизить, но не полностью устранить. Риск — это часть нашей повседневной жизни; мы рискуем, даже когда переходим дорогу по утрам. Гуманитарным организациям необходимо сопоставлять пользу для получателей (и для самой организации), связанную со скоростью и эффективностью электронных платежей, с возможными видами риска, о которых пойдет речь ниже. Таким образом, по-прежнему жизненно необходимо проводить оценку риска: выявлять

33 Laura Gordon, *Risk and Humanitarian Cash Transfer Programming: Background Note for the High Level Panel on Humanitarian Cash Transfers*, ODI, London, May 2015, доступно по адресу: https://cdn.odi.org/media/documents/9727.pdf.

и анализировать опасности, выяснять, какие из них можно уменьшить, а какие нет, принимать соответствующие меры и документировать принятые решения, что будет дополнительно способствовать совершенствованию отчетности и обучению.

Электронные платежи доступны не всем

Начинать рассматривать принцип недопущения нанесения цифрового вреда необходимо с акцента на самих пострадавших. Дело в том, что электронные платежи не доступны всем в той же мере, что и наличные деньги, и распространение цифровых платежей может усугубить цифровой разрыв (определяемый как неравенство с точки зрения доступа к технологиям и сопутствующим преимуществам). Расплачиваться наличными, если они есть и если имеются в наличии товары и услуги, за которые необходимо заплатить, может любой человек. При использовании наличных расчетов получателю не требуется никаких удостоверений личности и никакой физической инфраструктуры. Наличные средства не привязаны к определенному человеку и в силу этого не предполагают дискриминации или установления личности[34]. Для расчетов требуются только монеты или банкноты в качестве средства обмена и базовое знание арифметики[35]. Однако для использования цифровых платежных средств получатель должен обладать определенной цифровой и финансовой грамотностью. По оценкам специалистов, в основных финансовых понятиях ориентируется лишь треть взрослого населения планеты, при этом среди женщин и малоимущих уровень финансовой грамотности ниже[36]. Получателю потребуется лицевой счет в организации, которая оказывает финансовые услуги; кроме того, к нему будут применяться процедуры проверки контрагента[37], установленные для всех стран Группой разработки финансовых мер борьбы с отмыванием денег (ФАТФ), перенесенные государствами в национальное

34 AGIS Consulting, *Cash Essentials: Beyond Payments*, Paris, 2015, доступно по адресу: https://cashessentials.org/?ref=xranks.

35 Выдвигалось соображение о том, что оплата наличными является предпочтительным методом расчета у преступников, которые стремятся избежать обнаружения. Однако цифровизация приводит к изменениям и в этой сфере; существуют доказательства того, что «электронное отмывание денег является самым распространенным, но наименее контролируемым со стороны правоохранительных органов способом отмывания денег». Ron Teicher, "Transaction Laundering — Money Laundering Goes Electronic in the 21st Century", *Finextra*, 4 June 2018, доступно по адресу: https://www.finextra.com/blogposting/15423/transaction-laundering---money-laundering-goes-electronic-in-the-21st-century.

36 Leora Klapper, Annamaria Lusardi and Peter van Oudhuesden, *Financial Literacy around the world: Insights from Standard & Poor's Ratings Services Global Financial Literacy Study*, 2015, доступно по адресу: https://gflec.org/wp-content/uploads/2015/11/3313-Finlit_Report_FINAL-5.11.16.pdf?x28148.

37 Процедура надлежащей проверки клиента («Знай своего клиента», или KYC) позволяет компаниям проверять личность своих контрагентов во исполнение нормативно-правовых актов о противодействии отмыванию денег и коррупции и включает в себя сбор таких сведений о клиенте, как полное имя, номер удостоверения личности, номер телефона и адрес. PwC, *Know Your Customer: Quick Reference Guide*, January 2016, доступно по адресу: www.pwc.lu/en/anti-money-laundering/docs/pwc-kyc-qrg-final-interactive-2016.pdf.

законодательство и используемые каждым поставщиком коммерческих услуг. При том что требованиями ФАТФ предусмотрена «идентификация клиента и подтверждение личности клиента с использованием надежных, независимых первичных документов, данных или информации»[38], большинство государств трактуют это как требование предъявлять законодательно закрепленную форму удостоверения личности, такую как паспорт, свидетельство о рождении или иной документ государственного образца, подтверждающий личность владельца. По оценкам Всемирного банка, у 1 млрд людей — то есть у 13% мирового населения — официальное удостоверение личности отсутствует[39]. Около 91% из них живут в странах с низким уровнем дохода и уровнем дохода ниже среднего, половину из них составляют женщины из стран с низким уровнем дохода[40]. Существует множество причин, по которым у людей может не быть официального удостоверения личности, в том числе низкий уровень грамотности, зачастую высокая стоимость получения официальных документов (что является препятствием для беднейших слоев населения), юридические требования, которые могут различаться для разных групп населения в конкретной стране, отсутствие или недостаточное количество национальных систем выдачи удостоверений личности, нехватка ресурсов для регистрации всех граждан или просто отсутствие в некоторых сообществах традиции регистрироваться в органах власти. Эти проблемы часто усугубляются вооруженными конфликтами и иными ситуациями насилия, когда функционирование государственных служб может быть нарушено, а перемещение линии фронта может препятствовать передвижению людей и приводить к смене географических границ, в результате чего люди иногда оказываются на территории, где их удостоверения личности уже не считаются действительными.

Безусловно, если в сообществе нет доступа к электронным платежам, гуманитарные организации могут выбрать выплаты наличными, предоставление ваучеров, раздачу товаров или оказание услуг. Проблема возникает в том случае, когда у большинства населения доступ к электронным платежам есть, ведущие организации выбирают этот вариант, а в результате — пусть и непреднамеренно — те группы, у которых нет такого доступа, оказываются исключенными из программы. Гуманитарные организации всегда должны проявлять гибкость и предлагать несколько вариантов решения, чтобы никто не был забыт.

Электронным платежам часто отдается предпочтение на том основании, что они способствуют всеобщему пользованию финансовыми услу-

38 FATF, "FATF Recommendation 5: Customer Due Diligence and Record-Keeping", доступно по адресу: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

39 World Bank, "ID4D Data: Global Identification Challenge by the Numbers", доступно по адресу: https://id4d.worldbank.org/global-dataset.

40 Vyjyanti T. Desai, Anna Diofasi and Jing Lu, "The Global Identification Challenge: Who Are the 1 Billion People without Proof of Identity?", *Voices: World Bank Blogs*, 25 April 2018, доступно по адресу: https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity.

гами; однако это не обязательно влечет за собой финансовое благополучие. Установлена явная взаимосвязь между расширением пользования финансовыми услугами, сокращением нищеты и укреплением экономической безопасности, однако просто дать людям доступ к финансовым услугам недостаточно. Как показало исследование, проведенное в 2017 году МККК и Британским обществом Красного Креста в Нигерии и Кении, в этих условиях «основной проблемой для людей остается нищета, а не отсутствие доступа к финансовым услугам»[41]. Само по себе предоставление возможности получать электронные платежи не может автоматически обеспечить расширение пользования финансовыми услугами.

Повышенное внимание к связи между гуманитарной помощью в денежной форме и социальной защитой приводит к тому, что к этому набору добавляется государство — основной оператор систем социальной защиты, — в результате чего возникают сложные вопросы защиты и координации. Вследствие пандемии COVID-19 и прогнозируемого экономического спада во всем мире, которые заставят существующие системы государственной социальной защиты и гуманитарной помощи работать на пределе и даже за пределом своих возможностей, этот акцент лишь усиливается. Однако такая закономерность устанавливается не напрямую; судя по итогам недавнего опроса практикующих специалистов[42], в их восприятии основными проблемами в выявлении взаимосвязи между помощью в виде денежных средств и/или ваучеров и системами социальной защиты являются недостаточная координация действий участников, тот факт, что системы социальной защиты не предназначены для реагирования на чрезвычайные ситуации, нехватка опыта гуманитарных организаций в сфере социальной защиты и восприятие государства как недостаточно беспристрастного при удовлетворении потребностей самых уязвимых слоев населения. ООН отмечает:

> Многие законы, формально ограничивающие доступ определенных групп населения к социальной защите и общественному обслуживанию, были аннулированы. Тем не менее некоторые из препятствий, с которыми сталкиваются эти группы, — в том числе недостаток информации о своих правах и отсутствие возможности заявлять о себе или быть представленным на политическом уровне, чтобы воспользоваться такими правами, — по-прежнему усугубляются дискриминацией[43].

В условиях кризиса, и особенно конфликта, подобная дискриминация может проявляться еще сильнее. Там, где непрочно верховенство права и царит коррупция, некоторые люди и группы людей будут выигрывать

41 Paul Harvey, Kokoévi Sossouvi and Annie Hurlstone, *Humanitarian Cash and Financial Inclusion: Findings from Red Cross Movement Projects in Kenya and Nigeria*, British Red Cross and ICRC, London, February 2018, p. 6.

42 CaLP (примечание 2 выше), p. 144.

43 UN, *Promoting Inclusion through Social Protection: Report on the World Social Situation 2018*, New York, 2018, p. 18, доступно по адресу: https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2018/07/1-1.pdf.

от изменений экономической модели, вызванных конфликтом, а некоторые будут страдать от них. Гуманитарные организации должны сыграть свою роль в обеспечении поддержки маргинализированных групп и тех, кому грозит опасность, — независимо от того, оказывается ли такая поддержка посредством существующих систем или посредством гуманитарной защиты и помощи.

Существует также риск слияния цифровой и географической близости. Электронные платежи могут оказать жизненно необходимую помощь сообществам издалека, однако это не означает, что гуманитарным организациям нет нужды физически присутствовать на месте; выездные группы по-прежнему должны проводить оценку, чтобы получить истинное представление о потребностях, а затем отслеживать и оценивать влияние принятых мер на пострадавшие сообщества. Цифровая близость — например в виде электронных платежей — «не отменяет необходимости физического доступа к уязвимым сообществам и не подменяет собой работы, направленной на то, чтобы гарантировать им защиту в соответствии с действующим законодательством»[44].

Ответственное обращение с данными в гуманитарной деятельности

Для того чтобы обеспечить всеобщий охват электронными платежами, гуманитарным организациям необходимо собрать и обработать огромное количество данных, в том числе персональных данных пострадавших, желающих получить доступ к таким платежам. Будь то в рамках замкнутой системы, полностью управляемой самой гуманитарной организацией, или в сотрудничестве с местными поставщиками финансовых услуг — необходимо обеспечить безопасный сбор, обработку, хранение и передачу этих данных в соответствии с надлежащей практикой работы с информацией.

В отчете CaLP о состоянии денежных расчетов в мире за 2020 год подчеркивается, что «риск, связанный с цифровыми технологиями и работой с данными, является “новым”» и что «хотя некоторые крупные организации, оказывающие помощь в виде денежных средств и/или ваучеров, теперь (по собственному заявлению) отлично владеют принципами ответственной работы с данными, многие другие подобные организации по-прежнему не готовы обсуждать эту тему»[45].

В 2019 году состоялся ряд мероприятий[46]: некоторые из них были посвящены непосредственно помощи в виде денежных средств и/или вауче-

44 ICRC (примечание 4 выше), p. 9.

45 CaLP (примечание 2 выше), p. 52.

46 В декабре 2018 года МККК провел в Лондоне симпозиум, посвященный цифровому риску в условиях вооруженных конфликтов; см.: ICRC (примечание 20 выше). В апреле 2019 года в Женеве состоялся семинар CaLP, посвященный ответственной работе с данными; см.: CaLP, “Data Responsibility: Let’s Not Wait for Another Wake-Up Call”, 8 May 2019, доступно по адресу: www.calpnetwork.org/blog/data-responsibility-lets-not-wait-for-another-wake-up-call/. По итогам семинара CaLP в мае 2019 года Центр гуманитарных данных УКГВ совместно с некоммерческой

ров, остальные касались гуманитарной деятельности в целом; в ходе этих мероприятий исследовались виды риска, связанные с цифровыми технологиями, и понятия недопущения нанесения цифрового вреда и цифрового достоинства в рамках внедрения цифровых технологий в гуманитарную деятельность. При рассмотрении видов риска, связанных с цифровыми технологиями в гуманитарной деятельности, а точнее — с электронными платежами, возникает несколько вопросов, однако все они на самом деле могут сводиться к основной теме — ответственной работе с данными — «набору принципов, процессов и инструментов, которые обеспечивают безопасность, этичность и эффективность работы с данными в гуманитарной деятельности. К ним относятся конфиденциальность, защита и безопасность данных, а также иные практические меры, позволяющие уменьшить риск и предотвратить причинение вреда»[47]. Ответственная работа с данными требует от гуманитарных организаций добросовестности при сборе, обработке, хранении и предоставлении данных.

Вопрос ответственной работы с данными часто поднимается при обсуждении перспектив сотрудничества между гуманитарными организациями. Был предпринят ряд инициатив, связанных с оптимизацией сотрудничества в сфере оказания помощи в виде денежных средств и/или ваучеров, в том числе созданы Сеть сотрудничества в области выдачи денежных средств[48] и единая система денежных переводов в ООН[49]. Такой коллективный подход приветствовался в духе дальнейшего укрепления сотрудничества в соответствии с обязательствами, принятыми на себя в рамках договоренности Grand Bargain[50] в целях повышения эффективности, полезности и подотчетности деятельности по предоставлению помощи в виде денежных средств и/или ваучеров и наращивания поддержки пострадавших от кризисов[51]. Однако им пришлось столкнуться с рядом трудностей. Поднимались вопросы интеллектуальной собственности на совместно созданные системы, сложности налаживания взаимодействия и распределения

организацией Wilton Park провел первое совещание по вопросам ответственной работы с данными в гуманитарной деятельности; см.: Wilton Park, "Data Responsibility in Humanitarian Action: From Principle to Practice", доступно по адресу: www.wiltonpark.org.uk/event/wp1688/. На втором мероприятии Wilton Park, которое прошло в октябре 2019 года, обсуждалась более широкая тема цифрового достоинства в условиях вооруженного конфликта; см.: Wilton Park, *Digital Dignity in Armed Conflict: A Roadmap for Principled Humanitarian Action in the Age of Digital Transformation*, October 2019, доступно по адресу: www.wiltonpark.org.uk/wp-content/uploads/WP1698-Report.pdf.

47 Wilton Park, *Data Responsibility in Humanitarian Action: From Principle to Practice*, June 2019, доступно по адресу: www.wiltonpark.org.uk/wp-content/uploads/WP1688-Report-1.pdf.

48 См.: Collaborative Cash Delivery Network, "Our Story", доступно по адресу: www.collaborativecash.org/the-network.

49 См.: Inter-Agency Standing Committee (IASC), "Statement from the Principals of OCHA, UNHCR, WFP, and UNICEF on Cash Assistance", 5 December 2018, доступно по адресу: https://interagencystandingcommittee.org/other/content/statement-principals-ocha-unhcr-wfp-and-unicef-cash-assistance-5-december-2018.

50 См. официальный веб-сайт Grand Bargain по адресу: https://interagencystandingcommittee.org/grand-bargain.

51 IASC, "Increase the Use and Coordination of Cash-Based Programming", доступно по адресу: https://interagencystandingcommittee.org/increase-the-use-and-coordination-of-cash-based-programming.

полномочий и ресурсов между различными организациями. Недостаточная совместимость и слабый обмен данными между различными организациями, использующими коллективные платформы, существенно снижают качество программ, что ведет к задержкам в их осуществлении и невозможности максимизировать использование информации. Для обмена сведениями необходимо доверие к системам друг друга, а также к практике работы с данными и их защиты. В феврале 2019 года Всемирная продовольственная программа (ВПП) заключила соглашение о партнерстве на сумму 45 млн долларов США с компанией Palantir Technologies, которая занимается анализом данных и сбором информации; тем самым ВПП навлекла на себя критику

> со стороны правозащитников и борцов за прозрачность данных, утверждавших, что компания Palantir запятнана нарушением прав человека в ходе своей прежней работы с такими организациями, как Центральное разведывательное управление США (ЦРУ), Служба иммиграционного и таможенного контроля США и компания Cambridge Analytica. <…> Они утверждали, что во имя повышения эффективности и снижения затрат риску подвергаются в высшей степени конфиденциальные данные 92 млн человек, которым ежегодно помогает ВПП[52].

Это партнерство вызвало вопросы в связи с последствиями для единой системы денежных переводов ООН, способами защиты данных, собранных любой из участвующих организаций, а также в связи с возможным влиянием на пострадавших, которым система призвана помогать.

Развитие технологий цифровой идентификации личности и использование биометрии

В последние годы стали появляться новые технологические решения в области цифровой идентификации личности, которые часто используются в программах предоставления помощи в виде денежных средств и/или ваучеров. Что же такое цифровое удостоверение личности?

> Цифровое удостоверение личности представляет собой набор собранных и хранящихся в электронном виде характеристик человека, которые позволяют однозначно его описать. <…> Цифровое удостоверение личности может состоять из ряда атрибутов, в том числе из биографических сведений (таких как имя, возраст, гендерная принадлежность, адрес) и биометрических данных (таких как отпечатки пальцев, скан радужной оболочки глаза, отпечатки рук), а также другой информации. <…> [Эти данные] могут использоваться для идентификации человека посредством ответа на вопрос «кто это?»[53].

52 Barnaby Willitts-King, John Bryant and Kerrie Holloway, *The Humanitarian "Digital Divide"*, Humanitarian Policy Group Working Paper, ODI, London, November 2019, p. 15.

53 World Bank Group, GSMA and Secure Identity Alliance, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, July 2016, доступно по адресу: www.gsma.com/mobilefor-

В сочетании с другими анкетными данными эта информация также помогает ответить на вопрос: «Тот ли он, за кого себя выдает?»

Цифровое удостоверение личности не становится автоматически официальным или юридическим подтверждением личности владельца; юридическую идентификацию граждан может осуществлять только государство, хотя многие государства выбирают именно электронную форму такой идентификации. В Эстонии, которая считается мировым лидером в области внедрения цифровых технологий, каждый гражданин страны в возрасте старше 15 лет и каждый европейский гражданин, проживающий в стране, обязаны получить эстонское цифровое удостоверение личности[54]. А в Индии работает самая большая в мире система цифровой идентификации на основе биометрических данных, которая называется Aadhaar[55].

Таким образом, цифровые удостоверения личности, созданные гуманитарными организациями с целью обеспечить людям доступ к своим программам, не являются официальными юридическими документами и в связи с этим имеют ограниченное значение за рамками своего прямого назначения в отсутствие соответствующей договоренности с органами власти (как в случае с удостоверениями беженца, которые оформляет Управление Верховного комиссара ООН по делам беженцев (УВКБ ООН) и которые дают доступ не только к услугам УВКБ, но и к другим услугам, в том числе в некоторых случаях и финансовым[56]). Появление цифровых удостоверений личности также вызывает вопрос их принадлежности. В 2019 году организация Wilton Park провела конференцию о цифровом достоинстве в условиях вооруженного конфликта, по итогам которой был сделан вывод о том, что «для поддержания цифрового достоинства люди, получающие помощь, должны считаться информационными агентами, которые имеют свободу выбора в отношении своей цифровой идентификации и цифровой анонимности»[57]. При создании совместимых систем и механизмов идентификации может возникать существенный риск для уязвимых групп населения, у которых могут быть очень веские основания стремиться сохранить анонимность и которые могут столкнуться с дискриминацией или еще худшими последствиями в силу возможности их идентифицировать.

Биометрия — одна из форм цифровой идентификации личности. Изначально она разрабатывалась и использовалась для целей пограничного и миграционного контроля, а затем получила широкое применение в новых национальных системах идентификации. Преимущества биометрии опре-

development/wpcontent/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf.

54 World Bank Group, *Privacy by Design: Current Practices in Estonia, India, and Austria*, Washington, DC, 2018, доступно по адресу: https://id4d.worldbank.org/sites/id4d.worldbank.org/files/PrivacyByDesign_112918web.pdf.

55 Там же.

56 UNHCR, "Documentation", доступно по адресу: www.unhcr.org/registration-guidance/chapter5/documentation/.

57 Wilton Park, *Digital Dignity in Armed Conflict* (примечание 46 выше), p. 4.

деляются необходимостью юридической идентификации, отвечающей требованиям надлежащей проверки, поскольку биометрия обеспечивает и то, и другое. Однако такое размывание границ между иммиграционным контролем и борьбой с терроризмом или обеспечением безопасности вызывает особый интерес государств к биометрическим данным, собранным частными лицами и гуманитарными организациями[58].

Использование гуманитарными организациями биометрических систем в целях обеспечения цифровой идентификации личности значительно выросло, поскольку считается, что они позволяют повысить эффективность деятельности, укрепить подотчетность и, в частности, помогают сократить число случаев мошенничества[59]. Однако столь быстрый переход к биометрии вызвал много споров. Использование биометрии в УВКБ на раннем этапе считалось успешным, однако в ходе внутреннего аудита, проведенного ООН в 2016 году, выяснилось, что в четырех из пяти проверенных страновых офисов информация, которая была дана беженцам по поводу программы биометрии, оказалась недостаточной для того, чтобы признать их надлежащим образом информированными[60]. Например, в ходе работы с беженцами из числа народа рохинджа биометрические данные позволили УВКБ и его партнерам справиться с масштабным кризисом, который разворачивался с огромной скоростью, однако некоторые утверждали, что это создало риск для беженцев рохинджа:

> Биометрические данные, которые собирались гуманитарными организациями и правительством, используются не только для раздачи помощи народу рохинджа, но и для контроля за передвижениями. <…> В отношении народа рохинджа возникают опасения, поскольку такая система контроля, основанная на биометрических данных, может использоваться для отправки рохинджа обратно в Мьянму[61].

Оксфам принял решение не предпринимать поспешных действий и в 2015 году наложил мораторий на использование биометрии в своей работе[62], впоследствии заявив, что «с учетом количества неизвестных… мы

58 Резолюция Совета Безопасности ООН № 2396 требует от всех государств использования «биометрических данных, которые могут включать отпечатки пальцев, фотографии, данные распознавания лиц и другие соответствующие идентификационные биометрические данные, для ответственного и надлежащего выявления террористов, включая иностранных боевиков-террористов». См. резолюцию 2396 Совета Безопасности Организации Объединенных Наций, 21 декабря 2017 года, доступно по адресу: https://undocs.org/ru/S/RES/2396(2017); Fionnuala Ní Aoláin, "The UN Security Council, Global Watch Lists, Biometrics, and the Threat to the Rule of Law", *Just Security*, 17 January 2018, доступно по адресу: www.justsecurity.org/51075/security-council-global-watch-lists-biometrics/.

59 The Engine Room and Oxfam, *Biometrics in the Humanitarian Sector*, March 2018, p. 8, доступно по адресу: www.theengineroom.org/biometric-tech-review-report/.

60 Elsie 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: www.wired.co.uk/article/united-nations-refugees-biometric-database-rohingya-myanmar-bangladesh.

61 Там же.

62 The Engine Room and Oxfam (примечание 59 выше).

почли за лучшее не внедрять эту технологию на раннем этапе»[63]. МККК уже давно использует биометрию, но только для содействия в реализации своего мандата в тех случаях, когда без нее невозможно решить определенные задачи, например в области судебной медицины и восстановления семейных связей: «В данном случае МККК обрабатывает биометрические данные “в интересах общества” (при исполнении мандата МККК)»[64]. В отношении использования биометрии для взаимодействия с получателями пособий и для раздачи помощи МККК занимает иную позицию:

> Поскольку цель [использования биометрии] здесь преимущественно связана с эффективностью и поскольку помощь может предоставляться (и долгое время предоставлялась) без потребности в биометрии, МККК потребуется установить, что «правомерная заинтересованность» в создании системы идентификации личности на основе биометрических данных не перевешивает возможного влияния на права и свободы соответствующих лиц[65].

При том что использование биометрии в повседневной жизни растет — например, сканирование отпечатков пальцев рекламируется как простой способ обеспечить безопасность своего смартфона, — у людей есть возможность отказаться от нее. Однако в гуманитарных программах такая возможность во многом остается лишь умозрительной, поскольку способность подтвердить свою личность является условием получения помощи. Сама по себе биометрия не предполагает риска, но, как мы увидим ниже, обработка любых персональных данных является конфиденциальной и сопряжена с целым рядом опасностей и поводов для беспокойства.

Защита данных: защита жизни, здоровья и достоинства

Виды риска, перечисленные выше, коренятся в проблеме идентификации: как человек подтверждает свою личность, кому принадлежат эти данные, что происходит с идентификационными данными, которые предоставляют люди? С проблемой идентификации напрямую связана проблема защиты данных. Все, у кого есть адрес электронной почты, наверняка помнят об Общем регламенте Европейского союза о защите персональных данных, вступившем в силу в мае 2018 года, за чем последовал шквал писем с просьбой дать согласие на использование данных. Кто из нас вообще читает многостраничные условия использования, прежде чем купить что-нибудь в интернет-магазине или загрузить приложение на смартфон? Люди постоянно раздают свои данные направо и налево, не всегда задумываясь о последствиях, и желание обеспечить себе удобство и связь с миром

63 E. Thomas (примечание 60 выше).
64 Ben Hayes and Massimo Marelli, “Facilitating Innovation, Ensuring Protection: The ICRC Biometrics Policy”, *Humanitarian Law and Policy Blog*, 18 October 2019, доступно по адресу: https://blogs.icrc.org/law-and-policy/2019/10/18/innovation-protection-icrc-biometrics-policy/.
65 Там же.

часто перевешивает возможные опасности даже при низком уровне доверия к компаниям и к государству. Например, несмотря на первоначальные опасения по поводу скандала, связанного с разглашением информации в Facebook / Cambridge Analytica[66], и на то, что политика конфиденциальности Facebook по сути была улучшена совсем незначительно, число пользователей этой социальной сети ежегодно прирастает на 12%[67].

Защита персональных данных — неотъемлемая часть защиты жизни, здоровья и достоинства, в связи с чем защита персональных данных становится основополагающей для деятельности гуманитарных организаций. Они часто собирают персональные данные, чтобы исполнить свое предназначение, будь то для поиска пропавших без вести, для содействия восстановлению разлученных семей или для предоставления жизненно необходимой помощи. При осуществлении электронных платежей защита данных приобретает критическое значение, поскольку для отправки или получения денежных средств через поставщика финансовых услуг получателям приходится подтверждать свою личность, так что гуманитарные организации вынуждены собирать и раскрывать персональные данные. Поскольку новые технологии позволяют в разы быстрее и легче обрабатывать эти данные, вопрос сохранения их конфиденциальности становится все более животрепещущим. Хотя право на защиту от вмешательства в личную жизнь признается во всем мире в качестве одного из прав человека еще с 1948 года[68], право на защиту персональных данных было закреплено позже — первый региональный договор о защите данных вступил в силу почти сорок лет спустя [69]. Сегодня большинство государств, ООН и международные организации, работающие в гуманитарной сфере, признают основные принципы защиты данных, хотя содержание политики и законодательные рамки в разных странах различаются[70]. Однако сами обстоятельства, в которых действуют гуманитарные организации, то есть условия кризиса, создают особые сложности, связанные с защитой данных.

Получение согласия своих подопечных на обработку их персональных данных — одна из первых задач любой гуманитарной организации. Применительно к защите данных согласием считается свободно выражен-

66 Julia Carrie Wong, "The Cambridge Analytica Scandal Changed the World – but It Didn't Change Facebook", *The Guardian*, 18 March 2019, доступно по адресу: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook.

67 Dan Noyes, "The Top 20 Valuable Facebook Statistics", *Zephoria*, October 2020, доступно по адресу: https://zephoria.com/top-15-valuable-facebook-statistics/.

68 См.: Всеобщая декларация прав человека. Принята резолюцией 217 A (III) Генеральной Ассамблеи ООН от 10 декабря 1948 года, ст. 12; Международный пакт о гражданских и политических правах. Принят резолюцией 2200 A (XXI) Генеральной Ассамблеи от 16 декабря 1966 года (вступил в силу 23 марта 1976 года), ст. 17.

69 Конвенция о защите частных лиц в отношении автоматизированной обработки данных личного характера. Серия европейских договоров — № 108, 28 января 1981 года (вступила в силу 01 октября 1985 года), доступно по адресу: https://rm.coe.int/1680078c46.

70 United Nations Conference on Trade and Development, "Data Protection and Privacy Legislation Worldwide", доступно по адресу: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

ное и конкретное волеизъявление должным образом проинформированного субъекта данных (то есть получателя помощи) о том, что он согласен на обработку относящихся к нему персональных данных. Это означает, что «лицо должно быть в состоянии полностью оценить риски и преимущества обработки данных, в противном случае согласие не может считаться действительным»[71]. Использование согласия в качестве правовой основы для обработки данных отличается от того, как раньше гуманитарные организации использовали согласие в качестве основания для своей деятельности. Обработка данных гуманитарными организациями — в том числе МККК — часто «основана на жизненно важных интересах либо на важных соображениях общественного интереса, например когда организация исполняет свой мандат в рамках национального законодательства или международного права»[72]. Это означает, что для обработки данных не требуется действительное согласие при условии, что такая обработка производится на законном основании в интересах общества.

Однако следует признать, что само понятие свободно данного согласия в условиях кризиса звучит абсурдно, особенно если согласие на обработку персональных данных является обязательным условием для получения помощи. Когда человек потерял все, а кто-то предлагает ему помощь, он наверняка примет ее без лишних вопросов и не станет пристально изучать сложные юридические вопросы о том, что может произойти с данными и какой риск может или не может при этом возникнуть в будущем. Получение информированного согласия также представляет проблему, если в политике защиты данных присутствуют сложные юридические понятия, разобраться в которых было бы непросто многим из нас, независимо от уровня грамотности и образования. Одна из ключевых рекомендаций по итогам проведенной в 2019 году конференции Wilton Park гласит:

> Понятие информированного согласия следует переформулировать как согласие по сути, чтобы пресечь практику принуждения к согласию. В рамках альтернативы действующему механизму информированного согласия необходимо предусмотреть возможность отказа для людей, которые примут решение не предоставлять информацию. Это не должно препятствовать доступу к услугам. Возможность отказа позволит изменить расстановку сил и в некоторой степени устранит дисбаланс в отношениях[73].

Разумеется, защита данных имеет большое значение для всех направлений работы гуманитарного сектора, но особый резонанс эта тема приобрела в связи с электронными платежами. Для совершения электронных плате-

71 Christopher Kuner and Massimo Marelli (eds), *Handbook on Data Protection in Humanitarian Action*, 2nd ed., ICRC and Brussels Privacy Hub, Geneva, June 2020, para. 2.10.2, доступно по адресу: https://www.icrc.org/en/data-protection-humanitarian-action-handbook (Руководство по защите данных в ходе гуманитарной деятельности. Готовится к публикации на русском языке).

72 Там же, para. 3.1.

73 Wilton Park, *Digital Dignity in Armed Conflict* (примечание 46 выше).

жей гуманитарным организациям на различных этапах приходится привлекать сторонних подрядчиков, что может быть полезно с точки зрения эффективности и доступа к специфическому опыту и знаниям, но также приводит к потере части контроля над работой с данными. Электронные платежи по самой своей природе требуют предоставления данных третьему лицу — поставщику финансовых услуг, позволяющему провести эти платежи. После передачи данных гуманитарная организация уже не может их контролировать.

Основные поводы для опасений в связи с защитой данных возникают при проведении электронных платежей через поставщиков финансовых услуг, которые в силу национального законодательства обязаны соблюдать рекомендации ФАТФ[74]. Среди возможных видов риска — использование данных органами власти для целей охраны правопорядка, в том числе для установления слежки за людьми и включения их в свои базы данных, а также использование данных в коммерческих целях, например для размещения таргетированной рекламы или предложения услуг либо для проверки кредитоспособности клиентов. Кроме того, данные могут использоваться для проверки получателей по базам должников, в результате чего финансовая организация может вычесть сумму долга непосредственно из гуманитарной помощи, которую должен получить человек. Иногда такие опасения в связи с защитой данных приводят к тому, что использование электронных платежей становится нецелесообразным, даже если физически такая возможность присутствует. Это особенно распространенное явление в условиях конфликтов и в других щекотливых ситуациях, когда выбор поставщиков финансовых услуг зачастую ограничен, причем все они могут находиться под контролем одной из сторон в конфликте[75].

Во многих случаях люди уже пользуются услугами определенного поставщика финансовых услуг, например банка или оператора мобильной связи; эти люди уже приняли условия и выполнили требования (в том числе в отношении надлежащей проверки клиента), необходимые для получения доступа к услугам, и в силу этого принимают на себя сопутствующий риск и пользуются полученными преимуществами. Это не освобождает гуманитарные организации от ответственности за проведение необходимых проверок, однако между использованием финансовых отношений, в которые получатель уже вступил, и требованием вступить в новые отношения с единственной целью получить помощь в виде электронного платежа все-таки есть разница.

Риск, которому подвергаются люди, имеет огромное значение, однако существует и еще один уровень риска. Нельзя игнорировать тот

74 Важно отметить, что в соответствии с рекомендациями ФАТФ необходимо хранить данные, предоставлять их правоохранительным органам, создавать отделы финансовой разведки, докладывать о подозрительных финансовых операциях и так далее. См.: ФАТФ. *Рекомендации ФАТФ*, февраль 2012 года (в редакции от октября 2020 года). Доступно по адресу: https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF-40-Rec-2012-Russian.pdf.

75 ICRC (примечание 4 выше), p. 50.

факт, что к персональным данным, собранным гуманитарными организациями, через поставщиков финансовых услуг могут получить доступ органы власти и в свою очередь использовать эти данные для целей охраны правопорядка, а это может представлять риск для гуманитарной деятельности в целом. Как отмечает МККК:

> Этот риск касается не только отдельных людей. Он может затронуть и гуманитарные организации. Если данные, собранные гуманитарной организацией, впоследствии используются не в гуманитарных целях, будь то для обеспечения правопорядка или для извлечения коммерческой выгоды, это может подорвать нейтральность и независимость гуманитарного движения. В таком случае может сложиться впечатление, будто гуманитарная организация поддерживает одну из сторон в конфликте, предоставляя ей данные, что может представлять угрозу безопасности организации и/или повлечь за собой потерю доступа к значимой части населения[76].

Оба исхода могут в итоге привести к сокращению объемов оказания населению необходимых гуманитарных услуг.

Помимо возможности правомерного и законного использования данных, информация, которую собирают, хранят, предоставляют и анализируют гуманитарные организации, может представлять интерес и для сторон конфликта. Сведения, позволяющие установить личность человека, его местонахождение, круг общения и связи, могут использоваться с дурным умыслом отдельными людьми, группами или организациями. Речь идет не только об информации, которую мы привыкли воспринимать как персональные данные (такие как имя или номер телефона), но и о метаданных, о которых часто забывают, — это данные, которые позволяют получить сведения о других данных и представляют собой кладезь информации для тех, кто умеет ею пользоваться. Генерал Хайден, бывший руководитель Агентства национальной безопасности США и Центрального разведывательного управления, выразил это предельно ясно: «Мы убиваем людей, опираясь на метаданные»[77], подчеркнув, как метаданные используются для принятия решений, от которых зависит жизнь или смерть. В эпоху активной слежки риск, связанный с безопасностью определенных людей, вполне очевиден: «[х]отя программное обеспечение обычно не может убить человека так, как пуля, конечный результат часто бывает таким же»[78]. Метаданные существо-

76 ICRC (примечание 4 выше), p. 51.

77 David Cole, "'We Kill People Based on Metadata'", *New York Review of Books*, 10 May 2014, доступно по адресу: www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/. См. также: Johns Hopkins University, "The Price of Privacy: Re-Evaluating the NSA", Johns Hopkins Foreign Affairs Symposium, 2014, доступно по адресу: www.youtube.com/watch?time_continue=1022&v=kV2HD-M86XgI.

78 Ron Deibert, Citizen Lab, цит. по Stephanie Kirchgaessner, "'Cat and Mouse Game': How Citizen Lab Shone a Spotlight on Israeli Spyware Firm", *The Guardian*, 12 May 2020, доступно по адресу: https://www.theguardian.com/world/2020/may/12/cat-and-mouse-game-how-citizen-lab-shone-a-spotlight-on-israeli-spyware-firm-nso.

вали всегда — например, на почтовом конверте указывалась информация, которая могла ничего не сообщать о его содержимом, но позволяла получить сведения об отправителе и получателе. Однако в условиях потоков информации и операций — финансовых и любых других — в электронном виде количество создаваемых метаданных стало огромным. Например, при проведении мобильных платежей генерируется колоссальный объем метаданных. Проблема состоит даже не в объеме метаданных, а в тех выводах, которые можно из них сделать, в том числе о том, к каким социальным группам принадлежит человек (если оказание помощи осуществляется адресно определенной группе), куда он мог переехать после кризиса и кто входит в его «круг родственников и друзей, исходя из переводов, отправленных или полученных без участия гуманитарной организации. В свою очередь, можно получить информацию и об этих людях, даже если они сами не участвовали» в программе[79].

Весьма наглядный пример использования метаданных для благих целей с одновременным вмешательством в частную жизнь человека представляют собой приложения для отслеживания контактов, которые стали быстро развиваться в период пандемии COVID-19 и многие из которых требуют загрузки персональных данных пользователя, а также согласия на отслеживание его местоположения и раскрытия этой информации с помощью различных видов технологии геолокации. По данным на июль 2020 года, почти 50 стран ведут разработку приложений для отслеживания контактов или уже используют их для борьбы с распространением заболевания[80]. Некоторым странам, таким как Южная Корея, удалось оправдать использование подобных приложений тем, что кривая заболеваемости действительно выровнялась, что позволило взять вспышку под контроль, однако вопросы, связанные с неприкосновенностью частной жизни, все равно поднимаются. Анализ приложений, направленных на борьбу с COVID, силами благотворительной организации Privacy International позволил выявить некоторые из видов риска, сопутствующего внедрению таких технологий, не в последнюю очередь тот факт, что «приложения пользуются дурной славой из-за недостатка мер обеспечения безопасности и конфиденциальности и использования данных и устройств людей»[81]. Миллиарды людей во всем мире смирились с ограничениями в своей повседневной жизни ради того, чтобы взять пандемию под контроль, но всему есть свои пределы; теперь от людей «требуют доверять государству и предлагаемым им многочисленным приложениям. И это то самое государство, которое в прошлом не гнушалось использовать их данные»[82]. Ослабляя стандарты

79 ICRC and Privacy International, *The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era*, Geneva, October 2018, p. 74.

80 Niall McCarthy, "Which Countries Are Deploying Coronavirus Tracing Apps?", *Forbes*, 22 July 2020, доступно по адресу: https://tinyurl.com/j8wse55q.

81 Privacy International, "There's an App for That: Coronavirus Apps", 20 April 2020, доступно по адресу: https://privacyinternational.org/long-read/3675/theres-app-coronavirus-apps.

82 Там же.

обеспечения конфиденциальности, мы можем вступить на скользкий путь; если стандарты перестанут строго соблюдаться, будет очень сложно восстановить их обязательное применение.

Кибербезопасность и рост числа кибератак

Кроме того, для проведения электронных платежей требуется инфраструктура — как цифровая, так и физическая. Платежная инфраструктура включает в себя компьютеры и серверы, которые должны физически где-то находиться и которым требуются электропитание и техническая поддержка. Инфраструктура может ломаться и получать повреждения, особенно в условиях вооруженного конфликта[83]. В случае прекращения электроснабжения или выхода из строя компьютеров экономика может попросту встать. В 2018 году в результате масштабного отключения платежной системы Visa миллионы европейцев не могли совершать платежи[84]. Та же беда спустя несколько недель постигла и MasterCard, что привело к остановке платежей во всем мире[85]. Представитель Visa заявил, что проблема не связана ни с несанкционированным доступом, ни с кибератакой, однако такой риск вполне реален в отношении критически важной инфраструктуры, а финансовая инфраструктура, наряду с инфраструктурой здравоохранения, водоснабжения, энергетики и транспорта, действительно является критически важной. В 2019 году поставщики финансовых услуг заявили о колоссальном увеличении числа кибератак, взломов и случаев кражи данных по сравнению с предыдущим годом, причем 25% всех злонамеренных атак пришлось именно на финансовую сферу, которая заняла по этому показателю первое место среди 28 отраслей, участвовавших в исследовании[86]. Скорее всего, пандемия COVID-19 подтолкнет еще больше финансовых организаций к полной цифровизации, и по мере роста популярности электронной торговли и бесконтактных платежей потребуются постоянные капиталовложения в укрепление устойчивости платежных систем[87]. Однако гуманитарные организации тоже находятся в зоне риска: «Гуманитарные организации собирают, хранят, предоставляют и анализируют данные, которые представляют интерес для сторон в вооруженном конфликте. <...> В результате гуманитарные организации все чаще подвергаются цифровым

83 О защите, которую обеспечивает международное гуманитарное право в отношении последствий кибероперациий в ходе вооруженных конфликтов, см.: Двадцать лет спустя: международное гуманитарное право и защита гражданских лиц от последствий кибероперациий в ходе вооруженных конфликтов (опубликовано в этом выпуске журнала).

84 Patrick Collins, "Visa Card Payments System Returns to Full Capacity after Crash", *The Guardian*, 2 June 2018.

85 Martin Arnold, "MasterCard Customers Suffer Outages around the World", *Financial Times*, 12 July 2018.

86 Hadar Rosenberg, *Banking and Financial Services: Cyber Threat Landscape Report*, IntSights, April 2019, p. 3.

87 World Economic Forum, *Impact of COVID-19 on the Global Financial System: Recommendations for Policy-Makers Based on Industry Practitioner Perspectives*, Geneva, April 2020, доступно по адресу: www3.weforum.org/docs/WEF_Impact_of_COVID_19_on_the_Global_Financial_System_2020.pdf.

атакам и становятся объектами кибершпионажа, превратившись в весьма лакомые мишени»[88]. Летом 2019 года была совершена сложная кибератака на ООН: «В результате атаки были взломаны ключевые элементы инфраструктуры, — сообщил пресс-секретарь ООН Стефан Дюжаррик, назвав атаку "серьезной". <...> В числе пострадавших "ключевых элементов инфраструктуры" оказались системы управления пользователями и паролями, инструменты системного управления и брандмауэры»[89]. В случае электронных платежей данные, собранные для передачи денежных сумм получателям, могут быть похищены посредством взлома на стороне гуманитарной организации или на стороне поставщика финансовых услуг.

Риск нельзя полностью исключить

Как указано выше, полностью избежать риска при совершении электронных платежей не получится, его можно лишь уменьшить. При оценке преимуществ электронных платежей необходимо учесть существенные факторы риска, в том числе усугубление цифрового неравенства, рост числа кибератак и случаев нарушения целостности данных, неизвестные последствия создания и использования цифровых удостоверений личности и в целом опасения по поводу защиты данных. Решения следует принимать осознанно и в отдельности для каждой страны или группы населения, поскольку тяжесть последствий для разных групп в разных условиях может различаться. У пострадавших должна быть возможность отказаться от предоставления персональных данных (биометрических или иных) без потери доступа к базовой помощи. Анализ риска — определение соотношения цены и преимуществ — необходимо проводить, советуясь с самими пострадавшими. Хотя уровень риска для разных групп может быть одинаковым, его влияние на повседневную жизнь людей может кардинально различаться, поэтому следует прислушиваться к их мнению при принятии решений. По данным исследования, проведенного организацией Ground Truth Solutions, «пользователи предпочитают получать денежную помощь через гибкие и надежные механизмы, внушающие доверие»[90], и это увязывается с другими фактическими сведениями — итогами исследований и разрозненными свидетельствами, — демонстрирующими, что люди отдают предпочтение привычным механизмам, будь то электронные или физические способы получения средств. Ожидать, что люди, оказавшиеся в кризисной ситуации, будут готовы пойти на дополнительный риск или довериться незнакомой системе, было бы уже чересчур, и требовать этого от них можно не иначе как в их интересах и с их согласия. Беспокойство

88 ICRC (примечание 20 выше), p. 12.

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

90 Ground Truth Solutions, *Improving User Journeys for Humanitarian Cash Transfers*, December 2018, доступно по адресу: https://groundtruthsolutions.org/wp-content/uploads/2018/12/User_Journeys_Summary-Report_2018.pdf.

вызывают не только сегодняшние опасности: технологии развиваются слишком быстро, нам за ними не угнаться, и очевидно, что гуманитарные организации не могут точно представить все возможные будущие опасности. Несмотря на это, мы должны продолжать изучение преимуществ цифровых решений, в том числе электронных платежей, и присущего им риска, соблюдая принцип недопущения нанесения цифрового вреда.

Как снизить риск, связанный с электронными платежами

Теперь, когда мы разобрали некоторые из основных видов риска, присущего электронным платежам, полезно вспомнить обо всех подтвержденных преимуществах, которые подтолкнули гуманитарный сектор к тому, чтобы начать использовать такие платежи, особенно с учетом того, что все вышеперечисленные опасности и возможные ловушки, связанные с электронными платежами, в определенной степени можно смягчить. Всякий раз при выборе электронных платежей гуманитарным организациям следует задавать себе вопрос о том, достаточно ли таких смягчающих мер для достижения равновесия между риском и пользой. Как мы уже отмечали, без риска не бывает ничего, а в условиях конфликта это особенно верно. Взвешивая риск и пользу любого действия, мы сталкиваемся с одной из основных дилемм гуманитарной деятельности в условиях кризиса: выбором между риском, сопутствующим действию, и риском, сопутствующим бездействию.

Сокращение цифрового неравенства

Если электронные платежи не являются общедоступными, гуманитарные организации могут принять различные меры — в зависимости от обстоятельств. Иногда проблема состоит лишь в том, что люди никогда раньше не пользовались электронными платежами. В этом случае можно провести обучение по наработке базовой финансовой грамотности, чтобы люди спокойно себя чувствовали при использовании соответствующего платежного инструмента. Например, Корпус милосердия «придерживается широкого определения понятия активизации пользования финансовыми услугами, стремясь расширить доступ [и] повысить качество и частотность использования финансовых продуктов и услуг», а одна из его ключевых стратегий — наращивание финансового потенциала пользователей[91]. Для пропаганды использования финансовых услуг, всеобщего и ответственного доступа к финансам и были созданы такие организации, как Центр расширения доступа к финансовым услугам[92] и Консультативная группа помощи малоимущим[93]. МККК по возможности старается прибегать к услугам тех финан-

91 Mercy Corps, *Financial Inclusion: Approach and Principles*, 2019, доступно по адресу: https://tinyurl.com/1f9ejhfq.
92 См. веб-сайт Центра расширения доступа к финансовым услугам по адресу: www.centerforfinancialinclusion.org.
93 См. веб-сайт Консультативной группы помощи малоимущим по адресу: http://cgap.org/.

совых организаций, в которых у людей уже открыты лицевые счета, чтобы они получали привычное и удобное обслуживание в учреждении, где они уже прошли надлежащую проверку, и чтобы от них не требовалось выказывать доверие к незнакомой системе. Если проблема состоит в том, что люди не могут пройти проверку, решить ее уже может быть труднее. МККК может направить людей к юристам, чтобы те помогли им получить недостающие документы, такие как удостоверение личности, и даже, если потребуется, возместить расходы на получение этих документов. Такие гуманитарные организации, как Датский совет по делам беженцев, Норвежский совет по делам беженцев, УВКБ ООН и целый сонм местных организаций, в числе прочих услуг предоставляют юридические консультации и выдают или помогают получить основные документы. Если у людей нет доступа к электронным платежам, гуманитарные организации должны быть готовы предложить альтернативы, такие как выплаты наличными или помощь в натуральной форме. Обеспечить несколько вариантов на выбор может быть непросто; например, если людей, которые не могут принять электронные платежи, оказывается много, то организация наличных выплат в таком количестве может быть затруднительна, а создание новой схемы с закупкой и доставкой помощи в натуральной форме занимает время. Гуманитарные организации должны убедиться в наличии инфраструктуры и процессов для раздачи товаров, наличных, ваучеров или осуществления электронных платежей, где это уместно, чтобы при необходимости переключаться между этими вариантами.

Многие гуманитарные организации используют технологии — например, осваивают различные средства (двусторонней) цифровой связи, дистанционного наблюдения за передвижениями или осуществления электронных платежей для приобретения основных товаров и услуг, — чтобы обеспечить цифровую близость к получателям помощи, однако важно соблюдать баланс между цифровой и географической близостью. МККК продолжит вести переговоры по вопросам предоставления беспрепятственного доступа к людям, пострадавшим в результате вооруженных конфликтов. Подотчетность людям, пострадавшим от вооруженных конфликтов, — ключевой элемент организационной культуры и суть рабочей модели, которая основана на близости к пострадавшим.

Цифровая идентификация личности и персональные данные: защита данных, обеспечиваемая на конструктивном уровне

Гуманитарным организациям следует придерживаться взвешенного подхода к внедрению технологии цифровой идентификации личности. Если гуманитарные организации используют биометрические данные, тем самым создавая цифровые удостоверения личности, необходимо принять меры к тому, чтобы они применялись исключительно для указанных целей и тщательно охранялись. Пострадавшим следует предоставить информацию, необходимую для принятия осознанного решения, право распоряжаться

своим цифровым удостоверением личности и сохранять анонимность, а также возможность отказаться от создания для них цифрового удостоверения личности без ущерба для доступа к помощи. Можно предусмотреть компромиссный вариант за счет разработки различных форм суверенной личности, например основанных на технологии блокчейна: в этом случае для субъекта данных создается цифровое удостоверение личности, однако он имеет возможность контролировать доступ к нему.

Обсуждая вопрос об уменьшении рисков, связанных с защитой данных, необходимо проанализировать положение пострадавших. Для некоторых риск отрицательных последствий может быть выше в связи с индивидуальными признаками, такими как правовой статус, социально-экономическое положение, расовая принадлежность, религиозные или политические взгляды. В условиях вооруженного конфликта, который часто происходит на межэтнической или социально-политической почве, их положение может усугубиться. Кроме того, важно понимать, как поставщик финансовых услуг будет хранить и использовать данные, полученные от гуманитарных организаций для проведения электронных платежей. На порядок хранения и использования данных влияет и собственная корпоративная практика поставщика, и законодательство соответствующей страны. Так, в МККК применяются контрольные перечни, в которых отмечены проблемы, связанные с защитой данных, и вопросы, вызывающие беспокойство, — их необходимо обсуждать с поставщиками и договариваться о приемлемых решениях. Однако гуманитарному сектору важно не отрываться от действительности; с поставщиком услуг обычно можно договориться о том, что данные будут использоваться только для проведения электронных платежей, а не для маркетинга и не для проверки кредитоспособности получателей, однако отмена их действующих обязательств, таких как принудительное предоставление информации в соответствии с законодательством страны, не может быть предметом переговоров. Гуманитарные организации вкладывают большие средства в инструменты и инструкции, помогающие анализировать проблемы, связанные с защитой данных при совершении электронных платежей. В CaLP был подготовлен новый краткий курс, посвященный электронным денежным переводам и внедрению в обычную практику процедур защиты данных получателей[94]. Набор ELAN для начинающих работу с данными[95] разработан с целью помочь гуманитарным организациям в планировании и совершенствовании практики работы с данными, а в Руководстве Корпуса милосердия по осуществлению электронных переводов[96] содержится пошаговая инструкция для выполне-

94 CaLP, "E-Transfers and Operationalizing Beneficiary Data Protection", доступно по адресу: https://www.calpnetwork.org/blog/new-calp-online-training-course-e-transfers-and-operationalizing-beneficiary-data-protection/.

95 ELAN, *A Data Starter Kit for Humanitarian Field Staff*, доступно по адресу: www.mercycorps.org/sites/default/files/2019-11/DataStarterKitforFieldStaffELAN.pdf.

96 Mercy Corps, *E-Transfer Implementation Guide*, 2018, доступно по адресу www.mercycorps.org/sites/default/files/2020-01/EtransferGuide2018%2C%20Final.pdf.

ния электронных переводов средств, а также рекомендации по анализу нормативно-правовой базы и требований к надлежащей проверке контрагента и по включению в договоры с подрядчиками условий о защите данных. Многие организации, в том числе учреждения ООН и неправительственные организации, разрабатывают собственную политику и инструкции в области защиты данных.

Коротко говоря, каждая гуманитарная организация должна проводить надлежащую проверку. В МККК принято первым делом определять вероятность реализации риска — какова вероятность того, что данные будут похищены? — а затем уточнять воздействие этого риска на конкретного человека — насколько тяжелыми будут последствия для него и насколько они повлияют на восприятие и принятие МККК со стороны населения и участников конфликта? На практике это означает, что сотрудники МККК заполняют форму оценки последствий обработки данных, которая помогает выявить различные виды риска для неприкосновенности частной жизни отдельных лиц, определить обязательства МККК по соблюдению принципов защиты данных, защитить репутацию МККК и позаботиться о том, чтобы организация не нарушила нейтральность гуманитарной деятельности[97]. В свою очередь, партнерство CaLP поделилось руководством о защите данных при оказании помощи в виде денежных средств и/или ваучеров, в котором содержатся также шаблоны оценки влияния на неприкосновенность частной жизни[98] и на которое опираются в своей работе многие гуманитарные организации.

Очень важно, чтобы любая оценка риска, будь то в области защиты данных или в любой другой сфере, предполагала консультации с самими пострадавшими. В Афганистане МККК рассматривал возможность осуществления электронных переводов с помощью мобильных расчетов. Люди, жившие в местах, которые контролировались Талибаном, были прекрасно осведомлены о возможности определения местоположения с помощью мобильных телефонов, и хотя они говорили, что готовы доверить МККК защиту своих данных, — и часто давали сотрудникам организации свои телефонные номера, чтобы те могли с ними связаться, — их беспокоил вопрос о том, как этими данными распорядятся компании, осуществляющие мобильные расчеты, и каким группам могут быть переданы эти сведения. На Украине же получилось наоборот: когда сотрудники МККК подняли тему электронных платежей и технологий, местные жители с долей фатализма сообщили, что у властей уже есть все их данные (из паспортных столов, от мобильных операторов, из банков и даже из Facebook), и поэтому никакого дополнительного риска, связанного со сбором их данных Комитетом и предоставлением этих данных третьим лицам, они не видят. Эти два примера показывают, как по-разному люди могут воспринимать вероятность

97 C. Kuner and M. Marelli (eds) (примечание 71 выше), Chapter 5.

98 CaLP, *Protection Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in Cash and e-Transfer Programmes*, 2013, доступно по адресу: www.calpnetwork.org/wp-content/uploads/2020/01/calp-beneficiary-privacy-web.pdf.

реализации риска и его возможное воздействие и почему при проведении анализа риска так важно принимать во внимание взгляды пострадавших.

Исключительно с точки зрения защиты данных

> одним из возможных вариантов ограничения рисков для соответствующих лиц в рамках программ, использующих помощь в виде денежных средств и ваучеров, если это практически осуществимо для гуманитарной организации, является передача поставщику коммерческих услуг (например, банку или оператору сотовой сети) уникального идентификатора, не позволяющего получающей организации установить личность конечного получателя помощи, и суммы денежных средств, подлежащей распределению[99].

Это может быть особенно удобно для людей, у которых нет официального удостоверения личности, или в тех случаях, когда риск, связанный с предоставлением их данных поставщику финансовых услуг, оценивается как слишком высокий. Разумеется, такой подход не позволяет расширить доступ к финансовым услугам, поскольку лицевой счет в данном случае открываться не будет[100].

Оценка критически важной инфраструктуры

Доступность финансовой инфраструктуры оценить гораздо проще, чем ее безопасность. Гуманитарные организации могут проанализировать несколько параметров, в том числе ликвидность поставщика, его географический охват, включая количество офисов продаж (а также местоположение и пропускную способность тех точек, где получатели могут перевести полученные средства на другой счет или снять их наличными), и доступность клиентской поддержки. С увеличением риска кибератак на финансовую инфраструктуру анализировать ее безопасность становится сложнее. Помимо исследования прошлых инцидентов в данной стране и затронутых ими поставщиков — которое, вероятнее всего, придется проводить исключительно по открытым источникам, поскольку поставщики финансовых услуг не раскрывают всех случаев взлома, — гуманитарная организация мало что может сделать, чтобы убедиться в стабильности и безопасности финансовой инфраструктуры. Однако в ее силах обеспечить соблюдение соответствующих технических и организационных стандартов безопасности в своей собственной работе, поэтому необходимо внедрить процессы защиты персональных данных людей от потери, кражи, повреждения или уничтожения; для этого необходимы в том числе дублирующие системы и эффективные способы реагирования на нарушение безопасности и предотвращения несанкционированного доступа к данным, хранящимся в организации, их раскрытия или утери. В Руководстве по защите

99 C. Kuner and M. Marelli (eds) (примечание 71 выше), para. 9.3.3.
100 ICRC (примечание 4 выше), p. 26.

данных в ходе гуманитарной деятельности также содержится обращенная к гуманитарным организациям рекомендация «внедрять проектируемую защиту персональных данных, полученных ими от получатей помощи… Эффективным решением, направленным на удовлетворение этой потребности, могут являться шифрование и фрагментация информации»[101].

Ответственное обращение с данными: от теории к практике

Все эти меры снижения риска входят в обширную категорию ответственного обращения с данными. Центр гуманитарных данных УКГВ предпринял попытку устранить пробелы в действующих инструкциях с помощью серии публикаций об ответственном обращении с данными, в которых содержатся рекомендации по широкому кругу вопросов, в том числе по управлению инцидентами с данными[102]. Однако эта область по-прежнему остро нуждается во вложении ресурсов.

Конечно, гуманитарные организации не в силах предвидеть будущее; нам не дано предугадать все мириады способов использования собранных сегодня данных для будущих целей и с помощью технологий, которых, возможно, еще даже не существует. Однако всем гуманитарным организациям следует придерживаться принципа минимизации данных, то есть собирать и обрабатывать для конкретной гуманитарной цели проведения электронных платежей только те персональные данные, которые необходимы для идентификации получателей. Никакая «лишняя» информация собираться не должна, а если она была собрана, ее следует уничтожить. Мы должны позаботиться о том, чтобы технологии, используемые для создания цифровых удостоверений личности, для хранения, обработки и передачи данных, а также для связи с пострадавшими, были защищенными. Безусловно, поддерживать четкие стандарты защиты данных очень важно, но гуманитарному сектору придется смириться с тем, что полностью защитить данные от всевозможных взломов и недобросовестного использования невозможно. В более глобальном смысле мы должны исходить из того, что оказание гуманитарной помощи не должно зависеть от принуждения людей к раскрытию своих персональных данных[103]. Имея проработанную политику и практику ответственного обращения с данными и принимая решения обдуманно, мы можем проводить надлежащую проверку и принимать меры как для анализа риска, обусловленного тем, что из-за метода ока-

101 C. Kuner and M. Marelli (eds) (примечание 71 выше), para. 9.3.5.

102 OCHA, Centre for Humanitarian Data, "Guidance Note: Data Incident Management", August 2019, доступно по адресу: https://centre.humdata.org/wp-content/uploads/2019/08/guidanceNote2_dataincidentmanagement.pdf.

103 При оказании гуманитарных услуг важно собирать как можно меньше данных или вовсе их не собирать. Этот процесс минимизации сбора данных существует отдельно от вопроса определения надлежащей правовой основы для сбора и обработки данных, и этот принцип поддерживается в Руководстве МККК по защите данных в гуманитарной деятельности и соответствует принципу недопущения нанесения цифрового вреда, а также является одним из основных принципов защиты данных.

зания помощи (или из-за платежного инструмента в случае предоставления помощи в виде денежных средств и/или ваучеров) ее получатели окажутся в опасности, так и для снижения такого риска.

Заключение

Цифровизация денежных расчетов уже происходит независимо от того, участвует ли в ней гуманитарный сектор. Использование электронных платежей в гуманитарной деятельности имеет ряд доказанных преимуществ, в основном для получателей, но также и для гуманитарных организаций, оказывающих услуги, и сами по себе эти преимущества не оспариваются. Скорее, нам необходимо позаботиться о том, чтобы преимущества перевешивали риск и чтобы мы как гуманитарные организации проводили необходимые проверки ради людей, которым мы помогаем, осознавая, что риск — неотъемлемая часть нашего мира. Это не разовая акция — анализ риска и пользы необходимо проводить каждый раз, когда мы изучаем возможность использования электронных платежей, причем совместно с пострадавшими, чтобы учесть их точку зрения и их оценку риска.

Несмотря на развитие электронных платежей, наличные деньги никуда не денутся. Наличные (валюта в ее физическом выражении) не привязаны к конкретному человеку и поэтому не предполагают дискриминации или установления личности; наличные деньги останутся в обращении по крайней мере в ближайшие годы. Гуманитарному сектору следует продолжать работу и с наличными выплатами, и с электронными платежами, а также предлагать людям помощь в виде товаров и услуг — в зависимости от того, что лучше отвечает потребностям пострадавших от вооруженных конфликтов или иных ситуаций насилия. Мы должны всегда давать людям возможность выбора.

Гуманитарные организации часто сталкиваются с обвинениями в том, что они очень медленно внедряют изменения, особенно связанные с новыми технологиями. Технологии развиваются очень быстро, и никто из нас — ни как частное лицо, ни как сотрудник своей организации — не может за ними угнаться. Гуманитарные организации не поставщики финансовых услуг и не специалисты в области технологий; нам необходимо найти направления сотрудничества с частными сектором, чтобы воспользоваться имеющимися возможностями, но сделать это так, чтобы не ущемить интересы людей, пострадавших в результате кризиса. Выступая в 2018 году на симпозиуме МККК, посвященном цифровому риску в условиях вооруженного конфликта, профессор Натаниэль Рэймонд, который исследует влияние информационно-коммуникационных технологий на права человека и безопасность уязвимых групп населения, особенно в условиях вооруженного конфликта, сделал провокационное заявление: «Мы подрываем “женевские ценности” из довольно-таки слепого восторга по поводу возможных “перспектив Кремниевой долины”»[104]. Банкноты и монеты —

104 ICRC (примечание 20 выше), p. 5.

социальные блага, и компании не получают никакой прибыли от их использования — только от купленных на них товаров и услуг. Отсюда такое стремление к безналичным расчетам, поскольку электронные платежи приносят выручку поставщикам финансовых услуг, — а вместе с тем и больше возможностей для ведения слежки и больше риска недобросовестного использования данных. С этой точки зрения подход, которого придерживаются такие организации, как МККК и Оксфам, и который состоит в том, чтобы не торопиться и проанализировать все возможности и опасности новых решений, должен восприниматься как обдуманное и корректное проявление осторожности, а не как нежелание меняться. Гуманитарные организации должны «ставить опыты в лабораториях, а не на живых людях»[105].

МККК и в дальнейшем будет действовать исходя из своего принципиального подхода к гуманитарной деятельности, который предполагает первоочередное внимание к людям. При использовании возможностей, которые приносит цифровизация, — и электронных платежей, и других технологий — мы по-прежнему будем ставить на первое место в своем анализе тех людей, которым мы стремимся помочь.

В завершение я хочу обратиться к гуманитарному сектору с призывом сделать две ключевые вещи.

Во-первых, гуманитарным организациям следует определить, что означает принцип недопущения нанесения цифрового вреда в реальной жизни. «Прежде чем разрабатывать цифровые решения, потребуется изучить факторы риска, вопросы защиты, этические соображения и трудности и сформулировать обоснованную и важную гуманитарную задачу, ради решения которой мы создаем определенный цифровой потенциал или используем определенные данные»[106]. Цифровизация вызывает глубинные преобразования в жизни всего нашего мира, и эта цифровая революция оказывает на гуманитарную деятельность как положительное, так и отрицательное влияние. Организациям следует рассматривать не только способы предоставления гуманитарной защиты и помощи в мире, который опирается на цифровые технологии, но и собственное преобразование в цифровые организации. Нам необходимо внедрить свой принципиальный подход к гуманитарной деятельности в этот дивный новый цифровой мир.

Во-вторых, что еще важнее, — мы, как уже говорилось в этой статье, должны добиться того, чтобы люди, пострадавшие от конфликтов и других ситуаций насилия, по-прежнему были для нас в приоритете. Гуманитарные организации должны принимать и стратегические, и повседневные решения на основе общения с пострадавшими, которым мы оказываем помощь, и всегда ставить их интересы на первое место. Речь не просто о том, чтобы поддерживать механизмы обратной связи; мы должны активно слушать, что говорят люди, пострадавшие от конфликтов и других ситуаций насилия, размышлять над их словами и адаптировать свой подход к их предпочте-

105 ICRC (примечание 20 выше), p. 2.
106 Там же, p. 2.

ниям, потребностям и возможностям. Такой подход, основанный на интересах людей, необходимо применять и к анализу риска и пользы любого нашего действия, в том числе использования электронных платежей.

В целом гуманитарные организации должны более вдумчиво подходить к принятию решений по поводу электронных платежей и взаимодействия в цифровом мире, чтобы интересы пострадавших всегда стояли для них на первом месте.